T.C.
SELÇUK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER BİLİM DALI

21. YÜZYILDA ORTODOKS GÜVENLİK PARADİGMASININ AŞINIMI: ULUSLARARASI İLİŞKİLERDE SİBER GÜVENLİK

Yüksek Lisans Tezi

Hazırlayan
İbrahim KURNAZ
134229002002

Danışman
Doç. Dr. Metin AKSOY

Konya-2016

SELÇUK ÜNİVERSİTESİ

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Bilimsel Etik Sayfası

Öğrencinin

Adı Soyadı:	İbrahim Kurnaz
Numarası:	134229002002
Ana Bilim / Bilim Dalı:	Uluslararası İlişkiler/Uluslararası İlişkiler
Programı	Tezli Yüksek Lisans ■ Doktora ☐
Tezin Adı	: 21. Yüzyılda Ortodoks Güvenlik Paradigmasının Aşınımı: Uluslararası İlişkilerde Siber Güvenlik

Bu tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Öğrencinin imzası
(İmza)

Alâaddin Keykubat Kampüsü Selçuklu 42079
KONYA Telefon : (0 332) 241 05 21-22 Faks : (0 332) 241 05 24
e-posta : sosbilens@selcuk.edu.tr Elektronik Ağ : www.sosyalbil.selcuk.edu.tr

SELÇUK ÜNİVERSİTESİ

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

SELÇUK ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ 1983

Yüksek Lisans Tezi Kabul Formu

Öğrencinin

Adı Soyadı: İbrahim KURNAZ

Numarası: 134229002002

Ana Bilim / Bilim Dalı: Uluslararası İlişkiler/Uluslararası İlişkiler

Programı: Tezli Yüksek Lisans ■ Doktora □

Tez Danışmanı: Doç. Dr. Metin AKSOY

Tezin Adı: 21. Yüzyılda Ortodoks Güvenlik Paradigmasının Aşınımı: Uluslararası İlişkilerde Siber Güvenlik

Yukarıda adı geçen öğrenci tarafından hazırlanan 21.Yüzyılda Ortodoks Güvenlik Paradigmasının Aşınımı: Uluslararası İlişkilerde Siber Güvenlik başlıklı bu çalışma 21/09/2016 tarihinde yapılan savunma sınavı sonucunda oybirliği ile başarılı bulunarak, jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Unvanı, Adı Soyadı	Danışman ve Üyeler	İmza
Doç. Dr. Metin AKSOY	Danışman	
Doç. Dr. Nezir AKYEŞİLMEN	Üye	
Yrd. Doç. Dr. M. Cüneyt ÖZŞAHİN	Üye	

Alâaddin Keykubat Kampüsü Selçuklu 42079
KONYA Telefon : (0 332) 241 05 21-22 Faks : (0 332) 241 05 24
e-posta : sosbilens@selcuk.edu.tr Elektronik Ağ : www.sosyalbil.selcuk.edu.tr

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin

Adı Soyadı:	İbrahim KURNAZ
Numarası:	134229002002
Ana Bilim / Bilim Dalı:	Uluslararası İlişkiler/Uluslar arası İlişkiler
Programı	Tezli Yüksek Lisans ■ Doktora ☐
Tez Danışmanı:	Doç. Dr. Metin AKSOY
Tezin Adı:	21. Yüzyılda Ortodoks Güvenlik Paradigmasının Aşınımı: Uluslararası İlişkilerde Siber Güvenlik

ÖZET

Tarihsel süreçte, ortodokslaşan güvenlik anlayışını derinleştirip genişletmeden öte aşındırma sürecine sokan unsur 21. yüzyılda siber alanın ön plana çıkması olmuştur. Güvenliğin derinleştirme ve genişletmeden öte aşınımını müessir bir şekilde hızlandıran siber alan aynı zamanda "fiziksel olmayan güvenlik" kategorisinde yer alan güvenlik tehditleridir. Ağlara dayalı bilgi teknolojilerinin gelişimi ile beraber siber tehdit, saldırı, terörizm ve savaş şeklinde adlandırılan siber güvenlik tehditleri eyleme dönüşmüş en ciddi çıktılar olarak göze çarpmaktadır. Bu bağlamda kendine has özellikleri ile siber uzaydan kaynaklı siber güvenlik tehditleri ve bu tehditlere karşı alınan tedbirlerin siber güvenlik olarak adlandırıldığı durum artık uluslararası sistem de, geleneksel güvenlik anlayışının dayattığı paradigmaları hasara uğratmıştır. Nereden geldiği belli olmayan ve uluslararası hukukta henüz kapsamına dair açıklayıcı tanımlamalar yapılmayan bu tehditler güçlü ya da güçsüz farkı gözetmeksizin her devleti aynı ölçüde saldırıya açık ve vurulabilir duruma sokmaktadır. Dolayısıyla hâlihazırda derinleşip genişlemesi sonucu dönüşüme uğrayan kavramın, 21. yüzyılda siber alanın disiplinin alt dalı olan güvenlikte karşılık bulması ve disipline hâkim olan ortodoks güvenlik paradigmasını neredeyse tüm yönleriyle aşındırması sebebiyle yeni bir güvenlik anlayışı çerçevesinde yeniden düşünülmesi gerektiği ortaya çıkmıştır. Çünkü ortodoks güvenlik paradigması kendine has özellikleri ile siber güvenlik tehditlerini ele almada yetersiz kalmaktadır.

Tüm bu noktalardan hareketle, çalışma üç bölümden oluşmaktadır. İlk bölümü ortodoks güvenlik paradigmasını meydana getiren kavramsal çerçeveye, paradigmanın tarihselliğine ve ona dair kuramsal yaklaşımlara değinirken, ikinci bölümde ise siber güvenliğin kavramsal çerçevesine yer verilmiştir. Nihayet üçüncü bölüm ise siber güvenliğin ortodoks güvenlik paradigmasını aşınıma uğratan yönlerine odaklanılmıştır.

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin
Adı Soyadı: İbrahim KURNAZ
Numarası:134229002002
Ana Bilim / Bilim Dalı: Uluslar arası İlişkiler/Uluslararası İlişkiler
Programı : Tezli Yüksek Lisans Doktora ■ ☐
Tez Danışmanı: Doç. Dr. Metin AKSOY

Tezin İngilizce Adı: Erosion of Ortodoxs Security Paradigms ın the 21st Century: Cyber Security in Internatıonal Relatıons

SUMMARY

In the historical process, beyond the deepining and enlarging, cyberspace has let to ortodox security paradigm erosion in 21st century. Cyberspace that accelerant erosion of the security also be a part of "non-physicalsecurity" threats. Together with the development of information technology which based upon networks, cyber security threats emerges as a cyber threats, attacks, terrorizm and war. In this context, these cybersecurity threats and precautions which caused by cyberspace damage to ortodox security paradigms understanding. Thanks to the its specific character these threats that inscrutable, dubious and also lack of comprehensive description in international law created vulnerability in aspect of states promiscuosly between power states and weak states. Hence, in consequence of transformation and alteration on the traditional security threats scope and definition ortodox security paradigms degrade to in terms of tools, perception field and theory because of the cyber securtiy threats in 21st century. After all is said, the thesis of this study claims that the ortodox security paradigm remain in capable in terms of handle with cyber security threats.

From all this point forth, this study comprise of three section. While the first section mentions to conceptional framework which create to ortodox security paradigm, historicity of paradigm and its theoritic approach, the second section mentions about conceptional framework of cyber security. Finally, the third section focus on components of cyber security which erose the ortodox security paradigm.

KeyWords: Security, paradigm, erosion, cyber security

ÖNSÖZ

21. yüzyılda önüne eklendiği her sözcüğe bilinen anlamından öte farklı anlamlar yükleyerek gün yüzüne çıkan yeni bir hareket alanı doğmuştur. Kendine has anarşik yapısı ile eşsiz kılınan özelliklere sahip bu alan siber uzay olarak nitelendirilmektedir. Bilişim ve iletişim ağlarını içeren ve şekillendiren bir platform olarak siber uzay, verileri saklayan bilgisayarlara ek olarak bu verilerin akışını sağlayan sistem ve altyapıları birleştirerek sanal dünya ile fiziksel dünyayı bir bütün haline getirmektedir. Sunduğu kolaylıklar sebebiyle günümüzde de neredeyse bireyden devletlere kadar her birimin hayat alanına entegre olan siber ortam, hayatı kolaylaştırıp yaşam standartlarını yükseltmekte ve dolayısıyla kendisine olan bağımlılığı da artırmaktadır. Bununla birlikte güncel hayatın işleyişinde bir takım kolaylıklar sunan siber ortam paradoksal bir şekilde bireyden devlet düzeyine kadar bazı güvenlik hassasiyetlerini de gün yüzüne çıkarmıştır. Genelde teknolojinin özelde ise bilgisayar aletlerinin etkili kullanımının yaygınlaşmaya başlaması -sağlanan ağlar vasıtasıyla- bilgi güvenliğini ve bu noktadan hareketle de devletlerin güvenliğini de saldırıya açık hale getirmiştir. Bütün bilişim sistemlerini ve kullanıcıları ihtiva eden ve mekân olarak da siber uzay şeklinde ifade edilen bu tehditler günümüz dünyasında güvenliğin ulaştığı çok boyutlu ve derinlikli yapıyı ortaya koymuştur.

Bununla birlikte güvenliği yeniden düşünmeye dair yaklaşımların had safaya ulaşmasına katkıda bulunan bir diğer kayda değer gelişmede küreselleşme ve bununla ilintili olarak da teknoloji ve bilişim aygıtlarının yaygınlaşması olmuştur. Küreselleşme olgusunun derinden hissedilmeye başlamasıyla beraber Uluslararası İlişkiler disiplininde mevcut olan diğer alanlarda olduğu gibi güvenlik ve tehdit algılamaları genişlemiş/çeşitlenmiş ve derinleşmiştir. Ancak derinleşme ve genişlemeden de öte güvenliğin aşınımını hızlandıran en dikkat çekici örnek de literatürde aynı zamanda "fiziksel olmayan güvenlik" kategorisinde yer alan bilgi ve teknolojiye dayalı siber güvenlik tehditleri olmuştur. Bilişim teknolojilerinden neşet eden bu tehditler siber tehdit, terörizm ve siber saldırılar şeklinde adlandırılmaktadır.

Öyle ki, Soğuk Savaşın sonlanmasına değin ajandasında komünizmi haiz olduğu bloğuna karşı en önemli tehdit unsuru olarak gören NATO, 1990'lar sonrasında ise siber terörü ve saldırıları güvenliğine yönelik yeni tehdit tanımlamasında en üst sıralara yerleştirmiştir. Zira Kosova çatışması sırasında, NATO bombalamasına Sırp bilgisayar korsanları tarafından siber saldırılarla karşılık verilmesi, yine 2007 yılında Estonya devlet kurumlarına ve bankalarına yönelik gerçekleştirilen siber saldırıların verdiği hasarın yüksek olması devletlerin ve özellikle de Batı bloğunun savunma kanadı olan NATO'yu yeni bir siber savunma stratejisi inşa etmeye ve uluslararası sistemdeki güncel tehditleri de kapsayacak bir strateji oluşturmaya temayüllüğünü zorunlu kılmıştır.

Tüm bu noktalardan hareketle, küreselleşme süreci ile birlikte ivme kazanan geleneksel güvenlik tehditlerinin kapsamının ve tanımının derinleşip genişlemesi sonucu dönüşüme uğrayan kavramın yeniden revize edilip tanımlanmasının gerekli olduğunu iddia eden akademik görüşler paralelinde ilerleyen bu çalışma da, devletlerin ve bireylerin/toplumların bilişim teknolojilerinden kaynaklı siber saldırılar ve tehditler üzerinden 21. yüzyılda yeni bir güvenlik algısı geliştirmeleri gerektiğini iddia etmektedir. Nereden ve ne zaman geleceği müphem olan siber tehditlerin, geleneksel güvenlik araçları ve mütekabiliyet anlayışı bağlamında savuşturulamayacağı dolayısıyla, zikredilen araçların ve politikaların yerine bilgiye ve teknolojiye dayalı araçların ikame edilmesi zorunlu kılınmıştır. Bu sebeplerle, özellikle güvenlik çalışmalarının kuramsal temelini ortaya koyan akademik çalışmalar, Anglo-Saxon dünyada yaygınlaşmış vaziyette iken Türkiye'de bahsi geçen kavramın tekniğin özüne inerek bu yöndeki teorik ve pratik çalışmalara temel kaynak teşkil edecek bir çalışma bulunmamaktadır. Dolayısıyla bu vesile ile yapılmak istenen Türkçe literatüre bu konuda bir çalışma kazandırmaktır.

Nihayet çalışmanın her aşamasında usta-çırak ilişkisi içinde çalışmaya yön veren, çalışmada göze çarpan eksiklikleri gösteren, düzelten ve oldukça dağınık bir literatürden bir bütünsellik oluşturabilmemde önemli katkıları olan danışmanım Doç. Dr. Metin AKSOY'a; gerek yüksek lisans ders aşamasında gerekse de tez döneminde her türlü kolaylığı sağlayan ve yardımcı olan Selçuk Üniversitesi Uluslararası

İlişkiler bölümü öğretim üyelerine; tez savunmasında yorumlarıyla konuya ilişkin bakış açımı zenginleştiren Doç. Dr. Nezir AKYEŞİLMEN'e; ve ayrıca bu çalışma sürecinde yardımlarını esirgemeyen meslektaşım ve arkadaşım Arş. Gör. Yasin AVCI'ya teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

ARPANET: Gelişmiş Araştırma Projeleri Dairesi Ağı

BM: Birleşmiş Milletler

CCA(CyberCaliphateArmy): Siber Halife Ordusu

DDOS(Distributed Denial of Service Attack): Dağıtık Hizmet Engelleme

IŞID: Irak ve Şam İslam Devleti

NATO:(North AtlanticTreatyOrganization): Kuzey Atlantik Antlaşması Örgütü

S.S.C.B.: Sovyet Sosyalist Cumhuriyetler Birliği

SCADA (Supervisory Control And Data Acquisition): **Merkezi Denetleme Kontrol ve Veri Toplama**

SOME: Siber Olaylara Müdahale Ekibi

USCYBERCOM: Birleşik Devletleri Siber Komutanlığı

GİRİŞ

Küreselleşme sürecinin ivmelesiyle birlikte bilgi-iletişim-teknoloji alanı devrimsel nitelikli birçok gelişmeye tanık olmuştur. İnternetin icadı, bilgisayarların boyutlarının giderek küçülmesi buna mukabil işlevselliklerinin artması, sosyal paylaşım ağlarının ulusal suni sınırları aşarak toplumlar arası etkileşimi arttırması, bununla ilintili olarak yığınların mobilizasyonunun artması ve dolayısıyla kontrol edilebilirliklerinin azalması, internet ortamının finans kapitalin uluslararasılaşmasını daha da kolaylaştırması gibi fenomenler bahse konu gelişmelerin örneklerindendir. Dolayısıyla 20. yüzyılın ortalarında bilgisayarın icadı ile oluşmaya başlayan siber alan 21. yüzyılın başlarında bırakınız kendi alanını genişletmeyi gerçek alanları bile etkiler hale gelmiştir. Başka bir anlatımla bilgisayar ve onun kendisine yarattığı siber alan günümüzde örneğin banka işlemlerini, haberleşmeyi ve e-devleti kendisine bağımlı kılmıştır.

Bir mit halini alan ve fakat modern uluslararası sistemin tarihi anlatısında önemli bir yer tutmaya devam eden Westphalia Antlaşması'ndan bu yana ise devlet mevcut düzeni şekillendirmektedir. Hatta küreselleşme süreci ile birlikte modern devlet egemenliğinin aşınıma uğradığı iddiaları bile sorgulanmaya muhtaçtır. Zira buna sebep olarak gösterilen örneğin uluslararası örgütlerin artması, uluslararası örgütlerin ancak devletlerin bu yönde kurucu irade beyanı göstermeleri ile varlık gösterebilmeleri göz önüne alındığında devlet egemenliğini aşındırıcı bir etki yapmaktan uzaktır. Yine sermayenin uluslararasılaşmasının devletler nezdinde yarattığı etki bahse konu küresel sermayeye direnemeyen az gelişmiş ve gelişmekte olan devletler için geçerlidir. Arttırılabilecek bu örneklerin ortak özellikleri en azından bazı devletlerin bu süreçlere ayak uydurabilmesi ve dolayısıyla her devlet için aynı etkiyi doğurmalarının mümkün olmamasıdır.

Ancak bilgi-iletişim-teknoloji alanlarındaki gelişmelerle etki kapasitesini arttıran siber alan için benzer yorumu yapmak mümkün değildir. İlk olarak verilen örneklerde modern devlet süreci yönlendirebilecek yegâne aktör olma özelliğini korumuşken siber alanın doğası gereği birey, devlet altı örgütlenmeler, çok uluslu şirketler gibi aktörler de bu alanda etkin olabilmektedirler. İkinci olarak devlet

egemenliğinin aşındığı yorumlarını beraberinde getiren gelişmeler yaşansa da Westphalia ile oluşan ve BM ile perçinlenen sistem hala daha sınır, egemenlik, müdahale etmeme, tanıma, egemen eşitlik gibi ilkeleri uluslararası sistemin temel prensipleri olarak örneğin uluslararası hukuk nezdinde korumaktadır. Oysa siber alana dair devlet egemenliğini veya devleti önceleyen uluslararası bir hukuk mekanizmasından bahsetmek henüz mümkün değildir. Üçüncü olarak siber alan bir silah olarak kullanılabilmektedir. Ancak bu askeri silahın tek sahibi devletler olmadığı gibi tek bir birey bile bu silahı devlete yönelik kullanabilmektedir. Öz bir şekilde ifade etmek gerekirse siber alan devletin meşru güç kullanan yegâne aktör olma özelliğini sarsmıştır. Dördüncü ve son olarak modern uluslararası sistem sınır mefhumu üzerine bina edilen ilkeler vasıtasıyla işlerken siber alanın bahse konu sınırları sanal yollarla gerçekten aşındırdığı yorumu dikkate değerdir.

Dolayısıyla siber alanın gelişmesi ve genişlemesi durumunun Uluslararası İlişkiler disiplini kapsamında değerlendirmesi bir zaruret halini almıştır. Zira daha önce de vurgulandığı üzere siber alan, küreselleşme ile ilintilendirilerek devlet egemenliğini ve dolayısıyla Uluslararası İlişkiler'i etkilediği düşünülen gelişmelerle kıyaslandığında sanal olmasına rağmen bu alanda gerçek bir etki yapmıştır. Konunun Uluslararası İlişkiler kapsamında en yakından ilintili olduğu alan da güvenliktir. İlk olarak vurgulandığı üzere siber alanın herhangi bir hukuk alanının düzenlemesine tabii olmaması onun bir tehdit ve dolayısıyla güvenlik meselesi olarak öncelenmesini beraberinde getirmektedir. İkinci olarak siber alan devlet egemenliği üzerinde de etki doğurduğu, modern uluslararası sistem halen devlet merkezli olduğu ve Uluslararası İlişkiler'deki devlet merkezli yaklaşım kırılamadığı yani devlet eksenindeki gelişmeler disiplinde epistemik kırılmalar yarattığı için siber alan güvenlik alanında etkili bir yansıma yaratmıştır. Öz bir şekilde ifade etmek gerekirse devletin sınırları üzerine bina edilen egemenlik fenomeni her ihlal edildiğinde bunun genelde Uluslararası İlişkiler'de özelde ise onun bir alt dalı olan güvenlikte yansıma bulması kaçınılmazdır. Üçüncü ve daha da önemlisi siber alan, disiplinin alt dalı olan güvenlikte karşılık bulsa da disipline hâkim olan ortodoks güvenlik paradigmasının siber alanı ele almaktan aciz oluşu bu çalışmanın en temel iddiasıdır.

Çalışmanın temel tezini oluşturan üçüncü maddeyle ilintili olarak bölümlendirmelere geçmeden önce çalışma kapsamında sıklıkla vurgulanan bazı kavramların neye refere ettikleri sorusunun cevaplandırılması gerekmektedir. İlk olarak siber alan ile kast edilen temelinde ve yaratımında bilgisayar olan sanal dünyadır. Başka bir anlatımla, siber alan bilgisayarın icadı ile başlayan ve günümüzde gerçek alanları bile etkisini altına alan sanal âleme refere etmektedir. Bununla birlikte kavramın tanımında dikkat çeken birkaç husus bulunmaktadır. İlk olarak kavram sanal yani görünürde gerçek olmayana tekabül etse de aslında ve yarattığı etki bakımından tamamen gerçektir. İkinci olarak siber alan gerçek alandaki durumu asimetrik olarak katlayan bir yapıdadır. Başka bir anlatımla örneğin gerçek alanda etkinliği ve yetkinliği oldukça az olan bir birey siber alan sayesinde ve bu alanda yaptıklarıyla etki ve yetkinliğini üst düzeylere taşıyabilmektedir. Üçüncü olarak siber alan büyük ölçüde gerçek kimliklerin askıya alındığı ve dolayısıyla gerçek dünyadaki hukuki sorumluluk ve yaptırımların işlemesinin sekteye uğradığı bir alandır.

Çalışma kapsamında paradigma ile kast edilen ise Guba ve Lincoln'ün işaret ettiği gibi herhangi bir araştırma sorunsalının bilimsel iştigaline yön veren ön kabullerdir. Başka bir anlatımla çalışma nezdinde ve örneğinde paradigma güvenlik fenomeninin bilimsel incelenmesinde kabul edilen ontolojik, epistemolojik, metodolojik, aksiyolojik ve pedagojik varsayımlardır. Bu çerçevede, ortodoks güvenlik paradigması ile vurgulanan tüm yönleri ile devlet merkezli duruştur. Başka bir anlatımla ortodoks güvenlik paradigması ontolojik olarak devleti temel aktör olarak kabul etmekte, epistemolojik olarak devlet merkezli bilgiyi temeline konumlandırmakta, metodolojik olarak ve analiz düzeyi/analiz birimi ekseninde devleti dikkate almakta, aksiyolojik olarak paradigmanın ileri epistemik kırılmaları yani mevcudu aşan yaklaşımları devlet merkezli şekillenmekte ve nihayet pedagojik olarak da disiplin öğrencilerine devlet merkezli bir eğitimi vermektedir. Dolayısıyla tezin de temeline konumlanan siber alanın ortodoks güvenlik paradigmasını aştığı şeklindeki sav bu haliyle bile geçerlilik kazanmaktadır.

Nihayet çalışmanın başlığını da şekillendiren bir diğer önemli kavram aşınımdır. Yaklaşık aynı anlama gelseler de, çalışmada aşma veya aşınma

kelimelerinin niçin kullanılmadığı önemli bir nüansa tekabül etmektedir. İlk olarak ikili bir ilişki kapsamında aşma kavramı aşan tarafın görece daha fazla etkin olduğu bir durumu ifade eder. Başka bir anlatımla aşma eyleminde aşan taraf oldukça etkin bir fail görünümü kazanırken aşmaya maruz kalan taraf ise edilgenliğe bürünmektedir. İkinci olarak aşınma eylemi ise tam tersi manada eyleme maruz kalan tarafa yüksek bir direnç düzeyi vermektedir. Bir başka deyişle aşma kavramında olduğu gibi taraflar arasında eylemin aktifliği bakımından ciddi bir farklılık olmasa da aşınıma direnen tarafa öncellik kazandırmaktadır. Dolayısıyla aşınım kavramı diğerleri ile kıyaslandığında görece taraflar arası eylemde aktiflik eşitliğini vurgulayan bir nosyondur. Bu çerçevede ve tez kapsamında aşınım ilişkisi günümüz siber alanının ortodoks güvenlik paradigmasını sarsan eylemselliğine buna mukabil de ortodoks güvenlik paradigmasının siber alanı kendi bünyesi dâhilinde ele alma çabasına atıf yapar. En azından günümüz için taraflar arasında böylesi bir karşılıklı ve neredeyse birbirine yakın eylemsellik aktivasyonu bulunmaktadır.

Tüm bu noktalardan hareketle siber güvenliğin ortodoks güvenlik paradigması kapsamında ele alınamayacağı temel iddiası üzerine bina edilen çalışma üç bölümden oluşmaktadır. Temel iddia ortodoks güvenlik paradigmasının aşınımı olduğu için çalışmanın ilk bölümü bu paradigmayı oluşturan kavramsal çerçeveye, paradigmanın tarihselliğine ve ona dair kuramsal yaklaşımlara tahsis edilmiştir. Başka bir anlatımla paradigmanın hangi yönlerinin aşınıma maruz kaldığını ortaya koymak için paradigmanın bizatihi kendisini tasvir etmek bir elzemdir. Bununla birlikte ilk bölümüm kendi içinde çalışmanın temel iddiasını destekleyen savları bulunmaktadır. Buna göre güvenlik kavramı tarihi-sosyal her kavram gibi tarihseldir. İkinci olarak kavramın tarihsel oluşu onun muğlak tanımını da beraberinde getirmektedir. Nihayet çalışmanın birinci bölümünde ortodoks güvenlik paradigmasının bir parçasını oluşturan kuramsal yaklaşımlara yer verildiği için örneğin yeşil teori, feminizm ve Marksizm gibi güvenlik kavramını ortodoks bağlamından koparmaya çalışan teoriler çalışmanın dışında bırakılmışlardır.

Çalışmanın ikinci bölümünde ise siber güvenliğin tasvirine odaklanılmıştır. Bu noktada ise siber güvenliğin anlaşılmasını kolaylaştıracak kavramlara da yer verilmiştir. Böylesi bir durumun ise iki temel sebebi bulunmaktadır. İlk olarak siber

güvenliğin anlaşılması için ilk olarak bilgi teknoloji alanındaki gelişmeleri ve siber kavramının bizatihi kendisinin ele almak gerekmektedir. İkinci olarak güvenlik kavramı her kavram gibi kendi karşıtı veya kendisiyle çelişen kavramlar vasıtasıyla da anlaşılabilmektedir. Bu çerçevede örneğin birçok teorisyen güvenliği tehdidin yokluğu olarak tanımlamışlardır. Daha öz bir şekilde belirtmek gerekirse güvenlik kendisiyle çelişen kavramların yokluğu olarak da tanımlanabilmektedir. Bu çerçevede çalışmanın ikinci bölümünde siber savaş, siber tehdit ve siber terörizm nosyonlarına da yer verilmiştir. Zira bahse konu kavramların pratiklerinin olmayışı siber güvenliğin tesis edildiği anlamına da gelmektedir. Nihayet çalışmanın temel iddiasını vurgulamak adına siber güvenliğin devlet nezdindeki yansımalarına yer verilerek örneğin bireyler, çok uluslu şirketler ve devlet-altı gruplar gibi diğer aktörler çalışmanın sınırlılığı kapsamında dışarıda bırakılmışladır. Hâlihazırda ortodoks güvenlik paradigmasının aşınıma uğrayan yönleri ortaya koymak adına bahse konu paradigmanın öncelediği aktör olan devleti çalışma kapsamında görece merkeze konumlandırmak bir gerekliliktir.

Nihayet çalışmanın üçüncü bölümünde ise siber güvenliğin ortodoks güvenlik paradigmasını aşınıma uğratan yönlerine yer verilmiştir. Bu çerçevede ele alınan noktalar ise paradigmanın oluşmasının görece önemli noktalarıdır. Dolayısıyla üçüncü bölümde paradigmanın aşınıma uğrayan yönleri fail, eylemin niteliği, uluslararası hukuk, güvenliğin tesisi ve Uluslararası İlişkiler teorileri yönlerinden irdelenmiştir.

BİRİNCİ BÖLÜM: ORTODOKS GÜVENLİK PARADİGMASININ KAVRAMSAL ve KURAMSAL ÇERÇEVESİ: GÜVENLİĞİN TARİHİ-POLİTİK GELİŞMELERE BAĞITLI EVRİMİ

1.1. Güvenlik Fenomeninin Muğlak Kavramsal Çerçevesi

Sosyal bilimler bünyesindeki kavramların ekseriyetinde gözlemlendiği gibi güvenlik nosyonu da üzerinde ortak bir kanıya varılamayan tanımlama sorununun muhatabıdır. Dolayısıyla tarihsel süreçte her dönemin kendine baskın siyasal anlayışları, güvenlik kavramını statik kılmış ve bu durum kavramla ilgili gelecekte nasıl tanımlanabileceğine ve hangi pratik eylemlere karşılık gelebileceğine dair aksiyomların yapılmasını engellemiştir. Öyle ki, kavramın normatif değerleri barındırması ancak 1970'lerde Barış Çalışmaları Grubu'nun girişimleri ile başlamıştır (Bilgin, 2008: 45). Bu meyanda kavramın ideolojik söylemleri de ihtiva etmesi güvenliğe dair müşterek bir tanımlamayı zorlaştırmıştır.

Uluslararası İlişkiler disiplinindeki geleneksel yaklaşımların tek merkezli ve indirgemeci aktör düzeyi üzerinden yorumladıkları geleneksel güvenlik paradigması anlayışında olduğu gibi, Soğuk Savaş sonrası dönemde disiplinde çok boyutlu ve aktörlü bir güvenlik analizi ortaya koymaya çalışan yeni güvenlik yaklaşımları da yine evrenselci, politik ve hatta ideolojik paradigmalarla kuramlarını beslemişler ve kavramın tanımlanmasında olması gereken sınırlılıklara pek dikkat çekmemişlerdir. Dolayısıyla güvenliğe dair literatürün ekseriyeti kavram hakkında yapılmış tanımlamalar hakkında ne düşünüldüğü ve yapılan tanımlamaların hangi politik doktrinler çerçevesinde ya da hangi bilimsel veriler ışığında yapıldığı ve uyumlandırıldığı üzerinedir (Daase and Frıesendorf, 2010: 1-4).

Ancak, tüm ilginin tanımlama ve episteme üzerine yoğunlaşması güvenliğe yönelik hem içeriksel hem de kavramsal tartışmada esas sorulması gereken güvenliğin ne hakkında/konusunda olduğu ve hangi etmenler etrafında şekillendiği sorularının gözden kaçmasına neden olmuştur. Buna karşılık daha geniş zeminde kavramla ilişkili tartışılmaya ve doğal olarak da yansımaya başlayan durum güvenliğin önemli sacayaklarını oluşturan tehditler, tehditlerin tanımı ve içeriği ve bunlara karşı alınacak önlemlerin ne olması gerektiği gibi birtakım uygulanabilir politik önerilerin verilmesi olmuştur.

Elbette, sosyal bilimlerde alt-disiplinlerin muhtevası olan güvenlik kavramının algılanabilen bir fenomen olma özelliğini barındırması, üzerinde ortak yaklaşımlara dayanan tanımlamaları zorlaştırmaktadır. Çünkü kavramın soyut özelliği kavramı nesnel tanımlamalardan uzaklaştırabileceği için kavram üzerinde oydaşma sağlanması da pek mümkün gözükmemektedir (Jackson, 2010: 190-196). Örneğin, herhangi bir x ülkesinde a nesnesi ya da olayı bir tehlike unsuru oluştururken, aynı a nesnesi ya da olayı y ülkesinde farklı algılandığı için güvenliğe yönelik tehdit unsuru oluşturmayabilmektedir. Daha açık bir örnekle, ABD'nin güvenliği gerekçesiyle Irak'ı işgal etmesi aynı zamanda Irak'ın güvenliğine yönelik tehditleri ihtiva ettiğinden bu noktada Irak'ın güvenliğinin ne şekilde tanımlanacağı önemli bir sorundur.

Öte yandan içinde ortaya çıktığı şartlar çerçevesinde anlam kazanabildiği için nitelik olarak değişebilen ve nicel kontekste ölçülebilir özellik taşımayan güvenlik kavramı birtakım kuramsal zorlukları da beraberinde getirmektedir. Güvenlik nedir ve nesnel midir? Güvenliğin referans nesnesi nedir? Güvenlik kimin için sağlanmalıdır? Devlet düzeyinde bir güvenlik anlayışından söz edilecekse uluslararası sistemin güvenliği nasıl tanımlanmalıdır? Güvenliğin araçları nelerdir? Bu tarz sorulara net cevaplar vermek özellikle 1980'ler sonrasında güvenlik nezdindeki aktörlerin, güvenliğin kapsamının, içeriğinin ve araçlarının teorik zeminde yeniden tartışılmaya başlanması ile birlikte zorlaşmıştır. Çünkü vurgulanan sorulara farklı teorik yaklaşımlar çerçevesinden farklı cevaplar verilmektedir. Örneğin güvenlik fenomenine dair liberal ve realist bakış açıları, teorisyenleri kavram konusunda farklı önermelere götürebilecektir. Başka bir anlatımla, güvenlik objesini tanımlayan süjenin beslenmiş olduğu teorik temayülden azade bir tanımlama mümkün değildir.

Bu çerçevede Brauch kavramın sosyal bilimlerde genel çerçeveye karşılık gelebileceğini ve böylece kavramın farklı dönemlerin sosyo-politik yapısına göre değişebileceğini ve uyarlanabileceğini belirtmiştir (Braunch, 2012: 27-45). Brauch'un kavram için kullanmış olduğu "uyarlanabilir" sözcüğü aynı zamanda güvenlik fenomeninin mevcut koşullara adapte olabileceği imasını da taşımaktadır. Barry Buzan da kavramın zikredilen karakteristik özelliğinden dolayı birtakım riskler

barındıracağını ifade etmiştir (Buzan, 1983: 1-9). Yine Huysman bilimsel perspektiften anlaşılmasını güç bulduğu kavramı Buzan'ın görüşü paralelinde tartışmalı bulmuştur (Huysmans, 1998: 226-228). 1980'ler sonrası dönemin şartlarında McSweeney ve Morgan da güvenliğin barış durumu, düzen, adaletsizlik gibi -temel ihtiyaçlar bağlamında- sosyal kavramları ihtiva ettiğini belirterek tanımlanmasının girift bir hal aldığını ileri sürmüşlerdir (McSweeney, 1996: 83; Morgan, 1992: 465-470). Müşahede edildiği üzere semantik bağlamda izafi ve aynı zamanda devingen özellikler taşıyan güvenlik kavramı objektif bir tanımlamaya bürünememiştir (Owens, 1942: 303-308).

Tüm bu tanımlama sorununa rağmen yine de literatürde güvenlik için belli başlı tanımlamalar yapılmıştır. Güvenliğin etimolojik kökenine dair süregelen tartışmalarda kavramın menşei olarak Latin ve İngiliz olmak üzere iki gelenekten beslendiği görülmektedir. Latince kökeninde *securus* olarak telaffuz edilen kavramın ilk hecesi olan *se* "olmadan" manasını karşılarken, *curus* da endişe, kaygı ve tasa anlamına gelmektedir (Rothscild, 1995: 61; Waver, 2007: 99). Yani Latin sözlüğünde *securus* kavramı orijin olarak endişe, kaygı ve tasalanmanın olmaması manasına gelerek aynı zamanda emniyette olma durumuna tekabül etmiştir (Arends, 2007: 264). Latince'den İngiliz literatürüne *security* şeklinde tevarüs eden kavram tercümede kısmen farklı yorumlanmıştır. Buna göre, İngiliz tercümesinde se "olmadan-meden-meksizin" anlamına denk gelirken Latince'deki *curus* İngilizce'de *curity* olarak tebdil edilerek mental ve fiziksel manada tedirginliklerden ve endişelerden ırak olma anlamında kullanılabilmektedir. Kavramı Batı'nın geleneksel kodlarında ve İngiliz kökenbilimi doğrultusunda *securitas* olarak kullananlar Cicero ve Lucretius olmuştur (Arends, 2007: 264). I. yüzyılda Roma'nın Hıristiyanlığı Roma dini şeklinde kurumsallaştırması (Ağaoğulları ve Köker, 2013: 203) *securitas*'ın muhteviyatına dini de eklemiş ve böylece kavram kilit bir politik nosyon olarak lanse edilmiştir (Brauch, 2008: 75).

Güvenliğe dair günümüze değin yapılan bazı tanımları kategorize etmek gerekirse güvenliğin çeşitli vasıflandırmalara maruz kaldığı görülmüştür. Sözlük ve ansiklopedilerde güvenlik ile tehditlerden muaf olma durumu kastedilmiştir (Dağ, 2009: 410; TDK, 2009). Ayrıca güvenlik tüm endişelerden, uzak anlamında da

kullanılabilmiştir. Yine herhangi bir aktörün vesayeti altında yaşamama durumu ve bu duruma sebebiyet vermeyecek koşulların garanti altına alınması da kavramın tanımlama kategorisine girmektedir (Oxford English Dictionary, t.y). Uluslararası İlişkiler ve Diplomasi Sözlüğü de güvenliği bir devletin ulusal sınırları ve çıkarlarının başka devletlerin saldırı ve tehdidinden uzak durması olarak tanımlamıştır (Dağ, 2009: 410). Kavramı askeri ve siyasi boyutuyla tanımlayan Sönmezoğlu'na göre güvenliğin amacı varoluşsal bir gayeyi barındırdığından kavram doğrudan memleketin savunulmasına gerek bıraktırmayacak şekilde önlemlerin alınması olarak anlaşılmaktadır (Sönmezoğlu, 2012: 369).

Kavramı klasik formunda değerlendiren Terrif'e göre güvenlik, zarar veya tehlikeli durumlara karşı korkusuzluk hissine sahip olmaktır (Terrf, 1999: 1). Uluslararası İlişkiler dâhilinde güvenliği kuramsal perspektiften ele alan Wolfres ise kavramı objektif ve subjektif değerler bağlamında tasnifleyerek tanımlama çabasına gitmiştir. Ona göre güvenlik denilen fenomen, nesnel olarak elde edilmiş ya da kazanılmış değerlere yönelik tehditlerin bulunmaması hali iken, öznel olarak da bu tehditlerin değerlere yönelik saldırı hissi bulundurmaması halidir (Wolfers, 1952: 484). Wolfers'ın formüle ettiği bu kuramsal çerçeve doğrultusunda incelendiğinde kavramın objektif yanları dışarıda bırakıldığında tanım farklılıklarına sebebiyet veren noktanın sübjektif yanlar olduğu daha belirgin bir şekilde anlaşılabilmektedir. Çünkü subjektif güvenlik anlayışı devletler ve devlet-dışı gruplar tarafından tehdit unsuru oluşturmayan bir olgu ya da eylem, bir tehdit unsuruna dönüşebilir. Dolayısıyla her şeyden ve her olaydan şüphe duyma, belirsizlik durumu ve korku gibi hissi duyguların ortaya çıkaracağı güvensizlik durumu oluşacak ve bu durumda güvenlik açısından en önemli bir sorun olarak teşkil edecektir (Buzan, 1991: 1-3).

Elbette Wolfers tanımlamada atıfta bulunduğu değerler amilini kastederken bu değerlerin hangileri olduğunun ve bu değerlere yönelik tehditlerin ne tür güvenlik araçlarıyla savuşturulacağının belirginleştirilmesinin gerekliliğini vurgulamıştır. Hâlihazırda kavramın muğlaklığından dem vuran Wolfers güvenliği değerler bazında inceleyip aynı zamanda bu değerleri de belirli sorularla somutlaştırarak bir nevi objektif olarak güvenliğin bilimsel bir tanımlamasını ve incelenmesini kolaylaştırmaya çalışmıştır (Tanrısever, 2014: 108). Wolfers'ın eldeki kazanılmış

değerler şeklinde formüle ettiği devlet merkezli güvenlik analizini Walter Lipmann da devlet merkezli bu duruşu benimseyerek öz değerler üzerinden açıklama yoluna gitmiştir. Buna göre bir devletin öz değerlerini muhafaza etme saikiyle savaşabileceğini, bunun için de öz değerlerine yönelik herhangi bir tehdit unsurunun yokluğunda bile bu öz değerleri koruma kapasitesine haiz olduğu oranda kendini güvende hissedebilir (Aktaran: Wolfers, 1952: 484). Miller da güvenliği var olan değerlere karşı tebarüz edecek olan tehlikeleri mümkün olan en yüksek seviyede bertaraf edebilme potansiyeline sahip olma şeklinde tanımlamaktadır (Miller, 2001: 6).

Devlet odaklı özdeğerler çerçevesinde kavramı değerlendirenlerin tanımlarından da anlaşılacağı üzere düşünürlerin esasında dile getirmiş oldukları güvenlik nosyonu kapasiteye bağlı sahip olunan caydırıcılık özelliğidir. Zikredilen tanımlamalarda devletler güvenliklerini garanti altına almak ve aynı zamanda hayatlarını idame etmek için güvenliği kapasiteleri bağlamında doğru zaman-mekân ve araçlarla sağlayabilecektir. Realist ekol içerisinden alternatif güvenlik yaklaşımlarına karşı güvenlikle ilgili hususi olarak tanımlama getiren Walt'a göre güvenlik tehditler, askeri güç unsurları ve bu unsurların güvenlik aracı olarak kullanımı şeklinde tanımlanmaktadır (Walt, 1991; 212). Güvenliği tartışmalı bir kavram olarak gören ve Wolfers gibi değerler üzerinden kavramı ifade eden John Baylis'e göre de, güvenlik en nihayetinde temel değerlere karşı tehlike ve tehditlerden özgür olunması durumudur (Baylis, 2008: 495-496).

Luciani ise kavramı Lipmann'ın öz değerler anlayışına paralel olarak devletlerin barış şartlarında ve dönemlerinde eldeki değerlerini tehdit olasılıklarına karşı koyabilmesinin yanında muhtemel savaş durumlarında üstün çıkmaları durumu şeklinde tanımlamıştır (Luciani,1998: 153). Literatürdeki politik ve askeri tehditler haricindeki tehditlerin güvenlik tehdidi temayülü göstermediğini ve bu yönle aslında kavramın politik bir bakış açısına sahip olduğunu dile getiren Ayoob da güvenliği devletlerin kurumsallığı, rejimi ve sınırsal egemenliğinin tezahürü olan üniter yapısına karşı tehdit koşullarının olmaması şeklinde tanımlamaktadır (Ayoob, 1995: 2). Öte yandan kavramı herhangi bir analiz biriminden bağımsız değerlendiren Sponvill de kavramı nihai bir amaç taşımadığından dolayı her daim uğruna

savaşılacak bir araç olarak görmüştür (Bal, 2003: 21). Kavramı sosyolojik tabanda ele alan Giddens'a göre güvenlik kişilerin, toplumların ya da herhangi bir sistemde sistemi oluşturan grupların birbirlerine güven duygusunu taşımaları durumudur. Başka bir anlatımla güvenlik güvenmek ve itimat etmektir (Giddens, 2014: 38-42).

Fikirsel bağlamda Barış Çalışmalarından etkilenen 1980'ler sonrası yeni güvenlik anlayışları da güvenliği analiz birimi açısından farklı ele aldıkları için tanımlamasını da farklı açılardan yapmışlardır (Waver, 2004: 53-54). Galtung'un formüle ettiği yapısal şiddet kavramsallaştırması çerçevesinde doğrudan ve dolaylı hissedilen şiddetler, bireyler ve toplumlar nezdinde güvensizlik hissiyatına sebep olmuştur. Bu durumda güvensizliğin tanımını yapısal şiddetin varoluşuna bağlayan Galtung, aynı zamanda güvenliği de ulusal ve uluslararası mecrada yapısal şiddetlerin yoksunluğuna bağlamıştır (Galtung, 1969: 168). Hususi olarak güvenlik kavramından ziyade barış kavramına odaklanan Galtung'un güvenlik kavramına dair çizmiş olduğu bu dolaylı güvenlik tanımı kendisinden sonra gelecek olan farklı alternatif güvenlik yaklaşımlarını ve müntesiplerini etkilemiştir (Bilgin, 2008: 129). Öyle ki, Barış Çalışmaları Grubu'ndan sonrada birey ve toplum temelli yeni güvenlik tanımlamaları literatürde revaçta olmuştur.

Galtung'un yapısal şiddet kavramsallaştırmasında vurguladığı dolaylı/görünmeyen şiddet unsurları Ken Booth'un, eleştirel teoriden miras kalan özgürleştirme kuramında yeni bir güvenlik anlayışı olarak telakki etmiştir. Booth güvenliği insanların yapmalarını arzuladıkları şeyleri gerçekleştirmekten alıkoyan tüm fiziki ve beşeri sınırlayıcı etmenlerden özgür kılınma durumu olarak tasvir etmiştir (Booth, 1991: 319). Bireylerin olması gereken olanaklardan var olan engeller yüzünden faydalanamaması durumunu birey ve toplum açısından güvenlik sorunu olarak algılayan Booth, bu sorunun da ancak bireylerin bilinç kültürüyle elde edeceği özgürleşme (emancipation) ile çözüleceğini dile getirmiştir. Ona göre özgürleşme ile güvenlik aynı madeni paranın iki yüzü gibidir (Booth, 1991).

Tehdit unsurları ve riskler bakımından güvenliğin askeri konular dışında da ele alınmasının gerekliliğini ifade eden Ullman da kavramı devletlerle beraber bireyler ve diğer grupların da haiz oldukları yaşam biçimlerine herhangi bir tehdidin yokluğu olarak tanımlamıştır (Ulman, 1983: 133-134). Yine, kavramı askeri kaynaklı

olmayan boyutlardan değerlendiren Fischer de insan ya da devlet olsun güvenliğin salt beka, savaştan korunması ve önlenmesi barındırdığını belirterek, hattı zatında kavramı sosyal ve siyasal birimlerin hayatta emniyetli bir şekilde devam etmesi şeklinde tanımlamıştır. Post yapısalcılığın öncü isimlerinden olan Foucalt ise devleti merkeze alan güvenlik anlayışını reddederek tıpkı Uluslararası İlişkiler'i açıklamada kullandığı iktidar-bilgi arasındaki karşılıklı ilişki yoluyla kavramı tanımlamıştır. Güvenliği bir politik fenomen olmaktan öte, siyaset yapma şeklinin aracı olarak gören Foucalt, kavramın iktidar ilişkilerinden müstakil bir yapıya sahip olduğunu ve başlı başına kavramın kendisinin bir iktidar inşa etmenin formu ve yönetme şekli olduğunu dile getirmiştir (Foucalt, 2009: 19-38). Bu hususlar ışığında, güvenliğin tanımına ve tasvirine dair açık ve net olarak göze çarpan özellik kavramın tüm zamanlar ve mekânlar için geçerli olabilecek yegâne tanımının bulunmamasıdır (Bilgin, 2010: 76).

Dolayısıyla güvenlik terimine alan çeşitliliği ve tarihin değişen koşullarına bağlı olarak her daim farklı anlamlar yüklenmiştir (Şahin, 2004: 1-35; Melvyn: 1990: 143-145). Ancak kavram üzerinde belki de oydaşmaya varılan yegâne çerçeve güvenlik kavramının kendinden menkul sebeplerle, özünde tartışmaya açık bir inceleme konusu olduğudur (Huysmans, 1998: 228). Örneğin, Soğuk Savaşın bitimine kadar devlet odaklı tanımlanan güvenlik, akabinde birey, çevre, cinsiyet ve diğer toplumsal katmanların ihtiva ettiği olguların üzerinden tanımlanmıştır. Bu çerçevede, insanlığın bidayetinden günümüze değin her daim neşet eden yeni güvenlik alanları var olmuş ve bununla ilintili olarak da güvenlik alanları değişim sürecine girmiş, belirsizlikler, tehditler, riskler artmış ve de güvenliğin referans aktörleri sürekli değişime uğramıştır. Beşeriyetin başlangıcındaki güvenliğin referans nesnesi savunmasız olarak bilinen insan iken, güvenliğin tehdit edici unsuru olarak da doğa görünmüştür. Ancak, akabinde siyasal örgütlenme oluşumlarının -şehir devletleri, medeniyetler- tebarüz etmesiyle toplumsallaşmadan ve farklı gereksinimlerden mütevellit evvelinde insan dışı doğa kaynaklı olan tehdit unsurunun yerini bizatihi insan toplulukları tehdit unsuru olarak algılanmıştır (Harman, 2015: 1-44, Ateş, 2012: 4).

Orta Çağ döneminin güvenlik referansı kutsi Hristiyanlık doktrinleriyle bezenen sınırlar iken (Eco, 2015: 12-18) Westphalia sonrası dönemde ise seküler anlayışla yönetilebilen ve verili ulusal topraklar üzerinde egemenliğini idame ettiren devlet, güvenlik referansı olarak kabul görmüştür (Philpott, 2001; Gross, 1948; 27-28). Yine, Soğuk Savaş'ın bitimine müteakip, sınırlarının ötesindeki güvenliğini bütünleşme ve genişleme politikalarında uygun gören ve Doğu Avrupa'ya açılan AB, günümüzde sınırları içerisinde yaratacağı göç, sınır ve demografik sorunlar hasebiyle aynı bütünleşme ve genişleme politikalarının güvenliğine zarar vereceğini düşünebilmektedir. Mekânsal bağlamda kavramın farklılığına örnek olarak; Afrika'nın Somali ülkesinde açlık, susuzluk ya da Nijerya'da salgın hastalıklar gözle görünür tehdit unsuru oluştururken, dünyanın örneğin İskandinavya gibi farklı bir bölgesinde güvenliğe tehdit unsuru iklime dayalı koşullar oluşturabilmektedir. Yine, Ortadoğu'da hem kendi içinde bölünmüş otoriter yönetimlerden hem de bölgesel ve küresel savaşlardan neşet eden korku bölgenin stabil güvensizlik ortamını muhafaza ederken (Chourou, 2007: 776-789) küresel ekonomik pazarda en önemli güç olma yönünde ilerleyen Çin için ise enerji kaynaklarının arzının güvenliliği önemli güvenlik unsuru olmuştur (Hunter ve Liu Cheng, 2007: 839-865). Örnekleri kolaylıkla çoğaltılabilecek bunlara benzer durumlardan da gözlemleneceği üzere tarihsel süreç içerisinde yaşanan tarihi dönüm noktalarından müteşekkil güvenlik kavramı sosyal bilimler literatüründe algıda ve içerikte hep muallakta kalmıştır.

Güvenlik teriminin neden belirsiz olduğuna dair farklı bir bakış açısı getiren Haftendorn da kavram olarak güvenliğin yekpare bir anlamının bulunmamasının sebeplerinden birini ontolojik bağlamda sorunsallaştırmaktadır. Ona göre "güvenliğin bir amaç mı, yoksa bir araç mı olduğu", "analize tabi tutulup sorunsallaştırma alanına girmesi gerekip gerekmediği" ve hatta "bir disiplin olup olmadığı" gibi önemli sorular cevaplandırılmadığı müddetçe kavramın muğlaklığı da devam edecektir (Haftendorn, 1991: 5-15). Bu yüzden güvenlik mefhumu ister devlet merkezli tanımlansın ister birey ya da toplumsal değerler üzerinden tanımlansın otonom bir anlama haiz ol(a)mamıştır (Art, 2004: 179-150).

1.2. Ortodoks Güvenlik Kavramı ve Paradigmasının Siyasi Tarihteki Epistemik Kırılmalara Bağıtlı Evrimi

Sosyal bilimlere dair muğlak ve göreceli anlamlar ifade eden birçok kavram aynı zamanda tarihsel süreçlerin süzgecinden evrilerek modern dönemin anlam kalıplarında yer edinmektedir. Bu çerçevede güvenlik kavramının arka planı da insanlığın bidayetine kadar gidebilmektedir. Konargöçerliğe dayalı yaşam biçiminin benimsendiği ilkel dönemde insan gruplarının temel ekonomik kaynakları avcılık ve toplayıcılık gibi üretime dayanmayan, sadece ikame ettikleri yerlerde bulunan bitki ve hayvanlar olmuştur. Bu dönemde insan toplulukları için temel endişe kaynağı beslenme ve güvenli bir şekilde barınma ihtiyacı olmuştur. Çünkü çetin doğa koşullarının yaşandığı bu dönemin insan toplulukları, doğaya karşı oldukça zayıf konumdadır (Anderson, 2013: 18-28, Heller, 1970: 18-28). Doğaya karşı güvensiz konumda olan insan toplulukları güvenliklerini zorunlu olarak yardımlaşarak sağlama yoluna gitmişlerdir. Yani, ilkel dönemin konjonktüründe güvenliğin referans nesnesi insan grupları iken, bu insan gruplarına yönelik tehdit unsuru da diğer doğa canlılarıdır (Mann, 2012: 15-17).

Daha sonraki dönemlerde -tarımsal devrimden sonra- doğanın olanaklarından faydalanmaya başlayan insan grupları tedricen toprağı kullanıp tarımsal üretime geçerek onun getirisi olan yerleşik yaşamı benimsemişlerdir. Bu yeni yaşam biçiminin toplumsallaşmaya dayalı köy düzenini ikame etmesi ile birlikte toprağın nitelikli işlenmesi (Haas, 1982: 20-31; Friedman ve Rowland, 1978: 34-46) tüketimden arda kalan üretimi artırmış ve ticaretin doğmasına vesile olmuştur. Ticari hayatın gelişmesi yeni bir tarihi-sosyal-siyasal formasyon olan şehir yapılarının inşasını hızlandırmıştır. Bu durumda, şehir devletlerinde yöneten ve yönetilen ilişkilerinin de başladığı dönem olmuştur (Ağaoğulları, 2012: 21-22, Ateş, 2012: 4). Bu dönemde ticari canlanmanın had safhaya çıkması beraberinde ekonomik ilişkilerin belirlediği sınıfsal yapıları ortaya çıkarmış ve artık insanlar için tehdit kaynağı doğadan ziyade kendi aralarındaki mücadelelerden dolayı bizatihi kendileri olmuştur (Parson, 1977: 22-24).

Şehir devletlerinin bölünmüş siyasi yapıları birbirleriyle ekonomik temelli çatışmaları da hızlandırmış ve başlangıçta insan merkezli mana kazanan güvenlik

anlayışı tedricen şehir devletlerinin güvenliği anlayışına kaymıştır. Ticari kaygılarla herhangi bir şehir devleti kendinde olmayan kaynaklar için diğerleriyle çatışma içine girebilmiştir. Göçebe topluluklar zengin şehir devletlerine yönelik saldırılar düzenlemiştir. Çünkü göçebe yaşayan topluluklar ihtiyaçları olan maddeleri savaşarak elde etmeye çalışmışlardır (Childe, 1950: 3-6). İlaveten, dönemin şehir devletlerinin bölge ve yerleşke anatomisinden dolayı sürekli saldırıyla karşı karşıya kalmaları ve devletlerarasında sınırların belirsizliği bölgede her daim savaşlara sebebiyet vermiştir. Böylelikle dönemin güvenlik anlayışı da şehir devletlerinin yayılmacı tutumlarına yönelik olmuştur (Sander, 2012: 27-36, Jones ve Kautz, 1981: 64-68). İşte, İnsanlık tarihinin, güç doğa koşullarına yönelik algısında yer alan güvenlik kaygısı bundan böyle tarım ekonomisine dayalı ticaret üzerinden varlığını idame ettirmeye çalışan şehir devletlerinin birbirleri arasındaki mücadeleler üzerinden şekillenmeye başlamıştır. Güvenlik algısında ve pratiğinde tarihsel sürecin bu döneminde yaşanan gelişmeler çalışmada da sıklıkla telaffuz edilecek olan klasik güvenlik paradigmasının ilk formel biçimini oluşturmaktadır.

Kent devletlerinin siyasal, ekonomik ve sosyal alanda giderek kurumsallaşması uygarlıkların inşasına ve de bu uygarlıkların global nitelik almaya başlamasına vesile olmuştur. Özellikle tarımın ticari zeminde nitelikli kullanımı, ürün çeşitliliğini had safhada artırmış bu durumda devletlerin yükselişlerinde ve çöküşlerinde müessir olan ekonomi-güç ilişkisini ortaya çıkarmaya başlamıştır (Kennedy, 2009: 1-24). Ekonomik gücün aynı zamanda siyasal gücü de beraberinde getirmesi kent devletleri arasındaki çatışmalarının dozunu artırmaya başlamış ve yaşanmaya başlayan güvenlik ikilemleri askeri araçların da sistemde görünmesini beraberinde getirmiştir.

Bu bağlamda, Thukydides'in Peloponnesos Savaşı'nın tarihinde anlattığı olaylar o zaman ki sistemin anarşik örgütlenmesinden kaynaklı güvenlik ikileminin devletler nezdinde en büyük tehdit endişesi olduğunu gözler önüne sermiştir (Thukyidides, 2010). Yunan dönemine özgü güvenlik anlayışında -ilk çağ şehir devletlerinde olduğu gibi- devletler güvenliğin temelini oluştururken, devletlere yönelik tehdit kaynağı da yine harici rakip devletlerden neşet eden tehditler olmuştur. Bununla ilintili olarak da güvenliğin sağlanması noktasında da araçlar askeri temelli olmuştur.

Yunan medeniyeti, Roma döneminin klasik sonrası dönemin tedricen değişmeye başlayan siyasal ve sosyal pratiklerinin öncüsü olmuştur. (Ağaoğluları, 2012: 190). Hristiyanlık dini aracılığıyla aynı zamanda Roma'nın birliğini ve de yüceliğini kendisinde bedenleştirilerek imparatorluğa tapılmasını sağlama hedeflenmiştir. Dolayısıyla, toplumu bir arada tutan evrensel Hıristiyanlık dini bundan böyle önce Roma'da akabinde de uzun yıllar sürecek Ortaçağ da, hem Hıristiyan dünyada hem de Hıristiyanlık dışı devletlere karşı devletle beraber en önemli güvenlik nesnesi haline gelmiştir (Brown, 1961: 23-36).

Özellikle kilisenin Roma imparatorluğunun ertesinde oluşan siyasal, sosyal, kültürel ve ekonomik güç boşluğunu devralması dini, kıta Avrupa'sında siyasal odak noktası haline getirmiştir. Papalık kurumu ile dünyevi iktidarın temsilcisi krallıklar arasındaki güç paydaşlığı sorunu hâlihazırda parçalı siyasal birimlerin arasındaki mücadelelere dinsel bir boyut eklemiştir (Lee, 2012: 114). Yani, Roma dönemi ile başlayıp akabinde Ortaçağ diye adlandırılan dönemin kilise anlayışının da güçlenmesiyle birlikte din fenomeni devlet unsuru ile beraber güvenliğin kapsamına girmiştir.

Bu dönemin göze çarpan bir diğer özelliği de imparatorluğun idamesi için askeri güç kapasitesine sürekli sahip olma mantığıdır. Çünkü dönemin tüm imparatorluklarının ve derebeyliklerinin kökenini oluşturan olgu savaştır (Parker, 2014: 106). Sürekli savaş ortamı askeri araçlara sahip olmayı ve bu araçları geliştirmeyi gerekli kılmaktadır. Özellikle Avrupa'nın bilimsel ve kültürel bağlamda geçirmiş olduğu teknolojik devrim savunma ve saldırı mekanizmalarında değişimi ve dönüşüm sürecini hızlandırmakla birlikte tehdit alanını ve güvensizlik hissini de beraberinde getirmiştir. Barut devrimi, ateşli silahların yükselişi, deniz ulaşımının artık daha kolay yapılması gibi askeri etmenler savaşların alanını genişletirken aynı zamanda savaşların yıkıcı etkisini de artırmıştır (Parker, 2014: 125, Quincy, 1942: 24-36). Bundan böyle Avrupa güçleri askeri teknolojinin birikimsel olarak ilerlemesiyle kıta Avrupası'nın öte sınırlarına hâkimiyetini genişletme çabalarına girişmiş ve böylelikle başka devletler için yayılmacı yayılmacı politikalar güvenlik için tehdit unsuru olmuştur. Bahse konu tarihsel gelişmeler güvenliğin muhteviyatındaki alanları, sınırları, konuları ve dolayısıyla araçları da genişleterek

bir bakıma güvenlik alanı ile çıkar alanlarını da eş konuma getirerek klasik güvenlik paradigmasınınözünde perçinleşmesini sağlayarak içerik ve pratik bağlamda yeni boyutlar eklemiştir.

Askeri ve ekonomik bağlamda tebarüz eden teknolojik yenilikler dünya ölçeğinde makropolitik etkilere haiz olmuştur. Ekonomik üretim ve ilişkilerin niteliklerinin değişmesi ile beraber toplumsal ve siyasal güç pozisyonlarında yaşanan değişimler ülkesel bütünlüğe özgü toprak anlayışını ve bununla ilişkili olarak da devletlerarası sistemin değişen kurumları ve pratikleriyle gün yüzüne çıkmasına yön vermiştir. Bu bağlamda siyaset teorisi ile ilinti olan felsefik düşünce de bahsi geçen değişimlere teorik zemin hazırlamaya devam etmiştir.

Bu bağlamda, 14. ve 16. yüzyıllarda rönesans teorisyenleri artık siyasal birim donesi olarak devleti ele almışlardır. Elbette ele aldıkları bu devlet amili modern dönemin devlet tahayyülüne tam olarak tekabül etmemektedir. Bahsi geçen siyasal organizasyon bir şehir devlet yapılanmasıdır (Tilly, 1975: 4-84; Finer, 1975: 85-100). Bu rönesans ruhunun temsilcileri olan Makyavelli ve Hobbes da iktidar salahiyetini dini otoriteden dünyevi otoriteye tahvil edilmesi gerektiğini ileri sürerek hükümdarın mevcudiyeti üzerinden devleti kutsamışlardır (Walker, 1993: 30). Bu bağlamda insan ürünü olan verili devletin bekası temelli güvenliği için doğası gereği bencil olan insanoğlu ve toplumun, devletten daha değerli bir konuma haiz olması düşünülemezdi. Çünkü Makyavelli ve Hobbes'a göre devleti yaratan toplum için en büyük güvence devletin güvenliğidir (Skinner, 2003: 432). Makyavelli ve Hobbes da benzer şekilde siyasal iktidarın ulusal çıkar doğrultusundaki amacının hâkimiyet kurma çabası ve güç elde etme isteğinin geldiğidir. Dolayısıyla da, aynı anda savaş ve güvenlik meseleleri yüksek bir politika (high poltics) şeklinde lanse edilirken bunun ötesinde toplumsal, ekonomik ve kültürel meseleler de düşük politika kategorisine girmektedir (Arı, 2013: 92-94).

Din temelli çatışmalarından ve güvenlik sorunlarından kopuşu simgeleyen ve uluslararası ilişkilerin kaderini belirleyen olay Westphalia Antlaşması'nın antlaşmasının imzalanması olmuştur (Macrae, 2005: 160-164, Gross, 1948: 20, Krasner, 1995: 115). Modern uluslararası sistemi inşa eden bu antlaşma temel aktörlerin tekliği ve belirginliği ve bu aktörlerin sistemde davranışlarını belirleyen

saiklerin neler olduğu gibi klasik orta çağ döneminin ve siyasal sisteminin cevap veremeyeceği soruları açık bir şekilde çözümlemiştir.

Bundan böyle merkezileşen devlet yapısında derebeyi ve papa gibi devlet dışı siyasal, sosyal ve dini aktörlere yer yoktu. Modern uluslararası sistemin bundan böyle temel aktörü siyasal egemenliğin tezahürü olan teritoryal bütünlüğe haiz devletti. Siyasal egemenlik yetkisini elinde bulunduran kurumsallaşmış devlet iç ve dış politikada kaçınılmaz olarak güvenliğinde yegâne unsuru ve nesnesi konumunda olmuştur (Cruz, 2005: 151; Farr, 2005: 156-159). Çünkü artık sınırlar belirginleşmeye başlamış ulusal ve uluslararası sistemin hiyerarşisi içerisinde devlet en üstte yer edinmiştir. Belirli kurallar çerçevesinde şekillenen ve aralarında düzenli ilişkiler bulunan devletlerin oluşturduğu bütün, bir başka deyişle uluslararası sistem bugün anladığımız anlamda Westphalia ile doğmuştur (Sander, 2012, Bewes, 1993: 61-73).

Westphalia sisteminin temelini oluşturan egemenlik nosyonun hem ulusal hem de uluslararası ilişkilerde kadiri mutlak bir devletin kriteri olması aynı zamanda güvenlik kavramını da anlam ve içerik bakımından dönüşüme uğratmıştır. Çünkü belirli bir toprak parçası ve burada yaşayan insanlar üzerinde mutlak egemen olarak tanımlanan devletin ülkesel bütünlüğünün güvenliği esas sorun teşkil etmiştir (Wheatcroft, 2011: 11-17). Bu sebeple, egemenlik kavramı ile güvenlik kavramı da tarihsel süreç içerisinde kahır ekseriyette paralellik arz etmiştir. Örneğin, Westphalian düzen öncesi sistemde devletin tezahürü görünümündeki kralın egemenliği ve güvenliği temel kaygı iken, Westphalia sonrası düzende ise bizatihi bir devletin egemenliği ve bununla ilintili olarak güvenliği esas sorun ve kaygı teşkil etmiştir. Bunun için de içte ve dışta ulusal değerlerini koruma gayretindeki devletin güvenliği birincil kaide olmuş ve bu kaide 1980'lı yıllara değin uluslararası ilişkilerde geleneksel güvenlik paradigmasının olmazsa olmazı olmuştur. Adeta Ortodoksi bir anlayışa bürünen geleneksel güvenlik paradigması çerçevesinde bir devlet kendisine yönelik tehditleri bir başka devletten beklemiş ve güvenliğini sağlama noktasında askeri güç araçları ile siyasal gücünü artırma yoluna gitmiştir.

Felsefe ile siyaseti harmanlayarak devlet merkezli bir güvenlik anlayışının temellendirmelerini sunan siyaset teorisyenlerinin önermeleri siyasal zeminde

karşılık bulmuştur. Devletlerarasında cereyan eden rekabetin süreklilik kazandığı anarşik uluslararası sistemde çatışmaların ve savaşların kaçınılmaz olduğu mottosu egemen devletlerin güvenlik anlayışını başka devletin hâkimiyeti altına girmeme şeklinde algılamasına neden olmuştur. Böylelikle devletlerarasındaki rekabet sürekli kızışmış ve ulusal boyutlarda değerlendirilen güvenlik anlayışı uluslararası boyutları da ihtiva etmiştir. Süreklilik kazanan uluslararası boyutlardaki savaş ve çatışmaların kurumsallaşan hukuk ve kolektif barış anlayışı ile çözümlenebileceğine dair fikirler ortaya atılmıştır (Corquodale ve Panglanhan, 2001: 865-871).

Sistemden kaynaklı tebellür eden güvenlik endişelerinin sadece savaşlar aracılığıyla giderilebileceği algısını reddeden Kant ve Fitche gibi bu yüzyılın siyaset felsefecileri bunun karşısında yer alarak öneriler sunmuşlardır. Onlara göre ulusal ve uluslararası sisteme yönelik en büyük tehdit kaynağı devam eden savaşlardır ve bir devlet güvenlik kaygısı yaşamak istemiyorsa uluslararası sisteminde güvenliğinden endişe etmelidir. Bu mantık çerçevesinde Kant uluslararası sistemde güvensizliğin kaynağı olan savaş yerine barışın devletlerin müşterek uzlaşmasına dayalı uluslararası hukukun inşasını salık vermiştir. Ayrıca, herhangi bir kural koyucunun olmadığı uluslararası sistemin güvenliğinin çatışmalara ve savaşlara gebe olmaması için de oluşan kolektif devlet yapılarının sistemde –bugün anladığımız şekliyle Avrupa Birliği gibi- ebedi barışı sağlayacağını ileri sürmüştür (Kant,1960: 10-56)

Fransız İhtilali ve Sanayi Devrimi sonrasında yaşanan gelişmeler modern uluslararası sistemin temellerini inşa eden Westphalian düzeni teyit eder şekilde gelişmiştir. Uluslararası sistemin yapısı ve işleyişi egemen devlet birimi üzerinden değerlendirilmeye devam etmiştir. Daha önceki yüzyıllarda farklı siyasi birimlerin farklı güvenlik kaygılarından neşet eden çatışmalar bundan böyle türdeş özelliklere ve haklara sahip devletlerarasında cereyan etmiştir. Ve egemen siyasal örgütlenme biçimi olarak tebarüz eden devletlerin arasında üstünlük kurma yarışı başlamıştır. Uluslararası sistemin adeta işleyici mekanizması haline gelecek olan bu üstünlük kurma yarışı güçler dengesini koruma adı altında bu kez egemen devletlerarasında sürekli rekabet ve çatışma alanı açmıştır. Ticari alanda kurduğu hegemonik güç aracılığıyla önce Hollanda (Armaoğlu, 2013: 30), akabinde kral Louis önderliğinde ulus ötesi sınırları kolonileştirmesiyle Fransa ve nihayet denizlerdeki hamiyeti,

sanayileşmesi ve finansal kaynaklarının küreselleşmesi hasebiyle 19. Yüzyılın Britanya'sı güç dengesinde üstünlük kurmayı başarmışlardır (Lee, 2014; Hobsbawm, 2013: 10-45, Schroeder, 1986: 2-26).

Ancak anarşik sistemin doğal sonucu olarak beliren güç dengesinin sağlanmasına zarar veren bu üstünlük kurma mücadelesi uluslararası sistemin güvenliğine tehdit unsuru oluşturmaya başlamıştır. Çünkü 19. yüzyılda her alanda üstünlük kurmak isteyen güçler için artık yegâne güvenlik kaygısına ülkesel sınırları muhafaza etmenin yanında ulus ötesi farklı coğrafyalarda kurdukları sömürgelerin muhafazası da eklenmiştir. Öyle ki bu durum bahsi geçen devletlerarasında, birbirlerine karşı statik bir hal alan üstünlük kurma yarışları için güçler dengesini koruma bağlamında ittifaklar sistemini doğurmuş ve bu ittifaklar sistemi en sonunda I. Dünya Savaşı'na giden yolu açmıştır (Potyemkin, 2009: 287-304). Güç dağılımında da uluslararası sistemde dengesizliğe yol açacak olan güçler dengesinin bozulması sistemin diğer türdeş aktörlerinde güvenliklerine yönelik korku ve kaygılar beslenmesine sebebiyet vermiş ve bu durumda güç artırımını hızlandırmıştır (Kratochwil, 1986: 27-52). İşte bu ortam sistemde sürekli savaş ve istikrarsızlıklara gebe kalmasına sebebiyet vereceğinden uluslararası sistemin ve bununla ilintili olarak devletlerin güvenliğine tehdit oluşturmuştur (Bridge ve Bullen, 1980; Schroeder, 1984; 2-25).

Sanayileşmenin hızlanması ile beraber silah teknolojisinde de ivme kazanan değişim ve gelişim devletlerin silahlanmasını da artırmıştır. Artan bu silahlanma yarışının askeri araçların önemini ve değişimini hızlandırması ve ittifaklar sisteminin katılaşması gibi yapısal değişiklikler, uluslararası sistemin güç dengesini devam ettiren çok kutupluluğa yönelik özellikle güvenlik ikilemi bağlamında büyük tehdit unsuru oluşturmuştur (Keohane, 1986: 240-290, Gilpin, 1981: 13-15, İkenberry, 1986: 55-67). Uluslararası sistemin dengesini bozan bu gelişmeler I. Dünya Savaşı'nı tetiklemiş ve kısa barış döneminden sonra otoriteryan ideolojik rejimlerinde siyaset sahnesinde yer almasıyla birlikte uluslararası sistemin güvenliğinin tüm boyutlarıyla kapsamını genişletip başka evreye girmesini hızlandırmıştır. Liberal çözümlemelere dayanan ortak güvenliğe dayalı uluslararası sistem temayülü krizlere -1930 Etiyopya

ve Mançurya- çözüm getirememesi hasebiyle başarısızlıkla sonuçlanmış ve yeni savaşın patlak vermesine engel olamamıştır.

Savaş alanlarında kullanılan yeni askeri teçhizatların ve özellikle de dünyanın tüm gruplarına yönelik en büyük tehdidi oluşturan atom ve nükleer çağın habercisi olan II. Dünya Savaşı sistemsel değişiklikleri ile beraber yeni güvenlik anlayışında devletlerin politika ajandasında en üst sırada yer almıştır. 1990 yılına değin ittifaklar sisteminin öncülüğünü elde eden Amerika Birleşik Devletleri (ABD) ve Sovyet Sosyalist Cumhuriyetler Birliği (S.S.C.B) arasında zuhur eden ideolojik ve askeri temelli bloklaşmalar uluslararası ilişkilerde siyaset yapma biçiminde belirleyici etken olmuştur. Bu iki güç arasında yaşanan siyasi ve askeri rekabet dönemin güvenlik siyasetine yön vermiştir. İki kutupluluğa dayanan Soğuk Savaş dönemindeki güvenlik anlayışı da bu iki güç arasında yaşanan çekişmeler sayesinde devletlerin ulusal güvenlikleri ile ilgili kaygılarını canlı tutmuştur. Buna karşılık bu dönemde güvenlik askeri güç ile orantılı olarak düşünülmüştür (Gaddis ve Paul, 1980: 164-175, Yergin, 1990: 46-52). Dolayısıyla yaklaşık yarım asır ülkelerin dış politika manevra kabiliyetlerinin ve alanlarını sınırlayacak olan Soğuk Savaş dönemi güvenlik anlayışında ulusal güvenlik kısmını birincil ve en yüksek politika vaziyetine getirmiştir (Buzan, 2007: 555-558).

Güvenliğin bu dönemde sadece askeri kaynaklı mülahazalarla sağlanabileceği algısı silahlanma yarışına sebebiyet vermiştir. Ulusal güvenliğin sağlanması noktasında benimsenen çözüm yolu askeri temelli olmuştur. Öyle ki, bu dönemin güvenlik anlayışına yön verecek olan askeri kapasite artırımı, askeri güç elde etme ile aynı kefeye konmuş ve uluslararası sistemde güvenliğin algılanış şeklini de salt ulusal zeminde tahkim etmiştir (Mearsheimar, 1998: 10-11, Waltz, 1959). Rakip konumdaki iki güç arasındaki tehdit algısı nükleer kapasiteye ve artırıma dayalı caydırıcılık hamlelerinin hızlanması uluslararası sitemi fazlasıyla germiş ve savaş korkusunu yine fazlasıyla hissettirmiştir. Nükleer kış olarak tabir edilen bu dehşet dengesinde her iki rakip gücün sıfır toplamlı oyun anlayışında birbirini yok etme girişimi dönemin güvenlik anlayışının çerçevesini oluşturmuştur. Bunun için de bir gücün silahlanma yönünden güç artırımına gitmesi diğer rakip gücün de aynı yolu seçmesini beraberinde getirmiştir (Mearsheimar, 2001).

Soğuk Savaş döneminde güvenliğin salt askeri temelli yöntemlerle düşünülmesi kavramı sınırlı alana hapsetmiştir. Rakip iki güçten birinin güvenliğini sağlama noktasında başvurduğu güç artırımı tedbiri bir diğeri için güvenlik kaygısına sebebiyet vermiş ve Soğuk Savaş döneminin en büyük güvenlik sorunlardan olan silahlanma yarışını kızıştırmıştır. Örneğin ABD'nin önce atom bombası daha sonra nükleer kapasiteye erişmesi rakibi Sovyetleri güvenlik algısında korku ve gerginliğe sevk ettiğinden kendisini tehdit altında hissetmiştir. ABD'nin sahip olduğu bu kimyasal ve hidrolojik silahlara karşılık Sovyetler de silahlanma çeşitliliği bakımından nükleer kapasite artırımına gitmiş olmakla beraber aynı zamanda uzaya da uydu göndererek karşılık vermiştir. Yani rakip devletlerin güvenliklerini artırma ve sağlama şiarı ile silahlanma seçeneğini benimsemeleri karşılıklı bir şekilde tehdit algılanması neticesinde içine düşecekleri güvensizlik sarmalını doğurmuş ve bundan dolayı Soğuk Savaş dönemi ortamı her daim savaş olasılıkları ve tedirginliklere gebe olmuştur (Schelling, 1966; Best, 2012: 265).

Soğuk Savaş dönemi ile birlikte ulusal ve uluslararası sistemin politik gündemin ana sorununu oluşturan güvenlik, karar vericiler nazarında siyaset yapma biçiminde adeta birincil siyasi malzeme olmuştur. Soğuk Savaş döneminin 1950'li yıllarında ABD başkanı Truman'ın ulusal güvenlik yasası şeklinde tebarüz eden yeni güvenlik anlayışı adeta bir politik fikrin tasarımı ve ifadesi haline bürünmüş ve iki rakip gücün peyki konumundaki diğer devletler tarafından da kullanılmıştır (Freeland, 1979: 419, Paterson, 1972: 73). Bununla birlikte, dönemin akademik camiasında sistematik olarak analiz edilmeye başlanan güvenlik kavramı içerikleri ve pratikleri ile konusunu ulusal güvenlikten almaya başlamıştır. Özellikle II. Dünya Savaşı'nın hemen ertesinde ABD'nin dünya sahnesinde politikalarını ifa etmek amacıyla kamuoyunun desteğini elde etmek için sıklıkla başvurduğu ulusal güvenlik doktrini Soğuk Savaş döneminin hâkim güvenlik anlayışının da temelini oluşturmuştur. Bloklar arasında Soğuk Savaşın tedirginliğinin had safhalara eriştiği evrelerde böylelikle devletler ulusal çıkar nosyonu edasıyla dâhilîden ve hariciden gelecek tehlikelere karşı acil durumlarda güvenliklerini sağlamak için önlemlerini alma durumuna gelmişlerdir. Bu sebeple, ulus devlet nosyonu etrafında ulusal güvenlik mottosu şeklinde algılanan Soğuk Savaş dönemi güvenlik anlayışı askeri

güç ile doğru orantılı düşünülmüştür. Yani herhangi bir sorun askeri güç unsurlarını barındırıyorsa güvenliğin kapsamına dâhil olmuştur (Baldwin, 2007: 10-12).

Uluslararası ortamın muayyen ittifaklar sistemine dayanan iki kutupluluk düzeninde taraflar her daim güvenliklerini daha da güçlendirme güdüsüne kapılmıştır. Bu durumda Soğuk Savaş döneminin güvenlik bağlamında en büyük sorunsalını oluşturan nükleer caydırıcılık gibi askeri araçların güvenlik kaygısında en üst sıralarda yer almasına neden olmuştur. Daha öz bir şekilde ifade edilirse, Soğuk Savaş döneminin Uluslararası İlişkiler tartışmalarında merkezi konumda kendine yer edinen güvenlik kavramının tartışmasız olarak temel nesnesi devlet olmuş ve devletin güvenliğinin sağlanması da askeri araçları barındıran askeri güç unsurunun niceliği ve niteliği olmuştur (Buzan, 2013: 83-88). Dolayısıyla bu durum da, geleneksel güvenlik paradigmasının algı ve araçlar bağlamında en katı yaşandığı dönemi temsil etmektedir.

Soğuk Savaşın bitimi ile birlikte diğer sosyal bilimlerde olduğu gibi genelde Uluslararası İlişkiler disiplininde özelde ise güvenlik yaklaşımlarında ve algılamalarında belirgin bir değişim yaşanmıştır. Bununla birlikte güvenlik anlayışında yaşanan dönüşüm ve değişimler aynı zamanda güvenlikle doğrudan ilintili olan tehdit, risk ve tehlike durumlarının da farklı boyutlarda değerlendirilmesine ortam hazırlamıştır. Uluslararası sistemin tek kutupluluğa evrilmesi uluslararası alanda siyaset yapma biçimlerinde farklı aktörlerin de sahne almasına zemin hazırladığından sistemde farklı ve yeni denge faktörlerinin etkili olması kaçınılmaz olmuştur. Yeni bir ortamda kurucu aktör konumundaki devlet dışı aktörlerin ön plana çıkmasıyla beraber güvenlik yaklaşımlarında da yeni ve alternatif kuramlar ve yaklaşımlar ileri sürülmüştür. Özellikle Kopenhag Okulu'nun öncülüğünde güvenliği askeri, siyasal, toplumsal, çevre ve sosyal sektörleri ihtiva eden anlayışla yeniden ele alan okul güvenliğe yönelen tehditleri de çeşitlendirmiştir (Buzan, 1983; Buzan, Waver ve Wilde, 1998).

Hâlihazırda güvenliği devlet merkezli ele alan okul bununla birlikte devlete yönelecek tehditlerin salt askeri kaynaklı olmaktan öte farklı boyutlardan da hissedilebileceğini ileri sürmüştür. Çünkü Sovyetlerin dağılımına müteakip donmuş çatışma alanlarında patlak veren etnik ve dini temelli çatışmalar ve siyasi ve

ekonomik sıkıntılar hasebiyle baş gösteren karmaşıklıklar hem uluslararası sistemin hem de bireylerin güvenliğini tartışmalarını ön plana çıkarmıştır. Önce devlete yönelik tehditlerin çeşitlendiği vurgusu yapılarak yenilenmeye çalışılan güvenlik anlayışına daha sonra devlet ötesi birey, çevre, toplum ve ekonomi gibi alt birimlerin güvenliğini çalışmalarının odak noktası haline getiren alternatif güvenlik yaklaşımları eklemlenmiştir (Buzan, 1983; Buzan, Waver ve Wilde, 1998).

Bundan böyle salt devlet merkezli ve askeri terimlerle ele alınan geleneksel güvenlik tanımlamaları ve pratikleri yeni dönemin uluslararası siyasetine yön veren dinamiklerine ve yapısına cevaz vermemekteydi. Uluslararası siyasetin değişen mantığı güvenlik siyasetinin de mantığı değiştirdiğinden yapılan analizler aktör ve düzey bağlamında devletten ziyade bireylerin güvenliğinin ön planda tutulması üzerine olmuştur. Devletin güvenliğinden öte yeni dönemde merkeze yerleştirilen güvenlik objesi artık insan olmalıydı. İşte Soğuk Savaş döneminin ertesinde güvenliğin tüm boyutlarıyla yeniden ele alınmaya başlanması gerektiğini öne süren yaklaşımları aracılığıyla Uluslararası ilişkiler disiplinin temel konularından olan güvenlik, kapsam olarak genişlerken boyut olarak da derinleşmiştir.

Tarihsel süreklilik içerisinde güvenliği anlam ve içerik boyutlarında dönüşümüne ivme kazandıran en önemli temel dinamiklerden biri de küreselleşme paradigmasıdır. Anthony Giddens'ın öz ifadesiyle küreselleşmeye atıfta bulunmayan hiçbir siyasal konuşmanın tam olarak anlaşılamayacağını dile getirmiştir (Giddens, 2014: 41). Pratikte olduğu kadar teorik minvalde de sosyal bilimlerin neredeyse tüm fenomenlerini etkileyen ve farklı yaklaşımların gün yüzüne çıkmasını hızlandıran küreselleşme mottosu (Keyman, 2014: 337) güvenliğe dair yaklaşımların da yeniden kurgulanmasına vesile olmuştur.

Siyasi erk konumundaki devletlerin kontrolü dışında bilgi ve iletişim teknolojilerinin uluslararası ortamda bilgi akışkanlığına fırsat tanıması ulus devletlerin ülke içi ve dışındaki güç konumlarına ve yapılarına zarar verebilmektedir. Soğuk Savaş sonrası dönemde küreselleşmenin siyasi, ekonomik ve teknolojik boyutlarından neşet eden uluslararası göç dalgaları, organize suçlar, nükleer ve kimyasal silahların yayılımı, siber saldırılar yeni yüzyılın karşılaştığı güncel ve çözümlenemeyen güvenlik tehditleri olarak göze çarpmaktadır (Held ve McGrew,

2008). Bununla birlikte küreselleşme olgusu devletlerin karşısına asimetrik güç elde edebilen ve dolayısıyla küresel ölçekte örgütlenebilen birimlerin ortaya çıkmasını ve bununla ilintili olarak da devletlerin güvenliğine yönelik artan yeni tehditlerle baş edebilmenin yöntemini ve araçlarını da dönüşüme uğratmıştır. Çünkü geleneksel güvenlik paradigmasında düşmanın belli tehditlerin kimden, nasıl ve ne olduğunun belirgin olduğu Soğuk Savaş döneminde güvenliğin araçları da salt askeri olarak kabul görmüştür. Ancak 1990'lar sonrasında devletlerin güvenlik algısına dâhil olan sosyal, siyasal, ekonomik ve çevresel faktörlerin etkisiyle güvenliği sağlamada askeri araçlardan çok müşterek hareket etme güdüsüyle kurumlar aracılığıyla ortak hareket ederek tehditleri savuşturma amaç edinilmiştir. İşte, tarihsel süreç içerisinde Soğuk Savaşın bitimiyle birlikte yaşanan bu kırılma özellikle İkinci Dünya Savaşı sonrası ortodoksi bir anlayışa ve algıya bürünen geleneksel güvenlik paradigmasının boyutları, algılamaları, içerikleri ve pratikleri ile aşınıma uğratmış ve güvenliği adeta yeniden tanımlama noktasına getirmiştir.

Elbette tarihe bağıtlı olarak değişkenlik gösteren güvenlik kavramını sınırlandırmak manasız ve kahır ekseriyette sonuç üretmeyecek eylem olacaktır. Çünkü kavram değişkenlik arz edebilen devletlerarası sistemin ve sistemi oluşturan aktörlerin türüne göre amaç ve araç bakımından da semantik genişlemeler yaşamıştır ve yaşamaktadır. Ancak tarihsel süreç içerinde siyasal olduğu kadar sosyal bir kavram da olan güvenlik, parçası olduğu değerleri yansıttığından değerden arındırılamamıştır ve dolayısıyla da özünü koruduğu görülmektedir. Dolayısıyla uluslararası ilişkilerde siyaset yapma biçimine ilişkin kuramsal ve kavramsal yaklaşımlar ileri süren farklı teorilerin güvenlik fenomenine dair temellendirmelerini incelemek önem arz etmektedir.

1.3. Ortodoks Güvenlik Paradigmasının Kuramsal Çerçevesi: Uluslararası İlişkiler Teorilerinde Güvenlik Fenomeni

Liberalizm yaklaşımı güvenliğin referans nesnesi olarak devletle beraber insanı da gördüğünden devletin siyasal formasyonunu da birey öncelikli devlet-güvenlik ilişkisi sarkacında değerlendirmiştir. *State of nature* yani doğa durumunda insanların düzen sağlayıcı bir örgütlenmeden yoksun olmalarından dolayı oluşan güvensizlik ortamı, onları toplumsallaşmaya ve kendi aralarında oydaşarak kurdukları devletin

mevcudiyetine kanalize etmiştir. Bu nokta da, toplumun akideye dayanarak var ettiği yapay devlet, birey-devlet-güvenlik sarkacında bireylerin güvenliğini sağlamakla yükümlüdür (Locke, 2012: 19).

John Locke'un toplumsal sözleşmesini isnat ettiği ve de analiz düzeyi olarak ele aldığı birey odaklı güvenlik yaklaşımını özgürlük-güvenlik dengesinde devlet-toplum üzerinden yeniden analize tabi tutan Kant da, cumhuriyetçi liberalizm öğretisi aracılığıyla hem toplumu hem de bir nevi devletlerarası sistemi güvenliğin nesnesi konumuna yerleştirir (Burchill, 2013: 82-101, Navari, 2008: 30-34). Ona göre, küresel bazda kalıcı barış (perpetual peace) ve bununla ilintili olarak da güvenlik ancak ve ancak cumhuriyetçi liberal ilkelerin benimsenmesi vesilesi ile olacaktır. Kant, kalıcı barışın ve güvenliğin cumhuriyetçi liberalizmin amentüsü olan demokrasi ilkelerini özümsemiş demokratik rejimlerin karşılıklı ilişkilerinde ifa edecekleri barışçıl ve işbirliğine dayalı politikalar aracılığıyla gerçekleşebileceğini ileri sürmüştür. Bununla ilişkili olarak da Kant, demokratik rejim anlayışının uluslararası düzenin de huzurlu olmasını beraberinde getireceğini ve savaşlar ve anlaşmazlıkların yerini kalıcı istikrar ortamının ikame edilebileceğini salık vermiştir (Navari, 2008: 30-34). Yine, Kant devletlerin ve devletlerarası sistemin güvenliğinin tesis edilmesinde önemli bir etmen olarak karşılıklı bağımlılığa bina edilen serbest ekonomik ilişkileri görmüştür. Çünkü devletler çıkarları gereği ekonomik kazançlarını maksimum düzeyde tutmak istiyorlarsa devletlerarası sistemde barışın da inşa edilmesini elzem görmeleri gerekmektedir (Shimko, 2013: 86-90). Daha sonra ekonomik liberalizm *douce commerce* olarak da lanse edilecek Kant'ın bu görüşleri küresel güvenlik açısından Doyle'nin demokratik barış teorisinde kuramsallaşacaktır. Uluslararası sisteme barışa dayalı düzen, istikrar ve karşılıklı iş birliği imkânı takdim eden demokratik barış teorisine demokrasi ilkelerini benimseyen ülkelerin birbirleri ile savaşma ihtimalleri yok denecek kadar azdır. Bahsi geçen teorik anlayışta uluslararası sistemi belki de çatışma durumuna sokacak problemler güvenlik sorunsalından ziyade diplomasinin araçları olan müzakereler ve karşılıklı ilişkiye dayanan görüşmeler neticesinde ortak noktada çözümü kolaylaştıracaktır.Demokrasiye dayalı liberal ekonomik ilkelerin benimsenmesi ve bu ilkelerin liberal kurumlar aracılığıyla yayılması küresel bağlamda demokratik

sistemlerin kurulmasını tahkim edecek ve insan haklarının ve sivil toplum kuruluşlarının da inşa edilmesini hızlandıracaktır. Bu nokta da, liberalizmde/idealizmde güvenliğin ve bununla ilintili olarak da barışın sağlanması uluslararası hukuk normları ve uluslararası örgütlerin inşa edeceği kurumlar aracılığıyla sürdürülebilir kılınacaktır (Zacher ve Matthew, 1995: 114-115). Genel çerçevede, klasik güvenlik paradigmasının liberalizmdeki yansıması güvenliğin savaş halinin olmaması üzerine inşası üzerine olmuştur. Dolayısıyla da, savaş ve çatışmaları sonlandırmaya yönelik yaklaşımlar ileri sürülmüş ve bununla ilişkili olarak da devletlerin güvenliğinin uluslararası sistemin güvenliği ile beraber düşünülmesi gerektiği savı ortaya atılmıştır.

Güvenliğin tarihsel gelişim seyri incelendiğinde bir alt disiplin olarak gelişme bulmasına muazzam derecede katkı yapan geleneksel disiplin anlayışı realizmdir. Uluslararası sistemde mevcut anarşik yapıda devletlerin iç politikalarından farklılık arz etmesinin önemli olmadığını ileri süren realist teori dış politikaya vurgu yaparak devletlerin her ne olursa olsun esas amaçlarının güçlerini artırmak ve bu paralelde de güvenliklerini sağlamak olduğunu ileri sürer. Bu sebeple realizm devletlerin iç ve dış siyaset yapma biçimlerinin farklı olduğunu ve bundan dolayı güvenliğinde bizatihi kuramsal çerçevesini tarihsel süreç içerisinde revize etmesi gerektiğini iddia ederek kavramın gelişimine katkıda bulunmuştur (Tanrısever; 2014: 109). Realist teorinin klasik güvenlik paradigmasını kavramsallaştırmada bir diğer argümanı da devletin neden referans aktörü olarak kabul görülmesi gerektiğidir. Özellikle Eleştirel Teorilerin güvenlik yaklaşımlarında vurguladıkları insan güvenliği odaklı referans noktasına karşılık realistler devletlerin güvenliklerinin sağlanması ile bireylerin güvenliğinin sağlanmasının eşlenik olduğunu ileri sürmüşlerdir. Çünkü bütünsel bir yapı arz eden devletlerin içinde bireylerden meydana gelen toplulukların da aynı şekilde çıkarlara haiz olacaklardır ve bu noktadan hareketle tümevarımcı yöntemle bireylerin fiziksel güvenliklerinin muhafazası ve devamının da doğal bir sonucu olacaktır (Tanrısever, 2014).

Uluslararası ortamda aynı tarzda devam eden bir güvenlik ortamının husul etmeyeceğini dile getiren realist teori, bu iddiasını da devletin yapısına dair yapmış olduğu antropomorfik temellendirmelerine istinat ettirmiştir. Realistlere göre

insanoğlu karşılıklı olarak etkileşim ve iletişime dayanan toplumsal örgütlenme biçimlerinin bir organı olarak temayüz etmiş bir varlıktır (Morgenthau, 1974: 9-11, Niebuhr, 2013: 83). Anarşik ortamdan zuhur edecek olan kaotik ortam uluslararası sistemde bir güvensizlik atmosferi yaratacaktır. Bu güvensizlik ortamında da devletler güvenliklerini ancak güç maksimizasyonu aracılığı ile rölatif de olsa sağlayabileceklerdir. Metodolojik olarak soyutlamacı bir anlayıştan imtina edip bilimsel veriler ve de pozitivist yöntemleri benimseyen realist teori bu ilkesinden hareketle tarihin siyaset felsefesinden yararlanarak güvensizlik durumunun verili olduğunu, bu nedenlerle de mutlak bir güvenliğin sağlanamayacağını ileri sürer.

Devleti belirli toprak parçası üzerinde konumlanmış ve münhasır sınırlarla birlikte bütüncül özelliğe haiz verili siyasal formasyon olarak kabul eden realist teori bu bağlamda devletlerin güvenliğinin harici kaynaklı düşmanlara karşı ulusal değerleri koruyarak elde edileceğinin altını çizer. Bir başka anlatımla da, realist teori güvenliğe dair temel yaklaşımlarda sıkça sorulan kimin güvenliğine cevap olarak devletin güvenliği, neyi, kime karşı koruma sorusuna da; ulusal çıkarlar bütününü ve değerlerini harici düşmanlardan neşet eden tehlikelere karşı koruma olarak cevaplamıştır. Devlet dışındaki aktörlere uluslararası siyasetin her katmanında olduğu gibi güvenlik anlayışında da yer vermeyen realist teori bu temellendirmelerini de devletlerin hâlihazırda bütüncül bir yapı arz ettiğine isnat ettirmiş ve buradan da sistemin yegâne biriminin ulus devletler olduğunu vurgulamıştır (Mearsheimer, 2002: 23-33).

Yine bu ulus devletler, anarşik sistemin mevcudiyetinden müteşekkil çatışmaya ve rekabete dayalı ortamda yönetme salahiyetini ellerinde bulunduran karar alıcıların bekalarını idame ettirme saikiyle politika ifa etme sürecinde doğal olarak rasyonel davranırlar. Anarşik düzenden kaynaklı arz edecek olan bu rasyonel düşünme özelliği akabinde bekanın sağlanmasında güç metaforunun sistematik bir hal almasına sebebiyet verecektir. Müşahede edildiği üzere realist teori uluslararası ilişkileri ve bu ilişkileri etkileyen ve tetikleyen etmenleri ve pratikleri devlet temelli okumuştur. Güvenliğe dair devlet merkezli temellendirmelerini de bu çerçevede askeri kaynaklı çözüm araçları ile sağlanabileceğini dile getirmiştir. Çünkü realizmin amentüsü bilardo topu modelinden hareketle devletlerarası etkileşimler veya

mücadeleler devletlerin nihai kaygılarının güç ve hayatta kalma olduğu varsayımının yansıması biçiminde kahır ekseriyette askeri ve güvenlik konularıyla ilintilidir (Dougherty ve Pfaltzgraff 58-60).

Neorealizm de, klasik realizmden tevarüs eden güç, anarşi, çıkar, çatışma gibi uluslararası düzeni açıklayan önermeler ile hemfikir olmakla beraber sistemi açıklayan farklı nitelikte yapısal unsurların olduğunu ve bu unsurların ön planda tutulması gerektiğini ileri sürmüştür. Bir başka ifade ile neorealizm uluslararası ilişkilerin yapısal bütünlük arz ettiğini ileri sürmüştür. Uluslararası ilişkileri, insan doğası üzerinden okumasını ve devletlerin güç peşinde koşma siyasetinin ve mücadelesinin bir alanı olarak görmesini indirgemeci bir yaklaşım olarak gören Waltz'a göre, devletlerin davranışlarının belirlenmesine müessir olan unsur sistemin anarşik yapısından kaynaklı kendini koruma gayesi bir başka deyişle güvenliktir (Bostanoğlu, 2008: 100).

Mevcut uluslararası sistemde cisimleşen yasa koyucudan ya da herhangi bir otoriteden yoksun ortam çatışma ve rekabet ortamının hüküm sürdüğü bir güvensizlik atmosferini beraberinde getirecektir. Bu noktadan hareketle uluslararası sistemin başat birim konumundaki devletlerde anarşik yapının zorunlu kıldığı başkasına muhtaç olmama/kendi başına yapabilme düsturuyla benzer davranışlar sergileyeceğinden sistemde güçler dengesi sarmalı yaşanacak ve mutlak güvenlik söz konusu olmayacaktır. Yani, Waltz'un öncülüğünde neorealist teori uluslararası sistemin şekillenmesinde düzenleyici ilke olarak anarşiyi görür. Uluslararası sistemin belirleyici aktörü olarak sadece devleti görmeyen, bununla birlikte ekonomik, kültür, sosyal ve politik birimlerinde sistemi etkilediğini düşünen Waltz'a göre, devletler anarşik ortamda çıkarları doğrultusunda güvenliklerini sağlamak için bizatihi sahip oldukları araçlarla kendilerini savunmak zorundadırlar (Waltz, 2009). Buradan hareketle Baldwin'in de ifade ettiği üzere neorealizm güvenliği devletlerin nihai kaygısı olarak görüp onu kuramsallaştıran esas teoridir (Baldwin, 2007: 63).

Ancak yine de, Waltz devletlerin güç kapasitelerinin farklılığının sistem içerisinde de farklılıklara sebebiyet vereceğini ve bu güç kapasite farklılığının da en nihayetinde devletlerin güç dengeleme politikalarına başvurusunu teşvik edeceğini iddia etmiştir. Her ne kadar bütün devletler eşit düzlemde kabul edilse de,

uygulamada ve sahada eşit değillerdir. Bu nedenle, sistemde beliren yapının bütün birimler tarafından değil de, güçlü ve büyük aktör konumundaki birimler tarafından biçimlendirildiğini belirten Waltz, uluslararası sistemin başat kuramı olarak gördüğü güç dengesi (Waltz, 1979: 80) siyasetinin en iyi örneği olarak çift kutupluluğu temsil eden Soğuk Savaş ortamını göstermiştir. Çünkü genel bir eşitlik ve bütün devletlerin hegemonik tutkularını törpüleme temayülü gösteren ve hiçbir devletin diğerlerine üstünlük sağlayamadığı güç dengesi kuran bu dönem kısmen de olsa güvenliğin ve istikrarın temin edilmesine vesile olmuştur.

Yine bir başka neorealist anlayışa sahip olan Mearsheimer de, ABD ve S.S.C.B. gibi gücü elinde bulunduran ülkelerin liderliğindeki çift kutupluluğa dayanan uluslararası sistemi barışın ve de istikrarın bir başka tezahürü olan güvenliğin temini olarak görmüştür. Öyle ki, Mearsheimer, Soğuk Savaş döneminden sonra kimliğe dayalı etnik çatışmaların tırmanmasının güvensizliğe vesile olacağını ve bu noktadan hareketle de uluslararası ilişkilerin geleceğinde tarihsel süreç içerisinde yaşanan güç dengesi politikalarının yeniden hortlayacağını öngörmüştür (Mearsheimer, 1998). Çünkü Mearsheimer'e göre, uluslararası sistemdeki mevcut anarşik düzen devletlerin sadece kendi güçlerine güvenebileceğini ve bundan dolayıdır ki, kendi güvenliklerini sağlamanın yolunun da güçlerini artırmaktan geçtiğini ifade etmiştir (Mearsheimer, 2001: 33-40). Realistlerle benzer şekilde neorealistler de savaş halini devletlerarası ilişkilerin doğasında var olan bir olgu olarak görürler ve bu nedenle de savaşlardan kaynaklı çatışma ve şiddet ortamını da güvenlik anlayışlarının odak noktasına yerleştirirler. Uluslararası sistemde herhangi bir kural koyucu otoritenin olmaması oluşacak çatışma ve rekabetsizlik ortamında aynı zamanda kimin ne derecede ve nasıl kuvvet, güç ya da zora dayalı eylemler geliştireceğinin de muğlâk kalmasını doğurduğundan bizatihi anarşik yapının kendisi güvenliğe yönelik tehdittir.

Müşahede edileceği üzere, neorealist teori güvenliği uluslararası sistemde anarşik yapının düzenleyici ilkesi doğrultusunda devletlerin nihai amacı olarak görerek kuramsallaştırmıştır. Waltz'a göre anarşik ortamda yegâne gaye güvenliktir ve devamlılık muhafaza edilirse devletler sorumluluklarını yerine getirmiş olup çıkarları doğrultusunda kazançlı ve güçlü olabilirler. Bu kuramsallaştırmanın da ana

belirleyicisi anarşik ortam olmuştur. Bir nevi anarşi ile güvenlik arasında doğrusal bir orantı kuran neorealist teori bu nokta da güç unsuruna da bir araç olarak yaklaşmıştır (Waltz, 1988: 98-130). Çünkü güvenliğin sağlanmasında paye güç kavramına verilmiştir. Sistemde esas teşkil eden gayesi hayatta kalma olan devletler haiz oldukları bütün imkân ve kapasitelerinin tezahürü güç araçları sayesinde uluslararası politika da kendilerine yer edinip egemenliklerini ve güvenliklerini idame ettireceklerdir. İşte bu noktada da, denge faktörü devreye girecek ve uluslararası sistemde rakip devletlere karşı kendi güç kapasitesini optimum seviyede tutan ve fırsatları kovalayan devlet mevcut anarşik ortamda yasa belirleme salahiyetini elde etmeye, güç dağılımını belirleme ve de etki alanını tahkim kılmayı arzulayacaktır (Waltz, 1980: 21-37). Bu durumda da gücü elinde bulundurup maksimize etmeye çalışacak olan devletin karşısında da gücü dengeleme saikiyle diğer devletlerin farklı arayışlara girmesinin kaçınılmaz olduğunu dile getiren Waltz, sistemin yapısal unsurundan dolayı devletler gücün dengelenmesi için girişimlerde bulunacaklarını belirtir (Waltz, 1979). Waltz'a göre her daim devletler saldırgan ve çatışmacı bir tutum sergilemese de güvenliklerini garanti etmek zorunda oldukları için bu durumda ayrıca diğer devletlerin gücü ile kendi güçlerini hesap ederek sürekli dengeleme peşinde olurlar (Brown ve Ainley, 2013: 57). Bu da son kertede, aktörlerin bizatihi kendi pozisyonları ya da kazançları ile değil rakiplerinin ne kadar kazandığıyla ilgili durumu ortaya çıkarmaktadır (Grieco, 1988: 499).

Neorealizmin ortodoks güvenlik paradigmasına yönelik temel tehdit olarak gördüğü diğer en büyük korku savaş gerçeğidir. Uluslararası ilişkilerin doğasında savaşın bulunabileceğini dile getiren neorealist teoriye göre esas sorun teşkil eden unsur savaşın daim olmasından ziyade anarşik ortamın getirisi olan savaş çıkma olasılığı ve de kimin ne zaman, ne ölçüde ve ne tür bir tehdit oluşturacağının kestirilememesi durumudur (Waltz, 1979). Çünkü neorealizm uluslararası sistemde statükocu ve revizyonist olmak üzere iki tür devlet biçiminin var olduğunu iddia eder. Bu iki tür tipolojiden hangi devletin nasıl bir biçime büründüğünün belirsiz olduğunu ileri süren neorealist teori devletlerin niyetlerinin de doğal olarak kestirilemeyeceğini belirtir. Bu koşulda da devletler kapasiteleri doğrultusunda ya

güç artırımına giderek ya da ittifaklar dâhilinde güçlü bir devlete sırtını yaslayarak ya da peşine takılarak (bandwagoning) güvenliğini sağlayabilir (Waltz, 1979).

En nihayetinde, realizm ve neorelizmin güvenliğe dair temel dayanak noktaları uluslararası sistemin yapısal çerçevesinin belirlemiş olduğu sınırlılıklar hasebiyle egemen devletlerin hiçbiri mutlak olarak güvenliği sağlayamayacakları üzerinedir. Sistemin bu karakteristik özelliğinden dolayı da, devletlerin temel kaygısı ve amacı da güvenlik olacaktır. Neorealizme göre sistemin bu yapısal özelliği de devletlerin politik ajandalarında ulusal güvenliğe en üst seviye de tutmalarına yol açmaktadır (Buzan, 1991: 22). Temel güvenlik kaygısı da iç politikadan ziyade dış politikaya yöneliktir, çünkü uluslararası sistemin anarşik yapısı gereği dış politika da göreceli güvenlikten söz edilebilir, mutlak güvenlik elde edilemez (Waltz, 1979). Dolayısıyla devletlerin hayatta kalmalarını yani güvenliklerini idame ettirmelerini garanti altına alacak herhangi bir kurum yoktur. Bu nedenle de güvenliği elde etmenin yegâne yolu olarak da devletlerin sistemde kapasitelerini artırarak güç maksimizasyonu ilkesini benimsemeleri gerektiği ön plana çıkmaktadır. Bununla ilintili olarak, uluslararası sistemin başat aktörü olan devletlerin güvenliğin sağlanmasında araç olarak gördükleri güç artırımının da temel aracı askeri kapasitenin artırımıdır. Liberal teoride vücut bulan güvenliğin uluslararası arenada işbirliğinin tahkim edilmesi aracılığıyla azaltılabileceği anlayışını reddeden realist ve neorealist teori yine bu bağlamda kolektif güvenliği sağlamak için inşa edilen Milletler Cemiyeti ve BM gibi örgütlerin de anarşinin etkisinin kırılmasında rol oynayamayacağını dile getirmiştir. Çünkü göreceli kazanç mantığı ile hareket eden devletler bizatihi kendi kazançlarının yerine sistemdeki diğer devletlerin ne kadar kazandığına odaklandıklarından güvenlik temelli işbirliğine ve oydaşmaya dayalı kolektif anlayışların kalıcı olması beklenemez (Waltz, 1986).

Güvenlik kavramı ile güçlü bir ilişkisi olan bir diğer sosyal bilim inceleme konusu da Barış Çalışmaları adlı alt disiplin yaklaşımıdır. İki kutuplu Soğuk Savaş döneminin henüz başladığı yıllarda özellikle ABD ve Kuzey Avrupa'da devletlerarasındaki politika da baskın konumda olan realist perspektifin devlet odaklı yorumlamalarına karşı stratejik ve ulusal güvenlik çalışmaları dâhilinde yer alarak alternatif söylemler ve kavramlar geliştirmeye çalışmıştır (Brauch, 2012: 185). İkinci

aşamada ise kahır ekseriyette yıkıcı savaşlara sebep olan silahlanma yarışlarının dünya politikasında yaratacağı tahribatlara odaklanmıştır (Terrıf, vd., 1999: 69-70).

Esas olarak Barış Araştırmalarını, Barış Çalışmaları konseptine konumlandıran kişi de John Galtung olmuştur. Galtung, Barış Çalışmalarının muhteviyatına eşitsizlik adaletsizlik, açlık küresel bazda sosyo-ekonomik sorunları dâhil ederek aslında şiddetin yapısal nedenlerine değinerek bir nevi şiddet unsuruna sosyolojik zemin oluşturmuştur (Vorobej, 2008: 84-98, Wusten, 1996: 405). Kuramsallaştırdığı bu sosyolojik zemin azgelişmiş ülkelerdeki yapısal sorunlar sebebiyle güvensizlik ortamının da önemli sebepleri olarak görülmüştür (Gleditsch, 1993: 445-449). Bununda en iyi örneklerini Soğuk Savaş dönemindeki gelişmeler ışığında yaşanan güvenlik ve barış arasındaki doğru orantı ilişkisinin kurulması ile göstermiştir. Öyle ki, Soğuk Savaş döneminin yumuşama evresinde Barış Çalışmaları da ilgi alanını daha çok askeri konular dışındaki sorunsallar ve çözümlemelerle barış ve bununla ilintili olarak güvenlik konularına kaydırmıştır (Buzan ve Hensen, 2009: 53-55). Bahsi geçen değer yüklü normatif olgular incelendiğinde hâlihazırda Barış Çalışmalarının güvenliğin nesnesi daha çok insan ve doğal olarak da toplum olmuştur. Bu da geleneksel teorilerin güvenliğe yönelik temellendirmeleriyle daha da perçinleşen ortodoks güvenlik paradigmasına yönelik ilk ciddi meydan okumaların geldiği grup olmalarını sağlamıştır.

Galtung'un tanımladığı yapısal şiddet nosyonuna göre, toplumsal düzenden dolayı insanların kapasiteleri doğrultusunda elde edemedikleri fırsatlarda bir şiddet biçimidir. Ayrıca, Soğuk Savaşın bitimine müteakip tebarüz eden kimliğe dayalı çatışmaların yol açtığı insani, toplumsal, çevre ve devlet altı örgütlenmelerden kaynaklı tehditler gibi unsurlar Barış Çalışmaları'nın kapsamına keskin bir şekilde dâhil olan sorunsallar olarak göze çarpmıştır. Galtung'un negatif ve pozitif barış kuramsallaştırma yöntemi sonrasında Barış Çalışmaları'nın güvenliğe dair düşünceleri de barış üzerinden olmuştur (Buzan ve Hensen, 2009: 102). Çünkü barışçıl araçlarla elde edilecek olan barış aynı zamanda güvenliğin de sağlanmasında önemli katkı verecektir (Lawler, 2008: 80). Hedeflenen barış durumu da savaşın bütün hatlarıyla ortadan kaldırılması olarak görülmemelidir, bunun yanında Galtung'un pozitif barış diye adlandırdığı ve görünmeyen normatif değerleri ihtiva

eden sosyal sorunlarında giderilip insanlık toplumunun bütünleşme sürecinin (integration of humonsociety) tamamlanması ile oluşacak evredir (Galtung, 1996: 2). Bunun için, Barış Çalışmaları yaklaşımı barış kavramı üzerinden aslında güvenliğin nesnesi olarak bireyleri, toplumsal grupları ve hatta devletlerarası sistemi dahi analize tabi tutup soruna yerel bazla birlikte, bölgesel ve küresel perspektiften gözlemlemektedir (Lawler, 2008). Ve yine bu sebepledir ki, toplumsal realitelere bigâne kalıp çatışma, savaş ve güvensizlik durumunu yekpare devletlerarası askeri mücadelelerin cirit attığı bir alan olarak gören realistleri eleştirip insanoğlunun sosyalleşerek küresel toplum hassasiyeti oluşturacağına inanmaktadır (Lawler, 2008: 82).

Bu hususlar ışığında müşahede edildiğinde yapısal şiddet kavramını kuramsallaştırarak bir nevi şiddetin kökenlerine inip sosyolojik bir çehre kazandıran Galtung'un liderliğindeki Barış Çalışmaları barışla paralel olarak gördükleri güvenliği devlet merkezli analiz eden geleneksel güvenlik paradigmalarının çözümlemelerini eleştirmiş ve sosyal olgulardan neşet eden şiddetin kökenlerinin yeteri derecede analize tabi tutulmadığını dile getirmiştir. Barış Çalışmalarının vurgulamak istediği nokta, güvensiz bir uluslararası sistemin ve toplumun oluşmasında ve devam etmesinde en önemli rol oynayan faktör sosyal ve ekonomik boyutların gözden kaçırılmasıdır. Ve barış çalışmaları kendinden önceki realist ve liberal teorilerin argümanlarını bu yüzden eleştirmiş ve güvenliğin temininde barış kavramını da yeniden revize etmiştir. Esasen Barış Çalışmaları yaklaşımı aktör ve içerik olarak devlet merkezli düşünen başat teorilerin güvenliğe dair paradigmatik söylemlerini eleştirerek aşındırmaya yönelik ilk ciddi adımları atmış ve güvenliği kavramsal olarak derinleştirip genişletmek isteyen eleştirel güvenlik yaklaşımlarına da ilham kaynağı olmuştur (Booth, 2007: 68).

Güvenliğin sadece devlet aktörü üzerinden yorumlanıp temininde araç olarak askeri unsurların dikkate alınmasını kavramın dar kalıplara hapsedilmesine neden olduğunu ileri süren Barış Çalışmaları yaklaşımından hareketle kavramın içeriğini revize eden kişi Barry Buzan olmuştur. Geleneksel güvenlik anlayışı paralelinde Buzan da güvenliğin nesnesi olarak devleti görmüştür. Güvenliğin içeriğini askeri, siyasi, toplumsal, ekonomik ve çevresel düzlemde sektörlere ayırarak aynı zamanda

güvenliği içeriksel bağlamda derinleştirmişlerdir (Buzan, 1991). Ancak, gözlerden kaçmaması gereken nokta Buzan'ın tasniflemiş olduğu bu beş sektörleşme alanı da devletlerin menfaatleri etrafında şekillenmiş ve devletleri merkezde ana birim olarak konumlandırmış olmasıdır (Booth, 2007: 162).

Devlet merkezli bir güvenlik analizi çerçevesi ortaya koyan Buzan askeri tehditler dışında yer alan bazı unsurların da devletin güvenliğine yönelebilecek tehditler grubuna girmesi gerektiğini dile getirmiştir. Ona göre, güvenlik kavramsal açıdan derinleştirilmeliydi; çünkü ulus- devletlerin kuruluş kökenine yani fikrine ve ideolojik beslenme damarına yönelen tehditler olacağı gibi, devletlerin vatandaşlarına ve zaruri temel kaynaklarına ve de kurumsal kimliğine ve bütüncül yapısını oluşturan siyasi sistemine yönelik tehditler de olacaktır (Buzan, 1991: 65). İşte bu veçhe de, Buzan da yukarıda bahsi geçen beş güvenlik sektörünü devletin farklı birimlerine yönelecek tehditler kapsamında yorumlamıştır. Askeri güvenliği devletlerin askeri kapasiteleri doğrultusunda şekillenen saldırı ve savunma saikiyle karşılıklı etkileşeme dayanan politik ve stratejik niyetlerin karşı tarafta bıraktığı izlenimlerle açıklayan Buzan, politik güvenliği de, yine devletlerin kurumsal devamlılığı ve var olan hükümet sistematiği ve de bu hükümete yasallık bahşeden siyasal ideolojilerin güvenilirliği ve oturaklılığı muhafaza etmesiyle açıklamıştır.

Bunlara ilaveten, 1973 yılında OPEC petrol krizi ile başlayan siyasi krizlerin, daha sonra fiyatlarda yarattığı yükselmeler, dalgalanmalar ve ABD dolarında sebep olduğu değer kaybı gibi ekonomik sorunların da hem uluslararası güvenliğe hem de devletlerin ekonomik güvenliğine yönelik bir tehdit olduğu gözlemlenmiştir (Sheehan, 2005: 65). Bu noktada, Buzan ekonomik güvenliği devletlerin maddi ve manevi gücünü ve refah seviyesini makbul bir düzlemde muhafaza ederek zaruri kaynaklara, finansmana ve de pazarlara müessir bir şekilde erişebilme olarak nitelendirmiştir. Buzan'a göre tehdide açık bir diğer sektör alanı da toplumsal güvenlik olmuştur. Devletin tüm sosyal ve siyasal bileşenlerinin toplamı olarak gördüğü toplumsal güvenliği de devletlerin bir diğer endişe kaynağı olarak görmesi gerektiğini dile getirmiştir. Son olarak da, sektörleşme bazında Buzan'ın güvenlik ajandasına yerleştirdiği son alan da çevre olmuştur. Ona göre, yine devletin tüm unsurlarını ihtiva eden ekolojik sistem bölgesel ve küresel ölçekte korunmalıdır

(Buzan, 1991). Buzan güvenliğin gündemine dâhil ettiği bu sektörleşme alanlarını birbirinden bağımsız yapılar olarak görmemiş aksine tüm bunların birbirlerine sıkı bir şekilde bağımlı olduğunu dile getirmiştir. Daha sonra Kopenhag Okulu'nun diğer müntesipleri tarafından da benimsenecek olan sektörel tasnifleme alanları Ole Weaver'ın temellerini atacağı güvenlikleştirme yaklaşımında birbirleri ile ilgili ve bağıtlı bir düşünce ve nesneler dizisi görünümü şeklinde arz edecektir. Şöyle ki, bu sektörler dâhilinde güvenliğe dair herhangi bir sorun daha önceden siyasal alana (*nonpoliticized*) dâhil edilmemiş bile olsa karar verici iktidar sahipleri tarafından siyasal alanın (*politicized*) kapsamına dâhil edilip bir tehdit unsuru olarak güvenlikleştirilebilmektedir (Buzan, vd., 1998: 23-24).

Görüldüğü üzere, Buzan devletin farklı unsurlarına yönelen tehditler üzerinden güvenliğe dair analizlerini sunmuştur. Bir başka anlatımla, Soğuk Savaş döneminin sona ermesiyle askeri tehdit unsurlarının giderek arka planda kalmaya başlaması ile birlikte devlete yönelecek farklı tehditlerden bahsederek yine devlet merkezli güvenlik analizleri sunmuştur. Her ne kadar güvenliğin içeriğini ve konularını genişletmiş olsa da, realizmin devlet merkezli yapı düşüncesini benimsemesi onu realistlerle benzer kılmaktadır. Muhtemeldir ki fallen realist olarak da adlandırılması bu sebeptendir (Booth, 1994).

Yine Buzan'ın kılavuzluğu aracılığıyla kurulan ve yeni bir kavramsal çerçeve sunan Kopenhag Okulu temsilcileri güvenlik kavramını salt askeri odaklı perspektiften çıkarıp muhteviyatını genişletmişler ve yeniden tanımlama yoluna gitmişlerdir (Balzacq, 2005: 172). Çünkü Soğuk Savaşın sona ermesi güvenliği genişletmeye ve derinleştirmeye yerindelik ve inanılırlık imkânı tanımıştır. Bu noktadan hareketle Huysmans da güvenliğin salt askeri-siyasi odaklı anlayışından sıyrılmasının ve de özünde kavramın anlaşılmaz bir şekilde tutarsızlıklardan kurtarmaya çalışılmasının Kopenhag Okulu'nun hedeflediği ana motivasyonlar olduğunu dile getirmiştir (Huysman,1998: 480-482). Sovyetlerin dağılımından müteşekkil, çeşitli tehditlerinin gün yüzüne çıkması güvenliğin katı bir askeri anlayışla kavramsallaştırılmasını yüzeysel kılmıştır. Daha önce Soğuk Savaş dönemi sebebiyle gölgelenen farklı seviyede ve çeşitlilikteki tehditler ortaya çıkmıştır. Ve artık uluslararası güvenlik algısı kati bir şekilde Sovyetlerin ve ABD'nin caydırıcılığı

üzerinden yorumlanamayacak ve de büyük güçler arasında olası bir nükleer savaş korkusu üzerinden şekillenmeyecektir. Artık dikkat edilmesi ve vurgulanması gereken güvenlik tehditleri sadece devletlerin birbirlerine karşı algıladığı kaygılardan değil aynı zamanda Soğuk Savaşın bitimine değin bigâne kalınan çevresel, göç ve yerel milliyetçi direnişler gibi farklı alanlardan ve aktörlerden de kaynaklanmaktadır.

Ayrıca Kopenhag Okulu kavramın Westphalian egemen devletler sisteminin getirisi olan batı merkezci okumalara maruz kalmasını da eleştirmiş bu çerçeve de güvenlik kontekstine devlet dışı birimleri de dâhil etmişlerdir. Westphalian mitinin çizmiş olduğu çerçeve de şekillenen ve 20. yüzyıl Batı merkezli perspektiften analiz eden güvenlik okumaları farklı bölgelerin güvenlik sorunlara bigâne kalmıştır (Ayoob, 1995). Özellikle Sovyetlerin dağılımı ile birlikte uluslararası atmosferde cereyan eden etnisiteye ve kimliğe dayalı toplumsal ve siyasal çözülmeler devlet dışı birimlerin/aktörlerin de analize tabi tutulmasını gerekli kılmıştır. Buzan da bu noktadan hareketle Kopenhag Okulu'nun revize etmeye çalıştığı güvenlik anlayışına toplumsal güvenlik kavramını kazandırmıştır. Buzan'ın toplumsal güvenlik yaklaşımına göre ulusal devleti oluşturan önemli sacayaklarından biri olan toplumun kültürünün yani dilinin, geleneklerinin ve kimliğinin muhafazası önem arz etmektedir (Buzan, 1991).

Yeni bir kavramsal çerçeve sunan Kopenhag Okulu içerik ve adlandırma bakımından güvenliğe sektörleşme kavramını kazandırarak literatürü de zenginleştirmiştir. Askeri temelli güvenlik sektörü ile beraber politik, ekonomik, çevresel, toplumsal ve de insani güvenlik sektörlerinin de güvenlik alanında yer bulmasını sağlayan Kopenhag Okulu böylelikle literatürü de genişletmiş ve derinleştirmiştir. Elbette Barry Buzan'ın ifade ettiği üzere, geleneksel güvenlik anlayışı bundan böyle Soğuk Savaş dönemi ertesinde uluslararası sistemin ve konjonktürün geçirmiş olduğu dönüşümler vasıtasıyla ulusal güvenliğe ait dar kalıplara sıkıştırılmış bir anlayıştan sıyrılmalıydı. Çünkü artık Soğuk Savaş döneminin nükleer tehdit kâbusu arka plandaydı. Soğuk Savaşın bitimine yakın tebarüz eden çevresel ve ekonomik meseleler ve 1990 sonrası vuku bulan kimliğe dayalı etnik çatışmalardan kaynaklı tehditler birincil önem arz etmekteydi (Buzan ve vd., 1998: 2).

Uluslararası ilişkiler literatürüne Kopenhag Okulunun güvenlik bağlamında kazandırdığı bir diğer kayda değer kuramsal çerçeve de Ole Waver tarafındankavramsallaştırılan güvenlikleştirme teorisidir. Kopenhag Okulu içinden geleneksel güvenlik anlayışına yönelik eleştiri getiren bir diğer kişi de Ole Weaver olmuştur. Buzan gibi Ole Weaver da askeri tehditler dışında farklı unsurlardan gelecek olan tehditleri ihtiva eden yeni bir güvenlik anlayışı geliştirilmesi gerektiğini dile getirmiştir (Waver 1998: 69-118). Ole Weaver da Buzan'ın devleti gönderge nesnesi olarak görmesini benimseyip özellikle Soğuk Savaş dönemi sonrası gün yüzüne çıkan farklı ve yeni tehdit unsurlarından dolayı güvenlik tehditlerinin genişletilmesi gerektiği görüşünü paylaşmıştır. Kopenhag Okulunun anahtar kavramlarından olan güvenlikleştirme yaklaşımının mimarı olan Weaver, bu kuramında elbette askeri sorunların kahır ekseriyette güvenlik gündemini belirleyeceğini ancak (askeri kaynaklı tehdit dışı tüm tehdit oluşumlarının da gündeme dâhil olmaması gerektiğinin altını çizerek) sadece askeri kaynaklı tehdit dışı unsurlardan da neşet edecek olan geniş ve kapsamlı bir güvenlik ve bununla ilintili olarak tehdit anlayışının benimsenmesi gerektiğini vurgulamıştır (Waver, 2007: 48-86). Bu kapsamlı ve geniş güvenlik tehditlerini de Weaver güvenlikleştirme teorisi aracılığıyla kuramsallaştırmıştır.

Güvenliğin kavram olarak manasının ne olduğu sorusunun modern uluslararası ilişkiler literatüründe ve pratiğinde hala güncelliğini koruduğunu ve bu nedenle de güvenlik çalışmalarının odağında konumlandırıldığını dile getiren Weaver bir tehdidi güvenlik sorunu yapan etmenin gerçekte söz edim (*speech act*) aracılığıyla inşa edildiğini savunmaktadır (Weaver, 2007). Söylem olarak inşa edilen güvenliğin bir nevi telaffuz eylemi ile kurgulandığını dile getiren Kopenhag Okulu temsilcileri bu noktadan hareketle güvenlikleştirme yaklaşımının siyasi bir sürece dayandığını ve tehditlerinde yine bu yaklaşıma göre kurgulandığını dile getirmişlerdir. Örneğin, nasıl bir gemiye isim veriliyor ya da bir şey hakkında iddiaya girilip sözler veriliyorsa söyleyişinde bizatihi kendisiyle harekete geçilmiş olduğunun örneğini veren Weaver, herhangi bir devlet temsilcisinin de herhangi bir konuyu telaffuz ederek o konuyu güvenlik tehdidi olarak özel politika alanına dâhil edip yine o konuyla ilgili her ne gerekiyorsa yapar ve devletin tüm aygıtlarını harekete geçirip

kullanabileceğini iddia eder (Waver, 2007). Bir başka ifade ile bir sorunun somut olarak gözlemlenen ya da hissedilen bir tehdit olup olmadığından ziyade sorunu söz edimi aracılığıyla güvenliğin odağı haline getirmek aynı zamanda o sorunu bir güvenlik problemi haline de getirmektir. Öyle ki, güvenliğin hayatta kalmayla aynı anlama geldiğini ileri süren Waever, bu nedenle söz edimi kuramıyla güvenlikleştirme sürecinin ilk safhasının bir sorunu bir referans nesnesine yönelik tehdit olarak sunulmasıyla başlandığını belirtmektedir.

İkinci aşamada Waever, bir meselenin güvenlik sorunu olması için elitlerin o meseleyi güvenlik sorunu olarak dile getirmesi gerektiğinin altını çizer (Waever, 2007). Daha sonra da, güvenlikleştirme sürecini başlatan elitlerin dile getirdiği varoluşsal tehditlere karşı alınması planlanan tedbirler için meşru zemin oluşturulur. İşte bu nokta da yine Weaver, varlığa yönelik varoluşsal tehditlerin telaffuz edilerek açık bir şekilde kamuoyuna sunulmasının karar verici elitlere güvenlik problemlerinin üstesinden gelinmesi için kuvvet kullanımı başta olmak üzere farklı olağan dışı yetkilerden faydalanmayı haklı gösterebilecekleri imkânın sunulacağını ileri sürmektedir. Weaver, nihai aşamada, tehditlerin varoluşundan ve bu tehditlere yönelik tedbirlerden söz edebilmek için alıcı olan dinleyici kitlenin (audience) de var olması ve de ikna edilmesi gerektiğini ifade eder.

Bununla birlikte, güvenliğe dair ilişkinin yekpare bir özne ya da nesne ile açıklanmasının mümkün olmadığını ileri süren okul, güvenliğe dair bilinmesi gereken pratiğin özneler arasında geliştirildiğidir (Buzan ve vd., 1998: 31,). Okulun bu söyleme dayalı güvenlik unsurlarının özneler arasında inşa edildiği model savı güvenlikleştirme yaklaşımını eleştirel inşacı bir kurguyla temellendirildiğini göstermektedir (Açıkmeşe, 2011: 57-59).

Kopenhag okulunun temel anahtar kuramı olan güvenlikleştirme yaklaşımının meta teorisine bakıldığında uluslararası ilişkiler disiplininin farklı teorilerinden faydalandığı görülmüştür. Tehdit gündemini belirleyen aktörün referans nesnesine yönelik varoluşsal tehditlerin tehlike arz etmesi sonucu tebarüz eden hayatta kalma riskine karşılık tüm acil önlemleri alması gibi güvenlik politikalarının kavramsal ve içeriksel kökenini neorealist kuramın öncüsü Kenneth Waltz'un devletlerin nihai amacının güvenliklerini sağlayarak hayatta kalma stratejisi yaklaşımı

oluşturmaktadır. Nitekim Weaver da güvenlik mefhumunun beka ile alakalı olduğunu ve bu nedenle de varlığa yönelik hedeflenen tehditler koşulunda elzem olan bütün ivedi ve olağanüstü tedbirlerle karar vericiler tarafından beka sağlanması yoluna gidileceğini ileri sürmüştür (Weaver, 2011: 465-480). Güvenlikleştirme yaklaşımının esas vurgusunu teşkil eden söz edimi anlayışı dilbilimsel felsefenin öncüleri Austin ve Derrida'nın kuramlarından faydalanmıştır (Sritzel, 2007: 357-383). Söz edimlerini içeren cümlelerin nesnelliğine, öznelliğine ya da doğrulanabilir olup olmadığına bakılmaksızın sözcüklere dökülen telaffuz etme biçimleri meseleyi siyasal bir olgu haline dönüştürerek gerçeklik yaratır (Stritzel, 2007). Farz-ı mahal, Queen Elizabeth isminin denize sürülen bir gemiye törenlerde verilmesinin söz edim yoluyla takdim edilmesi politik bir eylem bazında bir gerçeklik yaratmadır (Austin, 1962: 5). Yine ABD Başkanı George W. Bush'un Ocak 2002 tarihinde Şer Ekseni olarak nitelendirdiği İran, Irak ve Kuzey Kore'ye yönelik kitle imha silahları geliştirip ABD'yi ve tüm dünya toplumunu tehdit ettiği söylemi söz edimselliği yoluyla inşa edilen güvenlikleştirme politikasına en iyi örneklerdendir (Açıkmeşe,2014: 252).

Müşahede edildiği üzere, dilbilimsel felsefe kuramı vasıtasıyla bir konuyu politize etmek için söz edimi şeklinde ortaya çıkan güvenlikleştirme kuramı aynı zamanda varoluşsal tehditler ve bu tehditleri savuşturarak vurgusu yapılan güvenlik nesnesinin bekasını sağlamak için tüm önlemlerin alınması gerektiği savı kuramın farklı anlayışlardan faydalandığını ortaya koymaktadır. Bir başka deyişle, Kopenhag Okulu güvenlikleştirme kuramının teorik altyapısını dilbilimsel teoriler aracılığıyla kurgularken, bir diğer taraftan da, siyaset teorisi ile özneler aracılığıyla dayanan sosyal inşacılık anlayışlarından faydalanarak nev-i şahsına münhasır bir güvenlik söz edimi anlayışını geliştirmiştir (Açıkmeşe, 2011).

Dünya siyasetini açıklama noktasında uluslararası ilişkilere dair bir diğer önemli analiz yaklaşımı da eleştirel teoriden gelmiştir. Marksizm'in nüvesini oluşturan tarihsel materyalizm ilkesi üzerine kendine özgü temellendirmelerini inşa eden eleştirel teori geleneksel teorilerin adeta genel yasası olarak kabul edilen devlet merkezli epistemolojik ve de ontolojik savlarına karşı çıkmıştır. Bu hususlar çerçevesinde sosyal bilimlerin bir alt dalı olan güvenliğe dair yeni yaklaşımlarda

eleştirel teori'nin kuramları kahır ekseriyette geleneksel güvenlik paradigmasının temellendirmelerinin reddi ile beslenmiştir.

Bu bağlamda geleneksel güvenlik anlayışının tamamen zıttı şeklinde Eleştirel Güvenlik çalışmaları ve bu çalışmaların şemsiyesi altında toplanan ve daha sonra farklı kollara ayrılan güvenlik yaklaşımlarının güvenliğin nesnesinin kim olduğu sorusuna eserleri aracılığıyla vermiş oldukları net cevap daima birey olmuştur (Bilgin, 2010). Devlet dışında yer alan tüm birimlerin tarihsel süreç içerisinde ve realitesinde her daim baskıya, eşitsizliğe ve güvensizliğe maruz kaldığının altını çizen Eleştirel Güvenlik çalışmaları da bahsi geçen bu yapısal sorunların özgürleşme ideali ile beraber çözüme kavuşacağını ve akabinde de bu yolla güvenliğin referans aktörünün devletten birey temelli düşünceye tahvil edileceğini vurgulamıştır (Booth, 1991: 320). Eleştirel teoriye göre özellikle de Soğuk Savaş döneminin sona ermesinin ertesinde vuku bulan devletlerarası ve devlet içi iç savaşlarda varlığına yönelik en büyük tehlike bireyler tarafından hissedilmiştir. Sosyo-ekonomik ve siyasal zeminde her türlü eşitsizliğe, adaletsizliğe ve maruz kalarak gizli şiddete maruz kalan bireyler, Soğuk Savaş sonrasının yeni çatışmacı ikliminde fiziki olarak da şiddetin ve tehditlerin birincil unsurları olmuşlardır.

Eleştirel güvenlik çalışmalarının çizmiş olduğu bu resimde bireye yönelik tehlikeler devletten kaynaklanabilmektedir. Yani son kertede vatandaşına karşı güvenliği sağlama ile yükümlü olan devlet aksine bireyine karşı güvensizlik unsuru teşkil edebilmektedir. Bu nedenledir ki, eleştirel güvenlikçiler geleneksel güvenlik anlayışının aynı anda hem referans varlığı olarak devletin ele alınmasını ve hem de sorumluluğu altındaki birimlerin güvenliğini sağlamada yegâne aktör konumunda devleti işaret etmesini reddetmişlerdir (Mabe, 2003: 135-136, Floyd, 2007: 330-333). Yine bu hususlar ışığında, geleneksel güvenlik çalışmalarının disiplinde ve uluslararası sistemde genel yasası olan nesnel olgu verisi devletin hareket tarzlarına, tutumlarına ve siyaset yapma biçimlerine odaklanarak uluslararası sistemde ona merkezilik konumu payesini vermelerinin neticesinde doğal olarak güvenliğin de referans nesnesi olarak devletin öne çıkarılması tehditler bağlamında da alanı sınırlamaktaydı. Çünkü geleneksel anlayışın çizmiş olduğu bu çerçeve de güvenlik nesnesine yönelik tehditler askeri güvenlik boyutuyla sınırlı kalacaktır. İşte bu

anlayışı mevcut düzenin idamesinde temel yapı taşı olarak görüp reddedip Kopenhag ekolünün başlattığı güvenliğin genişletilmesi fikrine ilaveten eleştirel güvenlik çalışmaları aynı zamanda kavramın tüm boyutlarıyla derinleştirilip revize edilmesi gerektiğini ileri sürmüşlerdir. Bireylerin krizler ve savaşlar sonucunda yaşamış olduğu göç, gelir adaletsizliği, yoksulluk, sağlık sorunları gibi saklı yapısal şiddet unsurları aracılığıyla güvenlik kavramına normatif bir boyut kazandırarak kavramı sosyal içeriklerle yapılandırmıştır. Eleştirel güvenliğin birey temelli bu normatif duruşu güvenliğin evrensel bakış açısıyla ele alındığının da tezahürüdür (Bilgin, 2008: 92-99, Booth, 2007). Çünkü eleştirel güvenlik bireylerin güvenliğini baz alırken herhangi bir ulusun ya da grubun güvenliğinden öte dünya toplumlarının güvenliğinden bahsetmektedir.

Yukarıda bahsi geçen bireyin maruz kaldığı yapısal tehditler toplumdaki bilinçlenme özgürleşme vasıtasıyla çözümlenecektir. Elbette özgürleşmenin başarılı bir şekilde nihayete ermesinin ilk adımı da bireyin bilinçlenme süreci başlatacaktır. Özgürleşme bilinci, bireylerin o zamana değin maruz kaldığı eşitsizlik, adaletsizlik ve güvende hissetmeme gibi doğrudan ya da dolaylı yapısal ve sosyolojik şiddetlerden korunmanın reçetesi olacaktır (Booth, 1991). Eleştirel güvenlikçiler, geleneksel teorilerin devlet merkezli savlarına özellikle bu noktada yüksek sesle eleştiri getirmiştir. Çünkü geleneksel teorilerin ileri sürdüğü statik devlet merkezli ve askeri temelli güvenlik yaklaşımı uluslararası toplumda savunmasız insanların yaşadıkları güvenlik sorunlarına bigâne kalmıştır. Müşahede edildiği üzere Galtung'un yapısal şiddet kavramsallaştırmasından tevarüs eden kuramsal felsefeyi güvenlik çerçevesinde tekâmül ettirip yen bir perspektiften ele alan eleştirel güvenlik de bireylerin imkânları dâhilinde yaşaması mümkün olan hayatlarının yapısal şiddetin unsurları tarafından engellenmesini güvensizlik durumu olarak açıklamaktadır.

Bu noktada eleştirelciler de insanın özgürleşme bilincini harekete geçirip doğrudan gözlemlenebilen ve doğrudan hissedilebilen yapısal şiddetin kökeninin ne olduğunun farkına erişip özgür iradeleri aracılığıyla tercihlerde bulunabilecek ve kendilerini kısıtlayan koşullardan muaf tutacaklardır (Booth, 1991). Kısacası, güvenliğin referans nesnesi olarak devlet dışı aktörleri oluşturan bireyleri ve

bireylerin oluşturduğu diğer toplumsal katmanları gören eleştirel yaklaşım, güvenliğin sağlanmasında ise temel hareket noktası olarak bilinçli bir özgürleşmeyi salık vermektedir. Aslında, özgürleşme kavramına güvenlik çalışmaları literatüründe yeni bir görünüm kazandıran Booth'un güvenlikleştirme ve özgürleşme aynı paranın iki tarafı gibidir ile güç veya düzenden ziyade, özgürleşme hakiki anlamda gerçek güvenlik sağlar (Booth, 1991) ifadesi okulun güvenliği bakışını özetlemektedir.

Güvenliğin kavramsal olarak derinleştirip yapılandırılması güvenliğin nesnesinin kim olacağı sorusunun cevabını çeşitlendirirken bir diğer taraftan güvenliği sağlayıcı aktörün kim olacağı sorusunun cevabının da çeşitlenmesini beraberinde getirecektir. Çünkü güvenliğin sosyal olarak inşa edildiği ve pratikte de uygulandığı baz alındığında boyutlarıyla ve aktörleriyle de genişleyen ve derinleşen kavramın doğal olarak sorunsal olarak dile getirilmesinde ve de sorumluluk üstlenilmesinde devlet-dışı aktörlerinde payı olacaktır (Rothschild, 2007: 11-17).

Hâlihazırda kavramın özünde de tartışmaya açık olduğunu belirten bu yaklaşım bir diğer taraftan da güvenliğin muhtevasının ve boyutlarının sürekli değiştirilip yeniden formüle edilmesinin de kavramın belli amaçlar için türetildiği kanısındadır (Booth, 1994). Eleştirel Teori kuramcısı Cox'un teori her daim bir amaç aşkına ve de birilerinin çıkarınadır iddiasını baz alan eleştirel güvenlik çalışmaları temsilcileri de güvenliğin aktörler, nesneler, tehditler ve bu tehditler üzerinden şekillenen söylemler ve süreçlerin de aslında objektif bir biçimde değerlendirilemeyeceğini çünkü kavramın pratiğini hazırlayan amil birimler arasında yerleşmiş olan algı sonucundaki varsayımlardır (Booth, 2007). Bu varsayımlarda her zaman bir amaca hizmet etmek için vardır. Ken Booth'un daha öz ifadesi ile güvenliğin ne ifade ettiği ya da nasıl tanımlandığını belirleyen şey birimler arasındaki farklı görüşler ve söylemlerdir (Booth, 1991: 313-325). Bu ifadesiyle Booth aynı zamanda güvenliğin sosyal ve siyasal katmanda inşa edildiğini savunmaktadır. Bu noktada eleştirel güvenlik çalışmalarının tıpkı fikirsel olarak beslendiği Eleştirel teori gibi konstrüktivist yaklaşımın fikir, söylem ve bilgiyi ön planda tutan idealist çabalarından etkilendiği de gözlemlenmektedir (Sönmezoğlu, 2012: 214).

İKİNCİ BÖLÜM: SİBER GÜVENLİĞİN KAVRAMSAL ÇERÇEVESİ

> *Risk altındayız. Amerika bilgisayarlara bağımlı haldedir. Yarınların teröristleri bize klavyedeki tuşlar dizileri aracılığıyla bombalardan daha fazla zararlar vereceklerdir* (National Academy of Sciences 1991:7).

2.1. Enformasyon Çağında Bilgi-Teknoloji Alanının Güvenlik Meselesi Haline Gelmesi

Yukarıda zikredilen ifadeler ulusal güvenliğe yönelik büyük ve yeni olarak tabir edilen tehdidin etkilerini örneklendirme bakımından önem arz etmektedir. 21. yüzyılda teknolojinin vasıl olduğu boyutlar hasebiyle siber uzay olarak tabir edilen, uzamsal mekândan kaynaklı tehditler ulusal ve uluslararası düzeyde tüm katmanları etkilemiştir. Bilgi ve teknolojiden neşet eden bu güvenlik tehditleri güvenliğin tüm boyutlarının yeniden irdelenmesini de gerekli kılmıştır. Her ne kadar bu tehditler yeni olarak tabir edilse de hâlihazırda evvelden de mevcuttu. Ancak hem Soğuk Savaş döneminin siyasi atmosferinin güvenliği salt askeri temelli düşündürmesi hem de teknolojik küreselleşmenin tesirli hızının ve etkisinin 21. yy.'daki gibi hissedilmemesi bu yeni tehditlerin güvenlik algısında fazla yer edinmesini engellemiştir. Ancak 21. yüzyılda bilişime dayalı teknolojilerin geçirmiş olduğu hızlı ve keskin değişimler aracılığıyla eriştiği yeni evreler idari ve finansal işlerini bilgisayar ortamında gerçekleştiren devletler, özel kuruluşlar ve de bireyler açısından farklı ve yeni güvenlik sorunsalları teşkil etmiştir. Daha önceki dönemlerde farklı bilgisayar terminallerindeki kişiler arasındaki elektronik iletişim ağlarının oluşturduğu uzamsal ve mekânsal ortamı ifade eden ve metoforik bir indirgemecilikle ele alınan bu alana siber uzay denmiş ancak hem kuramsal hem de kavramsal olarak geniş yelpazede güvenlik açısından ele alınmasında bilgi, iletişim ve teknolojinin tüm araçları ile alana sirayet etmesiyle olmuştur.

Öte yandan, belirtildiği üzere bireylerin ve de devletlerin bilgi ve teknolojik gelişimlerin çabukluğundan ve kolaylığından faydalanarak bu alana bağımlı hale gelmeye başlaması maliyeti yüksek olmayan ancak zarar verme etkisi fazla olan siber uzaydan kaynaklı tehditleri ve riskleri de beraberinde getirmiştir. Çünkü siber uzayın imkân ve kapasiteler bağlamında en büyük getirisi devlet dışı aktör konumundaki terör ve suç gruplarına olmakla birlikte bireysel suçlulara da olmuştur. Çünkü evvelinden sadece devletlerin sahip olduğu klasik savaş araçları maliyet yükünden dolayı devlet ötesi grupların ve bireylerin sahip olamayacağı araçlardı. Ancak siber uzayın bahşetmiş olduğu fiziki sınırsızlık ve kuralsızlıklar bu grupların bu ortamda hedefledikleri eylemleri yerine getirmede kolaylıklar sağlamaktadır. Terör grupları için eylemi yerine getirmede sadece bir bilgisayarın ya da bir cep telefonunun yeterli olacağı bir ortamda devletler için bilişim ve teknoloji güvenliğinin sağlanmaması ulusal güvenliğe yönelik ciddi sorunları barındırabilmektir. Bu noktada, bilişim ve teknolojik odaklı keşifler devletlere sağladığı faydalar ve kazançların yanında devletlerin kendi aralarındaki ilişkilerinden kaynaklı güvenlik tehditlerini oluştururken, bir diğer taraftan da devlet ötesi grupların devletlere yönelik güvenlik tehdidi oluşturabilmektedir. Bu doğrultuda devletler bilgi teknolojisi aracılığıyla artık klasik güvenlik araçlarını salt askeri odaklı değil aynı zaman da bilgi odaklı düşünmeye başlamışlardır. Bununda ötesinde bilgi teknolojisine dayanan saldırı, savunma, istihbarat gibi dijital ortamda yürütülen savaş biçimlerini askeri kabiliyetlere dönüştürme uğraşısı içine de girmişlerdir (Reed, 2003: 633-641, Libicki, 1998: 411-412). Bilgi teknolojisinde elde edilen üstünlük siber uzayda yapılacak olan mücadeleler de devletlere aynı zamanda savaşların biçimini, yöntemini ve niteliğini belirleme olanağı verecektir. Dolayısıyla bilgi ve iletişim teknolojilerindeki yaşanan gelişmelerin siber güvenlik tehditlerini artırdığı görülmektedir.

Bilgi teknolojisine dayanan üretimin gelişimi, erişimi ve kullanıma açık hale gelmesi siber uzayda gerçekleşmektedir. Siber uzayda bilginin elektronik ortamlarda paylaşılması ve kullanılması herkese açık olabildiğinden aynı zamanda günümüzde devletler nezdinde başlı başına önemli bir güç haline gelen bilginin bir takım tehlikelere maruz kalabileceğine de gözlemlenmektedir. Yani, 21. yüzyılın

yenidünya düzeninde teknolojide yaşanan muazzam devrimler devletlere güç anlamında elverişli olanaklar takdim ederken bunun yanında devletlerin zihnini kurcalayacak yeni tehlikeleri ve riskleri de beraberinde getirecektir (Light, 2000: 10-12). Bu durum da bilişim sistemlerinin güvenlik nosyonuna yeni bir bakış açısı kazandırmakta ve bununla doğru orantılı olarak bilişim sistemlerinin yaşam bulduğu yer olan siber uzayın da güvenliğinin sağlanmasını devletler nezdinde elzem kılmaktadır. Çünkü askeri, ekonomik, sosyal ve siyasal düzlemde icra ettiği işleri siber ortama transfer eden devletler için bu alan ulusal güvenlik kapsamına dâhil olmaktadır. Bu çerçevede siber uzay devletlerin ulusal güvenlikleri kapsamında yekpare askeri unsurları değil ekonomik, siyasal ve sosyal unsurları da çekim alanına dâhil etmektedir (Gay, 2012: 28-30; Ghanea, 2012: 81-89; Hansen ve Nissenbaum, 2009; 1155-1175).

Her ne kadar Soğuk Savaş döneminde de siber âlemden neşet eden saldırılar mevcut ise de, siber saldırıların asıl etkisinin ve şiddetinin 21. yüzyıldan sonra yaşandığı görülmektedir. İsrail'in Suriye'ye yönelik Orchard operasyonu, Rusya'nın 8.8.8 savaşında Gürcistan'a karşı gerçekleştirdiği siber saldırılar, İran'ın nükleer üretim merkezlerine yapılan 2010 yılı stuxnet saldırıları gibi yaşanmış siber saldırı örnekleri siber uzaydan kaynaklı saldırıların, tehditlerin, savaşların ve de tehlikelerin göz ardı edilemeyeceğini gözler önüne sermiştir. Belli başlı fiziki sınırlılıklardan ve yasalardan yoksun ortamdan kaynaklı saldırıların, terör ve de savaş gibi olguların önüne siber kelimesi eklendiğinde artık siber uzaya dair görüş ve algıların metaforik bir soyutlamadan ziyade bir gerçeklik alanı haline dönüştüğü devletler tarafından kabul edilmektedir (Owens vd., 2009; Zhang, 2012). Uluslararası sistemin anarşik ortamında devletler hayatta kalmayı ve ulusal güvenliklerini birincil amaç kabul ediyor ise, ekonomik, askeri, siyasal ve toplumsal alana yönelik fırsatları barındırdığı gibi ciddi derece de tehditleri ihtiva eden siber uzayı da ulusal güvenlik kapsamının ayrılmaz bir parçası olarak görme temayülünde olmaları gerekmektedir. Çünkü ulusal güvenlik nosyonu ekonomik, siyasal, askeri ve siyasi tüm boyutlarıyla bütünsellik arz ettiğinden ve siber uzayda tüm bu unsurların güvenliğine tehlike oluşturduğundan dolayı güvenlik kapsamında önem arz etmiştir. Böylelikle bilgi teknolojilerine bağımlılığı her geçen gün daha fazla artan devletlerin ve devlet ötesi

grupların operasyonlarda, istihbaratta ve de savaşlarda kullanmaya başladığı yeni teknolojik araçlar güvenliğe dair tehdit algılamalarında ve alanlarında yeniden düşünme sürecine katkıda bulunmaktadır.

Müşahede edildiği üzere teknolojinin inkişafı ve bununla beraber ortaya çıkardığı düzen anlayışının diyalektik bir şekilde bilgi ve iletişim teknolojilerine istinaden kümelenen siber tehditleri yine bilgi ve iletişim teknolojilerine dayalı araçlar ve yöntemlerle ortaya çıktığı görülmektedir. Dolayısıyla siber uzay menşeli teknolojik araçları aktif olarak kullanan devletler yine bu alandan ulusal güvenliklerine yönelik tehditlere karşı özellikle siber saldırı ve savunma ile alakalı sistematik yöntemlerini geliştirerek önlem almaya çalışmışlardır.

2.2. Siber Güvenlik ve İlintili Kavramsal Çerçeve

Siber ağların ulusal sınırları aşan ve fiziksel olarak sınırlandırılamayan evrenselleşmiş yapısı ortaya çıkardığı siber güvenlik tehditleri bakımından artık uluslararası ilişkilerinde konusuna dâhil edilmelidir. Bu durum aynı zamanda kendi içerisinde birçok alt dallara ayrılabilecek başka çalışmaların konusunu teşkil etmektedir (Öğün ve Kaya, 2013: 148). Siber ortamdaki güvenlik tehditlerinin pratiğe dökülmüş halleri olan siber terörizm, tehdit ve savaş olguları bahse konu alt dalların muhteviyatı içerisinde ele alınacaktır.

Siber güvenlik ilk defa 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanılmış fakat akabinde bu güvenlik sorunlarının yıkıcı sosyal sonuçlar doğurabileceğinin ortaya çıktığı gelişmeler meydana gelince bunlar zamanla politikacılar, özel şirketler ve medya tarafından batı dünyasına büyük bir tehdit olarak değerlendirilmiş ve "Elektronik Pearl Harbor"lar olarak dile getirilmiştir (Singer ve Fıedman, 2015: 59). 11 Eylül olayları, bilgi teknolojileri, bilgisayarlar güvenliğe odaklanılmasını sağlamış, özellikle de bilgi teknolojileri altyapılarının korunması, elektronik gözetleme, teröristlerin interneti iletişim vasıtası olarak kullanmasına dikkat çekmiştir (Hansen ve Nissenbaum, 2009: 1155-1175). Siber güvenliğe yönelik ağlar üzerinden tehdit oluşturan temel saldırı araçları da ortamın kendine has doğası itibariyle farklıdır. Ağlar üzerinden casus yazılımlar, ağ şebeke trafiğinin dinlenmesi,

manipüle edici yemlemeler, istem dışı elektronik postalar, servis dışı bırakma, kurtçuklar ve köle bilgisayar anlamına gelen bootnetler bahsi geçen siber ortamdaki saldırı araçlarıdır.

Joseph Nye bu noktada devletlerin siber güvenliğine yönelik temel tehditleri devletlerin birbirlerine karşı oluşturduğu siber tehditler ve devlet dışı aktörlerin devletlerin siber güvenliğine yönelik tehditler şeklinde sınıflandırmıştır. Bu sınıflandırmaya göre de, siber savaşlar ve ekonomik temelli casusluk ve istihbarat tehditleri daha çok devletler ile ilintilendirilirken, siber ağlar aracılığıyla işlenen suçlar ve siber terörizm ise devlet dışı aktörler ile ilintilenmiştir (Nye, 2011).

Siber ortamın gün geçtikçe tüm aktörler nezdinde artan önemi siber tehdit, siber savaş, siber terörizm gibi farklılaşan yönleri ile ve nereden nasıl geleceği belli olmayan tehlikelerin ifadesi olan kavramların güvenliğin sözlüğüne girmesine neden olmaktadır. Öyle ki, Batı ülkelerinin kolektif savunma örgütü olan NATO özellikle üyesi Estonya'ya yönelik siber saldırılar sonrasında siber ortam asimetrik tehdit oluşturan hareket alanı olarak kabul edilmiş ve akabinde 2008 yılında Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre Of Excellence-CCD COE) kurulmuştur (Hathaway ve Klimburg, 2012, Bıçakçı, 2013). Ayrıca, 2008'te gerçekleşen Bükreş Zirvesi sonrasında yayınlanan deklarasyonda NATO, üyelerinin bilişim sistemlerini siber saldırılara karşı güçlendirme konusuna kararlılığını devam ettireceğini ilan etmenin yanı sıra zirvede siber savunma siyasetinin kabul edilmesini sağlamış ve bunu geliştirecek yapılar ile gerçekleştirecek otoriteler oluşturulmasına karar vermiştir. Ayrıca NATO'nun siber güvenlik politikasının esasının savunma olduğu vurgulanmıştır (Bıçakçı, 2012: 121). Elbette siber ortamdan kaynaklı saldırıların farklı boyutları ile gittikçe artan etkisi, güç ile eşlenik hale gelmiş ve bunun sonucunda bu ortamın hâkimiyetini elinde tutmak niyetiyle ağ destekli yetenekleri ve hareket noktalarını ihtiva ederek siber savaşı icra etme kabiliyetine haiz olmak, ulusal odaklı modern ordular ve NATO gibi uluslararası kuruluşlar için temel amaç olmuştur (Bayazıt, 2005: 19-31; Czossek, vd., 2013: 72-92). Bunun içinde NATO siber güvenlik kapsamında inşa ettiği savunma birimlerine taarruz birimlerini de ekleyerek siber saldırı kapasitelerini artırmıştır. Bu minvalde geleneksel güvenlik anlayışının ve araçlarının da dönüşümünü gerekli gören NATO

ağ destekli muharebe ve operasyon, etki odaklı operasyon, bilgi odaklı savaş ve harekâtı gibi askeri kavramları içeriğine dâhil etmiş ve bu yetenekleri icra edebilmek için de Ağ Destekli Yetenek Programını çeşitli ülkelerde startını vermiştir (Bayazıt, 2005: O'Connell, 2012: 187-209).

21. yüzyılın yeni konjonktüründe devletler açısından ulusal güvenlik çerçevesinden gözlemleme yapıldığında siber ortamın ürettiği teknolojik gelişmelere adapte olabilmesi birincil derecede önem arz etmektedir (Huhtinen ve Laitinen, 2012: 65-80). Çünkü siber ortamdan neşet eden araçlar kullanılarak oluşturulan tehditlere karşı alınacak önlemlerin başında yine bu araçların kullanımına ve bilgisine sahip olma gelmektedir. Bu nedenle bir devletin politikasının, diplomatik kararlarının ülkenin güvenliğine yönelik özellikle de askeri alandaki mahremiyetini alakadar eden sırların korunması için alınan önlemlerden oluşmaktaysa, bu durumda klasik manadaki askeri temelli olmayan bu tehditlerle mücadele biçimi de askeri olmayan araçları elzem kılmaktadır.

21. yüzyılda önemli bir güç bileşeni haline gelen siber ortamın sunmuş olduğu bilgi çağı, beraberinde sosyo-ekonomik, siyasi ve askeri kurumları da dönüşüm içine sokmuştur. Bu nedenle, bilginin bölüşülmesi, yayılması ve muhafaza edilmesi ve ilaveten hasım devletlerin bilgiye dayalı sistemlerinin çökertilmesi, düşman derinliğini görebilme, hareket kabiliyeti, esneklik ve hafiflik gibi unsurlar aynı çatı altında toplanmakta ve gerek teşkilat yapısında gerekse de silah teçhizat sistemlerinde tümünün bir arada bulunmasına özen gösterilmektedir (Gürsoy, 2003: 138-140). Bu durumda doğal olarak ülkelerin askeri yapılanmalarını tekrardan revize etmelerini hızlandıracaktır. Çünkü bundan böyle 21. yüzyılda devletler daha güçlü ve müessir askeri birimler ve teçhizatlar için bilgiye ve teknolojiye dayalı bilimi teşvik edici bir unsur olarak kullanacaktır.

Bununla birlikte, yaşanan hızlı ve etkili bilgiye dayalı dönüşümler devletlerin askeri yapılanmalarının yanı sıra yeni ve farklı güvenlik tehditlerini de gün yüzüne çıkarmış ve üstelik hâlihazırda olan klasik tehditlerin boyutlarını da artırmıştır (Castells, 2005: 3-23, Herz, 1996: 98-113). İşte bu doğrultuda da her devletin kendi siyasi, coğrafi, askeri, sosyo-politik ve ekonomik şekline göre bilgi unsurlarını belirleyip yine bu bilgi unsurlarına uygun bilişim sistemlerini geliştirme ve kullanma

stratejilerini oluşturması gerektiğinden (Don, 1999: 42-46, Weis, 2005: 295-313) güvenlik literatüründe güvenliğin siber uzay boyutu da eklenmeyi mecbur bırakmıştır. Çünkü siber ortamdan türeyen teknolojik gelişmeler durağan bir yapı arz etmemekte, aksine her geçen günde boyutları ve etkileri ile daha da fazla görünür olmaktadır ve bununla ilintili olarak da tehditler de aynı oranda artacağından siberin güvenlik boyutu ulusal güvenliklere karşı ciddi tehditler arasında dillendirilmeye başlanmaktadır.

Hava, deniz, uzay ve karadan sonra beşinci boyut olarak nitelendirilen siber uzayın karmaşık ve çok boyutlu kendine has ortamı siber güvenlik nosyonunun öncelikli güvenlik alanlarından biri haline getirmiştir. Siber ortamdaki her türlü bilginin korunması şeklinde tanımlanan siber güvenlik aynı zamanda bilginin üretimi, depolanması, işlevsel kılınması ve de iletimiyle de ilgilidir. Bu çerçevede en genel manada siber güvenlik siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan; araçlar, politikalar, güvenlik kavramları, risk yönetimi yaklaşımları, faaliyetler, eğitimler ve en iyi uygulamalar ve teknolojiler bütünü şeklinde tanımlanabilmektedir (Stevens, 2015: 20-41). Güvenliğin bu yeni boyutunun nihai hedefine ulaşabilmesi için siber ortamda bazı güvenlik kriterlerinin ve niteliklerin sağlanması ya da bulunması gerekmektedir. Bunlar; gizlilik, özgünlük, doğruluk ve de bütünlük, tutarlılık, güvenilirlik, süreklilik, erişilebilirlik ve ölçülebilirlik şeklinde olmalıdır (Gorman, 2006: 239-257). Bilginin haiz olduğu bu nitelikler devletler düzleminde kullanılan bilişime dayalı sistemler ile varlıklarının yine karşı bilişim sistemlerinden türeyen saldırılar sonucunda vereceği hasar ve güvenlik açığı göz önünde bulundurulursa yaşanacak olan kaos ortamı devletleri zor duruma düşürecektir. Örneğin, 2007 yılında Estonya'da meydana gelen siber saldırı bir ülkenin kritik altyapılarının internetten gelen tehlikeler karşısında ne kadar savunmasız olabileceğini gözler önüne sermiştir. Estonya açısından bu tehdidin hayati olarak algılanmasının sebebi, ülkedeki kamu ve özel sektöre ilişkin birçok faaliyetin internet üzerinden yürütülmesidir (Gücüyener, 2015: 18). Yine, Avustralya'da öfkeli bir işçinin bilgisayar sistemlerini manipüle ederek nehir ve parklara saldığı atık sular, yazılımlar aracılığıyla ABD'de 11 kişinin ölümüne yol açan ve 50 milyon kişinin çaresiz kalmasına neden olan elektrik sisteminin

aksatılması ve İran'a nükleer tesislerine yönelik gerçekleştirilen Stuxnet saldırıları akla gelen örnekler arasındadır (Işıklı, 2011). Dolayısıyla siber uzay ile bütünleşik olan ve ağlar üzerinden erişilebilen kritik altyapı sistemlerinin devletlerin milli güvenliği açısından önem teşkil ettiği düşünüldüğünde yüz yüze kalınabilecek saldırılardan korunması da önem arz etmektedir.

İşlediği bilginin gizliliği, bütünlüğü ya da erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin tahrip olmasına sebep olabilecek bilişim sistemlerini barındıran altyapıları şeklinde tarif edilen kritik altyapılar bu nedenle ülkelerin "Ulusal Siber Güvenlik Stratejisi ve Eylem Planları" dokümanlarında en üst sıralarda kendine yer edinmiştir. Dünya da Strateji ve Eylem Planları şeklinde adlandırılan bu dokümanlar da 2016-2019 dönemini kapsayan, mevcut riskleri, belli ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar genel hatları ile;

1. Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar (Ek-B) tarafından denetlenmesi ve siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması.

2. Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi ve kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hataları ve afetlerden de korunması için düzenlemelerin yapılması.

3. Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması ve siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması önemlidir. Ayrıca siber güvenlik alanında yetkin personel yetiştirilmesi ve bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesi de önemle vurgulanması gereken noktadır.

4. Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması.

5. Kurumsal ve sektörel SOME'lerin (Siber Olaylara Müdahale Ekibi) (Ek-C) etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesi.

6. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması ve kamu kurumları, özel sektör, STK'lar (Sivil Toplum Kuruluşu), denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyon hedefi ile ulusal siber güvenlik eko-sisteminin oluşturulması.

7. Ulusal Siber güvenlik eko-sistemi içinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılmasının yanı sıra bilişim sistemlerinin kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin içerdiği açıklıkların kötüye kullanılmasına engel olmak üzere açıklık analizi ve sertifikasyon çalışmalarının yapılması.

8. Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması. Siber güvenlikte dışa bağımlılığı azaltmak için Ar-Ge faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi.

9. Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi ve Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması şeklinde çerçevesi çizilmiştir (UDHB, 2016: 10-11).

21. yüzyılda küreselleşen dünyamızda, modern devletin ekonomik kalkınma ve toplumsal refahının sağlanmasında kritik altyapılarının güvenliği ve kritik altyapı sistemlerinin 7/24 esasına uygun ve kesintisiz olarak sürdürülmesi hayati bir öneme sahiptir (Caşın, 2015: 5-17). Kritik altyapılar ülkeden ülkeye değişmekle birlikte; çoğunlukla bankacılık, enerji, bilgi ve iletişim, elektronik haberleşme, sağlık ve temel kamu hizmetleri gibi sektörler ve bunlara ait altyapılar kritik altyapı unsurları

olarak ele alınmakta ve bu altyapılar muhtelif sivil ve askeri tehditlere maruz kaldığından ulusal düzeyde korunması gereken stratejik sistemler kapsamında değerlendirilmektedir (Çifçi, 2013: 10).

Paralel bir şekilde AB'de zarar görmesi veya ortadan kalkması halinde vatandaşların hayati toplumsal fonksiyonlarına, sağlığına, emniyetine, güvenliğine, sosyal refahına ve üye devletlerin etkin işleyişine ciddi seviyede olumsuz etkisi olabilecek varlık, sistem ve hizmetler şeklinde tanımladığı kritik altyapı bileşenlerini de; enerji, bilgi ve iletişim teknolojileri, su, gıda, sağlık, finans, kamu-hukuk düzeni ve güvenliği, sivil yönetim, taşımacılık gibi unsurlardan oluşturmuştur (Commission of The European Communities, 2005).

ABD'de yaşamsal öneme haiz kritik altyapıları, yetersizliği veya ortadan kalkması halinde güvenlik, ulusal ekonomi güvenliği ulusal halk sağlığı ve emniyeti ya da bu unsurların herhangi bir kombinasyonuna olumsuz etkisi olan fiziksel veya sanal sistemler ve varlıklar şeklinde tanımlayan ABD'de kritik altyapı bileşenlerini; ticari tesisler, iletişim, barajlar, savunma sanayi, enerji, finans, gıda ve tarım, bilgi teknolojisi, nükleer, devlet yönetim tesisleri şeklinde kurgulamıştır (Homeland Security, t.y).

Müşahede edildiği üzere kritik altyapı tasnifleri ve bileşenlerinin tamamının bilişim sistemlerine bağımlı olduğu ve dolayısıyla bilişim sistemleri tarafından kontrol edildiği görülmektedir. Bu da, yazılım tabanlı sistemlerle işlevselliğini idame ettiren bu altyapıları siber uzayın bir bileşeni durumuna getirmiş olmasının yanı sıra özellikle de farklılaşan tehdit boyutları ile klasik güvenlik anlayışını da aşınıma uğratacak olan siber güvenlik kavramını gün yüzüne çıkarmıştır.

Siber güvenliğin katmanlarını Uygulama Güvenliği, Hizmet Güvenliği ve Altyapı Güvenliği şeklinde, kapsadığı alanı ve boyutlarını erişim denetimi, kimlik doğrulama, veri gizliliği, iletişim güvenliği, veri bütünlüğü, ulaşılabilirlik ve devletlerin mahremiyeti şeklinde sınıflandıran Ünver ve Canbay'a göre bu katmanlar ve ürettikleri boyutlara yönelik yok etme, hasar verme, silme, ifşa etme, engellemeye yönelik tehdit ve saldırılar siber güvenliğin muhteviyatını belirlemektedir (Ünver vd., 2009: 3). Bir başka deyişle, siber güvenliğin temel amaçları da gizlilik, bütünlük,

erişilebilirlik, inkâr edilemezlik ve mahremiyeti sağlamaktır (Ünver vd., 2009). Bunun içinde siber güvenliğin kilit faktörü konumundaki bilginin teminat altına alınması ancak bilginini erişilebilirliği (umulmadık olay ve saldırılara karşılık gereksinim duyulduğunda erişilebilir, kullanıma hazır ve işlevsel bir halde bulunma durumudur), bütünlüğü (transfer edilen ve paylaşılan verilerin doğruluğuna karşı kritik altyapıların veri bütünlüğünün sağlanması için bilişim sistemleri aracılığıyla iletilen, alınan ya da bilişim sistemlerinde saklanan verilerin noksan ve manipüle edilmeden depolanması durumudur), gizliliğidir (bilişim sistemleri üzerinden gerçekleştirilen iletişim ve haberleşmenin gizlenen verilerin muhafazasını konu edinmektedir. Özellikle önemli ve hassas verilerin tamamının iletimi ve haberleşme süresince devletlerin mahremiyetinin korunmasını gizlilik yoluyla korumaktır). Bu kapsamda da bilginini ve sahip oldukları nitelikleri korumayı hedefleyen siber güvenlik siber tehdit ve saldırılarla birlikte bilişim sistemlerinden neşet eden güvenlik açıklarını asgari düzeye indirmeyi hedeflemektedir.

Bu hususlar ışığında, ülkelere özellikle de kritik altyapılarına yönelik topyekûn bir şekilde siber tehdit olasılıklarının artması ve bunların büyük mali kayıplarla birlikte kamu düzeni ve güvenliğini etkileyecek noktaya gelmesi konunun gerek ulusal gerek bölgesel gerekse de uluslararası kurum ve kuruluşlarca ele alınmasını gerektirmiş ve bu gereklilik dolayısıyla 1990'ların sonlarında başlayan siber güvenlik çalışmaları son yıllarda hızla artmıştır (Ünver, 2009). Siber güvenliğin sağlanması noktasında yapılan çalışmalar siber güvenlik çalışmalarının önemli unsurlarını; ulusal politika ve bu politika çerçevesinde hazırlanmış bir siber güvenlik strateji gerektiği, siber tehdit ve saldırıların, genellikle cana ve mala etki eden, sonuçları olası olduğundan siber güvenliğin sağlanmasında bu sonuçların ve bu sonuçlara yol açan fiil ve yöntemlerin suç olarak tanımlanması ve cezalandırılması, özellikle siber saldırganların caydırılması noktasında, büyük önem arz etmektedir. Teknolojik gelişmelere paralel olarak siber saldırı araç ve yöntemlerinin değiştiği de göz önünde bulundurularak ülke mevzuatının gözden geçirilmesi gerek esasa gerekse de usule ilişkin varsa eksikliklerin giderilmesi gerektiğinden bu konuda yasal bir çerçevenin oluşturulması gerekmektedir. Ayrıca yazılım, donanım ve iş süreçlerinin kalitesinin artırılarak daha güvenli kılınması için teknik tedbirlerin geliştirilmesinin yanı sıra

siber güvenlik konusunda kurumsal yapılanmanın belirlenmesi, Ulusal bazda iş birliği ve koordinasyonun sağlanması ve kapasitenin geliştirilmesi, farkındalığın artırılması, Uluslararası iş birliği ve uyumun sağlanması siber güvenliğin sağlanmasında önemli unsurlar olarak göze çarpmaktadır (Gjelten, 2010: 33-42, Ford, 2010: 52-67).

2.2.1. Siber Uzay

1980'li yıllarda bilim-kurgu alanından neşet eden ve Türkçe'ye siber alan, siber ortam ve siber uzay şeklinde tercüme edilen (Çifçi, 2012: 2) *cyberspace* mefhumu 21.yüzyılda kavramsal olarak kayda değer gelişim göstermiştir. Özellikle internetin ve diğer bilgi ve iletişim teknolojilerinin gelişimine paralel bir şekilde gelişim seyri izleyen siber uzay yenidünya düzeni olarak tabir edilen 21.yüzyılda yeni bir anlaşmazlık ve çatışma alanı olarak tebellür ederken, ekonominin tüm sistemlerinin de dâhil olduğu daha geniş toplumsal düzlemde ise bilgilenme ve bilgilendirme katmanı olarak görülebilmiştir (National Research Council, 2005: 20-32, Dunne, 2009: 101-150). Her ne kadar iletişim dalında telgraf ve radyo gibi haberleşme araçlarının kullanımı daha kadim olsa da önce devlet eliyle kullanılan akabinde zaman içerisindeki inkişafı sayesinde bireylerinde tanışma olanağı bulduğu bilgisayar ve internet, siber uzay kavramına odaklanmaya sebebiyet vermiştir. Tarihsel açıdan bakıldığında siber uzaya erişim ve katılım, alanın karmaşıklığı arz eden doğası gereği birçok aktörün bu ortamda etkinliğini de kısıtlıyordu (Leiner vd., t.y.). Buna karşılık 21.yüzyıl sonrası itibariyle siber uzayın etkinlik alanlarına erişim ve katılım dünya genelindeki devletler ve insanlar için kullanılabilir hale gelmiştir. Bugün dünyada yaklaşık olarak 2 milyar insan internete rahatlıkla erişebilmekte iken 30 trilyondan fazla da bireysel web sayfası mevcuttur (Singer ve Friedman, 2014: 14).

Özellikle bilgisayar ve internetin hızlı ve etkin yükselişi siber uzayın siyasi ve sosyal formasyonlar nezdinde iki ucu keskin bıçak misali hem lehte hem de aleyhte fırsatlar ve tehditleri aynı anda bünyesinde bulundurduğu gözlemlenmektedir. Bu veçhe de, yakın dönemlerde yaşanan siber uzay menşeli saldırılar ve bununla doğru orantılı olarak tehditler ve riskler kavramın mahiyetine dair merakı artırmakla kalmamış aynı zamanda kavramın uluslararası ortamda da sıklıkla kullanılmasını da

vesile olmuştur. 21. yüzyıla değin siber uzaydan kaynaklı güvenlik sorunlarına bigâne kalan devletler yakın dönemlerde kritik altyapılarına yönelik saldırıların etki ve nitelik bağlamında geçmişe nazaran çok daha savunmasız olması üzerine bu alanı politika ajandalarında üst sıralarda yer vermişlerdir (Clarke ve Knake: 2010: 40-44, Betz ve Stevens, 2011: 27-133).

Bidayette bilgi ortamı olarak ortaya çıkan akabinde teknolojide yaşanan gelişmelerle devlet ötesi aktörler tarafından eylem geliştirme alanı bulan siber uzay uluslararası ilişkilerde de gündem belirlemeye başlamıştır (Gücüyener, 2016; Nye, 2012). Uluslararası ortamda devletler tarafından siber uzaydan neşet eden tehlikeleri ve saldırıların tespit edilip önlenmesi ve bu doğrultuda planlı tepkiler verilmesi devletler için kilit noktadır. Bu sebeple uluslararası ilişkilerde 21. yüzyılda yaşanacak ve adına belki de "dijital mevzi savaşları" (Singer ve Frıedman, 2014) denecek olan bu yeni savaş türünün esas kaynağını oluşturan siber uzaya dair hem devletlerin savunma kurumları hem de yazınsal literatürde çalışmalar yapmışlardır.

Ancak, son yıllarda siber uzayla ilgili endişe ve kaygılar üst seviyede olmasından ötürü her ne kadar bu alan ciddiye alınsa da yine bu alanın güvenlik riskleri çerçevesinde kendine özgü taşıdığı boyutlar mevcut olduğundan tanımlaması da zor olmuştur. Örneğin siber uzaya dair devlet düzeyinde ilk ciddi hamleleri gerçekleştiren ve bu minvalde USCYBERCOM (Birleşik Devletler Siber Komutanlığı) adlı savunma kanadını kuran ABD Savunma Bakanlığı yakın zamana değin çeşitlenen tanımlamalar yapmıştır (Huğsa, 2010: 1). Yine aşağıdaki ifadelerde detaylı bir şekilde yapılmaya çalışılan yazınsal literatürdeki tanımlamalardan gözlemleneceği üzere siber uzayın tam olarak ne olduğu, fiziksel bir alanın mı yoksa sanal bir alanın mı tezahürü olduğu ve neleri içerdiği/kapsadığına dair açıklamalar üzerinde fikir birliği tam olarak sağlanamamıştır (Çömen, 2007: 210-256; Lessing, 1996: 1403-1411). Bununla birlikte siber uzay nosyonuna dair bilinmesi gereken ve üzerinde oydaşmaya varılan tek nokta kavramın ikinci ekinin yani uzay *space* son ekinin algılarda bilinen sonsuzluğa karşılık gelen boşluk anlamındaki uzay olmadığıdır. Çünkü siber uzay en başta insan ürününe dayanan bir yapıdır. Bu alanda üretilen, paylaşılan ve toplanılan bilgi ortamını kuran ve idamesini sağlayan insandır. Yine pek tabidir ki, siber uzay nosyonunnevi nema bulmasının olmazsa olmazı olan

dijital aletlerin kullanımının, yönlendirmesinin çok boyutlu ve işlevsel çözümlemelerinin faili insandır (Reed, 2012: 44-78). Yani siber uzay insan toplulukları aracılığıyla özellikle kritik altyapıları da içeren bilgi ortamıyla beraber bilginin depolanması, ağlar aracılığıyla paylaşılması ve yayılması gibi fiziksel altyapıları barındırmasından dolayı bir zamanlar atfedildiği gibi sanal âlemden öte bir konumdadır (Web, 2009: 49-56; Rheingold, 1991: 14-26). Bu nedenle siber uzay ile fiziksel katman bütün bir hale gelmiştir. Çünkü siber ortaya çıktığı dönemlerdeki gibi bilim kurguya dayalı üç boyutlu mekânı temsil etmenin ötesine geçen siber uzay bilişim ve teknolojilerin gelişimi ile paralel kavramları, araçları ve etkileri ile sürekli evrim geçirmiştir. Dolayısıyla, boyutlarıyla ve etkileriyle siber uzay belli bir fiziksel altyapıya sahip aynı zamanda da belli coğrafyaları etkilediği için sanal bir platformdan öte fiziksel ortama daha yakındır (George, 2015: 12).

Kavramın kökenbilimi incelendiğinde yakın dönemde tanımlanan ve anlam kazanan semantiğinin bir hayli uzağında ve farklı alandan türediği görülmüştür. Siber ifadesi, eski Yunan medeniyetleri döneminde Kübernetes olarak telaffuz edilmiştir (Heylighen ve Cliff 2001: 3). 1948 yılında ise matematikçi Norbert Weiner tarafından hayvanlar ve makinalar arasındaki kontrol ve iletişim disiplinini inceleyen bir bilim dalı olarak tebarüz edilen Sibernetik kavramı tekrardan diriltilip detaylandırılmıştır (Heylighen ve Joslyn 2001: 4). Ön ek konumundaki siber kelime anlamı olarak bilgisayar ve elektronik merkezli teknolojilerini refere etmektedir (Nye, 2011: 19).

İşte, siber uzay kavramı da sibernetik sözcüğünün ilk öbeği ile uzay kelimesinin birleşmesi ile oluşmuş bir kavramdır. Kavramın bu şekildeki yapılanmasının ve günümüz semantiğindeki anlamına yakın kullanılmasının mimarı da William Gibson'dur. Gibson siber uzay kavramını 1982 yılında yayınladığı kısa hikâyede karmaşık değişkenleri içeren teknik bir alan olarak yorumlarken, 1984 yılında Neuromancer adlı romanında ise daha kapsamlı ve teknik temayülde milyarlarca ağlar tarafından karşılıklı olarak transfer edilen iletilerin zihinde canlandırılması zor olan ve muazzam derecede karmaşıklıkları içeren grafiksel bir platform olarak tanımlamıştır (Gibson, 1995).

Kavramın bilişim ve teknolojilerinin gelişimi ile beraber tedricen etkisini ve pratiğini hissettirmesi tanımına dair esasları ve boyutlarını da dönüşüme uğratmıştır. Siber uzayın boyutlarının gösterdiği etki sadece teknik boyutlarda değil siyasi ve toplumsal katmanlarda da yer bulmuştur. Bir zamanlar sadece iletişim amaçlı kullanım alanı bulan siber uzay 21.yüzyıl sonrasında ise bankacılık sektöründen, ulaşım, haberleşme, sağlık ve enerji tesisleri gibi daha birçok kritik altyapıları da ihtiva eder hale gelmiştir. İlaveten, bahsi geçen sektörlerin gözleyici kontrol ve veri toplama üzerinden komuta ve kontrolünü sağlamak SCADA (Supervisory Control and Data Acquisition) yine fiziksel altyapılara sahip olan siber uzayın bilgisayar teknolojileri aracılığıyla sağlanmaktadır (Sanal, 1998: 81-82). Böylelikle hâlihazırda karmaşık bir teknik sisteme sahip olan siber uzay teknolojilerinde kaydedilen gelişmeler ve bununla ilintili olarak kullanımındaki artışlar siyasal ve sosyal alandaki değişimlere zemin hazırlamaya imkân vermiştir.

Bu sebeple farkındalığına varılan siber uzayın münhasıran bir alan olarak billurlaşmasına değin her dönemde özünde internet ve ağ şebekeleri üzerinden tanımlanmış ve gün geçtikçe ilave kavramlar ve etkenlerle alanını daha da genişletmiştir (Libicki, 2007: 1-14, Bomse, 2001: 1717-1749). Örneğin kavram uzmanlarca 1990'lı yıllarda bilgisayar aracılığıyla sürdürülen, erişilen ve üretilen küresel ağ bağlantılı sanal ve yapay iletişim alanı olarak tanımlanırken (Benedikt, 1991: 119-224) bir başka yaklaşımda ise ayrı bilgisayarlar arasındaki etkileşimliliği barındıran sistem şeklinde tanımlanmakta ve sanal mekândan (Koepsell ve Rapaport, 1995, Chang 2002, Yu Li chang, 2002; 1-18) öte olduğunu vurgulamak içinde bilgisayarlar arasındaki etkileşimliliği muhafaza eden ve düzenleyen unsurun insan olduğuna istinaden kavramın fiziksel alana daha yakın olduğunu dile getirilmektedir. Bir başka deyişle kendine has özellikleri ile 1980'lerde yeni keşfedilmeye başlanılan siber uzay mecrasına dair tartışmalar içerik ve tanımlamadan ziyade genel olarak kavramın ontolojik tabanlı hem boyutuna hem de mekânsallığına dair olmuştur (Gibson, 1984, Sterling, 1985, Shields, 1996: 4-10, Quarterman, 1990: 140, Dodge ve Kitchin, 2001: 172).

Siber uzayın sanal-reel ortamın insanları tarafından kullanılan ve faydalanılan birçok temel bilgileri içermesi, yani reel dünya ile sanal dünyanın kesişen varlığı

siber uzaya dair yekpare bir alan tartışmasını 21. yüzyılın yeni ortamında anlamsız kılmaktadır. Çünkü siber uzay artık hem fiziksel hem de sosyal yapı unsurlarına aynı anda sahiptir (Jiang ve Ormeling, 1999: 4-12, Madge ve O'Connor, 2005: 83-97, Singer vd., 2014, Armitage ve Roberts, 2002: 21-34). Fiziksel yapıya sahiptir çünkü bilgi teknolojileri altyapıları tarafından hareket alanı bulmaktadır, sosyal yapıya sahip olmasının nedeni de alanın insanlar, kurumlar tarafından dikkate alınmaya, konuşulmaya ve düşünülmeye başlanmasıdır (Crangs, 1999: 11-13, Shields, 1996). Yani siber uzay kendine özgü araçları, içerikleri, sembolleri ve yöntemleriyle kara, hava ve deniz alanları gibi belli bir hareket alanına sahiptir (Murray, 2007: 3-12: Biegel, 2003: 25-51, Bryant, 1992: 138-155, Heylighen, 2008: 1-20).

Siber uzay tabanlı bilgi teknolojilerinde kaydedilen gelişmeler ve bu bilgi teknoloji araçlarının arka planında yer alan dijital dünyanın yerlisi konumundaki insan olgusunun doğal olarak bu alandan kaynaklı problemleri üretmede ve çözmede gerekli çözümün içerisinde yer alması alanın toplumsal ve siyasal temelli değişimlere yön vermesine neden olabilmiştir (Nayar, 2004: 211-261). Gün geçtikçe artan yüksek teknoloji araçlarının ve bilgi sistemlerinin yanı sıra bununla ilintili olarak artan kullanıcı sayısı siber uzayda insandan, terör gruplarından ve eş düzeyindeki bir rakip devletten gelebilecek tehditlere karşı hedef konuma gelen devletler nezdinde olumlu yanlarını barındırdığı gibi olumsuz yanlarını da barındırmıştır. Yakın dönemlerde yaşanan siber menşeli saldırı örneklerinde gözlemlendiği üzere bu alandan neşet eden tehditler ve risklerin kimden geldiğinin, belirlenemezliği ve muhteviyatının hangi derecede olduğunun geç fark edilmesi gibi unsurlardan dolayı siber uzay devletler için 21. yüzyılda yaklaşan en büyük tehdit alanı olarak tebarüz etmektedir. Çünkü bu alan devlet ötesi suç örgütlerinin ve hatta bireylerin hedefleri doğrultusunda herhangi bir devletin ulusal güvenliğine hasar verebilecek fırsatları vermektedir. Ve doğası gereği siber uzay birey, suç örgütleri ve devlet gibi farklı düzeydeki aktörlere eşit kullanım ve faydalanma imkânı sunmakla birlikte aynı zamanda riskler ve tehditler oluşturmada açıklıklar da oluşturmaktadır. Bir başka deyişle bahsi geçen aktörler arasında siber uzayda sınırları çizilmiş ve kuralları belli yasalar mevcut olmadığından bu ortamdan meydana gelecek riskler ve tehditler bireylerden, suç örgütlerinden ve devletlerden de kaynaklanır olabilecektir. Ancak

siber uzayın artık küreselleşen doğasında tehdit eden aktörün kimliği isnat edilmediğinden bu durumda tehditlerin ve risklerin fail aktörünün muammalığı sorunsalını devlet nazarında oluşturacağı için siber uzay ortamı güvenlik bağlamında yeni ve farklı koşullar yaratmaktadır.

Siber uzayın farkındalığının artması uluslararası ilişkilerde yeni mücadele alanlarının ve politika formlarının teşekkül etmesini de beraberinde getirmiştir. Bu çerçevede, kendine has özellikleri ile çelişkili bir yapı arz eden siber uzayda devletler için gücü elde etmek ve idame ettirmek zor belirlenebilir bir hale gelmiştir (Eriksson ve Giacomello, 2006: 226-228). Bu nedenle devletler 21.yüzyılın başlarına değin ulusal güvenliklerine yönelik tehditler ve riskler bakımından sufli politikalar (low politics) kategorisinde değerlendirdikleri siber uzayı, yeni dönemde alandan neşet eden yeni tehditler ve bu tehditlerin çok boyutluluğundan dolayı ulvi politikalar (high politics) kategorisinde değerlendirmiş ve bu yeni koşullara göre tanımlamalar ve önlemler geliştirmişlerdir (Singer and Fried man, 2015; Clarke ve Knake, 2010).

ARPANET aracılığıyla internetin kurucusu ve ilk kullananı konumundaki ABD'nin savunma bakanlığıyla ortak yaptığı tanımlamaya göre siber uzay tarım, sağlık, acil çağrı merkezleri, savunma sanayi ve teknoloji üsleri, enerji, ulaşım ve haberleşme ve banka sistemleri gibi ülkelerinin kritik altyapılarını ihtiva eden etmenlerin merkezi sistemi konumundadır (Report Organization of American States, 2015: 8-14). Dolayısıyla siber uzay ABD penceresinden birbirine bağlı bilgisayarlar, birden fazla ağı birbirine bağlayan yönlendiriciler ve fiber optik kablolardan oluşan ve bu kablolar sayesinde kritik altyapılarının çalışmasına meydan veren sistem şeklinde tanımlanmaktadır. Böylelikle ABD sağlıklı işleyen bir siber uzay alanının ekonomik güvenlikleri ve de bununla ilintili olarak ulusal güvenliklerinin sağlanması noktasında devamını elzem görmektedir (Wills ve Ashenden, 2012: 110-123).

Ancak, 11 Eylül saldırıları sonrasında siber uzay alanına dair farkındalığı daha da artan ABD Savunma Bakanlığı bilişim sistemlerini yoğun bir biçimde kullanan topluluklarının etkileşimi ile beraber değişen ve dönüşen siber alan coğrafyasıyla ilgili tanımlamalarını güncellemiştir. 2003 yılında siber uzayın maddi altyapılarına vurgu yaparak yapmış olduğu tanımı 2006 yılında ABD Savunma Bakanlığı siber uzay operasyonları için geliştirilen ulusal askeri strateji bildirilerinde kritik

altyapıları da kapsayacak şekilde bilgisayar ağları ile dijitalleştirilmiş iletişim ağları ile iç içe geçmiş olan sistemlerde verileri saklama, manipüle etme ve iletme işlevselliğiyle elektronik ve elektromanyetik spektrumun kullanımı şeklinde nitelendirmiştir (C4ISR Integration Conference, 2006). Ancak zikredildiği üzere ışık hızında ilerleyen siber uzayın evrimi hasebiyle yapılan bu tanımlamalarda sürekli evrim geçirmiş ve 2009 ve 2010 yıllarında ABD savunma algısında anakronik bir tanım arz etmiştir. Artık bilgisayar ağları aracılığıyla dijitalleştirilmiş bilgilerin transfer edildiği düşünsel ortamın tezahürü olan iletişimden ve mekân olarak da siber uzaydan öte bir coğrafyayı temsil eden bir platform konumunda olan siber uzay 2010 yılı ABD savunma bakanlığı tarafından interneti de dâhil eden bilgi teknolojileri altyapılarının ağları, telekomünikasyon ağları ve bilgisayar sistemleri ile bütünleşik işlemci ve kontrol yöneticilerini içeren bilgi ortamındaki küresel alan olarak vasıflandırılmıştır (Department of defence Dictionary, 2010: 44). 2010 yılında yapılan bu tanım alanın etkisi ve boyutlarıyla özellikle küreselliğine vurgu yapılarak daha kapsamlı ele alınmıştır.

Elbette ABD'nin dile getirmiş olduğu bu tanımlama diğer devletler bazında uyumluluk arz etmemiştir. Örneğin İngiltere siber güvenlik stratejisinde siber uzayı dijital ağlar boyunca yürütülen eylemlerin ve içeriklerin dâhil olduğu tüm ağ şebekelerini sarmalayan dijital etkinlik olarak tanımlarken (The UK Cyber Security Strategy, 2011), Kanada ise siber uzayı birbirine bağlı olan bilgi teknolojileri ağları tarafından yaratılan elektronik bir alan olarak tanımlamıştır (Royal Canadian Mounted Police, 2014). Ancak siber uzayın artık donanım, yazılım ve bilişim sistemlerini içeren internetinde ötesinde insanında dâhil olmasıyla bahse konu ağlar bünyesinde kurmuş olduğu sosyal etkileşim sayesinde farklı manalar taşıdığından ülkelerde geliştirdikleri tanımlamaları bu cihette yeniden revize etme yoluna girmişlerdir.

İngiltere bu bağlamda 2011 yılında yapmış olduğu tanımlamaya ek olarak 2015 yılında kavramın tanımlamasını yeniden gözden geçirmiş ve bu kez bilgiyi depolayan, değiştiren ve ileten dijital ağların kritik altyapı ve servisleri de içerecek şekilde teşekkül ettirdiği dijital network alanı olarak tasvir etmiştir (The UK Cyber Security Strategy, 2016). Avustralya'nın siber güvenlik stratejisi belgesinde ise siber

uzay kavramı yerine internet kavramı tercih edilmiş ve yapılan tanımlama da internet ve interneti oluşturan tüm bileşenler şeklinde tanımlanmıştır (Australıa's Cyber Securıty Strategy, 2016).

Siber savunmadan sorumlu birimler kuran ve bu alanda üyeleriyle saldırılara karşı iş birliği ve savunma kabiliyetlerini geliştirmek için etkinlikleri yürürlüğe koyan NATO siber uzayın internetten daha fazlasını kapsadığını dile getirmiştir. Soğuk Savaş sonrası askeri savunma ittifakından küresel güvenlik örgütüne dönüşüm süreci yaşayan NATO, 2011 yılında yapmış olduğu tanımda alanın bilgisayarlar ve ağlarının tecelli ettirdiği, insanların ve bilgisayarların bir noktada beraber olabildiği ve çevrim içi etkinliklerinin bütün yönlerini içeren sayısal dünya şeklinde tanımlamıştır. BM ise küresel çapta bir mesele olarak gördüğü ve dolayısıyla yine küresel çapta yaklaşımlarla ilgi gerektiren bir alan olarak gördüğü siber uzayı, internete, iletişim altyapılarına ve dijital ortamda bilgileri saklama ve işleme araçlarına birleşik ve öte yandan bağlı küresel sistem şeklinde tanımlamıştır (United Nations, UN Terms, t.y.). 2010-2020 "Dijital Ajandası" içerisinde bilgi güvenliği meselesini güvenlik anlayışının önemli stratejilerinden biri haline getiren ve bu minvalde siber uzaydan türeyen saldırı ve tehditlere karşı pratik çözüm önerileri üretme ve geliştirme çabası içine giren AB'de (Henkoğlu ve Yılmaz, 2013: 451-460) siber uzayı bütün dünyayı kapsayan kişisel bilgisayarların elektronik bilgilerinin ve girdilerinin gezindiği sanal âlem şeklinde tavsif etmiştir.

Bu doğrultuda, 21.yüzyılda uluslararası sistemin temel değişken aktörü konumundaki devletler nezdinde siber uzaydan türeyen saldırıların, tehditlerin ve risklerin çok boyutlu ve karmaşık yapısı hâlihazırda miadının dolduğu iddia edilen geleneksel tehdit algılamalarının ve bu tehditlerle mücadele yöntemlerinin işlevsizliğine dair tartışmaları daha da kızıştırmıştır. 21. yüzyılda küreselleşme ekseninde şekillenen parametreler sosyal bilimlerin diğer fenomenlerinde olduğu gibi güvenlik sürecine de aktörler, tehditler, pratikler ve araçlar bağlamında dönüşüm ve değişim sürecinde katkıda bulunmuştur. Uluslararası ilişkilerde de yaşanan bu değişim ve dönüşümler bahse konu yeni güvenlik tanımlamalarını gerekli kılmakla birlikte yerküre üzerinde birbirinden tamamen farklı koşullarda ve farklı yerlerde yaşayan insanları ve devlet ötesi diğer grupların internet aracılığıyla bilgiye

erişebildiği, coğrafi bütünlükten ve sınırlılıktan yoksun ve de herhangi bir karar alıcı denetim mekanizmasının ve hukuki kaidelerin bulunmadığı anarşik sistemi andıran siber uzayın ulaştığı boyutlarda göz önüne alındığında güvenliğin sağlanmasına dair devletlerin yeni mücadele araçlarını da devreye sokmaları gerektiğini gözler önüne sermektedir. Görüldüğü üzere Soğuk Savaş sonrasının değişen dünya dinamiklerinde hâlihazırda aktör türlerinin ve niceliklerinin artması ve bu aktörlerin karşılıklı ve çok sayıda yeni ilişki biçimleri ortaya koymaları, sınır aşkın etkinliklerinin artması, bilim ve teknolojideki hızlı gelişme, bilinen farklı ve çok sayıdaki dengenin değişmesi ve çeşitlenmesi süreci (Dedeoğlu, 2014: 77) 21. yüzyılda kendine özgü temel çerçeve ve dinamikleri ile yeni bir tehdit ve güvenlik parametresi olarak tebarüz eden siber uzay aracılığıyla daha da tahkim edilmiştir. Bu durumda 21.yüzyıla değin uluslararası ilişkiler camiasında uluslararası sisteme etkileri bağlamında neredeyse hiçbir merak uyandırmayan ve dikkate alınmayan siber uzayın artık yazınsal literatürde de kavramsal ve kuramsal düzlemde ele alınmasının yolunu açmıştır

Bu hususlar ışığında Denning bilgi tabanlı işlemcileri ve bilgi sistemleri üzerinden yorumladığı alanı bilgi ortamı olarak lanse ederek basılı bilgiler, bilgisayar ve iletişim sistemleri vasıtasıyla bilginin kullanıldığı, faydalanıldığı ve saklandığı her çeşit fiziksel yapı şeklinde tanımlamıştır (Denning, 1999: 239- 287). Teknolojik devrimlerle beraber olumlu ve olumsuz yanlarını beraberinde getiren ve paradoksal bir şekilde güvenlik kaygıları, riskleri ve tehditleri arz eden siber uzay alanın temel çerçeve ve dinamikleri ile nasıl bir şekilde işlediğine dair kapsamlı bir tartışmayı ele alan Sınger ve Frıedman da siber uzayı özünde bilginin çevrim içi kullanıldığı bir bilgi ortamı olarak ifade ederken, ortaya çıkan, saklanılan ve de en önemlisi paylaşılan dijital verilerden ve ilaveten bu verileri saklayan bilgisayarlara ek olarak bu bilgi tabanlı verilerin akışına izin veren sistem ve altyapıları birleştiren ağ tabanlı bilgisayarların internetini, kapalı intranetleri, hücresel teknolojileri, fiber optik kabloları ve uzay tabanlı iletişimi kapsadığını dile getirmektedir (Singer ve Frıedman, 2015). Yine alanın artık homojen bir yapıda olmadığını ve internet ağlarını da içerecek şekilde iç yüzünde telefon, uydu ve medya araçlarının da dâhil olduğu bilişim ve iletişim ağlarını da formüle eden alanı ifade etmektedir (Whittaker, 2004: 5).

Çünkü 21. yüzyılda siber uzay hızlı ve çabuk büyüyen küresel doğası gereği çok katmanlılığı haiz olmuş ve bununla bağıtlı bir şekilde her bir katman dijital, iletişim ve haberleşmede etkileşme bakımından farklı formlar sunmuştur (Dodge ve Kitchin, 2000). Genel mahiyette Dodge ve Kitchin bu katmanları işlemcileri, kabloları, yazılım ve donanımları ve uydulara sahip internet teknolojileri ve de telefon, faks ve medya gibi alışılagelmiş telekomünikasyon teknolojileri diye kategorilere ayırmıştır. Bu kategorilerinde hızlı ve birbirine bağlı gelişiminin yeni bir hibrid alanı ortaya çıkardığını dile getirmişlerdir (Dodge ve Kıtchın, 2001: 1). Yine siber uzayın yegâne fiziksel varlığına dayanan internet ortamı olarak düşünülmesini alanı monolitik bir yapıya büründüreceğini ifade eden Bıçakçı, insanların birbirine bağlı bilişim sistemleriyle etkileştiği ve yine kendi aralarında da birbirine bağlı özellikteki bilişim sistemlerinin kendi aralarında veya insanlarla iletişim içinde olduğu fiziksel olmayan alanı siber uzay şeklinde tanımlamıştır (Bıçakçı, 2010: 13). Siber uzayın olmazsa olmazının fiziksel katmanı oluşturan RAM'lar, işlemciler, anakartlar, diskler gibi ekipmanlardan meydana geldiğini dile getiren Bıçakçı siber uzayın fiziksel varlığının sadece bilgisayar ekipmanlarından oluştuğu kanısına varmanın eksik kalacağını bunun yerine ağ ortamında iletişim kuran ve kurmaya aracı olan tüm bileşim sistemlerinin farklı unsurlarıyla meydana geldiğini iddia etmiştir. Bu noktadan hareketle de bahse konu katmanların programlama dillerini yorumlayan teknolojinin ve insan unsuru gibi birçok bileşenin kontrol edilmesiyle oluşan siber alanın güvenlik noktasında zafiyetlere sıkça yol açacağını belirtmiştir (Bıçakçı, 2010).

Bugün hem devletler bazında hem de devlet altı gruplar bazında yeni bir savaş ortamı olarak tebarüz ettiğini ifade eden Clark da siber uzayı fiziksel coğrafyaya dair hiçbir sınırlama olmaksızın insanların ve toplulukların bilgisayar, iletişim ve haberleşme araçlarını içeren telekomünikasyon sistemleri vasıtasıyla bütün olarak birbirine bağlı olma platformu şeklinde açıklamıştır (Clark, 2010: 4). Öte yandan, Nye ve Scowcroft da analojik bir bakış açısıyla tıpkı deniz, hava ve kara alanı gibi siber uzayın kendine has araçlarını ve nitelikleri ile içeriklerini değerlendirmiş ve özellikle siber uzayın fiziki katmanının billurlaşmasını sağlayan fiber optik kablolar ve internet altyapısı gibi unsurların uluslararası ekonomik kuruluşlarının ve ayrıca

devletlerin egemenliğinin kontrol alanına girdiği gerekçesiyle alanın önemi dikkat çekmiştir (Nye ve Scowcroft, 2012). Yine, benzerliklerden çıkarım yaparak nasıl ki erken dönem modern Avrupa'nın gelişiminde barut devriminin, 19. yüzyılda Sanayi Devriminin ve 20. yüzyılın başında ikinci bir sanayi devriminin ve ortasında nükleer devrimin teknolojik gelişmeler ve değişimler aracılığıyla yaşanması bu yüzyıllara siyasi, sosyal ve askeri bağlamda damgasını vurduysa, hızı, araçları ve kendine has özellikleri ile uluslararası sisteminde dönüm noktası olmaya namzet gördükleri siber uzayı özünde bilgisayar ve elektromanyetik spektrumlarla ilişkili faaliyet alanı olarak belirterek 21.yüzyıla damgasını vuran platform şeklinde görmüşlerdir (Nye ve Scowcroft, 2012).

Ezcümle, yukarıda farklı ve dönemsel boyutlarıyla yapılan tanımlamalar ışığında siber uzay, zamana bağıtlı bir şekilde gelişen birbiriyle bağlantılı bilgi sistemleri ve bu bilgi sistemleriyle etkileşim içerisinde olan insan kullanıcıları dizisinden oluşan ve kendine has gayrı merkeziliğiyle ve muhteviyatı ile sanal ve fiziki katmanlarında barındıran bir platformdur. Burada zikredilen birbiriyle bağlantılı bilgi sistemlerinden kasıt elektronik ortamdaki bilgi, yazılım, donanım ve bu bilgisayar sistemli programları birbirine bağlayan iletim ortamıdır. Siber uzay alanının kilit unsurunu oluşturan insan kullanıcıları kavramı da özünde yapaylığı barındıran alana bu özelliği kazandıranın ve inşa edenin insan amilinin olduğu vurgusudur (Punday, 2000: 194-213, Giles, 2006: 464, Singer ve Friedman, 2015, Zhao, 2005: 387–405). Çünkü elektronik aygıtların ve bilgisayar sistemli programların arka planındaki envai çeşit sorunların ve bu sorunların çözümünde önemli bir rol oynayan kullanıcı ve tüketici konumundaki insan amili olmadan siber uzay dinamikliğini kaybedecek ve en nihayetinde bir tehdit unsuru olmaktan çıkacaktır. Ayrıca, kavramla ilgili tanımlamalarda üzerinde durulmayan ancak önem arz eden bir diğer kayda değer sorunsal alanın mahiyetinin zamana bağıtlı bir biçimde geçirdiği dönüşümdür. Bu sebeple de haiz olduğu dinamik yapı sebebiyle sürekli gelişim gösteren alan doğal olarak statiklikten de azade bir konumdadır. Bu durumda alanın bir diğer taraftan da karmaşık yapısını doğru orantılı bir şekilde artırmaktadır. İşte, bu nokta da, kavramın tanımlamasına, içeriğine ve etki ölçeğine

dair yapılan açıklamalar ve izahlar zamana bağlı değişkenlik vurgusunu elzem kılmaktadır.

Her ne kadar yapılan bu tanımda siber uzayın mekânsal, ontolojik ve epistemolojik düzlemde karmaşıklığı ve belirsizlikleri barındıran dinamik küresel doğasına tam anlamıyla uygun bir tanım teşkil etmese de, asgari düzeyde alanın bütününün önemli parçalarını oluşturan unsurlara değinerek bir genel ve öz tasvir yapılmıştır. Genel olarak yapılan tanımlamalardan da müşahede edildiği üzere, üzerinde mutabakata varılan bir siber uzay tanımlamasının mevcudiyetinin eksikliği göze çarpmaktadır. Bir başka deyişle, temelde bilişim ve teknolojinin gelişmekte olmaya devam etmesi siber ortamdan neşet eden siber tehditler, saldırılar, suçlar, teröristler, silahlar ve de güvenlik kavramlarının nihai çerçevesinin boyutlarını büyütüp genişlettiğinden dolayı bu alana ve alanın temel kavramlarına dair belli başlı bir çerçeve çizilmesini de zorlaştırmıştır.

2.2.2. Siber Tehdit

Çalışmada da sıklıkla vurgulandığı üzere, siber uzay kazandırdığı ve sağladığı olanaklar ile yararlı bir alan iken diğer taraftan da devletlerin ulusal güvenliğine yönelik kaynağı olduğu tehditler bakımından ise zararlı durumları barındıran iki ucu keskin kılıç misali bir karakteristiğe sahiptir. Devletlerin 21. yüzyıla değin bigâne kaldığı bu alandan oluşan tehditler her ne kadar daha önceki dönemlerde yaşansa da özellikle önce bilişim ve iletişim teknolojilerinin kullanıldığı 11 Eylül saldırıları (Weimann, 2004: 3-21, Heidenreich ve Gray, 2013: 8-23, The Natıonal Strategy To Secure Cyberspace, 2003: Lovelace, 2015: 86), akabinde NATO ülkesi olan Estonya'ya yönelik siber saldırılar sonrası farkındalığı uluslararası toplum nezdinde artmasıyla beraber devletlerin güvenlik politikalarının ve endişelerinin merkezinde yer edinmeye başlamıştır (O'Connell ve Arimatsu, 2012: Korns ve Kastenberg, 2009: 60-70; Herzog, 2011: 50-55). Anavatanı siber uzay olan bilgi ve iletişim araçlarının yaygınlaşması ve maliyetinin de düşüklüğü ile beraber düşünüldüğünde devletler için olduğu kadar, bireyler ve de en önemlisi suç örgütleri konumundaki devlet dışı aktörler için de başvurulması gereken zaruri bir alan haline gelmiş ve adeta erişilebilirliği, kullanım kolaylığı, ispat edilemezliği ve etkisiyle bağımlılık

yaratmıştır. Devlet dışı aktörlerin bilişim teknolojileri araçlarına gün geçtikçe daha bağımlı hale gelmesi geleneksel güvenlik anlayışının tehdit algısının aksine, niteliği ve niceliği bakımından asimetrik yeni tehditlerin uluslararası sistemde boy göstermesine yol açmıştır. Bu bağlamda 21. yüzyılın bu tehditlerine yeni dendiği için öncelikle eskinin ne olduğu ve adına yeni denilen tehditlerin hangi açılardan ve araçlardan eskiden farklı olduğunun tespiti gerekli kılınmaktadır.

Sözlük anlamı olarak korkutma, hiddet etme (Dağ, 2009: 442) anlamında kullanılan tehdit kavramı uluslararası ilişkilerin ortodoks güvenlik anlayışında devletlerin sahip olduğu öz değerlere yönelik tehlike, risk oluşturan/oluşturabilen olgular şeklinde tanımlanmıştır (Krahmann, 2005: 4). Tanımda ifade edilen ve çalışmanın da meta teorik kısmında açıklanan öz değerler ifadesi geleneksel güvenlik algısında askeri ve siyasi bağlamın olgularını içerirken, Soğuk Savaşın bitimine doğru Buzan'ın öncülüğündeki Kopenhag Ekolü tarafından bu ifade ilaveten ekonomik, toplumsal ve çevresel bağlamın olgularını da içermiştir.

Bir diğer taraftan Williams'ta bir tehdit tanımlaması yapılması için en başta tehdidin yöneldiği bir düşmanın mevcut olması gerekmektedir. Yani Williams tehdidin ötekiye ihtiyacı olduğunu belirtmiştir. Aslında tehdit kavramının ontolojisini tanımlı ve somut bir düşman ya da öteki üzerinden kurgulayan Williams bu durumda somut düşmana yönelen her türlü tehlikenin tehdit unsuru olacağını ileri sürmüştür (Williams 2009: 1-9). Dedeoğlu da, tehditlerin hem realiteye dayanan olgu ve olaylara dayanabileceğini belirtirken aynı zamanda algı ve tahminlere de dayanabileceğini belirtmiştir. Ancak en nihayetinde Dedeoğlu bir tehdidin tehlike olup olmadığını en nihayetinde gerçekleştiği zamanın belirleyeceğini ifade etmiştir. (Dedeoğlu, 2014: 32). Davis de, uluslararası ilişkiler literatüründe tehdidin siyasal ya da sosyal bir failin sahip olduğu imkân ve kabiliyetler aracılığıyla olumsuz sonuçlar doğuracak şekilde hasar verme niyeti olarak tanımlamıştır (Davis, 2003: 1-3).

Ayrıca Jovi de tehdit kavramının olmazsa olmazının; amaca uygunluğu, kapasite ve etkinlik bakımından inanılırlığı ve amaçları bağlamında tam manasıyla eksiksiz olması, tehdidin yöneldiği tarafın fark edeceği şekilde ve sert olması ve de son olarak açık olmasının gerekliliği üzerinden yorumlar (Jovi, 1998: 13-15). Kavramı niyetler ve kapasite bağlamında yapılabilirlik üzerinden tavsif eden

Roscini'ye de tehdidi, kötü niyetli düşmanların hedeflerine ulaşmada kullanacakları imkân ve kabiliyetlerinin değerlendirilmesi sonucunda net olarak belirlenebilecek ve ölçülebilecek bir takım tehlikeler şeklinde tanımlamıştır (Roscini, 2007: 231-232). Örneğin Soğuk Savaş evresinin ittifaklar sisteminde yer alan bir ülke karşı bloğunda yer alan düşman devletin uluslararası siyasetteki askeri güç, araç ve diğer her türlü etkinlik ve hareket alanını genişletmesini kendisine yönelik ölçülebilen, öngörülebilen ve de niyeti belli olan tehditler olarak algılamıştır.

David Singer da klasik güvenlik ve bununla ilintili olarak tanımladığı ve anlamlandırdığı tehdit kavramını yapılabilir olma niteliği bağlamındaki kapasitelerle niyetlerin çarpımı şeklinde yorumlamıştır. Yani Singer'a göre bir olayın, hareketin ya da eylemin tehdit olabilmesinin ilk koşulu icra edilebilirliğidir; icra edilebilmesi içinde kapasiteleri doğrultusunda inandırıcılığının ve inandırıcılık doğrultusunda da niyetlerinde gözle görünür olması gerekmektedir (Singer, 1958: 94-95).

Müşahede edildiği üzere yapılan tanımlamalarda göze çarpan unsur tehditlerin büyük oranda algısallığa ve olasılığa dayandığıdır. Tehditler olasılıksal olabilmektedir; çünkü kimi zaman gerçekleşebilir ya da gerçekleşemeyebilirler (Farnham, 2003: 395-397). Ancak her ne kadar tarihsel süreç içerisinde tüm zamanlar ve mekânlar için belli ve içerikleri net olan bir tehdit tanımlaması olmasa da, özünde devletlerin haiz oldukları değerlerden mahrum olma tehlikesi şeklinde temel bir çerçeveyi de barındıran kavram kavramsallaştırmasında yorumlanma açısından süreklilik kazanmıştır (Rousseau ve Retamero, 2007: 744-771).

Devletlerin etkileşimleri ve siyaset yapma biçimleri neticesinde birbiriyle ilişkili birimler kümesi şeklinde tezahür eden uluslararası sistemde (Nye ve Welch, 2011: 61) tehdit unsuru da Soğuk Savaş döneminin sonuna değin ortodoks güvenlik algısına paralel bir şekilde sadece devletlere yönelik tehlike ve risk oluşturan askeri ve siyasal olgular bazlı ele alınırken (Çömen, 1978: 93-95; Singer, 1958) 21. yüzyılın değişen dünya dinamiklerinin dönüşen araçları vasıtasıyla artık algılanan kalıplarından taşmıştır. Şimdiye kadar tehditler geleneksel güvenlik mantığı çerçevesinde sadece bir devletten bir diğer rakip devlete yönelik tehlikelerden ve risklerden oluşuyordu. Bir başka deyişle tehditlerin kimden, nasıl ve hangi araçlarla

geldiği açık ve netti. Dolayısıyla savunma ve saldırı bağlamında alınacak önlemler buna göre şekillenmekteydi.

Devletlerin kendi aralarında cereyan eden çatışma ve anlaşmazlıkların boyut ve ölçekleri ile azalması, farklı hedeflerde farklı aktör türlerinin ortaya çıkması 21. yüzyılın uluslararası ortamına da yeni tehdit türlerini sunmuş ve tehdit kavramı ile doğru orantılı bir ilişkisi olan güvenlik anlayışında da kendine yer edinmiştir (Marchesin, 2003). Yeni bir güvenlik anlayışını zorunlu kılan unsurlardan küreselleşme ve görünürlük kazandırdığı iletişim ve haberleşme, internet ve bilgisayar teknolojilerini ihtiva eden tüm bilişim araçlarının ileri derecedeki değişim ve hızı, tehdit kavramının da klasik semantiğini ve tasvirini dönüştürmüştür. Bu bağlamda gelişimi ve yayılma evresi devam eden bilişim ve iletişim teknolojilerinden müteşekkil siber uzay, uluslararası sistemin başat aktörü devletlerin güvenliğini siber tehditler diye adlandırılan yeni bir tehditle baş başa bırakmıştır.

En azından temel çerçeve ve dinamiklerini çizildiği bu kavramsallaştırma takip edilirse, siber tehditler; siber uzay teknolojilerinin sağlamış olduğu olanakların araçsallaştırılmasıyla devlet gibi siyasal, devlet ötesi gibi toplumsal birimlerin siyasal, toplumsal ve ekonomik öz değerlerine yönelik içe ve dışa dayalı düzenlerini hasara uğratma olasılığı taşıyan tehlikeler kategorisine girmektedir. (Berner, 2003: 4). Ayrıca amaç ve araç olarak siber uzayda üreyen ve gelişen bilginin kötüye kullanılması, kamuoyuna afişe edilmesi ya da sistemli saldırılarla erişilebilirliğinin engellenmesi gibi arzu edilmeyen durumlara ve sonuçlara sebebiyet verme tehlikesi olarak tanımlanmıştır (Ünal, Canbay ve Mirzaoğlu, 2009). Bu tanımlamada siber tehditler sadece bilgi ve iletişim teknolojilerinden türeyen tehlikeler olduğu için bilişim araçlarının ve sistemlerinin araç olarak kullanıldığı vurgulanmıştır. Bu tanımlamaya uygunluk teşkil eden yerinde örneklemlerden biri ise Wikileaks belgeleridir. Kasım 2010 yılı itibariyle ABD'nin Irak savaşı ile ilgili kayıtlarının ve diplomatik elektronik yazışmalarının bilişim ve iletişim teknolojilerinin sağlamış olduğu imkânlar sayesinde Wikileaks web sitesinden hızlıca yayınlanması teknolojik bağımlılığı yüksek olan devletler nezdinde siber uzayın bir tehdit oluşturacağı kanısını ortaya çıkarmıştır. Öyle ki, kimilerince diplomasinin 11 Eylülü olarak tabir edilen Wikileaks belgelerinden sonra Foreign Policy dergisi siber alanı yaklaşan en

büyük tehdit olarak nitelendirmiştir (Singer and Frıedman, 2015). Çünkü Wikileaks gelişen teknoloji araçları ve hizmetleri ile devletlerin gizli kalması gereken politikalarını ifşa etmekle kalmamış bilgisayar ortamında peşi sıra ABD dışındaki ülkelerin büyükelçiliklerinin ve konsolosluklarından gelen tüm resmi yazışma ve mesajları paylaşmış ve çoğaltmıştır. 2006 yılında dünya genelindeki yozlaşma ve kötüye kullanmayı teşhir etme temayülü ile kurulan Wikileaks Web sitesi siber uzayın veri ve erişim ile olan münasebetinde devletlerin bilgi güvenliğine karşı tehdit oluşturmuştur. Nitekim henüz patlak vermeyen ifşa krizinden önce 2008 yılında ABD Savunma Bakanlığı Wikileaks ve benzeri web sitelerinin ABD ordusuna karşı istihbarat, hareket ve bilgi güvenliği açısından tehditler barındırdığını dile getirmiştir (Singer ve Frıedman, 2015:119).

Soğuk Savaşın bitimi çift kutupluluğa dayalı uluslararası sistemi değiştirmekle kalmamış aynı zamanda sistemin içerisinde devletlerarası etkileşim biçimine ve algısına yön veren önemli etkenlerden biri olan mahdut tehdit kavramının doğasını da dönüşüme uğratmıştır. Gayrımerkezilik özelliğiyle sınırların manasını ve önemini hükümsüz kılan siber güvenlik tehditleri de bu dönüşüm sürecini hızlandırmakla kalmamış aşınıma uğratmıştır (Cilluffo ve Pattak, 2000: 41-50, Huğsa, 2009: 19-21). Siber güvenlik tehditlerinin varlık alanında tanımlanmış, belirgin ve açık bir düşman tanımı mevcut değildir; saldırganlar 12-19 yaş grubu arasındaki ergen çocuklar olabileceği gibi, terörizme destek veren "haydut devletler", ya da bir takım inançlara ve ideolojilere sahip teröristlerde olabilmektedir. Siber tehditlerin gayrımerkeziliği ve karmaşıklığı saldırganların hasmane niyetlerinin ve tehditlerinin doğrulanabilir ve gerçekliği kanıtlanabilirliliğini zorlaştırmaktadır. Bilgisayar sistemli araçlara sahip bir kişi dünyanın başka bir coğrafyasında başka birine ve kuruma ait bilgisayara kısa sürede erişebilir ve bu bilgisayarları kontrolü altına alabilir. Çünkü teknolojinin ileri sevideki gelişmiş hali bu kolaylığı sağlamaktadır (Edwards, 2010: 30-33). Sahip olduğu deneyim, olanaklar ve kapasitelerle birlikte gereksinim duyduğu saldırı teçhizatlarına da erişebilen saldırganlar böylelikle devletlerin bilişim sistem güvenliğindeki açıklıklarından yararlanarak siber saldırılar gerçekleştirebilmektedir. ABD'nin federal kurumlarına ait bilgisayarlarına sızan ve lojistik bilgi sistemlerine dair bilgilere erişip bu bilgileri hükümetin farklı kurumlarına zarar vermek için

kullanan kişi 21 yaşındaki bir çocuktu. Yine ABD'nin uzay çalışmalarının yürütüldüğü kurum olan NASA'ya ve hükümetin diğer savunma bakanlığına ait kurumlara sızıp bilgilere erişen kişi 16 yaşındaydı (Wordpress, 2013).İnternet ortamında cirit atan ve tehlikeli kişi olarak adlandırılan ortaokul ve lise çağındaki bu ergen çocuklar skript kiddies olarak adlandırılmıştır. Skript kiddiesler hackerlığın mertebeler silsilesinde en alt sınıfı oluşturan tehdit unsurlarıdır. Bunlar genelde kendi yazılımlarını geliştiremeyen daha çok internetten hazır bir şekilde indirdikleri yazılımları ve kodları indirip kullanarak sıkıntılarını ve meraklarını gidermek isterler (Pctools, t.y.).

Gözlemlendiği üzere bilişim sistemdeki yaygın açıklıklar bu alana dair bilgiye, beceriye ve kısmen de olsa deneyime sahip olan saldırganlar için arzulanan ortamı rahatlıkla olanaklı kılmaktadır. Zaten alanın gayrımerkeziliği, zor ve yüksek maliyetli olmayışı ve isnat sorunu gibi kendine özgü sunmuş olduğu olanaklar bilişim teknolojilerinin gelişimine paralel saldırganların da niceliğini artırmış ve bu durumda doğal seyrinde tehditlerinde sayısını artırmıştır. Çünkü siber tehditler, kahır ekseriyette, bilişim altyapılarından türeyen kötü niyetler ve amaçlar taşıyan kötücül ve zararlı yazılım ve donanımların kullanılması neticesinde nevi nema bulduğu için bilgi teknolojileri ortamının değişen karakteristiği doğal olarak bu alandan kaynaklı oluşacak tehdit algılarını şekillendirmektedir.

Ulusal güvenlik ve bununla ilişkili olarak tehdit algısında ve politikasında 21. yüzyılda siber alandan kaynaklı bir diğer göze çarpan unsur bireysel ya da sayıca az olan grupların saldırıları ve bunun sonucunda yaratmış oldukları tehditlerdir (Kibaroğlu, 2002: 4). Klasik güvenlik anlayışında devletlerarasında zuhur eden askeri temelli tehditlere karşılık etkin bir müdahale ile cevap verilebiliyordu, ancak 21.yüzyılın güvenlik anlayışının genişleyen ve nitelik bakımından değişen tehditleri ve bu tehditleri amaçları doğrultusunda kullanabilme imkânına ve deneyimine erişebilen devlet-ötesi aktörleri ile beraber yeni dönemde saldırganların kimliği devletler nezdinde karşılık vermede mühim sorunsallar teşkil etmiştir. Tehditler devlet altı gruplardan devletlere yönelik arz ettiğinde devletlerin vereceği karşılıklar görünürde yasalar bağlamında tecelli edeceğinden bu durumda tehditlerin açıklığına, şiddetine ve isnatlığına dair bir takım cevapsız soruları beraberinde getirmektedir.

Örneğin, saldırıyı gerçekleştiren saldırgan ya da saldırganların kimliği belli midir? Kimin ya da neyin tehdit edildiği belirlenmiş midir? Ve özellikle siber uzayın küresel doğasının kimlik ve lokasyon bağlamında sunmuş olduğu bir takım avantajlardan mütevellit, siber güvenlik tehditlerinin arkasında devlet düzeyinde kimin olduğu belli midir? Gibi sorular siber tehditleri devletler nezdinde daha da dikkate alınması gereken güvenlik sorunsalı olarak günyüzüne çıkarmaktadır (Shackelford, 2014; 3-51, Stevens, 2015: 20-41).

Yukarıda da bahsi geçtiği üzere devletlere yönelik siber temelli güvenliğe yönelik tehdit hadiselerinin büyük çoğunluğu internet ortamında kötücül yazılım ve donanımları kullanarak tehlike unsuru oluşturan script kiddies olarak adlandırılan kişi ya da gruplar tarafından gerçekleştirilmiştir. Bu grupların bilgi, birikim ve etki bakımından en üst kademesini oluşturan ve politik, sosyal ve dini saikleri olan ileri düzeydeki hactivistler siber uzayı kullanarak özellikle devletlerin ulusal güvenlik bağlamında önemli yer tutan kritik altyapılarına gerçekleştirdikleri siber saldırılarla tehdit unsuru oluşturan bir diğer önemli gruplardır (Hua ve Bapna, 2012: 104-105, Brunst, 2009: 51-58). Türkçede bilgisayar korsanları olarak adlandırılan bu gruplar hackleme teknik ve yöntemlerini kullanarak devletlerin hem bilişim sistemlerine hem de bu bilişim sistemlerine bağımlı olarak çalışan kritik altyapılarına karşı ciddi hasarlar vermeyi amaçlamaktadırlar. Devletlerin web sitelerine yapılan DDOS (Distributed Denial of Service) saldırıları, bombalı mail mesajları, virüsler, içerik bozma ve manipüle edici yazılımlar ve donanımlar, internet hizmetlerinin kesilmesi ve kurtçuklar ve botlar gibi saldırı araçları bu aktivitelerine örnek teşkil etmektedir. Pratik bağlamda haktivistlerin aktif katılım gösterdiği ve gerçekleştirdikleri siber uzay kaynaklı saldırılar ilk olarak Kosova savaşında dikkatleri çekmiştir (Dun, 2008: 21, Wentz, 2002: 709, Geers, 2011: 2).

Elbette daha evvelki dönemlerde de bir takım siber saldırılar gerçekleştirilmiştir. Ancak uluslararası arenada etnik savaşlar hasebiyle yürütülen konvansiyonel savaşlarda aktif tüm devletlerin ve örgütlerin haktivistleri yaptıkları siber saldırılarla Kosova Savaşı'nın ömrünü biraz daha uzatmıştır (Borger, 1999; Miloseviç: 2015). Bilişim ve elektronik sistemlerinin alışılmışın dışında yollar benimsenerek kullanılıp saldırı amaçlı kullanılması aynı zamanda alışılmışın dışında

tehdit ve bununla alakalı olarak güvenlik algısı ve pratiği oluşturmaktadır. Özellikle devletlerin kamuya ait neredeyse tüm finansal, askeri ve sağlık, enerji ve iletişim gibi altyapıya dair sunmuş olduğu hizmetlerin büyük kısmının kritik altyapısının bilişim sistemlerine bağlı olması bilgi, beceri ve deneyimleri ile siber ortamı iyi kullanabilen hackerlere saldırı amaçlı tehdit oluşturmada farklı nitelikte bir hareket sahası ve tarzı yaratmıştır (Caplan, 2013: 93-108, Virtual Criminology Report, 2009).

Bununla birlikte, uygulama yöntemleri ile alışılmışın dışında bir tehdit türü yaratan bilgisayar korsanlığı sadece bireylerin ya da teknolojik olarak az sayıdaki maharetli bireylerden oluşan grupların faydalandığı bir tehdit yöntemi değildir. Terörist gruplar gibi kötü emeller taşıyan aktörlerin yanı sıra devletlerde siber ortamı saldırı amaçlı kullanabilmektedir. Çünkü siber uzay mütekabiliyet esası düzleminde değerlendirildiğinde tüm aktörler için neredeyse aynı imkânları ve fırsatları sunmaktadır. Bu alandan kaynaklı bir güvenlik tehdidi yaratma isteğinde olan herhangi zayıf ölçekli bir devletin ya da devlet ötesi aktörün ekonomik ve askeri bağlamda güçlü olmasına gerek yoktur. Aynı zamanda 21.yüzyıl öncesi klasik savaş dönemlerinde askeri araçların kullanımı profesyonel derecede bilgi gerektirdiğinden herkes tarafından kullanımını da zorlaştırıyordu; üstelik bu araçların maliyetinin yüksek olmasının zayıf devletler nezdinde dezavantajları beraberinde getiriyordu. Ancak günümüzde bir bilgisayar ve hatta bir cep telefonu gibi gerekli teknolojik teçhizatlara ve bu teçhizatların kullanım deneyimine, bilgiye sahip sayıca az insani personel tarafından organize olunduğu takdirde potansiyel saldırı ve tehdit oluşturma hedefine ulaşılabilmektedir (Rollins ve Wilson, 2007: 15-21, Herrington ve Aldrich, 2013: 299–3109).

Yukarıda bahsi geçen ve siber ortam üzerinden yürütülen ilk savaş olduğu iddia edilen Kosova savaşının yanı sıra, 2007 yılında cereyan eden Estonya'ya ile Rusya arasındaki gerginlikte, 2008 İsrail'in Suriye'de Kuzey Kore'nin inşa etmek istediği nükleer tesislerin altyapısını bilişim sistemlerini kullanarak yok etmesinde (Eran, 2009; Follath ve Stark, 2009) Pakistan-Hindistan arasındaki Kaşmir anlaşmazlığında (Al Jazera, 2010) ve İsrail-Filistin çatışmalarında kullanılan yoğun siber saldırılar (Allen ve Chris, 2003) rakip devletlerarasında gözlemlenebilen siber temelli savaş örnekleri olarak göze çarpmaktadır. Karşılıklı bilgi ağlarına ve bu bilgi

ağlarından beslenen kritik altyapılara yönelik gerçekleştirilen siber saldırılar devletlerin günlük siyasi, askeri ve sosyal pratiklerini felce uğratabilmekte ve ulusal güvenlik çerçevesinde sıkıntılar yaratabilmektedir.

Geleneksel güvenlik araçlarının mukavemet etmede yetersiz kaldığı 21.yüzyılın siber ortam kaynaklı bu yeni güvenlik tehditleri özellikle bilişim teknolojilerinin nimetlerinden faydalanan ulus aşırı grupların elinde daha da kontrol edilemez hale gelmiş ve bu bağlamda devletlerin sorgulanamayan egemenliğine ve otoritesine adeta meydan okumalara yol açmıştır (Thompson, 2002: 507-508). Öyle ki, bilgi ve teknoloji alanındaki baş döndürücü ilerlemeler birey düzeyinden devlet düzeyine kadar birçok faklı nitelikte aktörün ulusal ve uluslararası düzeyde etkinlikleri bakımından önemli roller oynamalarına şans vermiş olması uluslararası sistemin işleyiş ve yapısını da daha karmaşık hale getirmiştir. 21.yüzyıla değin Westphalian düzenin devlete bahşetmiş olduğu siyasal sistemin yegâne başat aktörü olma düsturu hâlihazırda Soğuk Savaşın bitimi ve ilaveten bilgi teknolojilerinin gelişim doğasının ivme kazandırdığı küreselleşme olgusu ile beraber tartışmaya açılmıştı (Mathews, 1997: 50-66, Ann, 2000: 17-49, Keohane ve Nye, 1998). Ancak tüm bilişim sistemlerinin kesişim kümesi noktasında birleştiği alan olan siber uzayın kendine has anarşik yapısı devlet dışı aktörlere de kendi saikleri doğrultusunda etkinlik gösterebilecek yeni alanlar açmıştır.

Soğuk Savaş sonrası sosyal bilimlere dair neredeyse her soyut kavram semantik ve kavramsal düzlemde geleneksel kullanımından öte anlamlar ve boyutlar barındırarak aşınıma uğramışsa tehdit nosyonu da zamana ve mekâna bağıtlı şekilde değişen anlamlar ve algılar barındırarak hem içeriksel hem de kavramsal bazda aşınıma uğramaya başlamıştır. Bu minvalde tehdit nosyonuna aşınım sürecini hızlandıran ve literatüre yeni tehditler şeklinde yansıyan düşünceleri sıklıkla görülmesini sağlayan etmen sınırların anlamını ve güce dayalı kontrolü ortadan kaldıran kendine has özellikleri ile asimetrik tehdit görüntüsü veren siber saldırılardır (Karagül ve Özkan, 2015). Küresel bilgi ağlarının uluslar ötesi işleyişi, ülke sınırlarının bu ağlar aracılığıyla esnekliğinin daha da artması 21. yüzyılın hava, kara, deniz ve uzaydan sonraki beşinci boyut olan siber ortamın geleneksel güvenlik anlayışıyla denetimi geçersiz kılmıştır.

Siber ortam uluslararası sistemde gözlemlenen tek, çift ya da çok kutupluluk düzeninin yerine devlet dışı aktörlerinde etkin ve söz sahibi olabileceği farklı ve çok kutuplulukla ikame etmiş ve alışılmışın dışında bir güç dengesi sistemi inşa ederek burada devletlerle bireyler ve ulus aşırı gruplar arasındaki hiyerarşiyi zayıflatan asimetrik güç ilişkilerini de ön plana çıkarmıştır (Karagül ve Özkan, 2015). Saldırganın muhatabı karşısındaki zayıflığına karşılık göreceli biçimde üstünlüklere sahip olması şeklinde tavsif edilen asimetrik tehditler genellikle muhatabın vermiş olduğu açıklıklardan ve zaaflarından yararlanılarak hedef ülkenin halkının korkularını kullanarak yönetim unsurlarına olan desteğini azaltmayı hedeflemiştir. Terörist gruplar bu yolla muhatabında siyasal ve ekonomik istikrarsızlıklar yaratmayı hedefleyerek, kolay erişim imkânı sağlayan bilişim teknolojilerinin de yardımıyla, boylarıyla ölçülmeyecek kadar büyük tahribata yol açan saldırılar gerçekleştirmeyi mümkün kılmayı amaçlamıştır (Erhan, 2003: 4). Dolayısıyla yarattığı ani ve hazırlıksız durum nedeniyle siber saldırılar, ülkelerin siyasal, sosyal ve ekonomik sistemlerinde çöküşlere ve istikrarsızlıklara neden olan, düşük seviyede teknoloji kullanarak etkin olmayı amaçlayan, kapsamlı ve yeni trende sahip nitelikte eylem biçimleridir (Bravo, 2005: 137).

Siber ortamdan kaynaklı 21. yüzyılın bu yeni trend tehditleri de, bilişim teknolojileri sayesinde kötücül amaçlar taşıyan bireyler ve ulus aşırı gruplar için her türden bilgiye kolaylıkla erişebilen bir atmosfer yarattığından bu grupların büyük ölçüde ve etkinlikte eylemlerini ifa etmede alışılmışın dışında bir nüfuz ve hareket alanı sağlamaktadır. Küresel doğası ile alışılmışın dışında, üzerinde herhangi bir kural koyucunun henüz hâkimiyet kuramadığı ve dolayısıyla belli ilkeleri, yasaları ve araçları olmayan, kimden, nasıl geldiği muamma olan tehditlere karşı ne şekilde ve hangi oranda karşılık verileceğine dair belli bir çerçevesi olmayan siber güvenlik tehditlerinin Soğuk Savaş döneminin sonlanmasına müteakip ortaya çıkan kitle imha silahların ulus aşırı grupların eline geçmesiyle güçlenecek olan terörizme, ayrılıkçı hareketlere, donmuş çatışma bölgelerinde patlak veren etnik dini çatışmalara sınırları aşan organize suç örgütlerinden neşet eden tehlikelere eklemlenmesi yeni yüzyılda yeni tehdit niteliği ve türü olan asimetrik tehditleri de bir hayli görünür kılmıştır. Nitekim NATO'nun temelleri atılan siber savunma teşkilatının, 2006 Riga zirvesinde

siber saldırılara asimetrik tehdit kategorisinde kabul edilmiş ve akabinde 20007 Estonya saldırısı sonrasında Müşterek Siber Savunma Mükemmeliyet Merkezi (Hathaway ve Klimburg, 2012: 1-32) kurulması kararlaştırılmıştır.

Bu minvalde Özcan'da, yeni milenyumda tehditlerin ve terörizmin yeni yüzü olarak gördüğü siber uzayın tehdit türleri, araçları ve hasarları bakımından devletlerin ulusal güvenliğe yönelik en büyük tehlike arz edeceğini belirterek alanın devletler için önemine ve etkisine dikkat çekmiştir (Özcan, 2004). Çünkü siber uzayın devlet ötesi suç örgütlerine ve bireysel suçlulara sunduğu olanaklar bu örgütler için şimdiye kadar görülmemiş hareket alanı yaratmakta ve dolayısıyla uluslararası çapta devletlere yönelik meydan okumalarda kamuoyu oluşturmaktadır. Amaçları politik ve sosyal olabilen bu örgütler için siber uzay gerekli gördükleri teknolojiye dayalı saldırı araçlarını rahatlıkla temin etmektedir. Bu durumda, kritik altyapı sektörlerini bilişim sistemlerine bağımlı hale getiren gelişmiş düzeydeki devletleri ulus aşırı suç örgütlerinin sebebiyet verdiği tehditlerle yüz yüze bırakabilmektedir (Wenger, 2001: 8). Zira ulus-aşırı ve bireysel düzeyde olabilen suç örgütleri siber uzayın sunduğu ileri teknolojiden ve üstüne üstlük açıklıktan faydalanarak sahip oldukları imkânlarla bir devletin baraj kapaklarının, askeri kuvvetlerinin tüm saldırı ve savunma sistemlerinin, doğalgaz şebekelerinin basınç kontrol, ulaşım, haberleşme, su, sağlık ve bankacılık gibi kamu kurumlarının tüm sistemlerinin kontrolünü ele geçirip devletlerin işleyen sistemlerini kilitleyip tehdit edebilme imkân ve kabiliyetine sahip olabilmektedirler (Özcan, 2004). Bu saldırıları gerçekleştirecek olan saldırganlar için donanımı ve yazılıma haiz bir bilgisayar sistemli teknolojik alet yeterli olacaktır.

Siber uzaydan nemalanarak türeyen siber tehditlerin doğal olarak araçları da siber ortama özgü uyarlanmış olacaktır. Örneğin bu alandan neşet eden siber güvenlik tehditleri genelde kayda değer ve gizli olan verilerin rakip devletlerden askeri, siyasi ve de ekonomik fayda sağlamak için illegal bir şekilde iletişim ağları ve donanım ve yazılımlar aracılığıyla çalınması siber casusluk tehdidini meydana getirirken, hizmet dışı bırakma yöntemi ise rakip devletlerin hâlihazırdaki bilgi sistemlerini çalışamaz duruma getirerek ya da bilgi sistemin manipüle eden bir başka yeni siber tehdit türüdür. Bununla birlikte, özellikle bilişim sistemlerinden uydular

kullanılarak rakip devletlerin askeri araçlarının hasara uğratılması ve petrol, doğal gaz, elektrik, bankacılık ve ulaşım hizmetlerini içeren altyapılara yönelik saldırılar da bir diğer önemli siber güvenlik tehdit türleridir.

2.2.3. Siber Terörizm

Global değişimin katalizörü olarak siber uzaydan türeyen bilgi teknolojileri alanındaki (Karagül, Özkan, 2015) hızlı ve seri gelişmeler ve dönüşümler bir yandan toplumların ve devletlerin sosyo-ekonomik ve siyasi pratiklerini olumlu yönde etkilerken bir diğer yandan da asimetrik ve çok boyutlu tehdit unsuru oluşturmak isteyen terör grupları içinde politik hedeflerine erişmelerinde, güç ve kamuoyu oluşturmada etkinlik aracı olma fırsatı taşımıştır. Özcan'ın suç ve suçlu davranışlarını inceleyen bilim dalı olan suçbiliminin suçların fırsatları takip etmesi şeklindeki deterministik düsturundan hareketle ileri sürdüğü gibi siber alem bilişim teknolojileri vasıtasıyla kötü niyetli terörist gruplara eski tehdit unsurlarını ve yöntemlerini daha da kompleks bir görünüme sokan ve yeni yol ve yöntemlerle yeni tehdit unsuru oluşturabilecek olanaklar sağlamıştır (Özcan, 2011). Siber ortamın sunduğu fırsatlar sayesinde küreselleşen bilgiden devletlerin yanı sıra suç örgütleri de önemli oranlarda yararlanmakta ve internet üzerinden bomba yapım tekniklerini anlatma gibi fantazilere sahip olabilmekteyken; bunun yanında organize suç gruplarının ve terör örgütlerinin ellerinde bulundurdukları karapara ile teknik altyapılarını hızla geliştirmesi, oyunu güvenlik güçlerinin aksine bir kurala bağlı olmaksızın oynaması ve gerektiğinde bu alana çok büyük mali kaynaklar aktarması, devletlerin bilişim suçları ile mücadelede ciddi zorluklar ile karşılaşmasına neden olmaktadırlar (Özcan, 2002). Bu durumda 1990'lar sonrası uluslararası sistemin halihazırdaki kompleks yapısına aktör çeşitliliğinin artması ve teknolojik alandaki ilerlemeler ve değişimlerin devletlere sunduğu fırsatlar kadar bu fırsatların neden olduğu tehditler uluslararası ilişkilerde devletler nezdinde fırsat-tehdit paradoksuna yol açmıştır.

21. yüzyılda terörizm farklılaşan yön, nitelikleri ve kompleks sorunları ile devletlerin ve uluslararası toplumun yüz yüze kalmak zorunda olduğu problemlerin başında gelmektedir. Terörizme dair yaşanan kavramsal ve anlamsal karmaşa salt

kavramın tanımlanma sorunundan öte sebepler içermektedir. Bu sebepler arasında göze çarpan en önemli sorunsal teröristin ya da teröristlerin Soğuk Savaş dönemi sonrası yeni dinamiklerin sunmuş olduğu olanaklar aracılığıyla erişebildiği araçların ve imkânların çoğalmasıyla beraber benimsedikleri yöntem, amaç ve stratejilerinin de değişimi olmuştur. Uluslararası ilişkilerde siyaset yapma biçimi aktörler ve eylemler düzleminde baş döndürücü hızda değişmektedir. Bu veçhede devlet dışı illegal gruplarında amaçları, bu amaçlara erişebilmek için benimsedikleri araçlar ve stratejiler de değişime uğramaktadır. Günümüzde her türlü bilgisayar aletleri, yazılımlar, internet ağları ve iletişim araçları gibi siber ortamın dâhilindeki tüm araçları büyük oranda terör grupları tarafından rahatlıkla ve kolaylıkla kullanılabilmektedir. Misalen, IŞID internet dünyasında faaliyette bulunan Siber Halife ordusunu (CCA) saldırılar icra etme kapasitesi bakımından yetersiz bulmuş bunun yerine istihbaratı ve tam teşekküllü saldırıları da yapma kapasitesini artımak için siber ordu kurma gayreti içine girmiştir. IŞID üyeleri siber saldırı adımlarını ayrıntılarıyla paylaşarak kendi gruplarıyla ilintili siber asker ağını genişletmeye yönelik online bir kurs açarak, IŞID sempatizanı bir kişi batı istihbaratını hedefleyen "nasıl siber saldırı yapılır" dersleri vermeye başlamıştır (Siber Bülten, 2016). Halihazırda en yakın zamanda interneti propaganda aracı olarak etkili kullanan IŞID örneğinde olduğu gibi bu terör örgütleri aktif olarak kullandıkları kendi web sitelerinde daha fazla insana ve kamuoyuna erişebilmek için neredeyse her dilden yayın yapmaktadırlar (Theohary ve Rollis, 2011).

Devletler askeri, ekonomi ve hizmet sektörlerinde bilişim sistemlerini yaygın bir biçimde kullanırlar. Devletlerin bilgi teknolojilerine ve ağlar sistemine bağımlı hale gelmesi sadece meşruluğa uygun kabul edilen birimler tarafından değil aynı zamanda kötücül niyetlere sahip teröristlerin, sınır aşan suç örgütleri gibi diğer suç unsuru teşkil eden birimlerinde siber ortamdan faydalanmak için istifade ettikleri göze çarpmaktadır. Yakın döneme kadar klasik konvansiyonel savaş araçlarına erişemeyen terör grupları devletlere yönelik tehdit unsuru olma ve eylemleri aracılığıyla ses getirme şansını siber ortamın devletler aleyhine yaratmış olduğu açıklıklardan ve zafiyetlerden faydalanma olanağı ile yakalamış ve bilişim teknolojilerinin maliyetinin düşük olması her düzeyden aktörün sahip olunabilirliğini

de artırdığından devletlere karşı meydan okumalarda neredeyse eşit şartlar sunmuştur (Taliharm, 2010; 65-66; Schmid ve Jongman, 1988: 12-15). Zikredildiği üzere devletlerin ve toplumların bilişim teknolojilerine git gide artan bu bağımlılığı terör gruplarına devletlerin ulusal savunma ve kritik altyapı sistemlerine yönelik saldırı hedeflerini gerçekleştirmede farklı türde ve nitelikte güvenlik zafiyeti yaratmaktadır (Weiman, 2005: 129).

Günümüzde terörizme dair kavramsal ve politik düzlemde hem ulusal hem de uluslararası düzeyde yüksek perdeden sıkça tartışıldığı su götürmez bir gerçektir. Ancak, terörizm tehdidi Soğuk Savaş sonrası dönemin yeni dinamiklerinde ve düzeninde istikrarlı bir şekilde artış göstermeye devam etmektedir. Özellikle de, faillere tarif edilmesi ve anlaşılması zor tehdit oluşturma olanakları sunan muhtelif alanlarda yaşanan teknolojik ve teknik ilerlemelerinde katkısıyla terör gruplarının eylemleri ve meydan okumaları daha tehlikeli korkulu ve yıkıcı hale gelmiştir (Cooper, 2004: 158-185, Neumann, 2009: 2048, Shukla, 2006: 167-168). Devletlerin insanları, toplumunu ve diğer kurumsal organlarını koruması beklenen özel istihbarat sistemlerinin hareket analizleri ve bilgileri işleme sistemleri, güvenlik programları ve politikaları ve stratejik yöntemlerinin bahse konu bu yeni ve tahripkâr tehditlere ve hasımlara çoğu zamanlar galebe çalamadığı görülmektedir (Mythen ve Walklate, 2005: 379-398). Farklılaşan yönleri ve nitelikleri ile bu yeni terörizmle mücadele etmede yıllar boyunca geliştirilen strateji ve yöntemler kimi zaman etkisiz kalabilmektedir. Çünkü bu yeni terör, amaçlarını gerçekleştirmede sadece uçak kaçırma ya da intihar bombacılığını araç olarak kullanmamaktadır. Bunun yerine kullanımı, erişilebilirliği daha uygun olan ve maliyeti daha düşük olan siber ortam araçlarını araç olarak kullanabilmektedir. Siber ortamın araçlarının zaman, mekan ve kural tanımaksızın herkes tarafından kullanılması sanal ortamın aynı zamanda fiziksel ortamla olan bütünleşmesini artırmış ve bu durumda bu atmosferden kolaylıkla fayda sağlayacak olan devlet dışı suç örgütlerinin adına siber terörizm diyeceği yeni bir güvenlik tehdidi oluşturma kapasitesini kolaylaştırmıştır (Gordon ve Ford, 2003).

Terör örgütlerinin bilişim sistemlerini bir silah aracı olarak kullanmasında birçok sebep bulunmaktadır. Yeni yüzyılda farklılaşan yön ve nitelikleri ile siber

ortamdan kaynaklı yeni tehditler oluşturan siber terörizm klasik bağlamdaki terörizminde bir alt kümesi olmaya namzettir. Çünkü siber terörizm suçlulara gerçek isimlerini ya da kimliklerini gizlemede, olası büyük hasarlar oluşturmada, hedef ülkenin kamuoyunun psikolojik algısına etki etmede ve de medyada gündemde olma gibi seçenekler sunduğundan (Denning, 1999: 241; Rollins ve Wilson, 2007: 6). 21.yüzyılın modern teröristleri için de akıllıca bir seçenek oluşturmuştur (Berner, 2003: 2, Kostopoulos, 2008: 165). Terör örgütlerinin de tıpkı devletler gibi eylemleri ve davranışlarını ifa etmede ve bu eylem ve davranışlarının sonuçlarını hesaplamada rasyonel mantıkla hareket ettikleri göz önünde bulundurulursa, politik gündemlerini icra etmede siber terör saldırılarının uygun maliyeti ve muhtemel potansiyel yıkıcı ve akamete uğratıcı zararlar vermesi terörist gruplar nezdinde pek çok elverişli fırsatlar yaratmaktadır. Bununla birlikte, siber uzay terör gruplarına aynı anda birden fazla hedeflere yönelik saldırı imkânı vererek böylelikle gerçekleştirilen saldırıların etkisini ve şiddetini de artırmada ve ses getirmede kolaylıklar sağlamaktadır.

Siber terör ya da terörizm farklı ve kendine has doğası itibariyle 21.yüzyılda devletlerin ulusal güvenlik problematiğinde en güncel ve yeni bir konu olarak gündemde yer işgal etmektedir (Weimann. 2005). Ulusal ve uluslararası sistem kendini bu yeni ve klasik araçlarla üstesinden gelinemeyen tehdit ve muhtemel savaş ortamına karşı adapte etmelidir. Ancak, farklılık arzeden bu yeni terör biçimine karşı ulusal ve uluslararası düzeyde geliştirilecek ve benimsenecek stratejik güvenlik politikalarına değinmeden önce hâlihazırda üzerinde oybirliğine varılamayan terörizm kavramını ve bu kavrama ilaveten siber ön ekinin eklemlenmesiyle beraber karmaşıklığı daha da artan siber terörizm kavramını açıklamak daha elzemdir.

Terörizm kavramı tanımlanmadan ve anlamlandırılmadan siber terörizm kavramı da tam olarak anlaşılmasını zorlaştıracaktır. Bu nedenle terörizmin kurucu unsurlarını ihtiva eden muhtelif türlerini ve yöntemlerini idrak etmeden yapılacak olan analiz ve retorikler terör gruplarının siber ortamı kötüye kullanımını ve suiistimalini tam anlamıyla noksan kalacaktır ve siber terörizme dair var olan karmaşıklık algısını daha da artıracaktır. Bundan dolayı, geleneksel terörizmin amaçları, yöntemleri ve araçları gibi kurucu nitelikteki elementlerini siber terörizm kavramına uyarlamadan, klasik terörizmin siyasi yönelimlerini ve bünyesinde

bulundurduğu ana ögeleri saptamadan, dünyanın her yerinde çeşitlenen ve farklılaşan nitelikte ve nicelikteki terörist aktörlerin farkına varmadan ve bununla ilişkili olarak bu terör örgütlerinin bin bir türlü tefrikleşen amaçlarını saptamadan siber terörizm kavramı tam olarak anlaşılmayacaktır.

Genel çerçeve de terörizmin gerçek gücü ve etkisi adeta şiddet aracılığıyla yasallaşan korkudur. Bu nedenle terörizm bir eylemdir ve tanımlanmaya bu şekilde başlanmalıdır (Flemming ve Stoil, 2000, Kalay, 2013: s-1). Terörizm, daha geniş kitleler nezdinde yankı uyandırmak gayesiyle insanların, grupların ve toplumların korku ve endişelerini araç olarak kullanıp kasıtlı olarak icra edilen eylemler bütünü şeklinde tanımlanabilir. Beşeri, sosyal ve siyasal birimlerin günlük ezberlerinde ve pratiklerinde genelde iki ana motivasyon yön verir; mutluluğun ve hazzın peşinde koşma ve de acılardan ve ıstıraplardan kaçınma. İşte, terörizminde odak noktası da şiddet uygulayarak bahse konu birimlerde dehşet korkusu salmayı hedeflemiştir (Richardson, 2006: 3-4, Zarakol, 2011: 2311-2113).

21. yüzyılda devletler düzeyinde terörizm kavramına ulusal güvenlik ajandasında belki de en üst düzeyde yer veren ülke -özellike 11 Eylül saldırıları sonrası geliştirdiği "terörizmle savaş" bağlamında- olan ABD'nin anayasasının 22. maddesinde terörizm devlet altı gruplar ya da korsan failler tarafından çoğunlukla kitleler nezdinde yankı uyandırma saikiyle sivillere (non-combatant) yönelik siyasi motivasyonlarla planlanan ya da önceden tasarlanan şiddet kullanma yöntemi olarak tanımlanmıştır (Kallberg ve Thuraisingham, 2014: 19-31, Aning, 2010: 7-26). ABD'nin yapmış olduğu terörizm tanımlamasının olmazsa olmazı siviller kavramıdır. Yani siviller (non combatant) teröristler tarafından hedef (target) alınmaktadır. Terörist gruplar masum sivilleri hedef alırken aynı zamanda toplumu hedef aldıklarından sivil ya da savaşan arasında fark gözetmezler (World Islamic Front, 1998). Birleşmiş Milletlerin Güvenlik Konseyinde ise daimi terör atmosferi oluşturmak niyetiyle bir insan veya insanlar grubu tarafından politik amaçlarla niyet edinilen ve bu doğrultuda girişilen, aynı zamanda meşruluğunu vazetmek için de politik, ideolojik, ırkçı, etnik, dini ya da diğer somut ve soyut formel kavramlar kullanılabilen ve hiçbir surette ve koşulda masum karşılanamayacak suç unsuru

oluşturan eylem ve davranış biçimi şeklinde tanımlamaktadır (Briefing European Parliamentary Research Service, 2015).

Fransa kanunları terörü, baskı veya tehdit yoluyla, mevcut kamu düzeninin önemli derecede bozulması amacıyla bireysel ya da toplu olarak eylemde bulunulan herhangi bir faaliyet olarak tavsif ederken, İngiltere Terörle Mücadele mevzuatı ise terörü siyasi kurumlara karşı şiddet kullanımı veya toplumun çeşitli kesimlerinin korku içinde bırakılması amacıyla şiddet kullanılması şeklinde tanımlama yolunu tercih etmiştir (Balcı, 2013: 502).

Alexandera kavramı organize terör gruplarının siyasal ereklerine erişme maksadıyla tehdit etme ya da her zaman hissedilebilen korku ve dehşet unsuru oluşturabilmek için sıradan sivillere yönelik kullandıkları ve uyguladıkları şiddet eylemeleri şeklinde tanımlamıştır. Bununla birlikte kavramı tarihsel perspektiften de değerlendiren Alexandra'ya göre terörizm 1960'lı yıllardan sonra özellikle hızlı teknolojik gelişmelerin yaşanmasıyla birlikte gelen iletişim, haberleşme ve ulaşımın terör gruplarına rahatça ve kolayca uluslararası ve ulusal düzeydeki etkinliklerde bulunmalarına fırsat verdiğini dile getirmiştir. Tıpkı Wilkinson gibi Alexandra'ya göre de uluslararası ilişkilerde terörizme dair sorunlar ve konular uluslararası hukuk bağlamında ancak 1963 yılında değerlendirilmeye başlanmış ve 1970'li yılların ilk dönemlerinde uluslararası anlaşmalarca onaylanıp kabul görmüştür (Alexander, 2002, 4-22, Wilkinson, 2006).

Bir başka tanımlamada Jenkins grupların şiddet tehdidinin, bireylerin şiddet içeren eylemlerinin, öncelikli olarak korkuyu aşılanmasına yönelik şiddet içeren kampanyalara terörizm denebileceğini dile getirmiştir (Jenkıns, 1978: 115-123). Ergil ise terörizmi kaçırmadan öldürmeye kadar uzanan ve gayesi yıldırma olan şiddet eylemleri şeklinde nitelerken (Ergil, 1980: 1) uluslararası terörizm adlı bir başka çalışmasında daha geniş ve kapsamlı çerçevede ele aldığı kavramı terörizmin, saldırılan, veya korkutulan sivil ve masum kurbanlar aracılığı ile hedeflenenden daha büyük bir kitleyi yıldırıp, korkutarak, yasa-dışı stratejik ve siyasal amaçlarını gerçekleştirmeksizin bir grubun veya devletin, bilinçli ve planlı bir biçimde şiddet kul1anması veya şiddet kullanma tehdidinde bulunması şeklinde tanımlamıştır.

Terörizm kavramının tanımına dair yapmış olduğu istatiksel çalışmada Schmid kavramın yüzlerce farklı türde ve anlama tanımlamasının yapıldığını ve bunların yüzde ellisinden fazlasının "politik" ve "korku ve dehşet" (fear and terror) sözcüklerini içerdiğini belirtmiştir (Schmid, 1998, Weimann and C. Winn, 1994). Yine Schmid'in verilerine göre özellikle yakın dönemlerde kavram şiddet ve şiddet kullanma tehdidi üzerinden tanımlanma yoluna gidilmiştir (Schmid, 1988: 1-7).

Terörizmin tanımlanmasına dair uluslararası düzeyde ve entelektüel camiada ihtilaf ne kadar yüksekse siber terörizmin tanımlanmasına yönelik ihtilaflarda o kadar yüksektir. Ancak yine de siber terörizme dair yapılan tanımlamalar ve ileri sürülen bulgular en nihayetinde üst küme konumundaki geleneksel terörizmin niteliklerinin siber ortamda hangi şekillerde tecessüm ettiğinin ortaya konması tanımlamayı kolaylaştırmaktadır. Sonuçta siber ortamın yeni ve ileri seviyedeki teknolojik araçlarına erişebilen ve sahip oldukları bu teknolojileri araç olarak kullanabilen terör grupları politik bir gaye ve korkutulması hedeflenen bir kamuoyu kitlesi gibi amaçlarını eylemlerini gerçekleştirebilirler. Siber terörizme ve tehditlerine ilişkin göze çarpan ezber bozucu okuma yeni yüzü ve boyutlarıyla bilinemezliği ve bilgi yoksunluğu ya da daha da kötüsü haddinden fazla yanlış ve manipüle edilebilen bilgi ve bilgilendirme sorunudur. Öncelikle geleneksel manadaki terörizm ile siberin birleşimi olan siber terörizm bu minvalde kayda değer boyutlarda bilinemezlik arzeden teknolojiden ve terörizmden kaynaklı iki önemli modern korku biçimini aynı çatı altında toplamaktadır. Farklılaşan nitelikleri ile bu tehditler yakın dönemde bilinen tehditlerden daha ileri düzeyde tehditkâr olarak algılanabilmektedir (Colarik, 2006: 15-28, Archer, 2014: 631-636, Rathmell, 1997: 40-45).

Aslında siber terörizm kavramı özellikle 21.yüzyılın başından günümüze değin uluslararası yazılı ve görsel basında yer almış ve bu süre zarfında da sürekli güvenlik tehditleri sıralamasında ve algısında üst sıralarda yer almıştır (Conway ve Weimann, 2011: 765-769, Cox, 2015: 31-36). Küresel medya özellikle kritik altyapılara yönelik potansiyel felaket getirici tehditleri geçmişte yaşanan trajedilerle benzeşimler kurarak göz alıcı hikâyelerle meseleyi irdelemeye çalışmıştır. Siber terörizm nitelendirilmesi de 11 Eylül'den itibaren ABD basınında sıklıkla vurgulanmış ve kavram neredeyse basit hekleme suçundan, ciddi finansal zararlara sebep olan siber

saldırılara, olası yaralamalara ve ölümlere sebep olmaya kadar her vaka ve gelişme hemen hemen siber terörizm olarak adlandırılmıştır (Conway, 2005; Conway, 2008; Final Report, 2014). Bu durum kavramın anlaşılır ve tutarlı bir tanımlama çerçevesini oluşturmada birtakım engeller yaratsa da şüphesiz hatırı sayılır medya ilgisi -sayısız güvenlik raporlarının sunduğu avantajlarla- bahse konu varsayımların incelenmesinde ve siber terörizmin telaffuz edilmesinde önemli bir rol oynamıştır.

Siber terörizme ilişkin yapılan birbirinden farklı çalışmalarda bireysel olsun ya da bir grup tarafından olsun bilişim sistemleri kullanıcıları devletler tarafından ciddi tehdit unsuru oluşturabilmekte ve siber terörizm başlığı altında başa çıkılması gereken elzem konuların başında gelebilmektedir (Denning, 2001; Burton, 2015: 303-313). Çünkü, devletler siber terörizm tehlikesi altında egemenliklerinin aşınıma uğradığını dahi ileri sürmekte iken, bir diğer taraftan bu sava konuyla ilgili uzmanlar ise siber terörizmin medyanın herhangi bir verilere dayanmadan salt reyting odaklı yaklaşımlarının sorunu büyüttüğü ve dolayısıyla nesnellikten uzaklaştırdığını iddia ederek ampirik gözlemlerle ele alınmasının gerektiğini ileri sürmüşlerdir (Conway, 2005: 5-7; Choucrı ve Clark, 2012: 25-49; Betz ve Stevens, 2011; Klimburg, 2012). Yine Conway'a göre modern dönemin ulusal güvenlik konsepti iletişimsel olarak doğmakta ve medyanın merkezi rolü bu doğuşta önemli bir paya sahiptir. Çünkü politik tehdit algı/imaj yaratma ortamı hem bilginin açıklığını ve elverişliliğini hem de sıradan insanların bu bilgiyi ve bilgi ortamının yöntem ve tarzının ulusal güvenliğe ve politikasına dair endişelerini ve kaygılarını artırmada etkili bir araç olarak kullanılmaktadır (Conway, 2005).

Buradan hareketle, teorik çerçevesi çizilmeden komplovari bir temele dayanan ve farz edilen tehlikeler ile siber terörizm olarak kabul edilecek etkinlikler arasındaki kurgusal ve semantik boşluk siber terörizm etrafında dönen tartışmaları daha da tetiklemektedir; Örneğin, bazıları siber ortamın teröristler için devletlere yönelik yeni bir dijital Pearl Harbor tehlikesi oluşturan realist bir senaryo arz ederken (Sınger ve Friedman, 2014; Gartzke, 2013: 60-73, Libicki, 2014: 38) öte yandan karşıt bir diğer grup ise geleneksel terörizm yöntemlerinin ve motivasyonlarının kısmen siber terörizmde de gözlemleneceğini belirtmekle birlikte "dijital Pearl Harbor" şeklindeki analojilerin abartılı bulunduğunu ve bu senaryo şeklinde ileri sürülen tehditlerin

kavramın ciddiyetine ve kuramsallığına zarar vereceğini ileri sürmüşlerdir (Denning, 1999: 67-70, Weiman, 2004).

Siber terörizm kavram olarak ilk defa 1990'li yıllarda Barry Collin tarafından dile getirilmiş ve derinlemesine bir tanım olmasa da kavram siber ortam ile terörizm terimlerini yakınlaştırma amacıyla kullanımda ilişkilendirilmiştir (Collin, 1996: 1). Collin'e göre siber terörizm uluslararası ortamda bilgi sistemlerinin, network ağlarının tüm bileşenleri ile teröristlerce kötüye kullanımı şeklinde tarif edilmiştir (Collin, 1996). Collin'den sonra kavram uzmanlar tarafından güvenliğin sözlüğüne dâhil edilmiş ve literatürde tedricen adından söz ettirmeye başlamıştır. Collin'in dar kapsamlı bu tanımlamasından sonra genel anlamda kabul gören ilk tanımlamalardan biri olan 1998 yılı Center for Strategic and Internatıonal Studies kuruluşunun raporu ise önceden planlanan devlet altı gruplar ve yahut ta bireyler tarafından bilgi ve bilişim sistemlerine, bilgisayar programlarına, veri tabanlarına yönelik şiddet hadiseleri ile sonuçlanmayı hedefleyen ve savaşçı olmayan birimlere yönelik yasadışı tehdit ve hasar verici saldırılar olarak tanımlamıştır (CSIS Global Organized Crime Project, 1998).

Öncelikle devletler bazında siber terörizm kavramını terörizm yasasında ilk yer veren ülke İngiltere olmuştur. İngiltere'nin terörizm yasasına göre siber terörizm hükümeti ve toplumu etkilemek ya da baskı oluşturma saikiyle resmi birimlerin elektronik sistemlerine sızmak ve saldırılarla sisteme bozmak şeklinde tanımlanmıştır (United Kingdom Terorism Act, 2000). En basit anlamıyla bilgisayar ve bilgisayar sistemleri kullanılarak gerçekleştirilen saldırılar şeklinde tanımlanan siber terörizm gün geçtikçe bu tanımlamanın parametrelerini aşmış ve geleneksel terörizm kavramının temel unsurlarını da ihtiva ederek kapsamını genişletmiştir. Farz-ı mahal 2000'li yılların ortasında yapılan bir başka tanımlamada kavram bir örgüt tarafından politik, psikolojik, sosyo-ekonomik, prestij ve de en önemlisi güvenlik tehdidi oluşturma gayesine erişmek maksadıyla bilişim sistemlerinin devlet kurumlarına yönelik olarak yıldırma, göz dağı verme ya da baskı altında tutmak amacıyla kullanılması minvalinde tanımlanmıştır (Sever, 2006: 2). ABD'nin iç istihbarat ve güvenliğinden sorumlu FBI'n tanımında ise siber terörizm iletişim ve bilişim imkanları dahilinde bilgisayar kullanıcıları tarafından hükümetleri ya da

toplumu belirli politik, sosyal ve ideolojik gündemlerine intibak ettirmek için kamu hizmetlerini sağlayan kritik altyapı sistemlerine yönelik bozma ya da işleyişi durdurma niyetiyle ve bunun sonucunda toplum içerisinde karmaşıklığa sebep olarak bir korku yaratma eğilimindeki suç teşkil eden fiiller olarak tarid edilmiştir (Lourdeu, 2005). Colarik'de siber terörizmin küresel bilgi altyapısına yönelik saldırıları içermesi gerektiğini belirterek teröristlerin bu bilgi altyapılarına saldırarak sadece korku değil aynı zamanda şiddet iklimini sürekli kılmayı planladıklarını belirtmiştir (Colarik, 2006: 15).

Geleneksel terör mantalitesinin bir türü olarak kabul gören anlayış doğrultusunda siber terörizm politik güdülere sahip grupların bilgisayar, bilgi, gelişmiş ağlar ve teknolojik altyapılar kanalıyla yıkıcı ve kötü niyet barındıran eylemlerini yerine getirmek için kullandıkları bir terör türüdür. Bilişim sistemleri ve internet vasıtasıyla idare edilen bu kritik öneme sahip temel unsurlar göz önünde bulundurulduğunda birçok uzman siber terörizmin 21.yüzyılda geleneksel bağlamdaki terörizmden daha tehlikeli hal alabileceğini ileri sürmektedir (Councıl of foreign Relaıons, 2004; Rogers 1999, Verton, 2003, Ryder ve Lynch, 2012: 264-265). Bu bağlamda gerçek şu ki, siber terörizm eylemleri ile ilgili hedefler ve riskler hükümetlerin değerli kayıtlarına, hava trafik kontrollerine, barajların kontrollerine, tıbbi kayıtlarına ve de finansal ve ticari altyapılarına yönelik oluşturmaktadır (Hansen ve vd., 2007: 1362-1374, Gordon, 2015: 36-43, Einar, 2007).

Yukarıdaki tanımlamalar ışığında siber terörizme dair gözlemlenen okuma, eylemlerin politik ve sosyal motivasyonları barındırması ve hedef olarak da bilgisayar, network ağları ve bilgi sistemleri şeklinde lanse edilmesi, amaç olarak da yaralama, ciddi hasar, korku iklimi ve ölüme sebebiyet verme gibi hedef odaklı güdüleri ihtiva etmiş olmasının gerekliliği üzerine yapılan vurgulardır. Maras da hedef odaklı yapılan tanımlamalardan hareketle siber teröristlerin politik, dini ve ideolojik sebeplerden dolayı devletlerin gözünü korkutma ya da onları amaçları doğrultusunda zorlama veçhilesi için kritik altyapılara saldırmayı hedeflediklerini belirterek siber terörizme dikkat çekmiştir. Bu nedenle 21.yüzyılın bu yeni tehdidinin ABD'nin ekonomik unsurlarına zarar vermek için kritik altyapılarını hedef alabileceğini ve yaşam kayıplarına bile sebebiyet verecek cinste olduğunu

belirtmiştir. Öte yandan Marasa göre siber ortamdan kaynaklı bireylerin ya da organize olmuş terör gruplarının gerçekleştireceği her eylemin ya da saldırının siber terörizm teşkil etmeyebilir. Conway ile beraber Maras siber terörizmin ortak tanımlamalarında akla ilk gelen noktalarının yıkıma ve hatta ölüme sebep olması gerektiği ve politik ve sosyal güdülerle eyleme dökülmesi gerektiğini ifade etmiştir (Maras, 2015: 6-8; Conway, 2002: 2). Bu durumda Maras ve Conwayın ifadelerine göre siber terörizmin başlı başına büyük ölçekli yıkımlara ya da ölümlere sebebiyet veren gelişmeler olması durumunda terörizm kategorisine dâhil edilebilir.

Dorothy Denning'de tam olarak hangi eylemlerin ve saldırıların ya da yapılış usullerinin siber terörizm kategorisinde yer alabileceğini belirttiği çalışmasında kavramı şu şekilde tanımlamıştır.

"Siber terörizm genel olarak bilgisayarlara, ağlara ve buralarda gizli tutulan bilgiye yöneltilen kanun dışı saldırı ve de saldırı tehditlerinin siyasi ya sosyal amaçlara erişmek saikiyle bir hükümet ya da çalışanlarına baskı yapmak ve gözdağı vermek maksadıyla yapılması şeklinde anlaşılmaktadır. Buna ilaveten, bir saldırının siber terörizm olarak nitelendirilebilmesi için kişiler ya da mala karşı şiddetle sonuçlanması ya da en azından korku yaratacak kadar zarar verici olması gerekmektedir. Ölümle ya da yaralanma ile neticelendirilen saldırılar, patlamalar, uçak kazaları, su kirlenmeleri ve ciddi ekonomik kayıplar misal olarak gösterilebilir. Kritik altyapı sistemlerine karşı yapılan saldırılar etkilerine bağlı olarak siber terörizm şeklinde adlandırılır. Hayati önemi olmayan hizmetlere yönelik akamete uğratıcı ya da çoğunlukla düşük profilde rahatsızlık veren saldırılar siber terörizm olarak adlandırılmaz" (Denning, 1999: 269).

Denning'in bu tanımlama ve yorumlaması öte yandan siber terörizmin kavramsallaştırılmasına zarar veren karmaşıklığın giderilmesinin de kahır ekseriyette yolunu açmıştır. Çünkü Denning siber teröristler ile kötücül korsanlar, bilgisayar ortamında haşarı olarak (prankster) nitelendirilenler, kimlik hırsızlığı yapanlar, sanal zorbalar ya da casuslar arasında amaçları ve motivasyonları bakımından ayrım yaparak sınıflandırmıştır (Denning, 1999: 9). Denning ve Maras'ın çizmiş olduğu kavramsallaştırma siber terörizmin politik, sosyal motivasyonları ve aynı zamanda ciddi hasar vermesi ve korku iklimi yaratma gibi geleneksel terörizm pratiklerine istinaden tanımlanması ve sınıflandırılması gerekmektedir.

Yine Denning'in siber terörizmin tanımlamasına ilişkin çizmiş olduğu bir diğer önemli parametre ciddi hasar verme ölçütüdür. Buna göre bir eylemin siber terörizm

olarak adlandırılması için politik ve sosyal motivasyonları içermesinin yanı sıra geleneksel terörizmde olduğu gibi korku ve kaos ortamı yaratmak için büyük ölçüde de ciddi hasara yol açma koşulunu içermesi gerekmektedir. Elektrik üretim tesisleri, haberleşme sistemi, su üretim sistemi, petrol ya da doğal gaz üretim sistemi ve de finansal kuruluş gibi kritik altyapılara ait ciddi derecede yıkıcı ve işleyişi durdurmaya yönelik saldırılar siber terörizm dâhilinde değerlendirilebilmektedir. Benzer argümanla Brenner'de terörizm bağlamında değerlendirdiği hasar verme ölçütün halkın moralini ve psikolojisini bozma niyeti olarak ele almıştır. Böylelikle teröristler maddi ve manevi değerleri tahrip etmeye, yaralanma ya da ölüme sebebiyet vererek öncelikli ve doğrudan doğruya temel motivasyonlarından biri olan hedef ülkenin halkına saldırıya açık halde olduklarını gösterme amacındadırlar. Brenner'de bu noktada, tıpkı klasik terörizm anlayışında olduğu gibi siber terörizminde benzer amaçlara ulaşmayı hedeflediğini ancak bunu yaparken tarz olarak toplumun bu modern dönemde önemli derecede işleyişine bel bağladığı bilgiye ve bilgi sistemlerine olan güveni sarsmak için yine teknolojiyi kullandıklarını iddia eder (Brenner, 2007: 386). Bu doğrultuda 1998 yılında ABD'de yazılımları manipüle edip elektrik sistemlerine saldırılar gerçekleştiren ve 11 kişinin ölümüne sebep olan saldırı türü siber terörizme en çarpıcı ve açık bir örnek teşkil etmektedir.

Daha önce de bahsi edildiği üzere siber uzay muhtelif devlet dışı aktörlerin politik amaçlı saldırı ve eylemlerini icra etmelerinde ve propaganda amaçlı seslerini duyurmada popülerleşmeye başlayan önemli muharebe alanı olmaya namzettir. Özellikle Estonya merkezli NATO kuruluşunun yayınladığı 2009 yılı raporuna göre uluslararası ilişkilerde devlet dışı aktörlerin gün geçtikçe artan etkisi ve gündem belirlenmesinde kimliklerini gizleyerek gerçekleştirmiş oldukları siber ortamdan kaynaklı siber saldırılar ve network sızmaları önemli rol oynamaktadır. 2007 Estonya saldırısı ve 2008 Gürcistan saldırıları sadece buna verilebilecek bir kaç örnekten biri olabilir (Klimburg, 2012).

Yakın zamana değin politik güdülerle gerçekleştirilen ve herkesçe bilinen en popüler siber saldırı 2007 yılındaki Estonya'daki saldırısıdır (Kozlowski, 2014: 237-238, Saleem ve Hassan, 2009: 1-8). Bu saldırıda bilgisayarları ve bilgisayar sistemlerini hedef kullanıcı kitlesinin kullanmasını engellemek için yapılan DDOS

saldırı yöntemi kullanılmış ve Estonya hükümet kurumları, bankalar, medya kuruluşları ve özel şirketlerin web siteleri çalışamaz hale gelerek ülke içinde birçok işlev de çalışamaz hale gelmiştir (Russell, 2014: 15-48, Shackelford, 2009: 205-209). Rusları Nazi işgali sırasında kurtardıkları Estonya'da kurdukları Kızıl Ordu anıtının kaldırılması üzerine takriben bir ay süren siber saldırılar her ne kadar ispatlanamamış olsa da NATO nezdinde bir takım bulgular nedeniyle Rus istihbaratının ve saldırganlarının politik güdülerle bu eylemi gerçekleştirdiği düşünülmüştür (Shackelford, 2009: 205-209).

Bununla birlikte, siber terörizmin geleneksel terörizmin teorik konsepti ile uyumlu olan bir diğer önemli parametresi de korku unsurudur. Bu bağlamda, korku unsuru tıpkı geleneksel terörizmde olduğu gibi siber terörizm kavramı etrafında da ele alındığında etki odaklı ve niyet odaklı şeklinde tanımlama yapılabilmektedir. Buna göre, etki odaklı tanımda siber terörizm bilişim sistemlerinden herhangi biri aracılığıyla gerçekleştirilen ve yeterli düzeyde yıkıcı etkiye sahip saldırılar sonucunda oluşturulan korku havası şeklinde tanımlanırken, niyet odaklı tanımlamada ise siber terörizm yasa dışı ve politik saiklerle devletleri ve bu devletlerin toplumlarının gözünü korkutmak ya da bu birimleri kendi siyasal, ideolojik ve sosyal hedeflerine erişmede kabule zorlamak için bilişim sistemleri aracılığıyla gerçekleştirilen yasa dışı eylemlerdir şeklinde tanımlanmıştır (Wilson ve Rollins, 2007).

Belki bahse konu bu iki tanımlama geleneksel terörizm çerçevesinde sadece korku iklimi üzerine odaklanması hasebiyle basitleştirilmiş bir tanım olarak gözlemlenebilir. Ancak siber terörizm önemli bileşenlerinden olan korku unsuru iki açıdan ele alınmalıdır. İlki, korku ve karışıklığın siber terörizmin salt doğası gereği her zaman seviye ve boyutlar bakımından birbiriyle uyuşmayan özelliklerinin neticesinde ortaya çıkmış olmasıdır. Çünkü siber terörizmden neşet eden tehditlerin gözle görünür çarpıcı özelliği bilinemezlik, bilgi eksikliği ya da yanlış bilgilendirilme korkusudur. Bu durumda siber terörizm nosyonu hem teknolojinin hem de bu teknolojilerden kaynaklı terör tehditlerinin kayda değer bilinmezlikleri içerdiğinden yakın dönemde teknolojiden ve bununla ilişkili olarak terörizmden zuhur eden iki önemli korkuyu beraberinde getirmiştir (Weımann, 2005: 129-131).

İkincisi ise, gittikçe artan oranda devletlerin ve toplumların teknolojiye olan bağımlılığı büyük çaplı siber saldırıları durumlarında önemli derecede kaos ve hayatların idamelerini ve yönetimleri üzerindeki kontrol kaybına sebebiyet verebilmektedir. Her halükarda korku yaratma, kaos ve karışıklık siber terörizmin temel amacıdır (Choucri vd., 2014: 96-121).

Hasılı yukarıda kavramsal ve niteliksel özellikleri çizilen siber terörizmin hem geleneksel terörizme kıyasla hem de kendine has sunduğu olanaklarla kötücül niyetler barındıran birimlerin ilgi duymasının nedenleri oldukça fazladır. Öncelikle siber ortamın finansal ve de beşer bakımından daha az maliyetli olması, ileri derecede teknolojik araçların kullanımına ihtiyaç duyulmadan (kimi zaman bir cep telefonu, kimi zamanda tablet, laptop vs.) metotların daha kolayca uygulama alanı bulması, failler için kimliklerinin isnat edilemezliği, aynı anda birden fazla hedeflerin kısa sürede hedeflenebileceği, saldırının tür olarak yeniliği ve dolayısıyla çekiciliği hasebiyle basında ve görsel medyada daha rahat ve etkili propaganda şansı vermesi gibi etmenler terör gruplarına amaçlarına ulaşmada ihtiyaç duydukları ortamı sağlamaktadır.

2.2.4. Siber Savaş

Doktrinsel argümanlarda, savaş siyasal süreçlerden çokta farklı ve otonom bir fenomen değil aksine meselelerin üstesinden gelmede devletlerin politikalarını başka yöntemlerle idame ettirmede bir araç olarak kullanılma şeklinde tanımlanmaktadır (Clausewitz, 2003: 13). Bu minvalde Tilly'de "*devletler savaş yapar çünkü savaşlar devletleri kurar*" diyerek bir nevi savaşın devletlerin kurulum aşamasındaki önemine atıfta bulunur (Goldstone, 1991: 176-178). Savaş kavramı Westphalian düzen sonrasında tek siyasal model olarak tebarüz eden devlet mottosu ile birlikte, devletlerarasındaki ilişkileri ve davranış biçimlerini düzenleyen kurallar bütünü olarak tarif edilen uluslararası hukuk (Pazarcı, 2014: 4) çerçevesinde de tanımlanmıştır. Buna göre savaş birden fazla devletin birbirlerine karşı kabul ettirmek istedikleri istekleri ya da siyasi ve ekonomik saiklerle devletler hukuku vasıtasıyla düzenlenmiş kurallar çerçevesinde yaptıkları silahlı mücadeledir. Bu noktada savaş fenomeninin değişmeyen özüne dair ileri sürülebilecek yegane sav

kavramın geçmişte olduğu gibi gelecekte de yeri geldiğinde bir politik enstrüman olarak yeri geldiğinde de bir güvenliği korumak amaçlı varlığını koruyacağıdır (Taylor ve Botea, 2008: 3-8). Çünkü anarşik ortamın kuralsızlığında devletlerin birbirleriyle savaş yapma olasılığı her daim olasıdır.

Ancak, teknolojik gelişmeler, uluslararası güvenlik ortamında giderek görünürlüğü ve etkinliği artan devlet dışı aktörler, küreselleşme gibi nedenlerle geleneksel anlamda ulus-devletlerin tekelindeki en acımasız politik araç olarak görülen savaş olgusunun sorgulandığı yeni bir döneme girilmiştir (Gürcan, 2011: 131). Kavram düzeyinde savaş fenomeni tarihsel süreçte her dönemin kendine has koşullarının ve bağlamının gerektirdiği bir bilgi türünü tecessüm ettirmiştir. Bu bağlamda klasik olarak birincil güvenlik tehdidi şeklinde algılanan savaş olgusu artık siber uzaydan kaynaklı yeni savaş araçları ve nitelikleri ile güvenliğe yönelik de yeni tehditleri barındırmıştır (Libicki 2009: 117-179). Bu nedenle geçmişte gözlemlenen devletlerin ulusal güvenlik tehditlerine yönelik olası savaş durumları artık farklı amaçları, stratejik hedefleri ve araçları ile tehdit oluşturan yeni savaş türlerini de güvenlik gündemlerine dahil etmektedirler (Arquilla ve Ronfeldt, 1993: 41-55, Lind, vd., 1989: 22-26).

21.yüzyılın yeni savaş türü eskiye oranla savaş durumu ile barış durumu arasındaki muğlaklığı daha belirgin olmakla beraber nitelik bakımından da asimetrik savaş, terörizm ve gayri nizami harp gibi unsurlarla farklı kılmaktadır. Güçlü güçsüz ayrımı gözetmeksizin hem devletlerin kendi aralarında hem de devlet altı grupların devletlere yönelik asimetrik savaş aracılığıyla statüko güçlerini zayıf düşürebileceği savaş türlerinden biri de siber savaş ihtimalidir. Kimilerince teknolojideki gelişmeler ve bilgisayar sistemlerinin kullanımındaki artışların sonucunda deniz, hava, uzay ve karadan sonra yeni bir hareket alanı olarak ortaya çıkan siber uzaydan kaynaklı teknolojiler yeni güvenlik tehditlerini meydana getirmiş ve bu tehditlere yönelik verilecek reaksiyonların neticesindeki eylemler siber savaş olgusunu 21.yüzyılda ortaya çıkarmıştır. Bu yeni savaş türü klasik savaşı ortadan kaldırmamakla birlikte şeklini ve niteliğini dönüşüme uğratma potansiyeline fazlasıyla sahiptir. Çünkü geleneksel savaşın yöntem ve metotları bakımından karşılaştırıldığında siber savaş; Saldırının nereden geldiğini tespit etmek bakımından zor ve hata bazen imkânsızdır,

Işık hızındadır, çoğunlukla bilgi ve iletişim sistemleri alanından etkilidir, savaşanlar bir kişi, bir grup bir örgüt veya bir devlet olabilir, maliyet olarak genelde ucuzdur. Bir bilgisayarla etkili olmak mümkündür, çipler bilgisayarlar veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar en büyük silahlardır, çoğunlukla çok yüksek teknik ve teknolojiye ihtiyaç duyulmamaktadır, saldırı belirtileri açısından saldırının farkına varılmayabilir ve son olarak nerede ve ne kadar hasar oluştuğunu tespit etmek çok zordur (Çiftçi, 2012: 20).

Bu hususlar ışığında 21.yüzyılın dördüncü nesil savaş türünden biri olan siber savaş klasik savaşların şeklini değiştirmiştir. Cephe kavramını artık mekânsal bir olgu olmaktan çıkaran bu savaş türü siber dünya da en önemli savaş cephelerinden biri haline gelmiş ve özellikle hem barış ve kriz hem de savaş dönemlerinde çok boyutlu olarak icra edilebilen bilişim altyapılarını tahrip edici sabotajlarla hasım gücü itibarsızlaştırmak, moral gücünü zayıflatmak, yine gizli sızmalarla istihbarat toplamak amacıyla icra edilen siber saldırılar yeni nesil savaşın önemli parametrelerinden biri haline gelmiştir (Gürcan, 2011: 166). Yöntem, amaç ve araçlar bakımından geleneksel savaş kavramının içeriğindeki dönüşüme farklılaşan yönleri ile farklı boyutlar ekleyen bu savaş türü asimetrik olarak da ifade edilmektedir (Bıçakçı, 2012: 214, Pehlivan, 2013, Blank, 2003: 25-32, Josan ve Voıcu, 2015: 50-52). Çünkü savaş stratejileri bakımından güçsüz konumdaki birimlere ve devletlerin ihtiyaçlarına göre uyarlanma temayülündeki teknolojik yenilikler yüksek teknolojiye haiz bir düşman devlete kayda değer bir şekilde teknolojik yöntemlerle güvenlik tehdidi oluşturma olanağı sağlamaktadır. Çünkü siber uzaydan kaynaklı savaşlarda gerek duyulacak olan savaş tekniklerini icra edebilmek için güçlü ve de finansal olarak zengin olmanıza gerek yoktur (Libicki, 2012: 329-335). Bu durum da doğal olarak zayıf devletlerin ve terör gruplarının teknolojik bağlamda güçlü ve gelişmiş devletlerden belki de daha hızlı siber savaşı benimsemelerine sevk etmektedir.

Günümüzde de hem devletlerarasında hem de farklı birimlerin devletlerle olan asimetrik savaşlarda bilişim sistemlerine araç ve amaç olarak kullanma popüler hale gelmiştir. Çünkü siber uzayın kendine özgü anarşik doğası asimetrik bir savaş durumunda devlet ötesi gruplara asimetrik cepheler açma fırsatı vermektedir

(Chansoria, 2012: 105-110, Hughes, 2009: 19-21; Warner ve Good, 2013; 65-72). Öyle ki, iyi derecede organize olunmuş ve planlanmış bir siber saldırının neden olacağı etkinin ve yol açacağı yıkımın en az klasik bir savaşınki kadar yıkıcı ve öldürücü olabileceği gerçektir (Ege, 2012: 18-22). Ve hatta Çifçi'ye göre de askeri harekatlarda daha etkili olabilmek için operasyonel siber savaşların geleneksel askeri harekatların yerini alıp almama konusunda da tartışmaların yaşandığı gerçektir (Çifçi, 2013: 19). Derian'a göre de taklit ve simülasyona ait yeni teknolojilerinin yanı sıra izleme ve takip yetenekleri ve hız; gerçek ve sanal savaş arasındaki alanı, coğrafi mesafeleri ve kronolojik süreyi kısaltması savaş kavramının bilinen anlamından öte anlamlar taşıyarak gelişmesine neden olmuştur (Derrian, 2000: 771–788). Tabi bu durum yukarıda da bahsedildiği üzere tehditlerin ve savaşların siber aracılığıyla asimetrikleşerek kavramların içeriklerini dönüştürmesi doğru orantılı olarak güvenliği de dönüşüme uğratarak asimetrikleştirmiştir.

Bununla birlikte klasik savaş kavramının tarihsel ve kavramsal evrimine muteber katkı veren Sun Tzu'nun savaşı ya da mücadeleleri savaşmadan kazanmaya dayalı stratejisine atıfta bulunarak siber savaşı tanımlayan Carr'a göre de bu yeni savaş türü, savaşmadan ve düşmanının kanını akıtmadan ona galebe çalma sanatı ve bilimi şeklinde betimlemiştir (Carr, 2012: 2). Ayrıca siber savaşı ulusal hedefi yerine getirmek veya devam eden bir savaşı desteklemek amacıyla bir ülke tarafından ya da inisiyatifinde diğer bir ülkenin askeri ve sivil tüm bilişim sistem ve altyapısının fonksiyonunu engellemek, ortadan kaldırmak ve çıkarlar doğrultusunda kullanmak/istismar etmek için siber savaş metotlarının kullanılması ve bununla ilintili olarak buna karşı alınacak tedbirler veya süreçler şeklinde tanımlamada mevcuttur (Özdemir, 2003: 51). Özdemir'in bu tanımlamasında siber savaş geleneksel savaşlara destek olmada araç olarak da kullanılabilmektedir.

Birleşmiş Milletler terimler sözlüğü de kavramı bilgisayar sistemlerinin düşman sistemlerinde hasar yaratmak ya da sistemlerini ortadan kaldırmak amacıyla icra edilen bir savaş türü şeklinde tanımlamıştır (Department of Defence Dictionary of Military and Associated Terms (Joint Publications 1-02). Bahse konu tanımlamaların ortak özelliği siber savaşın teknolojiye ve bilişim altyapılarına dayanması ve bağlı olmasıdır. Bu durumda bağıtlı bir biçimde devletlerin karşılıklı

birbirlerinin bilişim ağ ve sistemlerini hedefleyerek saldırmalarını olağan hale getirmektedir. Özellikle 21. yüzyılda teknolojik olanakların hızlı ve yoğun bir şekilde gelişmesi ve bu teknolojik araçlara bağımlılığın artması devletlerin milli güvenlik teşkilatlarını askeri kanadında önemli avantajlar yarattığı gibi yine bu teknolojik gelişmeler ve araçları aynı askeri kanada dezavantajlarda yaratmaktadır. Çünkü ülkelerin doğrudan olsun ya da dolaylı olsun -özellikle kritik altyapılar ve sanayi merkezleri- bilişim sistemlerine ve teknolojilerine yüksek sevide bağımlı olması bir savaş esnasında tarafların kullanacağı rasyonel yöntemin hedef ülkenin bilişim sistemlerini, akıllı yazılımlar aracılığıyla elde edip engellemek ya da çökertmek olacağı düşünülmelidir (Ege, 2002).

Pratikte geleneksel bağlamdaki savaş türünü elbette ortadan kaldırmayan bu yeni savaş türü kimi zaman klasik savaşlarda dolaylı katkılarıyla araç olarak kullanılarak kimi zamanda klasik savaşlardan azade bir şekilde farklı bir savaş alanında salt siber savaş olarak ifa edilerek 21.yüzyılda klasik savaşın şeklini dönüştürmeye katkıda bulunmuştur. Çoğunlukla da siber savaş psikolojik ve elektronik harp aldatma, fiziki tahrip, bilgi taarruzu ve güvenlik önlemleri şeklinde de altı eylemi içermektedir (Ülgen, 2003: 192). Hedefler bakımından da devletlerin kamu merkezlerini, bakanlıklarını, stratejik komuta merkezlerini ve bu merkezleri destekleyen birimleri ihtiva eden politik hedefler; fiber obtik ağlar, bilgi işlem merkezleri, ağ ve uydu bağlantıları, finansal merkezler, hava ve kara trafik kontrol merkezleri ve enerji merkezlerini içeren yapısal hedefler ve en nihayetinde de uyarı sensörleri, savunma ve kontrol komuta merkezlerini ve de elektronik silah sistemlerini içeren askeri hedeflerden oluşmaktadır.

2001 yılında ABD Devlet başkanlığına siber güvenlik uzmanı olarak atanan ve bu konuda genel kabul gören tanımlama yapan Rıchard Clarke'ye göre siber savaş bir devletin başka bir devleti bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesintiye uğratmak amacıyla gerçekleştirilen sızma ve nufuz etme faaliyetleri olarak tanımlamıştır (Clarke ve Knake, 2010: 23). Siber savaşı devletlerin faaliyet alanı olarak gören bu tanımlama da temel kıstas karşı devletin sistemlerine hasar verme ve sistemlerin işlevselliğine yönelik engelleyici saldırılar gerçekleştirmektir. Örneğin, Kuzey Korelilerin 2007 yılında Suriye'nin doğusunda inşa etmeye

çalıştıkları nükleer tesisin İsrail tarafından bilişim sistemlerine bağlı Suriye'nin hava savunma sistemlerini aldatmaya ve manipüle etmeye yönelik saldırıları bu tanımlamasına örnek oluşturmaktadır (Clarke ve Knake, 2010). Yine, dünyada en fazla internete dayalı çalışan ülkelerden biri olan Estonya'ya ya yönelik ardı arkası kesilmeyen -kesin olmamakla birlikte- Rus yanlısı vatanseverlerin saldırıları sonucunda Estonya devletine ait kamu kurum ve kuruluşlarının, bankacılık hizmetlerinin, iletişim ve ticaret hizmetlerinin yaklaşık bir hafta çökmesi bir başka siber savaş örneği teşkil etmektedir (Clarke ve Knake, 2010).

Clarke kavramı daha belirgin ve somut hale getirmek için siber savaşın kendine has silahları, yöntemleri ve hedefleri ile gerçekte var olduğunu belirtmiştir. Siber savaşın karakteristiği çizmeye çalıştığı eserinde bu yeni savaş türünü şu şekilde kategorize etmiştir;

- Siber alanda şimdiye kadar gerçekleşen vakalar göstermiştir ki; siber savaş gerçektir ve şimdiye kadar ilkel siber silahlar kullanılmış olup taraflar gerçek yeteneklerini ve silahlarını devreye sokmamışlardır. Bunun nedeni, tarafların ellerinde bulundurdukları yetenekleri henüz göstermek istememeleridir. ABD ve diğer tarafların sahip oldukları gerçek yetenekler kullanıldığında bu saldırıların bir ulusun sonunu getirebileceği konusunda yorumlar yapılmaktadır.

- Siber savaşta, saldırı zamanı ile bu saldırının karşı tarafta yaratacağı etki neredeyse aynı anda gerçekleşmektedir. Bu durum aynı zamanda kriz yöneticilerinin karar alma süreçlerini ve ellerinde bulundurdukları zamanı önemli ölçüde zora sokmaktadır.

- Siber ortamın yapısı ve kullanılan tekniklerin karmaşıklığı, herhangi bir siber anlaşmazlık durumunun kolaylıkla küresel hale gelebileceğini ve birçok devleti bu savaşın içersine çekeceğini göstermektedir.

- Bankalardan savunma radarlarına kadar insanların ihtiyaç duyduğu ve güvendiği sistemler siber ortamdan erişilebilir durumdadır ve bu sistemler hiç kullanılmaya fırsat verilmeden devre dışı bırakılabilmekte ya da kullanılamaz hale getirilebilmektedir (Clarke ve Knake, 2010).

Clarke ve Knake bu türde özelliklere sahip siber savaşın tahmin edilemez sonuçlarının olacağını ve dünyanın askeri dengesini, temel politik ve ekonomik ilişkilerini değiştirme potansiyelinin varlığına işaret etmiştir (Clarke ve Knake, 2010: 24). Nitekim, siber savaşa göre doktrinini değiştiren ve konunun teknik ve hukuki boyutunu tartışan NATO (Yayla, 2013: 180-186), 8-9 Temmuz 2016 Varşova zirvesinde siber alanı tıpkı kara, deniz ve hava gibi yeni bir hareket alanı olarak ilan etmiş ve bu minvalde siber saldırılara da konvansiyonel silahlarla yanıt verilebileceğini duyurmuştur. Bir başka deyişle, değişen güvenlik tehditlerine uyum sağlamak amacıyla atılan bu adım, herhangi bir NATO ülkesinin ciddi boyutlara ulaşan bir siber saldırıya hedef olunması halinde, kolektif savunma öngören NATO'nun 5'inci maddesinin işletilmesine, konvansiyonel silahlarla karşılık verilebilmesine yeşil ışık yakıyor (Sabah, 2016).

ÜÇÜNCÜ BÖLÜM: ORTODOKS GÜVENLİK PARADİGMASININ AŞINIMI: SİBER GÜVENLİK

3.1. Klasik Güvenlik Paradigmasını Aşan Unsurlar

20.yüzyılda bilgi ve iletişimde vuku bulan gelişmelerin 21. yüzyılda devrim çapında ilerlemeye sahne olması bireyden topluma yaşamın her düzeyinde her katmanı farklı yönlerden etkilediği gibi devletlerin de düşünce, algı ve politika yapma biçimlerini etkilemiştir (Weiss, 2003: 107-110, Rosenau ve Johnson, 2012: 40-44). Bilgi teknolojilerinin türediği ve neşvü nema bulduğu siber ortamda her türlü bilgi ve verilerin kolay ve rahat bir şekilde arttığı, erişildiği ve paylaşıldığı atmosferde devletler de teknolojik bağımlılıklarını gün geçtikçe artırmışlardır. Ancak bu durum devletlerin ulusal güvenliklerine yönelik birtakım tehditleri de beraberinde getirmiştir. Çünkü her türlü bilginin ve verinin bilişim sistemleri aracılığıyla yüksek derecede transfer edilmesi, erişilmesi mekân ve zaman gibi hiçbir sınırlamanın olmadığı bu yeni siber ortam bireyden topluma, toplumdan güçlü-güçsüz devletlere kadar birçok siyasal ve sosyal formasyona güç ve fırsatlar bakımından asimetrik bağlamda önemli etkinlik alanı kazandırmıştır. Böylelikle, farklı düzeydeki her siyasal ve sosyal formasyonun etkinlik alanını hiçbir kural, ilke ve hukuki sınırlılığın olmadığı kendine has anarşik özellikleri ile siber ortama kaydırması, bu alana bağımlılığını gittikçe artıran devletler için siber güvenliğide ulusal güvenlik bağlamında ele alınmasını gerekli kılmaya başlamıştır (Nye, 2011: 18-35, Kramer, 2011: 136-150).

Özellikle bilgi ve teknolojinin de küreselleşmesi ile beraber siber uzayda yaşanan inanılmaz gelişmeler yine bu alana paralel ve özgü olarak tehditler ve bununla ilintili olarak güvenlik bağlamında 21. yüzyıl öncesinden farklı olarak yeni türde ve boyutlarda bir takım kavramların ortaya çıkmasına vesile olmuştur. Hâlihazırda Soğuk Savaş sonrası dinamik ortamın içerisinde tebarüz eden farklı alanlardan ve araçlardan kaynaklı tehditlere kendine münhasır gayri merkeziliği, ilke ve kuralsızlığı olan siber uzay kaynaklı tehditler eklenince doğal olarak klasik tehdit ve güvenlik paradigmaları ve algılamaları da dönüşüme uğramaya başlamıştır. Çünkü siber uzaydan kaynaklı yeni tehdit türleri ulusal güvenlik çerçevesinde ele

alındığında hem askeri hem de siyasi ve ekonomik boyutları da etkilediğinden yine bahse konu bu boyutların güvenliğini de ulusal güvenlik çerçevesinde değerlendirmeye itmiştir (Visner, 2013: 90-99, Taborn, 2010: 3).

Devletlerin siber ortamın başat aktörü konumuna gelmesiyle beraber bu alanda oluşacak suç ve tehdit unsurları da fazlalaşmaktadır. Çünkü siber uzayın gelişen ortamı bireylerden karmaşık siyasi organizasyonlara kadar sunacağı katkılardan dolayı tehdidin kaynaklarını da geniş yelpazeye yaymaktadır. İlerleyen teknoloji ile eş zamanlı olarak bilgi ve beceri yeteneklerini geliştiren aktörler icra edilen saldırıların isnat edilemezliği sayesinde kimliklerini gizleme fırsatı yakaladığından siber ortamda farklı türde tehdit türü her daim canlılığını koruyacaktır. Bu durumda bu aktörler arasındaki imkan, kapasite ve güç unsurları gibi sınırlamaları müphem kıldığından tehdidin kaynağını da müphem kılacaktır. Misalen, herhangi bir saldırgan ya da bir devlet tarafından ifa edildiği öne sürülen bir eylem aslında başka bir saldırgan ya da devletin istihbaratı tarafından casusluk amaçlı yapılabilmektedir (Ghanea, 2012: 81-89, Painter vd., 2012: 167-188).

3.2. Eylemin Faili Bakımından

Bilişim teknolojisinde yaşanan süretli gelişme ve bununla gelen her düzeydeki karmaşıklık siber ortamda da geleceğe dair belli türde çıkarımlar yapmayı da zorlaştırmaktadır. Çünkü ARPANET'in kurulumuyla başlayan ve akabinde tedricen küçük çaplı saldırılar ve tehditlerle devam eden 21. yüzyılda da organize olan terör gruplarının bilişim sistemleri aracılığıyla saldırılarda bulunmaları devletlerin ulusal güvenliklerini tüm yönlerden tehdit eder hale gelmiştir. Japonya'nın Tokyo metrosunda kritik altyapılarından biri olan havalandırma ve tren kontrol sistemleri bilişim sistemleri vasıtasıyla manipüle edilerek sarin gazı salınımının artırılmaya çalışılması siber ortamın terör gruplarına nasıl kolaylıklar sağladığına tipik bir örnektir (Q' Brien, 2003: 198). İşte, saldıran tarafa saldırılarını ve eylemlerini ifa etmelerinde gereksinim duydukları mobil telefonlar, kişisel bilgisayarlar ve geniş çaplı bilişim araçları gibi unsurlara kolayca ve düşük maliyetli erişim ve kullanım imkanı sağlayan siber ortam devletlerin ulusal güvenliklerinde birtakım açıklıklar yaratmaktadır.

Bunun ve devletlerin bilişim teknolojilerine olan bağımlılığı arttıkça bilgiyi emniyetli bir şekilde işleme, saklama ve transferini sağlamanın yanı sıra siber ortamda kritik altyapılara yönelik saldırı ve tehditlere karşı güvenlik tedbirlerinin alınmasının da ne güçlükte olduğu sorusu tebarüz etmektedir. Çünkü somut, caydırılabilir ya da belli araçlarla karşılık verilebilir tehditler ve tehlikeler üzerine kurulu olan klasik güvenlik anlayışına karşılık hem araçlar hem amaçlar hem de sonuçlar bakımından öngörülemeyen tehditler doğuran siber ortamdaki güvenlik anlayışı birbirinden kahır ekseriyette farklılaşmaktadır. 21. yüzyıl düşmanın kim olduğundan ziyade tehditlerin ve tehlikelerin artması ve çeşitlenmesi riski ile karşı karşıyadır. Bu durumun geleneksel güvenlik anlayışının mottosu haline gelen gücü elinde bulunduran egemen birimin koruduğu belli bir toprak parçası ve egemenliğinden ziyade Victor Cha'nın deyimiyle fiziksel olmayan güvenlik anlayışının (Cha, 2000: 395) gün yüzüne çıkmasını sağlamıştır. İşte, bu noktada, 21. yüzyılda tehditlerin ve tehlikelerin niteliği ve boyutları bakımından belirsizleşmeyi beraberinde getiren siber ortamın ürettiği güvenlik sorunları ve açıkları yeni güvenlik anlayışında fiziksel olmayan güvenlik anlayışına örnek olarak verilebilmektedir.

Uluslararası ilişkilerde uluslararası siyasetin özünü esas olarak devletlerarası ilişkiler oluşturmaktaysa da özellikle 1980'ler sonrası küreselleşme paradigmasının ekonomi, sosyoloji, kültür ve de teknolojik alan gibi siyasal ve toplumsal yaşamın tüm alanlarında hızlı bir çözülme sürecini başlatması hem uluslararası sistemde aktörlerin çeşitliliğini artırmış hem de diğer alanlarda olduğu gibi sosyal bilimlere dair kavramların içeriğini ve kapsamını da genişletmiştir. Bu bağlamda özellikle bilgi ve teknolojilerin küreselleşmesi uluslararası ilişkileri de etkisi altına almaya başlamıştır (Baylis, 2011: 230-245, Clark, 2000: 35-52). Öyle ki ilerleyen devrim niteliğindeki bilgi teknolojileri uluslararası sistemi her yönüyle karmaşık bir hale sokmuştur. Çalışmada da sıklıkla dile getirildiği üzere siber ortamın nevi şahsına münhasır özelliği devlet dışı suç teşkil eden ve edebilecek olan aktörlere etkinlik alanı yaratmış ve aynı zamanda dünya siyasetinin geleneksel devlet merkezli imajına da özellikle güvenliğin araç, amaç ve ontolojisine dair radikal bir şekilde meydan okumuştur.

21. yüzyılın siber çağında siber ortam temelli yeni güvenlik tehditleri ve yeni çatışma şekilleri ulusal sınırların aslında ne kadar kırılgan duruma geldiğini de göstermiştir (Demchak ve Dombrowski, 2013: 29-38, Hathaway, 2014: 301-309, Giacomello ve Mendez, 2001: 15-27. Sassen, 2012: 195-207). Siber ortamın araçlarından hem propaganda hem de araç amaçlı faydalanan 11 Eylül saldırısı dünyanın başat gücünün başat şehrinde ve aynı zamanda başkentine gerçekleştirdiği saldırılarla hasar verebiliyorsa diğer başat güç olmayan devletlere yönelik siber ortamdan gelecek daha şiddetli ve organize saldırılarda bu devletlerin durumu ne olacak? Çünkü 21. yüzyılda tehditler salt hasım bir devletten değil küresel düzlemde bir ağ olarak faaliyetlerde bulunan devlet ötesi suç ya da terörist gruplardan da gelebilmektedir. Devletlerin kritik derecede öneme haiz kurumlarının ağlara dayalı altyapılarının hackerler ve siber teröristler tarafından çökertilebilmesi 21. yüzyılda siber ortamın ulusal güvenliği tehdit eden önemli tehditlerden biri olacağının kanıtıdır (Özcan, 2014). Bu aktörler 21. yüzyıla değin maliyetin yüksekliğinden dolayı sadece devletlerin sahip olduğu araçlara sahip olamamışlardı; ancak yeni yüzyılda siber ortam bu gruplara geleneksel yöntemlerin yerine maliyeti bir hayli düşük ve bir o kadar da fazla ses getiren eylemler yapabilmelerine imkân tanımıştır (Clemente, 2011: 15-17). 21. yüzyıl öncesinde silahlar karmaşıklık arz edip aynı zamanda kolaylıkla satın alınabilen bir ucuzlukta değildi ve bu silahların yerleştirilmesi, kullanımı ve tamiratı için de kalifiye personele gereksinim duyulmaktaydı; ancak bugün bir bilgisayara sahip olan internet ulaşım imkanı olan ve farklı yazılımları bilen bir kişi ya da gruplar dijital altyapı kullanan tüm sistemler için muhtemel ciddi tehdit unsuru olmaktadır (Karagül ve Özkan, 2015: 122).

Örneğin, ABD'de Savunma Bakanlığına ve NASA'nın Ames Araştırma Merkezinin bilişim sistemlerine sızan Lyttle adlı bir genç her iki kurumun lojistik bilgi sistemlerini elde ederek devletin bilgisayar sistemlerine zarar verdiği gibi maddi zarara da neden olmuştur (Paulson, 2002). Buna benzer, Avustralya'da bir atık kontrol merkezi eski çalışanının ağ sistemine sızıp yaklaşık bir milyon litre atığın nehir ve sahil sularına dökülmesine sebep olması bir başka saldırı örneğidir (Curan, Concannon ve McKeever, 2007: 2). Yine, Türkiye'nin Diyarbakır ilinde PKK sempatizanı olan bilgisayar korsanının örgüt için casusluk yaparak Genelkurmay ve

Milli İstihbarat Teşkilatlarının sistemlerine erişmeye çalıştığı ve askeri birlikler ile emniyet müdürlüklerine ait bilgiler ve yerleşim planlarını örgüte sızdırmaya çalıştığı tespit edilmiştir (Cebe, 2008: Hürriyet). Müşahede edildiği üzere bir kişi ya da grup devletlere ait kamu kurum ve kuruluşlarının bilgisayar sistemlerine sızabilmekte, verileri elde edebilmekte ve bunun sonucunda maddi zararların yanında sistemlerin işleyişine zarar verebilmektedir. Siber ortam aracılığıyla gün geçtikçe daha fazla güç elde eden bu devlet ötesi aktörler bir bilgisayar ve bu bilgisayarın içerdiği muhtelif yazılım araçları ile devletlerin sistemlerine öngörülemeyecek düzeyde etkili boyutlarda zarar verme potansiyeline sahip olacaktır. Özellikle, ulusal orduların komuta, savaş, keşif, gözetleme, istihbarat ve casusluk ve silah sistemleri gibi kontrol sistemlerinin bütünü bilişim iletişim altyapılarına bağlı olduğundan bu durum devlet ötesi suç grupları için ele geçmez tehdit yaratma fırsatları doğuracaktır.

Geleneksel güvenlik paradigmasında görülen tehdidinin sadece belli olan hasım bir devletin askeri unsurlarıyla oluşabileceği kaygısı bu yüzyılın yeni konjonktüründe yeniden şekillenmiş ve değişime uğramıştır. Siber ortam bireyden devlet düzeyine kadar tüm aktörlerin etkinlik kurabildiği güncel bir alan yaratmıştır. Bu güncel alandan kaynaklı tehditlerin arkasındaki güdülerde geleneksel dönemin güdülerinden farklı bir şekilde tezahür etmiştir. Yani, evvelki dönemlerde Westphalian sistemin mantalitesi içerisinde tehditlerde devletlerin hudutlarının ve toprak bütünlüğünün ve de bu toprak bütünlüğü üzerinde kuracakları egemenliklerinin garanti altında olması ve bunun için de askeri kapasite ve siyasal gücün optimum düzeyde tutulması ön plandaydı. Bu geleneksel güvenlik mantığında devletlere yönelik en büyük tehdit unsuru oluşturan parametre sahip oldukları bütünlüğe sahip dokunulmaz toprak parçası ve bunun üzerindeki egemenliklerinin kaybı olmuştur. Bu nedenle tehditlerin arkasındaki güdü sınırların korunması ve bununla ilintili olarak da verilen cevap mantığı da belirgin aktöre karşı askeri olmuştur.

Ancak, 21. yüzyılın siber ortamındaki inanılmaz gelişmeler ve stratejiler konvansiyonel silahlar ve savaş tekniklerinin yerini gittikçe tamamlayıcı bir özellik arz eden siber saldırı ve savaşlara bırakmaya başlamış; ayrıca konvansiyonel terör saldırıları fiziki eğitim ya da psikolojik güdüler gerektiren ve ölüm riski içeren

niteliğe sahipken siber terör saldırıları devletin korumasındaki telekomünikasyon, ulusal güvenlik ağları gibi bilgilerin temini değiştirilmesi ya da terörist amaçlar için kullanılmasına yönelik olmuştur (Karagül ve Özkan, 2015: 123). Bir başka deyişle, bu alanı kullanan ulus aşırı aktörler kendine has saldırı araçları ile devletlerin bilişim sistemlerini çökertme, manipüle etme ya da bilişim sistemleri aracılığıyla istihbarat, casusluk ve hayati öneme haiz kritik altyapılarına gerçekleştirilen saldırılar ifa ederler.

Devlet dışı aktörlerin siber ortamın en çok siber suç ve siber terörizme dair alanların kolaylıklarından faydalanırlar (Nye, 2012: 21-44). Suçların fırsatları takip etmesi kuralında gözlemlendiği üzere siber ortamın takdim ettiği olanak ve fırsatlar bu aktörlere uluslararası suç trafiğinde farklı ve yeni boyutlar bahşetmektedir. Bir başka deyişle, siber ortam bireylerden güç bakımından zayıf olan devletlere kadar tüm aktörlere seslerini ve eylemlerini duyurabilmelerinde kayda değer işlevsel alan özelliği kazandırmaktadır (Weiman, 2006: 154). Ortamın gayri merkeziliği ve dolayısıyla kontrol edilemezliğinin yanı sıra, tüm gruplara ve birimlere açık olması, bilgi akışının ve transferinin bir hayli fazla olması, geleneksel savaş metotlarının ve araçlarına kıyasla hem kolay kullanılması hem de maliyetinin düşük olması, kimliğin belirlenemezliği ve de tüm medya araçlarında ciddi bir ilgi ve gündemde olma şansı yaratması gibi fırsatlar siber ortamı bu gruplara cazip kılmaktadır. Tabi bu devlet dışı suç grupları siber ortamı farklı amaçlarla kullanabilmektedir. Siber ortamı propaganda amaçlı taraftar toplamada, yayınlar yapmada ve fikirlerini yaymada kullanan suç örgütleri etkin iletişim ve eğitim için faydalanabildikleri gibi yine karşı tarafın bilişim sistemlerine ve bu bilişim sistemlerine bağlı kritik altyapılarına saldırı yapmada faydalanabilirler (Denning, 1999: 42-54).

Bu açıklamalara yerinde örnek teşkil edecek olay ayrılıkçı Tamil kaplanlarının Sri Lanka'ya yönelik gerçekleştirdiği saldırıdır. Ayrılıkçı Tamil Kaplanları birçok ülkede bulunan Sri Lanka yurtdışı elçiliklerine yaklaşık iki hafta boyunca bilgisayarlar üzerinden e-posta bombardımanına tutarak elçiliklerin tüm iletişim ve haberleşme sistemlerini çökertmiş ve kamuoyunda ve temsilciliklerde korku ve endişe yaratmıştır (Denning, 1999: 69-70). Yine küresel çapta yankı uyandırmak hasebiyle Pakistanlı G-Force ve Doktor Nuker adlı gruplar 1999, 2000 ve 2001

yıllarında Hindistan hükümetinin web sitelerine, parlamentosuna, hükümet kanalı, medyaya, Enerji Bakanlığına ve Savunma Bakanlığına ve Bhabha Atom Araştırma Merkezi gibi politik değer taşıyan kurum ve kuruluşlarının yanı sıra bilgi işlem merkezlerine de saldırılar gerçekleştirmiştir (Akşam, 2013). Bunun üzerine Hindistan hükümeti hem Keşmir hem de nükleer silah denemelerinde karşı karşıya kaldığı siber saldırılara yönelik olarak 1998 yılından günümüze değin siber savaşı da içeren yeni güvenlik konsepti doğrultusunda hareket etmiş ve yine bu doğrultuda Ulusal Savunma Kurumları ve Savunma İstihbarat Birimlerine bağlı siber savaş, psikolojik operasyon, elektro manyetik ve dalga teknolojilerinde uzman alt birimleri inşa ederek tedbirler almıştır (Gürkaynak ve İren, 2011: 269). Benzer şekilde, 1999 yılında patlak veren Kosova savaşına müdahil olan NATO anında Sırp korsanlar tarafından siber saldırılara maruz kalmıştır. Literatürde siber savaşın ilk örneği olarak gösterilen Kosova Savaşında Sırp Korsanlar ile NATO güçleri arasında karşılıklı olarak birbirlerinin altyapılarına yönelik saldırılar gerçekleştirilmiştir. Öncelikle, Sırp grupların siber ortamda interneti bilgi edinmede ve bilgiyi sunmada, destek sağlamak için propaganda amaçlı kullanma, muhalif grupları sindirme amaçlı kullanmış akabinde ise saldırı moduna geçip NATO karargahlarının kontrol ve komuta merkezlerine, web sitelerine ve sunucularına ve diğer haberleşme sistemlerine yönelik Dağıtık Servis Dışı Bırakma ve virüsler ve zararlı yazılımlar içeren e-posta bombardımanlarıyla siber saldırılarda bulunmuşlardır (Denning, 2005: 5-9). Kendilerini Birinci Dünya Savaşının başlamasında etkin bir gizli yer altı grubu olarak gördükleri The Black Hand olarak adlandırılan (Geers, 2008: 5) bu Sırp korsanlar NATO'nun tüm bilgi ve haberleşme hizmetlerine hasar vererek iletişimin ve koordinasyonunda sağlanmasında ciddi aksamalara neden olmuştur (Rosenfield, 2012: 87). Bununla birlikte, The Black Hand korsanları Rus ve Çin uyruklu hackerlerden de destek alarak NATO'yla birlikte ABD ve İngiltere'nin askeri ve kamu bilişim sistemelerine yönelik eş zamanlı siber saldırılar gerçekleştirmiştir (Tıme, 2014).

Görüldüğü üzere, gerçekleştirilecek olası çatışma durumlarında devletlerin kritik altyapı sistemlerinin sınır aşan organize suç örgütlerine ve aktörlerine açık hedef haline geldiği görülmektedir. Siber ortamda bireyler, sınır aşan organize suç

örgütleri ya da terör gibi devlet dışı aktörlerde etkin olmaktadır. Bu aktörlere siber ortamda hedeflerine ulaşmada internete bağlı bir bilişim teknolojisi aracı yeterli olacaktır. Politik, ekonomik ya da sosyal bir amaçla uluslararası kamuoyunda ses getirebilmek ve etki oluşturabilmek için bu devlet dışı aktörler yazılım, donanım ve ağlar üzerinden devletlerin siber ortamdaki açıklıklarından da faydalanarak ulusal güvenliklerine yeni tehditler oluşturabilme şansına erişmişlerdir (Carry, 2010: 15-31). Siber ortam devletler nezdinde 21. yüzyılda bir değer olarak kabul gören bilginin türediği yer olarak artık güvenlik ajandasının tepesinde yer almak zorundadır. Çünkü siber ortamda keşfedilen ya da üretilen bilgi ve bilgi sistemleri devlet dışındaki kötü niyetli şahıslara, organize gruplara ve özellikle de terör gruplarına tehdit oluşturmada olanaklar sunmaktadır. Özellikle maliyeti düşük olan ancak hasar yaratma kapasitesi yüksek olan siber ortam devlet dışı bu aktörlere devletlere karşı asimetrik bağlamda muteber bir güç ve konum kazandırdığından onları teknolojiyi araç olarak kullanmaya mütemayil kılmaktadır. Devletlerinde kritik altyapılarını bilgi ağları üzerinden kontrol ettiği düşünüldüğünde bahse konu kötü niyetli aktörlerin saldırılarının da odak ve çıkış noktasını da siber ortamın yarattığı görülmektedir.

Sistemin hızla küreselleştiği, sınırların esnekleştiği ve ulus devletlerin varlığının ve yapılarının sorgulandığı 21. yüzyılda, siber ortam asimetrik tehdidin, savaşın ve güvenlik anlayışının şiddetli bir şekilde yaşanacağı alan olarak uluslararası sisteme kazandıracağı aktörler ve stratejiler bağlamında gelişen bir alan olma yolunda seyir etmektedir. Siber ortamda artan tehditler, savaşlar ve saldırılar devletlerin milli güvenliğine yönelik önemli derecede tehdit unsuru oluştururken, ayrıca tehdit eden aktörlerin de çeşitlenmesi ve artması ulusal güvenliğin önemli sorunlarından biri haline gelmiştir. Soğuk Savaş öncesinde devletler için tedbir alınması gereken tehditler ve bu tehditlerin kimden geldiği ve bu doğrultuda bu tehditlere karşı güvenliği temin edecek nesne ve aktörlerde belirgindi. Bir başka anlatımla ulusal güvenliğe yönelik tehditlerin kaynağı yine devletlerdi. Ancak 21. yüzyılın dinamik siber ortamında devletlerin ulusal güvenliğine yönelik tehditlerin kaynağını sınır içinde hem de sınır dışında küreselleşen devlet dışı organize suç aktörleri de almıştır. Bilgi ve teknolojilerin bu aktörlere sunduğu anomimlik ve hızlı

ve hedefe ulaşmadaki müessirlik devletleri adeta siber ortamda zor duruma düşürmektedir (Bıçakçı, 2012: 128). İşte, 21. yüzyıl önceki dönemlerden farklı olarak farklılaşan yön ve etkileri ile yeni bir takım kavramları gün yüzüne çıkarırken, özellikle siber ortamın kendine has ortamıyla sunmuş olduğu imkan ve olanaklar yine bu yüzyılda aktör bağlamında devletlerin dışında da bazı birimlerin belirmesine şahit olmuştur.

3.3. Eylemin Niteliği Bakımından

Siber ortamda vuku bulan ilerlemeler ve gelişmeler 21. yüzyıl öncesinin harekat alanları olan kara, deniz ve hava gibi fiziki mekanlarına kendine özgü karakteristiği ile yeni ve bilinmeyenli denklemleri barındıran yeni bir hareket alanı kazandırmıştır. Niteliklerinden ve isminden de anlaşılacağı bu hareket alanında ifa edilecek olan eylemler araçları, amaçları ve nitelikleri bakımından klasik hareket alanlarında icra edilen ve edilecek olan eylemlerden kayda değer farklılıklar taşımaktadır. Öncelikle bu yeni hareket alanı klasik hareket alanlarının aksine insan unsuru ile kurulmuş akabinde ortamdan türeyen teknolojik araçların ve imkanların gelişmesiyle beraber devletten özel sektörlere kadar tüm birimlerin dâhil olduğu bir alan haline gelmiştir (Hariff, 2009: 2-21, Suhukla, 2006: 165-176). Siber ortam tüm birimlere bilgiye ve bilgi sistemlerine erişim ve transfer etme noktasında ışık hızı derecesinde kolaylık ve rahatlık sağlamaktadır. Ancak, daha öncede vurgulandığı üzere sağlamış olduğu imkan, olanak ve kolaylıklar sebebiyle bireyden devlete kadar tüm aktörlere oldukça geniş bir kullanım ve faydalanma alanı sunan siber ortam, öte yandan da küresel çapta tüm aktörlerin dâhil olduğu ve ilgilendiği ışık hızında bir küresel bir bilgi ağı fırsatı tanıdığından aynı aktörlere yönelik tehdit çıkmazı da yaratmıştır. Çünkü bu küresel ağ içinde birbirine bağımlı olan bilgi ve iletişim teknolojileri devletler nezdinde ulusal değer olarak kabul gören bilgi sistemlerine bağlı kritik altyapı ve diğer hizmetlerinin siber ortamdan neşet eden saldırılar ve tehditlere karşı da korunması gereksinimini ortaya çıkarmıştır. Devletler kritik altyapı sistemlerini ve hizmetlerini bilgi ağları üzerinden işlevsel kıldığından bu durumda siber saldırıların hareket noktasını oluşturmaktadır. Bu noktada ifade edilmeye çalışan durumu en iyi 2001 yılı ABD Dışişleri Bakanı olan Rice'ın

konuşması açıklamaktadır. Rıce konuşmasında ileri teknoloji ekonomimizi dinamik, askeri güçlerimizi daha da güçlendirirken bir diğer taraftan zaafımızı da oluşturmaktadır. Bu günümüzün paradokslarından biridir. Bilgi sisteminde bir çökmenin meydana gelmesi tüm ulusa ciddi zararlar verebilir diyerek yeni tekliheye dikkat çekmiştir (Rathmell, 2001: 7).

Her geçen gün daha da artan ve bununla ilişkili olarak sonuçlar doğuran siber kaynaklı tehditler, saldırılar ya da savaş olasılıklarının ulusal güvenliği tehdit edecek boyutlara ulaşması aynı zamanda devletlerinde bu güvenlik sorununa karşı çok yönlü ve kapsamlı tedbirleri alması gerekmektedir. Ancak, iki ucu keskin kılıç misali, sunmuş olduğu sınırlanamayan ve sınır tanımayan özgürlük ortamı siber dünyada yeni bir alan yaratırken, bununla birlikte aktörlerin bu alanda sahip oldukları bilginin güvenliği ve dolayısıyla siber ortamın güvenliği ön plana çıkmaktadır. Fakat 21. yüzyılda yeni ve bir o kadar da karmaşıklık getiren bir alan olarak tebellür eden siber ortamın güvenliğinin tesisi hem ulusal hem de uluslararası düzlemde bir takım zorlukları beraberinde getirmektedir. Çünkü siber uzayın yaratmış olduğu farklı ve yeni tehditler nitelik bakımından geleneksel güvenlik anlayışının üstesinden gelebileceği tehdit kategorisinde değildir (Aksu ve Turhan, 2012: 73). Öncelikle geleneksel tehdit algılamaları ve bu tehditlerle başa çıkma araçları ve yöntemleri siber güvenlik tehditleriyle mücadelede hükümsüz kalmaktadır. Bu bağlamda geleneksel güvenlik paradigmasının karşısına yeni türde tehditler çıkaran siber ortama karşı yeni mücedele araçlarının ve kurallarının devreye sokulması gerekmektedir. Kendine has anarşik doğası, karmaşıklığı, küreselliği ve asimetrik güç unsurlarıyla siber tehditlere yönelik devletler tarafından tedbirler alınmaya çalışılmasına rağmen mücadele etmenin oldukça zor olduğu görünmektedir.

Bu bağlamda siber uzaydan kaynaklı tehditlerin üstesinden gelmenin zorluklarından biri bu hareket alanında vuku bulan eylemlerin isnat edilmesinin zorluğudur. Yani siber ortamda saldırı gerçekleştiren saldırganları tespit etmek oldukça güçtür. Hâlihazırda yeni bir hareket alanı olarak ortaya çıkan siber uzaya dair derinlemesine ve detaylı planlanmış güvenlik stratejileri ve ulusal ve uluslararası çerçevede belirlenen hukuk düzenlemeleri yapılamamıştır. Sadece bu etken bile siber

uzayın uluslararası sisteme ulus aşırı yeni aktörleri ve bu aktörlerin eylemlerini ve stratejilerini kazandırmada yeterli olmaktadır.

Bu noktadan hareketle siber uzayın uluslararası sistemin tüm aktörlerine sağladığı en muteber rahatlık ve tehdit, alanın gayrı merkeziliğinin tezahürü olan coğrafi sınırların pek dikkate alınmamasıdır. Yani mekân fark etmeksizin herhangi bir saldırgan ya da saldırganlar grubu gereksinim duyduğu mevcudiyeti ve temini kolay olan küçük bir teknolojik alet ve elde ettiği bilgi ve tecrübe ile dünyanın herhangi bir ülkesinin herhangi bir yerinden ağ bağlantısıyla hedeflediği ülkenin bilgisayar sistemine saldırı gerçekleştirebilmektedir. Siber uzayın bu gayri merkeziliği buradan gerçekleştirilecek olan eylemlerin somutluğunu da belirsiz kılmaktadır (Blakemore ve Awan, 2012: 41-45, Dunn, 2008; 19-24).

Bir başka deyişle ve kısa anlatımla siber ortam saldırı amaçlayan ve gerçekleştiren faillere kimliklerini gizleme olanağı sunarak adeta çekim merkezi haline gelmiştir. Faillerin tespitinin ve yakalanmasının organize olunan saldırılarda çoğunlukla mümkün olmazken bireysel saldırıların bir kısmında ise faillerin tespitinin ve yakalanması uzun zaman alabilmektedir. Çünkü sınırsız özgürlük, erişilebilirlik, kolaylık ve gayri merkezilik yani isnat edilemezlik sunan siber ortamda failler bilgisayarın başındayken dünyanın tüm bilgisayarlarına ve bilgisayar sistemlerine aynı mesafede yer aldığından var olan sistemsel açıklıklardan faydalanarak arzuladıkları eylemleri gerçekleştirebilirler (Thomas, 2003: 115). Siber ortam faillere eylemlerini bulundukları lokasyondan farklı bir yerde yapılıyormuş gibi gösterebilme şansını verebilmektedir. Örneğin, 2008 yılında Gürcistan'da patlak veren Rus Gürcistan savaşında Gürcistan devletine ait tüm kanallar, web siteleri ve internet altyapıları çökertilmiş ve devlete ait tüm kanallarda Rusya lehine propaganda yapılmıştır. Öyle ki, Rusya sempatizanı bilgisayar korsanları Gürcistan'a ait trafiği destekleyen tüm yönlendiricileri ele geçirerek Gürcülerin dışarıdan bilgi almasını ve de e posta dahi göndermesini engelleyerek iletişim ve haberleşmeyi de kesmiştir. Bununla da yetinmeyen Rus korsanlar aynı anda Gürcistan üzerinden tüm dünyadaki bankalara saldırılar düzenleyerek Gürcistan ile bankalar arasındaki bağlantıları kesmiş ve böylelikle takas sistemlerine erişemeyen Gürcü bankaları da paralize olmuştur. Bu saldırı sonrasında hem Gürcü yetkililer hem de ABD'li

yetkililer Rusya'yı suçlarken, Ruslar da saldırılarda kendilerinin desteği olmadığını belirtmiş ve bu eylemlerin popülist bir tepki olduğunu dile getirmiştir. Burada dikkatlerden kaçmaması gereken unsur saldırıların arkasında hangi gücün ya da devletin olduğunun hala isnat edilemezliğidir. Her ne kadar Rus-Gürcistan savaşı patlak verir vermez siber saldırılar gerçekleşse de saldırıları yürüten bilgisayar sistemlerinin ağ bağlantıları Kanada, Türkiye ve Estonya'daki botnetler (köle bilgisayarları) üzerinden gerçekleştiğinden (Clarke ve Knake, 2010: 13-20) faillerin kim olduğu ve saldırıları tam olarak nereden komuta ettikleri ispat edilememiştir.

Buna benzer şekilde bir başka ispat edilemeyen siber saldırı örneği de İran'a yapılan Stuxnet saldırısıdır. Stuxnet isimli bir virüs 2010 yılında İran'ın nükleer tesislerine sızdırılmış ve nükleer çalışmaları da kesintiye uğratmıştır. Özellikle endüstriyel ve kritik altyapı sistemlerinin otomatik kontrolünü, denetlenmesini ve veri toplanmasını sağlayan SCADA sistemlerine yönelik üretim kumanda merkezi sisteminin işlevselliğini ve çalışma şeklini değiştirmeyi hedefleyen Stuxnet saldırısı İran'ın nükleer tesislerine virüsler aracılığıyla sızarak merkezi kontrol sistemlerini ele geçirip fiziksel ve de maddi olarak büyük hasarlar vermiştir (Karnouskos, 2011: 1-2). Öte yandan saldırının failine dair yapılan suçlamalar genelde ABD ve İsrail'i hedef göstererek yapılmasına rağmen yeterli ve tatmin edici delil ve kanıtlar bulunamadığından iddialar havada kalmıştır (Anderson, 2012; Langner, 2013: 5-12). Ancak Stuxnet saldırısına dair uzmanlar tarafından üzerinde karar kılınan nokta bu virüs türünün ve tehdidinin arkasında devletlerin desteği olmadan kullanım alanı bulamayacağı üzerinedir (Pamuk, 2010: Lindsay, 2013: 33-49).

Tıpkı Estonya, Gürcistan saldırılarında olduğu gibi İran'a yönelik kimin gerçekleştirdiği ispatlanamayan Stuxnet saldırısı da göstermiştir ki siber ortamda tehdit eden ve edilen birey düzeyinden devlet düzeyindeki aktörlere kadar her birimin gerçekleştirdiği ya da her birime yönelik gerçekleştirilen saldırıların faillerinin kimliğinin tespiti ve gerekli cezayı gerektiren müeyyidelerin ifa edilmesi henüz gerçekleşmemiştir. Bu noktadan hareketle de bu yeni hareket alanında etkinlikte bulunan her aktör bir devlete saldırı gerçekleştirebilir ve eyleminin somutluğunun ispatlanmamasından dolayı da herhangi bir cezai yükümlülüğe de katlanmayabilir (Denning, 2012: 676-678).

Oysa klasik güvenlik paradigmasının temel savında ulusal güvenliğe yönelik tehdidin somut kaynağı devletti ve bu tehditlerin yapısı da askeri nitelikteydi. Örneğin ittifaklar sisteminin tezahürü olan Soğuk Savaş döneminin devlet merkezli güvenlik anlayışında önemli olan devletlerin güvenliğiydi. Bu doğrultuda, belirli bir toprak parçası üzerinde intikal etmiş ve bu toprak parçası üzerinde egemen olma zırhıyla dokunulmaz sınırlarla çevrili toprak bütünlüğüne sahip sosyal ve siyasal formasyon olarak kabul gören devletin öz değerlerine yönelik askeri bir tehdidin yokluğu olarak tanımlanınca geleneksel güvenlik anlayışında rakip devletlerden korunması gereken güvenlik değeri de topraktı. Yani elde var olan bir ulusal değerin kimden korunması gerektiği açık ve net olarak bilinmekteydi. Soğuk Savaş döneminin iki kutuplu dünya düzeninde siyasal pratiklere yön veren devleti odak noktası olarak görme ve askeri gücü de merkeze alma anlayışı geleneksel güvenliğin popüler olduğu Soğuk Savaş döneminin iki kutuplu dünya düzeninde bir devlete yönelik gelebilecek tehdit potansiyeli karşı kutup devletten beklemekteydi. Örneğin ABD'nin nükleer güce sahip olması Sovyetleri ve bloğundaki ülkeleri tedirgin ettiğinden bloklar arasında güvenliği sağlamanın yolu silahlanmadan ve nükleer gücü elde etmekten geçmekteydi. Görüldüğü üzere geleneksel güvenlik anlayışına şeklini veren Soğuk Savaş döneminde somut tehdidi oluşturan fail devletlerin kendileriydi ve bu faillerin tehdit araçları da nükleer ve silahlanmaydı.

Ancak siber güvenliğin yeni güvenlik anlayışına eklemlediği dikkat çeken tehdit içeriği tehdidi yönelten failin somutluğunun belirlenememesidir. Yukarıda verilen Estonya, Gürcistan ve İran'a yönelik Stuxnet saldırılarının failleri ya da aktörleri henüz ortaya çıkarılamamıştır (Richardson, 2011: 1-25, Carry, 2010: 17-19). Çünkü siber uzayın kendine has küreselliği ve anonimlik özelliği buna fırsat ermemektedir. Failler herhangi bir ülkede ele geçirdiği bilgisayar ya da diğer bilişim teknolojileri aracılığıyla kendini başka bir ülkedeymiş gibi göstererek çok uzaklardaki bir başka ülkenin bilgi sistemlerine saldırıda bulunabilir. İşte, siber uzayın bahse konu bu kendine has doğası ve yapısı faillerin kim olduğunun tespitini diğer bir deyişle somutluğunu zorlaştırmaktadır. Daha da kötüsü kimi zamanlarda failin tespiti noktasında yanlış kişilere yönlendirmeye bile sevk etmektedir. Ayrıca saldırganın kimliğinin kanıtlanamamazlığının yanı sıra gerçekleşen saldırıların ve bu

saldırılar neticesinde oluşan etkinin tespiti bile kimi zaman zor olduğundan kısa sürede hasar tespit yapıp güvenliği sağlamaya koyulmak zaman almaktadır.

Dolayısıyla bu durum faillere politik, ekonomik, psikolojik, ün elde etme amacına ulaşmada devletlerin kritik altyapılarının bağlı bulunduğu ağ komuta merkezlerine gerçekleştirilecek olan yıldırma, sekteye uğratma ve baskı altında tutma hedefiyle saldırılar yapma imkânını sunmaktadır. Bu durum bahse konu siber ortamın sunmuş olduğu failin somut olarak tespit edilemezliği devletler nezdinde güvenliğin siber uzay boyutunu ulusal ve uluslararası düzlemde karmaşık hale getirerek zorlaştırmaktadır. Öncelikle, güvenliğin ana faktörü tehdidi tavsif etmek ve bu tehdidin nereden veya kimden geldiği ise siber ortam bunun sadece ilk koşulunu açık vermektedir. Yani, tehdit siber ortamdan kaynaklı bilişim sitemleri aracılığıyla gelmektedir; Ancak ikincil koşul olan tehdidin kimden ya da nereden geldiği sorusunu ise siber ortam cevaplamamaktadır. Bu da saldırıların teşhis edilip karşılık vermede muhatap alacağı faili meçhul kılmakta olduğundan önümüzdeki süreçlerde savaş, güç, tehdit ve bununla ilişkili olarak da güvenlik parametrelerinin asimetrik bağlamda yoğun bir şekilde yaşanacağı siber uzayın uluslararası sisteme ve ilişki biçimlerine 21. yüzyıl öncesinden farklı olarak yeni bir takım aktörlerin ve dolayısıyla yeni stratejilerin belireceği bir ortam sunmaktadır.

3.4. Uluslararası Hukuk Bakımından

Siber uzayın sınır tanımayan ve içermeyen gayri merkeziliği, ağlar üzerinden kurmuş olduğu yapısı onu belli güçteki kural koyucu bir devletin egemenliği altına almasına müsade etmediği gibi ulusal ve uluslararası çerçeve de herhangi bir hukuksal kontrol mekanizmalarının kontrolü altına sokmasına da müsade etmemektedir. Bir başka ifade ile anlatılmak istenirse siber uzaydan kaynaklı tehditlerin boyutunun belirlenmesindeki zorluklar ve de teknik ve operasyonel düzlemdeki zorluklar sebebiyle bu alana herhangi bir gücün tahakküm etmesi ya da egemenlik salahiyetinin nasıl belirleneceği gibi karışık ve yanıtlanması zor sorular meseleyi hukuksal zeminde de ele almayı zorlaştırmaktadır (Pehlivan, 2006: 10, Goldsmith 2013: 129-138).

Teknolojide yaşanan muazzam gelişmeler, siber ortamda birbiriyle bağlantılı olan ağların ve araçların sunduğu değişken ve çok yönlü imkân ve kolaylıklar daha öncede dile getirildiği gibi her düzeyden farklı amaçları olan aktörlerin alandan yoğun bir şekilde faydalanmalarını her geçen gün daha da artırmaktadır. Bu yeni ortam sunduğu bu olanaklarla saldırı niyeti taşıyan bu aktörlere daha evvelden karşılaşmadıkları yeni fırsatlar sunduğu gibi aynı zamanda suç işleme fırsatı da yaratmıştır. Pek tabi ki, siber uzay geliştikçe daha önceden maruz kalınmayan suç türleri ve yöntemleri tüm yeni boyutlarıyla gün yüzüne çıkmıştır. Siber ortamdan neşet eden yeni teknolojiler tüm aktörlere yeni fırsatlar sunduğu gibi yeni suç şekillerine de kapı açmaktadır; Öyle ki, özellikle son yıllarda siber uzay kaynaklı suçlarda büyük artışlar gözlemlenmektedir. Bu noktada, siber uzayın sunmuş olduğu sınırsız özgürlük atmosferi siber suçlara dair işlenen vakalarla ilgili verilerin doğruluğunu ve istatistikleri de tam olarak ortaya çıkaramamaktadır. Ancak, literatürde ve raporlarda yazılanlar ışığında incelendiğinde 21. yüzyılla beraber siber suçların tesirli, ardı arkası kesilmeyen bir şekilde arttığı da görülmektedir (IT-Onlıne, 2016).

Her düzeyde aktörün faydalandığı bu alan doğal olarak yine aynı aktörlerin birbirlerine yönelik oluşturacağı saldırı sonrasında bir ileri aşamada savaş ihtimalini daha da artırmaktadır (McGraw, 2013: 114, Cavelty, 2008: 19-36). Ağlar ve bilişim sistemleri üzerinden bilginin üretilmesi, depolanması, transfer edilmesi gerçekleştiğinden siber ortamda önce suç düzeyinde görülen eylemler gün geçtikçe terör ve savaş eylemlerine dönüşmektedir (Junio, 2013: 125-133, Rid ve McBurney, 2012: 6-13). Dolayısıyla, siber ortamdan türeyen bu suç, terör ve savaş tehditleri ile mücadelenin önemli sacayağını hukuku düzenlemeler oluşturmaktadır.

Bununla birlikte, icra edilecek siber saldırılarının savaş nedeni olamayacağını devlete yönelik politik bir siber saldırının tıpkı savaş olgusu gibi eski olan sabotaj, casusluk ya da harap etme hedefli bir saldırı aynı düzeyde neticeler doğuracağını ve konvansiyonel bağlamda silahlı kuvvet kullanılamayacağını ileri sürenler olsa da (Rid, 2012: 5-32, Singel, 2010), özellikle yakın dönemde gerçekleştirilen Estonya, Gürcistan ve İran'a yönelik siber saldırılar siber suçları, terörizmi ve savaşı tüm ciddiyetiyle açığa vurmakta, uluslararası hukuk ve savaş hukuku açısından da

konunun değerlendirilmesi; ayrıca düşman devlet veya devlet destekli alt gruplar tarafından yapılan siber saldırılar halinde saldırıya uğrayan devlet tarafından BM Antlaşmasının 51. maddesindeki meşru müdafaa hakkının kullanılmasını (Yayla, 2014; 183) gerektirmektedir. Çünkü her geçen gün uluslararası sistemin aktörlerinin hareket ve yaşam alanıyla olan bütünlüğü artmakta olan siber alan ve bu alandan kaynaklı güvenlik tehditleri hem ulusal hem de uluslararası hukuk düzleminde meselelerin yeniden ele alınmasını elzem kılmaktadır. Nitekim siber saldırıları engellemeye yönelik kollektif savunmayı öngören ve bunun içinde gerekli tedbirleri almak isteyen NATO, düzenlediği 2016 Varşova zirvesinde siber ortamı tıpkı kara, deniz, hava gibi operasyonel bir alan olarak değerlendireceğini belirterek siber saldırıları da 5. madde kapsamında değerlendirmenin ilk adımını atmıştır (Ware, 2016).

Kriminolojide suçların fırsatları kovaladığı düsturundan hareketle, siber ortam salt fırsatların bulunması değil aynı zamanda suç işleyecek irade, motivasyon, kimliğin gizlenmesi, araçlara yüksek meblağlar ödemeden sahip olunması ve ışık hızında eylem icra etme imkan ve olanağına haiz failler ile suçun oluşmasına mani olacak yeterli düzeyde koruma ve gözetimin olmaması suç unsurlarının meydana gelmesinde göze çarpan koşullardır. Alışılmadık bir ortamdan alışılmadık güvenlik tehditleri ile karşılaşacak olan devletler de bu yeni mücadele alanında diğer alanlarda olduğu gibi hukuki mücadelelerini de farklı ve yeni araç ve yöntemlerle vermek zorundadır. Çünkü siber alanın hem reel dünya da hem de sanal dünyada peyda ettiği boşluklar, tehditler bağlamında devletlerin ulusal güvenliklerini muhafaza etmede askeri, siyasi ve hukuki mecrada başvurdukları ve kullandıkları klasik araçlar, yöntemler ve düzenlemeler artık ihtiyaçlarını karşılamayı tatmin etmemektedir.

Elbette, bu sorunlar genellikle siber suçlarla ilişkilendirildiğinde yargı ve yetkilerle ilgili karmaşıklıklardan kaynaklanmaktadır (Melzer, 2011: 11-12, Schmitt, 2014: 272). Hâlihazırdaki geleneksel uluslararası hukuk kuralları sorunları ve uygulamaları fiziksel coğrafya ve sınırlar üzerinden yorumlamaktadır. Öte yandan fiziksellikten öte alanı ve unsurları barındıran siber uzay menşeili siber suçlar ise kolayca sınırları bölmesi ve sınırlar ötesi uygulamaları barındırması sebebiyle geleneksel hukuk kurallarının bu noktada tatmin edici cevapları barındırmadığı

ortaya çıkmaktadır. Mevcut hukuksal düzenlemelerde devletler sınırları içerisinde düzenlediği ve yasalaştırdığı hukuk kurallarını uygulama ve yargılama yetkisine sahiptir ve kendi sınırları içerisinde suç teşkil eden eylemlerin faillerini de yargılama yetkisine sahiptir. Ancak, siber suç yargılamaları ile ilgili hangi ülkenin sorgulama ve yargılama yetkisi olduğu ile alakalı sorular hala zindeliğini korumaktadır (Manolopoulos, 2003: 40-58).

Birçok ülke henüz siber suçlarla ilgili eylemler, caydırma noktasında yaptırım uygulamada yeterli düzeyde ve etkide yasal düzenlemelere sahip değildir (Fleck, 2013: 341-343, Roscini, 2010: 91-118) . Örneğin, Filipin vatandaşı Guzman adlı şahıs tarafından önce Filipin hükümet binalarına ve akabinde dünyaya yayıldığı iddia edilen ve dünyanın en tehlikeli virüslerinin başında gelen "I Love You" virüsü yaklaşık olarak 9 milyar dolar civarında bir hasara neden olmuştur. Ancak Filipin hükümetinin değil siber suçlarla ilgili yasal düzenleme yüzeysel suçları içeren bilişim suçları ile igili yasal düzenlemelere bile sahip olmaması failin serbest kalmasını sağlamıştır. 2000 yılında gerçekleşen bu olayın bir ay sonrasında ise Filipinler kapsamlı bilişim yasasını meclisten geçirmiştir. Tıpkı Filipinler gibi dünya genelinde de sadece ortalama her beş ülkeden biri değişik bir formda ortaya çıkan siber suçları içerecek şekilde mevcut yasalarını tecdit etme ya da tadil yoluna gitmiştir (Sahu, t.y., 2). Bunların da çoğu siber suçlara dair farklı açılardan yaklaştıkları için farklı hukuk kurallarını kanunlaştırmışlardır. Böylelikle, siber uzaydan kaynaklı bir siber suç icra edildiğinde ortaya birden fazla başvurulması ya da başvurulmaması gereken hukuki düzenlemeler çıkmaktadır.

Bununla birlikte, siber suçlarla mücadele de bir başka zorluk siber ortamda suç işleyen faillerin niyetlerini de tespit edebilme engelidir. Örneğin, özellikle bazı hackerlar devletlerin bilişim sistemlerine zarar verme niyetinde değil de sadece ağ sistemlerine eğlence amaçlı sızabilmektedir. Öte yandan, siber suçlarla mücadele bağlamında kurulacak olan altyapı ve diğer ekipmanların bilgi teknolojilerindeki gelişmelerle eş zamanlı olarak hızlı ve sürekli bir şekilde gelişen koşullarına daima ayak uydurmak zorundadır ve dolayısıyla sürekli yenilenmeleri gerekmektedir. Zira suçluların 21. yüzyılda gelişen teknolojilere erişimi bir hayli rahat ve kolay olmakta iken, devletin bürokratik kademelerindeki süreci yavaşlatıcı engeller ve

prosedürlersiber tehditle mücadele edecek olan kurumların işlevselliğini de zora sokmaktadır (Bae, 2003: 79-82, McCarthy, 2015: 19-42).

Yeni ve 21. yüzyılda bilgi teknolojilerinde yaşanan baş döndürücü gelişmeler hasebiyle bir o kadar da farklı boyutlarda karmaşıklığı barındıran siber alan henüz kavramsal ve kuramsal perspektiflerden olgunlaşmadığından hukuksal zeminde de siber suçların, saldırıların ve savaşların var olan uluslararası hukuk kaynaklarının siber ortama uyarlanabilirliği yasa ve yapılan anlaşmaların önemi ve de hangi konuları bünyesinde barındırması gerektiği gibi hukukun nasıl uygulanacağı ve yürürlüğe konulacağı merak edilen sorulardır (Roscini, 2015: 233-254, Schmitt, 2012: 245-260). Hâlihazırda birçok ülke bilişim hukukuna dair yasalarında yer vermemekte, yer veren ülkelerin birçoğu da siber ortamda saldırı ve savaş teşkil edecek eylemlerin neler olduğunu ve ne şekilde yapıldığına dair ulusal düzlemde kapsamlı ve derinlemesine hukuki bir çerçeve çizememiştir (Runciman. 2015: 56-57). Keza, uluslararası sistemde türeyen yeni aktörler açısından büyük fırsatlar yaratan bu durum uluslararası düzlemde de pek farklılık arz etmemektedir. Savaşı engellemeyi hedefleyen ya da savaşa dair ilke ve kurallarını belirleyen hukuk kaidelerinin bilgisayar ve iletişim teknolojilerini tüm etki ve boyutlarıyla gün yüzüne çıkmadan önce çerçevesinin çizilmiş olması var olan kuralların siber saldırılara uyarlanması konusunda yapılacak olan çalışmaları zorlaştırmıştır (Yayla, 2014; 183).

İlaveten, yeni bir hareket alanı olarak tebarüz eden siber ortamın henüz olgunlaşmamış yapısı ve bu alanda ifa edilen suç teşkil edecek eylemlerle ilgili kesin olarak elde edilecek verilerin imkânsızlığı, gayrı merkeziliği, yasal, teknik ve operasyonel zorluklarla birlikte alana dair devam eden kavramsal tartışmalar gibi siber ortamın kendine özgü karakteristiğinden kaynaklı zorluklar her ne kadar hukuki düzenlemelerin önünde bariyer olsa da uluslararası hukukun siber alandan türeyen suç teşkil eden tehditleri dikkate alarak kural ve kaidelerini revize etmesi gerekmektedir. Çünkü mevcut uluslararası hukuk kurallarında yer alan saldırı, savaş, terör, silah gibi kavramlar siber ortamda vuku bulacak siber saldırı ve savaşları tüm boyutlarıyla açıklamada eksik kalacaktır (Türkay, 2013; 1). Ayrıca, klasik suçlarla mücadelede benimsenen yol, yöntem ve araçların siber suçlarla olan mücadelelerde benimsenmesi 21. yüzyılın bu yeni tehditlerini savuşturmada anakronik kalacaktır.

En genel manada bilişim sistemlerine karşı bilişim araçlarıyla icra edilen suçlar ya da saldırılar şeklinde tanımlanan siber suçlar diğer tehdit unsurlarında olduğu gibi siber ortamın yapısı sebebiyle geleneksel suç türlerinden işleyiş ve nitelik açısından farklılıklar içermektedir. Eylemlerin somutluğunun belirsiz olduğuna bir başka ifade ile anomimlik sayesinde kimliklerini gizleme fırsatı vurgu yapan yukarıdaki alt başlıkta anlatılanlarla birlikte siber ortamın yapısından dolayı karşılaşılacak olan bir diğer hukuki zorluk da yargılama yetkisi üzerinedir (Schmitt, 2012a: 245-260, Hollis, 2015: 156). Çünkü genel olarak siber uzayda icra edilen ve suç teşkil eden eylemler birden fazla ülkeyi alakadar edebilmektedir. Bu durumda yargılama yetkisi ile ilgili suç teşkil eden eylemin uluslararası arenada işlendiği, herhangi bir devletin hudutları dâhilinde olmadığı ya da suçu icra eden fail ile suça muhatap olan mağdurun farklı ülkede ikamet etmeleri halinde klasik yargılamadan farklı bir durum ortaya çıkacaktır (Schmitt, 2012b: 283-293, Laurie, 2015: 180-224). Zikredildiği üzere siber ortamda icra edilen suç eylemleri birden çok ülkeyi hukuki soruna dâhil ettiğinden dolayı birden çok ülkenin de yargılama yetkisi sorununu ortaya çıkarmaktadır. Böylelikle birden fazla muhatap ülkenin yargılama yetkisine sahip olunan hallerde suçun icra edildiği suç mahallinin tam olarak belirlenmesi lazım geldiğinden bu da yeniden isnat edilememezlik sorununu ortaya çıkaracaktır.

Geleneksel hukuk kuralında devletler kendi hudutları içerisinde kendi hukuk kuralını yürürlüğe koyma yetkisine haizdir. Böylelikle suç eylemini icra eden kişi ya da kişiler suçun eyleme döküldüğü ülkenin yargılama yetkisinin altına girerler. Ancak siber ortamın doğası gereği sağlamış olduğu aynı anda birden fazla ve farklı ülkelerden saldırı yapabilme olanağı faillerin tespit edilmesini zorlaştırmaktadır. Örneğin fail bir ülkede bir bilgisayar üzerinden gerçekleştireceği saldırıyı aynı anda birden fazla ülkelerin bilgisayarları üzerinden gerçekleştirerek saldırının farklı ülkelerden yapılması imkânına sahiptir. Nitekim Rus hackerlerin Gürcistan'ın hükümet binalarına, web sitelerine ve tüm banka sistemlerine yönelik saldırılar Estonya ile birlikte Kanada ve Türkiye'de bulunan bilgisayarlar üzerinden gerçekleşmiştir (Clarke ve Knake, 2010: 20-23, Hollis, 2011: 3). İşte, geleneksel hukuk kuralı çerçevesinde ele alındığında suçlunun suçu icra ettiği ülke tarafından yargılanabilme yetkisi aynı anda birden çok ülkenin taraf olduğu ve failin kimliğinin

ve suçu işlediği yeri ispat etmenin çetrefilli olduğu böyle bir durumunda hangi kural belirli olacaktır? Ayrıca, üzerinde herhangi bir gücün hâkimiyet kuramadığı, niteliği ve içerikleri ve etkileri ile belirsizlikleri barındıran bu alanda hangi eylemlerin suç teşkil edeceği, suç olarak kabul edilen eylemlerin hukuki düzlemdeki tanımı, yaptırımların nasıl ve ne şekilde olacağı gibi farklı açılardan farklı sorunlarla yüz yüze kalınmaktadır.

Kısacası 21. yüzyılın değişen dünya dinamiklerinde siber uzayın eriştiği boyutlarla birlikte artan yeni tehditler siber güvenliği de ulusal güvenliğin önemli bir bileşeni haline getirmiştir. Bu nedenle siber ortamdan kaynaklanan illegal eylemler ve bunların neticesinde oluşan suçlar ve tehditlerle mücadelede geniş ve kapsamlı bir şekilde planlanmış hukuksal altyapıya ve düzenlemelere ihtiyaç vardır. Nitekim 21. yüzyılda siber tehdit tanımlamaları ve algılamaları gelişen teknoloji ve bu teknolojilere bağlı yapılan saldırılar sonrasında güvenliğin siber uzay boyutunda mücadele amacıyla ulusal ve uluslararası seviye de bir takım yasal düzenlemeler yapılmıştır.

Bu hususlar ışığında siber suçlarla mücadele de uluslararası boyutta siber suçlara dair atılan ilk ciddi adım Avrupa Konseyi Siber Suçlar Sözleşmesi olmuştur. Budapeşte Sözleşmesi olarak da adlandırılan ve bilgisayar ve internet suçları ile ilgili düzenlemeleri içeren bu anlaşma 23 Kasım 2001 yılında Avrupa ülkeleri tarafından imzalanmış ve 2004 yılında da yürürlüğe girmiştir. Dört kısımdan oluşan bu sözleşmenin birinci kısmı bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçları, bilgisayarla ve içerikle ilgili suçları, telif hakkı ve bununla ilişkili hakların ihlal edilmesine yönelik suçları ve tali yükümlülükler ve yaptırımları içeren maddi ceza hukuku alanındaki belli başlı suçların anlaşmaya üye devletler tarafından tanımının yapılmasını içeren maddelerden oluşmaktadır. İkinci kısmı ise yargılama yetkisini de kapsayan ortak hükümler, depolanan bilgisayar verisinin süratli bir şekilde korunması, üretim emri, depolanmış bilgisayar verilerinin aranması ve bunlara el konulması ve de bilgisayar verilerinin gerçek zamanlı toplanması gibi usul hukuku alanındaki düzenlemeleri içermektedir. Sözleşmenin üçüncü kısmını meydana getiren ve ulusal düzlemdeki siber suçlara dair hukuki düzenlemelerin bu sözleşme ile uyumlu hale getirilmesini

öngören maddeleri ise uluslararası iş birliğine, suçluların iadesi, karşılıklı yardımlaşma, uluslararası anlaşmaların yürürlükte olmadığı durumlarda yapılan karşılıklı yardım taleplerine dair genel ilkeleri ihtiva eden düzenlemelere vurgu yapmaktadır. Nihayet dördüncü kısmın içeriklerini de geçici tedbirlere yönelik karşılıklı yardımlaşma, soruşturma yetkileri konusunda karşılıklı yardımlaşma ve de yedi gün yirmi dört saat iletişim ağlarının işlevselliğini içeren özel hükümlerden oluşmaktadır (European Treaty Series, 2001: 4-25).

Sözleşmenin siber suçlarla mücadele bağlamında sunduğu çözüm önerisinde her ne kadar siber suç kavramına dair evrensel bir tanımlama yapılmadığı ve farklı devletler nezdinde farklı bir şekilde yorumlandığı iddiaları ileri sürülse de siber ortama dair belli başlı suç unsurlarının ve kaynağının çerçevesinin çizilmesi bakımından sözleşme önem arz etmektedir. Sözleşmeye üye devletlerarasında siber suçlarla baş etmede kolektif mücadeleyi öngören anlaşma oydaşmaya varılan ilke ve düzenlemelerin uluslararası iş birliği ortamında uygulanmasını da salık vermektedir. Sözleşmenin bir diğer vurguladığı nokta da, ulusal düzeyde alınacak önlemlerin içeriklerini belirleyerek saldırılara yönelik yasal düzenlemelerin yapılmasını ve yürürlüğe girilmesi koşullarını getirmektedir (Weber, 2003: 425-446).

Siber suçlarla ilgili uluslararası arenada göze çarpan bir diğer önemli hukuki düzenleme de Birleşmiş Milletler tarafından yürürlüğe konmuştur. 2000 yılında BM Ulus aşan Organize Suçlarla Mücadele Komisyonuna dâhil edilerek ele alınan siber suçlarla mücadele konusu ilk önce bilgisayar suçları adı altında ele alınırken daha sonra bu suçlarla etkin mücadele çerçevesinde siber güvenlik başlığı adı altında ele alınmıştır. BM'nin siber suçlara dair kayda değer aldığı sayılı kararlarca; i)Siber güvenlik meselesinde küresel platformda farkındalığı yaratma, sorumluluk, misilleme, demokrasi, risk değerlendirmesi, güvenliğin tesisi ve güvenliğin yeniden ele alınması ve ii) Siber güvenlikle alakalı küresel ve kolektif bilincin geliştirilmesi ve devletler nezdinde büyük öneme haiz kritik altyapıların korunması ile ilgili kararlar alınmıştır (Çifçi, 2013: 109).

Soğuk Savaş sonrasının dinamik ortamında güvenlik algılamalarının da değişmesi ve genişlemesi ile birlikte, 21. yüzyılda, uluslararası güvenlik literatüründe siber ortamdan türemesi pek de hayal olmayan siber savaş kavramı hem geleneksel

silahlı çatışma unsuru olarak hem de başlı başlına yegâne savaş unsuru olarak telaffuz edilmeye başlamıştır (Whittaker, 2004; 288-301). Önce 2007 yılında Estonya'ya ardından da 2008 yılında Gürcistan'a yönelik Rusyalı bir grup vatansever devlet dışı aktörlerin büyük çapta siber saldırılar gerçekleştirmesinin akabinde olayın vardığı boyutları ve vahametinin farkına varan NATO savunma paktı da cevap mahiyetinde geleneksel savaş açma hakkı ve savaşma kurallarını siber alana intibak ettirme saikiyle siber çatışma hukukuna benzer bir belgeyi yürürlüğe koymuştur. Tallinn'in El Kitabı olarak adlandırılan bu belge siber ortamdan kaynaklı olası siber savaşlarda siber ortama dair yazılacak savaş ve çatışma hukukun temelinin oluşmasında zemin hazırlayacak türde içeriklere sahiptir. Mevcut uluslararası hukukun çerçevesini çizdiği savaş açma ve savaşma kurallarının siber alana da uyumlanmasını hedefleyen bu çalışma siber güvenliğin siber hukukuna dair kapsamlı ve detaylı ele alınmasa da atılan ilk adım olarak gösterilebilir (Schmıtt, 2013). Öncelikle bu kitap, devletlerin sınırları içerisindeki tüm ağ sistemlerini ve bileşenleri üzerinde egemenlik salahiyetine sahip tek yetkili merci olarak görür ve dolayısıyla hükümlerinde de detaylı anlatılacağı üzere bu siber altyapılara yönelik gerçekleştirilecek tüm siber saldırı ve eylemleri de hukuk ihlali olarak görmektedir. Dolayısıyla bu nokta da mevcut geleneksel hukuk ilkelerinin silahlı kuvvet kullanılabilen durumları ihtiva eden kuvvet kullanma ve bununla ilişkili olarak da savaş hukuku devreye girmektedir. Çünkü siber güvenliğin sağlanması saikiyle gelecekte ister kavramlar ve normlar düzeyinde bağımsız olarak oluşturulacak olan siber güvenlik hukukunda olsun, ister geleneksel savaş hukukunun siber ortama uyarlanmasında olsun geleneksel savaş hukuk kralları her iki durumda da temel teorik ve kavramsal temeli oluşturacaktır.

Bu sebepler ışığında, uluslararası hukuk çerçevesinde savaş hukukunda hangi durumlarda kuvvet kullanılmasına izin verildiği BM tarafından yazıya dökülmüştür. BM anlaşmasının kuvvet kullanımına dair belirlediği 51. maddeye göre meşru savunma hakkına başvurulmasının birincil kaidesi silahlı saldırıya maruz kalma durumudur. BM'de saldırı kavramı bir devletin diğer bir devletin egemenliğine, ilke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu tanımda belirtildiği üzere, BM Antlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet

kullanılmasıdır şeklinde tanımlanıştır (BM Enformasyon Merkezi, 2002: 1). Bu noktadan değerlendirildiğinde silahlı saldırıya hedef olunması ana koşulunun anlamının açıklığa kavuşturulmasına gidildiği zaman başlıca şu sorularla karşılaşılmaktadır: i) Meşru savunma hakkına başvurabilmek için silahlı saldırının fiilen gerçekleşmiş olması mı gerekmektedir, yoksa çok yakın bir saldırı olasılığı bulunması da bu hakkı vermekte midir? ii) Meşru savunma hakkına başvurabilmek için saldırı eyleminin mutlaka bir devletin düzenli silahlı kuvvetlerince yapılması gerekli midir, yoksa bir devletin yardım ettiği ve desteklediği silahlı grupların ve düzen dışı kuvvetlerin eylemleri de bu nitelikli bir silahlı saldırı olarak kabul edilmekte midir? iii) Meşru savunma hakkına başvurulabilmesi için önceden Güvenlik Konseyinin herhangi bir kararına gerek var mıdır? Ve Güvenlik Konseyi karar aldıktan sonra bu hakkın kullanılma koşulları nelerdir?

Yukarıda, geleneksel hukuk içerisinde yapılan saldırı tanımı çerçevesinde hangi tür eylemlerin silahlı saldırı eylemlerinin niteliğini oluşturduğu açıklanmıştır. Öte yandan, kuvvet kullanımına ilişkin 4. maddenin 2. bendi yine bu nitelikli bir eylemin saldırı olarak kabul edilmesi için iki ek koşul daha eklemiştir. Buna göre, birinci koşul; Güvenlik Konseyinin değerlendirilmesi saklı kalmak üzere, saldırı olarak kabul edilecek eylem bu yönde ilk hareket eden devletin eylemi olacaktır. İkincil koşul ise takdiri Güvenlik Konseyine ait olmak üzere, bir eylemin saldırı olarak kabul edilebilmesi için bunun yeterli yoğunlukta olması gerekmektedir (Pazarcı, 2014: 522). İşte, mevcut geleneksel hukuk kurallarının yapmış olduğu saldırı tanımı çerçevesinde ve koşullarında silahlı kuvvet kullanımına izin vermiştir.

Bu bağlamda, elbette, siber ortamdan neşet eden ve edecek olan saldırıların geleneksel hukukun meşru savunma hakkı çerçevesinde yer alan kuvvet kullanımına uyumlanması konusunda bir takım sorunsallar bulunmaktadır. Bu doğrultuda kimilerine göre, teknoloji araçları ve bunları birbirine bağlayan ağ sistemleri aracılığıyla gerçekleştirilen saldırılar BM'nin silahlı saldırı kategorisine girmediğinden siber saldırılara maruz kalan bir devlette meşru müdafaa çerçevesinde silahlı kuvvet kullanımına başvuramayacağı üzerinedir. Ayrıca, buna paralel bir eylemin saldırı niteliğine haiz olabilmesi için gerekli olan yeterli yoğunlukta olma

gerekliliği de siber saldırılarının silahlı saldırı olarak nitelendirilmesini engellemektedir (Russell, 2012: 212-227, Buchan ve Tsagourias, 2012: 183-186).

Ancak, BM'nin saldırı kavramını tanımlarken kullandığı herhangi bir biçimde silahlı kuvvet kullanma belli bir silahlı çatışma araçlarını ve yöntemlerini belirtmemektedir. BM Antlaşması'nın 51. maddesinde, meşru müdafaa hakkının kullanılabilmesinin ön şartı olarak "saldırının" değil bir "silahlı saldırı"nın gerçekleştirilmiş olması kabul edilmiştir. Ancak, silahlı saldırı kavramının tanımına ne bu maddede ne de diğer madde hükümlerinde yer verilmemiştir. Saldırı ve silahlı saldırı kavramları, belli ölçüde birbiriyle örtüşen kavramlar olmalarına rağmen tam olarak aynı şey değildirler. Daha da önemlisi bunların hukuksal anlamları farklı olup pratikte farklı sonuçlar doğurmaktadırlar (Yayla, 2013: 111). Belli bir silahlı çatışma araçlarından bahsetmeyen bu tanımlama da boyutları ve etkileri ile herhangi bir devletin ülke bütünlüğüne verilecek olan potansiyel bir saldırı niteliği arz eden siber saldırılar sonuçlarının göstereceği etki üzerinden değerlendirildiğinde silahlı saldırı kategorisine girebilmektedir (Roscini, 2014: 133-157). Ayrıca, tüm kritik altyapı sistemleri ağ bağlantılarına bağımlı olan bir ülkeye yapılacak olan siber saldırı hem devletlerin egemenliğine hem de bütünlüğüne yönelik yeterli yoğunlukta şiddeti içerdiğinden kayda değer derecede hasara da neden olacaktır. Çünkü kritik altyapılar devletlerin fiziksel unsurlarıdır. Bu nedenle herhangi bir devletin nükleer tesislerine, petrol ya da doğalgaz hatlarına, hava ulaştırmasına, ya da elektrik altyapı sistemlerine yapılacak olan siber saldırılar sonucunda meydana gelebilecek olan ölümler ve hasarlar silahlı saldırı şeklinde kabul edilecektir. Nitekim ABD siber ortamdan kaynaklanacak saldırıları savaş sebebi saymaktadır (NTV, 2011).

Elbette siber ortamdan kaynaklanacak olan her bir saldırı tıpkı sınır olaylarındaki küçük silahlı çatışmalarda görüldüğü gibi kuvvet kullanımını gerektirmeyecek düzeyde olabilir. Bu noktada Schimitt'in siber saldırıların kuvvet kullanımı kategorisine girip girmemesinde etki, kapsam ve sonuçlar üzerine odaklanan etkiye dayalı analiz yaklaşımı daha aydınlatıcı olmaktadır. Buna göre Schmitt bir siber saldırının kuvvet kullanımına girmesi için ilk önce şiddet yoğunluğuna vurgu yapmıştır. Alınacak önlemler bakımından aciliyetlik durumuna, birbirine bağlı ağlar sistemine olan bağımlılıktan dolayı birden çok kritik altyapıya

yönelecek saldırının nüfuz edilebilirlik durumu, verilecek zararın ve kaybın ölçülebilirlik durumu, yasallık boyutu ve de nihayet sorumluluk boyutu da siber saldırıların kuvvet kulanıma girmesine neden olacak etmenler olduğunu ileri sürmektedir (Schmitt, 2010: 155-156).

Yine bir başka benzer tespitler de Tallinn El Kitabında yapılmış ve çözümlemeler de bu tespitler üzerinden sunulmuştur. Yukarıda da kısaca bahsedildiği üzere Talinn El Kitabı NATO tarafından Estonya ve Gürcistan'a yönelik gerçekleşen yoğun ve şiddetli siber saldırıları sonrasında "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı" şeklinde yayımlanan bir döküman niteliğinde eserdir. Bu eser mevcut hukuk kuralı olan kuvvet kullanımı çerçevesinde savaş açma ve savaşma kurallarının ilkelerini belirleyen düzenlemeleri siber ortamın içeriğiyle eşlenik kılmayı amaçlamaktadır. Tallinn El Kitabı, savaşa girmenin haklı nedenleri (jus ad bellum), savaş sırasında uyulması gereken kurallar (jus in bello), devletlerin ulusal politikalarının bir aracı olarak kuvvete başvurmak konusunu düzenleyen uluslararası hukuk, silahlı kuvvetlerin yönetimini düzenleyen uluslararası hukuk (savaş hukuku, silahlı çatışma hukuku, uluslararası insanlık hukuku da dâhil) konularını içermektedir (MGK, 2013).

Uluslararası siber güvenlik hukuku ve siber silahlı çatışma hukuku şeklinde iki ayrı bölümden oluşmaktadır. 1.kısmı oluşturan siber güvenlik hukukunun devletler ve siber uzay başlığında temel konular egemenlik, yargılama yetkisi ve kontrol ve devlet sorumluluğu konuları yer kaplarken, ikinci kısmı oluşturan silahlı çatışma hukukunun güç kullanımı başlığında ise; güç kullanımının yasaklanması, meşru müdafaa ve uluslararası kuruluşların faaliyetleri ile ilgili konular yer kaplamıştır (MGK, 2013).

Birinci bölümün konusu olan Siber Güvenliğin Hukukuna dair;

Egemenlik boyutunu kapsayan hükümde; devlet, kendi egemenlik bölgesi dahilinde, siber altyapı ve siber eylemler üzerinde kontrol yetkisini kullanabilir ifadesi

Yargılama yetkisi yetkisini kapsayan hükümde; Bir devlet, uygulanabilir uluslararası yükümlülükleri ihlal etmeden, -Kendi sınırlarındaki siber faaliyetlerle

ilgili kişiler üzerinde, kendi sınırlarındaki yerleşik siber altyapı üzerinde, - Uluslararası hukukla uyumlu biçimde, kendi sınırı haricinde de, yargılama yetkisini kullanabilir ifadesi

Devlet sorumluğu bakımından kapsayan hükümde; Bir Devlet, kendisine atfedilebilen ve uluslararası yükümlülük ihlali oluşturan bir siber operasyon konusunda uluslararası yasal sorumluluğa katlanır ve ayrıca karşı tedbir bağlamında uluslararası yanlış eylemlerden zarar görmüş bir devlet, sorumlu devlete karşı, siber karşı tedbirler dâhil olmak üzere orantılı karşı tedbirlere başvurabilir ibareleri bulunmaktayken;

İkinci bölümün konusu olan silahlı çatışma hukukunun

Güç kullanımı başlığının tehdit ve güç kullanımının yasaklanması öngören hükümde; Bir devletin sınırsal egemenliğine veya siyasi bağımsızlığına karşı tehdit ve güç kullanımını oluşturan veya Birleşmiş Milletlerin amaçları ile uyumlu olmayan diğer hallerde, siber operasyon, kanunsuzdur

Kuvvet kullanımı tanımını öngören hükümde; Bir siber operasyonun derecesi ve etkileri, siber olmayan operasyonla karşılaştırıldığında kuvvet kullanımı seviyesine yükseliyorsa, o siber operasyon kuvvet kullanımını oluşturur

Kuvvet tehdidi tanımı öngören hükümde; Bir siber operasyon veya siber operasyon tehdidi, tehdit edilen eylem, misilleme ise, kanunsuz kuvvet tehdidi oluşturur

Meşru müdafa başlığının silahlı saldırıya karşı meşru müdafaa hakkını öngören hükmünde; Silahlı saldırı seviyesine yükselen bir siber operasyonun hedefi olan bir devlet, asıl hakkı olan meşru müdafaa hakkını kullanabilir. Bir siber operasyonun silahlı saldırı oluşturup oluşturmadığı derecesine ve etkisine bağlıdır

Gereklilik ve orantılılık öngören hükümde; Bir Devlet tarafından üstlenilen siber operasyonla ilgili güç kullanımının, Devletin meşru müdafaa hakkının kullanılmasında gerekli ve orantılı olması zorunludur

Yakınlık ve Acillik öngören hükümde; Meşru müdafaada kuvvet kullanma hakkı, siber silahlı saldırı gerçekleşirse veya gerçekleşmesi yakın ise ortaya

çıkmaktadır. Aciliyet gerektiren hallerde ise, daha ileri düzeyde kuvvet kullanma hakkına konu olur

Uluslararası kuruluşların faaliyetleri başlığının Birleşmiş Milletler Güvenlik Konseyi hükmünde; Birleşmiş Milletler Güvenlik Konseyi, bir eylemin barışı tehdit veya ihlal ettiğini veya saldırı eylemi olduğunu belirlerse, siber operasyon dahil şiddet içermeyen tedbirlere izin 14/15 verebilir. Eğer Güvenlik Konseyi, bu tedbirlerin yetersiz olduğunu değerlendirirse, siber tedbirler dahil şiddet içeren tedbirler konusunda karar verebilir ibareleri yer almaktadır (MGK).

Son kertede, bir devlete, meşru müdafaa hakkı kapsamında kuvvet kullanma hakkını veren siber saldırının parametreleri konusunda 51. madde esasındaki yanıtın gereklilik, orantılılık ve aciliyet kriterlerini değerlendirmede devletlerin derin görüş ayrılıkları içinde olmaları ve bunun bir sonucu olarak, siber saldırılar konusunda ortak analitik çerçeve geliştirilememiş olmaları çözümü zorlaştırmaktadır (Yayla, 2013). Bu güçlüğe rağmen, devlet destekli siber saldırılar ve devlet dışı aktörlerin gerçekleştirdikleri siber saldırıların; hangi koşullar altında BM Antlaşması'nın 51. maddesi çerçevesinde silahlı saldırı teşkil edebileceği meselesini incelemeye devam etmek 21. yüzyılda büyük önem arz etmektedir.

3.5. Güvenliğin Tesisi Bakımından

Siber ortamda artarak devam eden baş döndürücü gelişmeler tahmin edilemeyecek sayıda saldırganların yine bu alanı kullanan ve bağımlılığı da aynı oranda artan devletlerin siber altyapılarına yoğun saldırıların icra edilmesini mümkün kılmaktadır (Tabansky, 2011: 63-74, Siboni, 2011: 98-100). Siber ortamı hedefleri doğrultusunda kullanan saldırganların düzeyi şahıslar, suç örgütleri, terörist gruplar ve devletler de olabilir. Siber ortamın sunduğu imkanları kullanmaktan imtina etmeyen bu gruplar politik ve ekonomik bağlamda etkinlik yaratabilme amacıyla kimi zaman direkt olarak ağ sistemlerine kimi zamanda ağ sistemlerine bağlı bulunan kritik altyapı sistemlerine saldırılarda bulunarak şimdiye kadar alışılmadık yeni güvenlik tehditleri yaratmaktadır. Daha da kötüsü, gelişmesi ve etkisi sonlanmayan ve tüm yönleriyle devam eden teknolojik yenilikler ve sistemler yeni güvenlik açıklıkları yaratmaya devam etmektedir. Devletlerde kendine has anarşik yapısı

itibariyle siber ortamın sebep olduğu farklı ve alışılmadık olan bu güvenlik tehdidi açıklıklarını tespit edip asgari düzeye çekme uğraşılarına girmektedirler (Lewis, 2006: 1-12). Bu ortamdan neşet edecek olan tüm açıklıkların ve tehditlerin bütünüyle bertaraf edilemeyeceğinin farkında olan devletler en azından ulusal güvenlikleri nezdinde kritik öneme sahip olan kritik altyapıların ve ağ sistemlerinin güvenliği için bir takım tedbirleri almak zorundadırlar.

Daha öncede sıklıkla bahsedilen siber ortamın kendine has doğasından, hukuksal ve teknik düzenlemelerin yetersizliğinden ve de bu konuda bilgili ve yetenekli insan ve araç gücünün eksikliğinden kaynaklanan operasyonel zafiyetlerinden dolayı siber tehditlerle mücadele de bir takım zorluklar yaşanmaktadır. Ancak bu zorluklardan dolayı siber tehditleri en azından kısa vadede ortadan kaldırmak mümkün gözükmese de bir takım önleyici strateji ve planlarla yeni tedbirler alınabilme imkânı mevcuttur.

Bazıları tarafından yeni bir tehdit, savaş, suç ve terör alanı olarak nitelendirmeye başlanan siber ortamın doğal olarak alacağı ya da alması gereken önleyici tedbirlerinde yeni olması gerekmektedir. Çünkü siber tehditlerin karakteristiği, araçları ve niteliği bundan önceki güvenlik tehditlerininkinden çok farklıdır. Geleneksel güvenlik anlayışının algısında var olan tehditlerin niteliği askeriydi ve bu nedenle de tehditlere verilecek cevaplarda askeri araçlarla sağlanmaktaydı. Ancak kahır ekseriyette belli bir coğrafyaya, devlete ve yahut ta devlet dışı aktörlere odaklanarak tespit edilemeyecek olan kaynağı belirsiz siber tehditlerin önlenmesi, çözümlenmesi ve buna müteakip güvenliğin tesisi anakronik kalan geleneksel güvenlik anlayışındaki mücadele yöntemleri ile sağlanamamaktadır (Bussolati, 2016: 46-54). Bu nedenle kapsadığı geniş alan ve bu alanın sahip olduğu kritik önem devletlerin güvenliğin tesisinde klasik araçlar yerine anlayışlar ve araçların benimsenmesini mecbur bırakmaktadır.

Geniş bir güvenlik perspektifinden bakıldığında, kavram olarak güvenlik tahayyülü nitelik, içerik ve algılama bakımından dönüşerek kabuk değiştirdiğinden dolayı tehditlerle mücadele etme yöntemleri de bu doğrultuda değişmek zorundadır. Bu minvalde siber tehditlerle mücadelenin en önemli ve birincil koşul uluslararası ortamda iş birliğinin benimsenmesidir (Bıçakçı, 2014: 123, Ünver ve Canbay, 2010:

94-99). Çünkü sınır anlayışı olmayan tehditlerin kaynağının nereden ve kimden geldiği belli olmayan bu alışılmışın dışındaki tehditlere yönelik mücadele biçiminde kolektif anlayışı ilke edinmeden bir başarı elde etmek zordur. Bunun içinde atılması gereken ilk adım devletlerin iç hukuk mevzuatlarında detaylı ele alınmayan siber hukuka dair düzenlemelerin uluslararası düzlemde düzenlenen siber hukuk mevzuatlarıyla uyumlandırılması ihtiyacıdır. Özellikle, siber ortamda suç teşkil edecek eylemlerde bulunan suçluların iadesi konusunda karşılıklı yardım iş birliğinin önemli bir parçasını oluşturmaktadır.

Öte yandan uluslararası düzeyde devletlerarasında günün her saatinde aktif halde olacak olan bir iletişim ağının gerekliliği de elzemdir. Çünkü devletler ışık hızında ve etkisinde olan siber tehditlerle mücadele konusunda günün her dakikasında etkileşim ve iletişim konumunda olmak zorunda olduğundan birbirleriyle eş zamanlı olarak hareket etmek zorundadır. Halihazırda bilgi ve iletişim teknolojileri sınır tanımayan özelliği sayesinde ülkeler arasında vuku bulan etkileşimlerin boyutunu derinleştirmektedir. Bilgisayar ve internet ortamında ani bir şekilde birbirinden mesafelerce uzakta olan ülkeler arasında herhangi bir vize engeli gibi sınırlamalar bulunmamaktadır ve bu ülkelerde sanal ortamda etkileşim ve iletişim kurabilmektedir. Tabi bu durum aynı zamanda daha öncede vurgulandığı üzere kilometrelerce mesafe uzaklıktaki bir ülkeye ani ve etkili bir şekilde ortaya çıkacak olan tehditlerinde dolaşımını hızlandırmaktadır. İşte, bu noktada tehditlerin en aza indirilmesi ya da bertaraf edilebilmesi için uluslararası sistemde tüm devletlerin eş zamanlı bir şekilde kolektif bir bilinçle hareket etmeleri gerekmektedir. Siber güvenliğin tesisi noktasında savunma ve taarruz, suçluların iadesi, birbirlerine saldırmazlık anlaşmaları, uluslararası mecrada farkındalık yaratma, bilgi ve teknoloji alanında ve de en önemlisi suçların engellenmesi ve suçluların yakalanmasında bilgi ya da istihbarat paylaşımı gibi konular akla gelen iş birliğine yönelik adımlardır (Bennett, 2012: 10-11, Theohary ve Rollins, 2015: 8-9).

Siber tehditlerle mücadele etmeye ve güvenliği tesis etmeye yönelik bir diğer önleyici tedbir adımı da özel sektörün de devreye sokulmasıdır. Çünkü bu tehditlere karşı tek başına devletlerin mücadele etmesi yetersiz kalacaktır. Bu bağlamda, özellikle özel sektörler kurumlarıyla sağlanacak olan koordineli iş birliği sonrasında

siber alana dair AR-GE çalışmaları, eğitim ve bilgi ve teknoloji altyapısı destekleri öne çıkan iş birliği adımlarıdır. Böylelikle, devlet ile özel sektör arasında iletişim ve koordinasyon sağlanarak iki birim arasında siber den kaynaklı tehditlere yönelik hangi türde ve şekilde iş birliği yapılacağının zemini hazırlanabilir. Bununla birlikte, karşılıklı bir şekilde sağlanacak olan bilgi alış verişi ve eğitim programları da ar-ge çalışmaları ile birlikte sorunların çözümünde daha hızlı ve kolay sonuca varılabilen olanaklar sunacaktır.

Ayrıca, belki de en başta yapılması gereken adım, siber ortama ve dolayısıyla buradan türeyecek olan ve henüz olgunlaşmayan tehdit ve suç olguları üzerinde oydaşmaya varılacak tanımlamaların ortaya konması gerekmektedir. Çünkü bu alana dair yaratılacak olan mutabık tanımlama ve teknik dil hukuk, strateji, planlama ve iş birliği alanlarında da güvenliği tesis etmek için atılacak olan adımları daha da kolaylaştıracaktır. Bununla birlikte, uzlaşıya varılacak olan ortak tanımlama sorunun ne ve hangi türde olduğunu ortaya koyacağından alınacak önleyici tedbirlerinde en azından neye karşı hangi türde alınacağını kolaylaştırarak, sorunun teşhis edilmesini ve teşhis sonrası karar alma süreçlerini de olumlu yönde etkileyecektir.

Siber güvenlik tehditlerini önlemenin veya en azından etkisiniazaltmanın en etkin yollarından biri de eğitimdir. Kurumsal olarak personeli siber güvenlik konusunda eğitmek ve son bilgilerle donatmak artık kaçınılmaz hale gelmiştir. Bununla paralel olarak kurumlardaki ve bireysel kullanımdaki bilgisayarlar en son teknoloji ve güvenlik yazılımları ile donatılmalıdır. Kurumlarda mutlaka risk değerlendirmesi yapılmalı ve olası saldırı ve aksaklık durumunda uygulanacak hareket şekli belirlenmelidir. Yedek planlar oluşturulmalıdır. Sistemlerin işleyişlerinin aksamadan devam ettirilmesi, gerek ekonomik gerekse sosyal anlamda çok önemlidir. Bu sebeple sistemler işler halde iken gerekli müdahalelerin yapılması son derece önemlidir. Bu tür durumlarda gereken müdahalelerin yapılması için oluşturulan koordinasyon büyük önem arz etmektedir. Kritik yapıların korunması için gelişmiş devletlerde olduğu gibi yasal ve idari çalışmaların bir an önce tamamlanması gerekmektedir. Ayrıca kritik altyapılarda kullanılan yazılımların tamamen milli yazılımlardan oluşması, yabancı yazılımlara bağlılığı ortadan kaldıracak ve bu yazılımların, içerisine yerleştirildiği vegerektiğinde kullanılabilecek

olduğu konusunda şüpheler oluşan gizli kodlar veya arka kapılar konusundaki endişeler ortadan kalkacaktır (Öğün ve Kaya, 173).

3.6. Uluslararası İlişkiler Teorileri Bakımından

Nazlı Coucrı ile Robert Reardon'un siber politiğin uluslararası ilişkilerdeki yerine dair yaptıkları literatür tarama çalışmasına göre siber alana dair kuramsal ve yapısal çalışmalar henüz istenen seviyeye gelmemiştir. 2001 ile 2010 yılları arasındaki dönemi kapsayan bu çalışmanın araştırmasına göre yeni alan siberin kuramsal ve yapısal açıdan uluslararası politikaya olan etkisine dair siyaset bilimi dergilerinde yayınlanan makale sayısı sadece 49'dur. Üstelik bunlardan sadece ikisinin siber ortamın bütünüyle uluslararası ilişkilerle olan etkisine ve pratiğine yer verildiğini ileri sürmüşlerdir. Geri kalanlar ise genelde küreselleşme ve sivil topluma, iktisadi gelişmelere ve siber alanın yönetimine dair vurguları kapsamaktadır. Ancak, konularına göre ayıklanarak sıralanan makalelerde Uluslararası İlişkilerin teorik ve kuramsal çerçevesini sunan başat teorilerin -realizm, liberalizm ya da konstüktivizm gib-i diğer yaklaşımların siber uzayı hareket alanı, analiz düzeyi ve güç bakımından nerede konumlandırdıkları ya da bu alanı nasıl tanımladıkları ön plana çıkması gereken çalışma konularıdır (Reardon ve Choucri, 2012: 1).

Her ne kadar, siber ortamın kendine has doğası ve yapısı hasebiyle geleneksel teorilerle ahenkleştirmek zor olsa da 21.yüzyılın uluslararası ilişkileri muhteviyatında yeni politik hamleler atılacağına inanılan bu alanın bahse konu kuramsal ve teorik çerçevede aydınlatılması çabası içine girilecektir. Siber uzay yapısı ve işleyişinde olduğu gibi akışkanlığı ile de daima değişkenlikleri barındıran yeni bir alan olduğu için uluslararası ilişkilerinde yürütülmesinde şekillenen yeni bir alandır (Choucri, 2013: 3-7).

Farklı türdeki sosyal ve politik etkinlik içerisinde büyüyen bağıntılılığı sayesinde gelişen siber uzayı küresel politika mecrasında da etkin olarak görmek makul bir beklenti olacaktır. Şayet, politika yapılan tanımlamalar doğrultusunda ve özünde kimin neyi ne zaman ve nasıl bir şekilde elde ettiği ise şu halde siber uzayda sosyal etkinlik içerisinde vuku bulan hızlı gelişimi, ve yine uluslararası güvenlik, küresel ekonomik, politik ve sosyal organizasyon ve fikirlerin yayılmasında ve

gelişmesi gibi önemli platformlarda artan önemi bu yeni alanın dönüşümsel etkisini görünür kılmaktadır.

Yine, kayda değer bir sosyal, ekonomik ve politik bir etkinlik mahalı olarak siber uzayın yükselişinin uluslararası ilişkiler uzmanları nezdinde ilgi görmesini ummak makul bir beklenti olacaktır. Bu önemli ve kamuya ait bir kaynak olarak doğan ve günümüzde siber güvenliği ve askeri stratejileri ve de kendisine erişimi ile sağladığı uluslararası küresel erişimi ihtiva ettiğinden artık farklı yönlere ve çeşitli açıları etkileyen siber uzayın bir siber politik alanı da olması kaçınılmaz olmuştur. Bu durum da, sosyal bilimcilerin artık bu alanı ve bu alandan kaynaklı sorunsallara değinmesi ve adres göstermesi gereksinimi ortaya çıkarmaktadır (Choucri, 2013: 3).

Uluslararası İlişkiler camiasının 21. yüzyılda kendine has doğası itibariyle siber ortamın güvenlik bağlamında uluslararası politika da araçları, mekansallığı, imkanları, içerikleri ve pratikleri ile dikkatini çekmesi gerektiğine inanan çalışmanın bu bölümü de geleneksel Uluslararası İlişkiler teorileri çerçevesinde kuramsal bir değerlendirmeyi amaçlamaktadır. Gayri merkeziliği ile sınırsızlığın tezahürü olan siber uzayda sınırları açık ve belli bir egemen devlet-merkezli anlayışın düsturu üzerinden yorumlamalar ileri süren geleneksel Uluslararası İlişkiler teorileri, geçirdiği gelişme aşamaları ile bu yeni ortamda uluslararası ilişkileri nasıl inceleyecek, açıklayacaktır ve de bir dizi meta teorik varsayımlar ileri sürecektir? Bu teoriler, bu yenidünyayı okumak ve anlamak için yeterli enstrümana sahip mi? Geleneksel Uluslararası İlişkiler anlayışıyla siber uzayda bir düzen kurmak mümkün mü? Bir siber barış anlaşması yapmak ya da süper siber güçlerin hegemonyasında bir sistem kurmak olası mı? Uluslararası siyasetteki yapı birim, faillik, süreç, konu ve eylemler hakkında muhtelif genelleme, kavramsal ve kuramsal çerçeve gibi belli başlı önermeler sunan ve bu önermelere istinaden de güçler dengesi, ulusal çıkar, savaş ve barış muhayyilesi, uluslararası toplum, emperyalizm, hegemonya, anarşi söylemi gibi kavramlar ile siyasetin güç mücadelesi olduğunu ve de bilginin siyasal olarak belirlendiği ileri süren uluslararası ilişkiler teorileri bu yeni ortamda nasıl bir analitik işlev yerine getirecektir, süper siber güç olmak için devlet olmak gerekli mi? Güç dengesinden bahsedilebilir mi? Gibi uluslararası ilişkiler disiplininin

muhtevitayında yer edinen geleneksel teorilere yönelik bu alanda sorulması gereken sorular olarak göze çarpmaktadır (Akyeşilmen, 2015).

Müşahede edildiği üzere kısa bir geçmişi olan uluslararası ilişkilerin tarihsel gelişim seyrinde devlet her daim disiplinin merkezinde yer aldığından siber alanda da devletin konumunu ve işlevini bilmek gerekmektedir. Soyut ve tarih dışı bir mevcudiyetten öte toplumsal ve de tarihsel olan devlet figürü her daim oluşum ve dönüşüm sürecindedir. Uluslararası ilişkilerin tarihi de bir bakıma devlet ve devletlerarasındaki ilişkinin doğası ve zamanla ne şekilde bir evrim geçirdiği üzerinedir (Goertz ve Dahl, 1992: 33-34), ve dolayısıyla uluslararası sistemde siyaset yapma biçimini yorumlayan teoriler aynı zamanda değişimlerin ve dönüşümlerin de kökenlerine ve dinamiklerini de incelemektedir. Ancak sözü edilen değişim ve dönüşüm olgusu burada inşa edilen alan olarak ve kendine özgü yarattığı gerçekliklerle siber güvenliğin kuramsal ve siyasal perspektifinden değerlendirilecektir.

Siber ortam tüm birimler nezdinde sosyal, ekonomik ve politik hareket tarzı olarak doğmuş ve bu yeni hareket tarzı aynı zamanda 21. yüzyılda uluslararası ilişkileri tüm analiz seviyelerinde ve dünyanın her yerinde güvenlik açısından talepler, kapasiteler, aktörler, çıkarlar, etki ve baskı gücü, küreselleşme gibi muhtelif dinamiklerle tanıtarak dikkate değer değişimleri hızlandırmıştır.

Toplumsal ve tarihsel bir olgu olan ve de sürekli oluşum ve dönüşüm içinde olan ülkesel ve egemen devlet sisteminin sınırlarının ihlal edilemezliğine belki de en büyük meydan okuma her tarafa yayılan ve dönüştürücü özelliği ile küreselleşme süreci olmuştur. Bu süreçle birlikte, geleneksel stratejiler ve davranış kuralları ve kalıpları cevap olarak yeni doğan ve hızla değişen ampirik parametrelerle uyumsuz hale gelmektedir. Bu durum günümüz uluslararası sisteminin kaçınılmaz ve zorlu bir gerçeğidir. 20. yüzyılın en önemli miraslarından biri Soğuk Savaş'ın bitimi ve akabinde ABD'nin süper güç olarak sahneye çıkmasıdır. Bununla birlikte, o zamana değin pek karşılaşılmamış olan ve dekolonizasyon sürecinden çıkış, Sovyetlerin parçalanması ve donmuş çatışma bölgelerinde iç savaşların patlak vermesi sonucunda egemen devletlerin sayısındaki artışı getirmiştir. Ayrıca, küresel boyutta etkin olabilmek, kaynaklar üzerinde rekabet eden ve yani politik arzuları olan

bölgesel güçler de sahneye çıkmıştır. Öte yandan 20.yüzyılın son çeyreği dünya genelinde çatışmaların ve şiddetin niteliğinde yaşanan dönüşümlerle de yüzleşmiştir. Sömürge yönetimlerine karşı devlet dışı aktörler tarafından başlatılan bağımsızlık savaşları yerini bu kez küçük gruplardan terörist gruplara kadar geniş yelpazede yer bulan devlet dışı aktörler arasında yaşanacak olan iç çatışmalara ve savaşlara bırakmıştır.

20. yüzyılın uluslararası sistemi ana hatlarıyla çift kutupluluğu, tek kutupluluğu ve çok kutuplulukları evreler halinde yaşamıştır. Ancak bu durum yerini 21. yüzyılın yeni yapısal biçiminin getirdiği gücün farklı alanlarda farklı birimlerle paylaşımı, farklı türde yeni asimetrik güçlerin belirmesi gibi nispeten devletlerarasında katı hiyerarşiyi aşındırıp daha zayıf ve geçişkenlik arz eden bir hiyerarşiye bırakmıştır. İşte, bu yeni yapısal değişimi siber ortamın doğası ile uyumlandırıldığında göze çarpan unsur siber ortamın şimdiye kadar görülmedik şekilde gücü ve etki etme kapasitesini farklı düzeydeki aktörlere seçilir kıldığıdır (Drezner, 2002: 477-498). Ağlanmışlığın gelişmiş ülkelerde oldukça yüksek olduğu, gelişmekte olan ülkelerde ise hızla yükseldiği günümüzde siber uzay, ulus-devlet içinde ve/veya ulus-devletten bağımsız yeni aktörler oluşmasına neden olmaktadır. Siber uzay üzerinden bireyler ulusal kimliklerinden bağımsız olarak dünya çapında örgütlenebilmektedir. Ortaya çıkan bu örgütlenmeler ulus-devletlere farklı konularda tepkilerini dile getirebilmek için hacktivizmi bir eylem biçimi olarak benimsemektedirler. Örneğin Edward Snowden, Julian Assange gibi bireyler fiziki yollarla elde ettikleri bilgileri siber uzay üzerinden kamuoyuna açıklayarak, ulus-devletlere olan bağlılığın sorgulanmasına yol açabilmektedirler (Ermiş, 2015).

Uluslararası sistemin günümüz düzeninde ve uluslararası ilişkilerin idaresinde halen devlet, sistemin merkezindedir ve de sistemin temel değişken aktörüdür. Ancak 21.yüzyılda uluslararası sistemi karmaşık ve karşılıklı bağımlılık içerisindeki aktörlerin süratli bir şekilde devinen ilişkilerinin bir bütünü olarak okunduğunda farklı baskın değişkenlerinde tebarüz ettiği görülmektedir. Bu değişkenlerden en önemlilerinden biri olan siber ortamda özellikle ulusal güvenliğe yönelik farklı türde ve nitelikteki kaynakları, araçları ve tehditleri ile siber güvenlik başlığı altında yeni boyutlarda ulusal güvenlik sorunsalları teşkil etmiştir.

Zayıf aktörler için ses getirmede ve güçlü aktörleri tehdit etmede emsalsiz yeni türde asimetrik güç unsurları ortaya çıkmıştır. Siber ortamdan kaynaklı bu yeni asimetrik güce sahip aktörler uluslararası sistemde yeni oyunlarda ve geçişlerde muhtemel unsurlar olacaktır. Siber merkezli güçlenen yeni aktörler yeni tehdit ve suç türleri ile uluslararası arenada tahmin edilemeyen belirsizlikler ve bulanıklıklar yaratmaktadır. Ulusal güvenliğe yönelik siber tehditler bu yeni hareket alanının araçları ile askerileşmesi, saldırılar sonrasında siber savaş ve bilgisayar ağlarına bağımlı olan kritik altyapılara saldırılar ve istihbarat ya da casusluk amacıyla kullanımdan oluşmaktadır. Devletler de eş zamanlı olarak politik ve sosyal bağlamda amacı kendilerinin güvenliğine tehdit oluşturmak, askeri ya da ekonomik saiklerle istihbarat toplamak olan bu yıkıcı grupların farkındadır.

Bu bilgiler ışığında uluslararası ilişkiler disiplininin hakim teorisi konumunda olan realist paradigma (Smith, 1986: Wohlforth, 2008); güce ve gücün devletler arasındaki dağılımının uluslararası ilişkilerdeki etkisine ve yönetişimine odaklanmaktadır. Çünkü realist teori güç nosyonunu aktörlerin birbirlerinin manevi ve maddi kapasitelerinin algılamasının bir işlevi olarak görür. Bir başka deyişe uluslararası sisteme karakteristik özelliğini veren gücün kayda değer önemi, gücün dağılımıdır (Waltz, 1986). Bunun sonucunda da uluslararası sistemin temel davranış ve siyaset yapma biçimini güç mücadelesi yapmak olduğunu ileri sürmektedir. Bu sebeple uluslararası politikayı da güvenli olmayan ve anarşik koşullar altında hayatta kalma, güvenliği temin etme ve ilaveten gücünü artırma ortamı olarak kategorize etmektedirler. Tüm devletlerin esas amacının hayatta kalmak olduğunu saptayan realizm başkalarının niyetlerini ile ilgili belirsizliğin olduğu ortamda devletlerin hayatlarını idame etme konusunda kendisinden başka kimseye güvenemeyeceğini ve bundan mütevellit herhangi bir kural koyucunun ve güvenin olmadığı anarşik düzende her devlet kendi başının çaresine bakmak zorunda olduğunu ifade eder.

Yukarıda siber ortama dair bahse konu edilen literatür taraması ile ilgili istatistikte Couchri'nin ifade ettiği üzere alanın Uluslararası İlişkiler disiplini ile ilintili olan kuramsallığı ile ilgili çalışma sayısı oldukça azdır. Nihayet siber ortamın Uluslararası İlişkiler disiplininin uluslararası politikayı yorumladığı güç, anarşi ve güvenlik parametreleri doğrultusunda ele alan kişi James Adams olmuştur. Adams'a

göre egemen devletler üzerinde belli başlı bir karar alıcının ve kural koyucudan yoksun olan anarşik bir ortamın tezahürü siber ortamda yeni güç mücadeleleri ve savaşlar mümkündür. Ona göre anarşik bir rekabet ortamının tezahürü olan bu yapıda her devlet belirsizliğin olduğu bu ortamda ya bizatihi kendi başına siber savunma ve gücü oluşturur ya da dar yelpazede anlaşmaya varabileceği müttefik güçlerle oluşturur (Adams, 2011). Bu nokta da, yine realist anlayışın temel kabullerinden olan güvenlik ikilemi ortaya çıkmaktadır. Çünkü başkalarının niyetleriyle alakalı ciddi belirsizliklerin olduğu bir siber ortamda herhangi bir aktörün aldığı güvenlik önlemleri diğerleri tarafından tehdit olarak algılanacaktır; diğerleri de kendilerini koruma saikiyle adım atacak; bu adımlar ise birinci aktör tarafından diğerlerinin tehlikeli olduğu yönündeki başlangıçtaki varsayımını doğrular nitelikte yorumlanacaktır; asılsız korkular sarmalı ve gereksiz savunmalar böylece sürekli devam edecektir. En nihayetinde de realistlerle benzer mantığa sahip Adams'a göre tıpkı realistlerin uluslararası sisteme ve politikaya dair ileri sürdükleri kimsenin asla tamamıyla güvende hissedemeyeceği böyle bir sanal ortamda rakip birimler dünyasında güç mücadelesi devam edecek ve güvenlik ve güç biriktirmenin kısır döngüsü de stabil kalacaktır.

Aslında Adams bu ifadelerle anarşik bir atmosferde niyetlerdeki güvenilmezliğin bir sonucu olarak da devletlerin sahip olduğu ve elde ettikleri her türlü kazancı diğer devletlerin sahip oldukları ve elde ettikleri kazançlar ile mukayese ederek değerlendirmiştir. Ancak, siber ortamda güç ve güvenlik anlayışı doğrultusunda her ne kadar bahse konu mutlak ve göreceli kazanç mantığı kısmen doğruluklar barındırsa da güvenliğin tesisi noktasında bu durum tezatlık da teşkil etmektedir. Çünkü realist teorinin güvenliğin tesisi bakımından öngördüğü kabul askeri araç kapasitesinin artırımıdır. Ancak, siber ortam da güvenliğin sağlanması çerçevesinde aynı yöntem istenen karşılığı bulamayacaktır. Çünkü bu ortamda devletler ne kadar fazla savunma ve saldırı araçlarını geliştirirse doğru orantılı olarak bir o kadar saldırıya açık ve maruz kalacaklardır. Yine bu noktada Adams'ta belki de konvansiyonel askeri güç bağlamında büyük imkân ve kapasitelere sahip ABD üzerinden verdiği örneklem de bu savı doğrulamaktadır. Adamsa göre bilgi teknolojileri bakımından dünya da ilk sırada yer alan ABD aynı zamanda yine bilgi

ve teknolojiler aracılığıyla siber saldırılar karşısında muhtemelen en savunmasız ülkelerin başında gelmektedir. Çünkü bu ortam hem devlet dışı suç teşkil eden aktörler düzleminde hem de güçlü olmayan devletler düzeyinde hiyerarşiyi zayıflatmakta ve asimetrik güç ilişkilerini görünür kılmaktadır. Böylelikle otoritenin parçalanmasının hızlanması, gücün aktörler düzeyinde dağılımının artmış olması ve niteliğinin değişmiş olması güvenlik yapılarını da ters yüz etmiştir (Karagül, 2015: 122).

Geçmişten bir örnekle durumu izah edilirse Adamsın ifade etmeye çalıştığı bu asimetrik tehdit ve risklerin engellenemezliği daha net bir biçimde açıklanmaktadır. 1998 yılında sofistike bilgisayar sistemlerini kullanan ve bunlardan faydalanan bir grup hacker NASA ve Pentagonun da bulunduğu devlet kurumlarına ait veri tabanlarına siber saldırılar gerçekleştirmiştir. Hackerler siber saldırılar aracılığıyla ABD'nin devlet kurumlarına ait binlerce gizli tutulması gereken belgeleri, kriptoları ve başka türde hassas bilgileri içeren dokümanları ele geçirmiştir. Akabinde gerçekleştirilen soruşturma sonucunda ise saldırıların kaynağının Rusya'ya ait IP adreslerini işaret etse de, bu saldırıların Rusya tarafından icra edildiği hiçbir şekilde ispatlanamamıştır (Adams, 2001).

Yine Adams'ın yakın dönemden sunduğu başka örnekleminden hareketle, 2010 Stuxnet saldırısı siber saldırılar nezdinde devletlerin hala savunmasız olduğunu göstermiştir. Birçok kurum ve kişiler tarafında İran'ın nükleer tesislerine ve kritik altyapılarına yönelik gerçekleştirilen bu saldırıların arkasında kahır ekseriyette devletlerin desteği olmadan gerçekleştirilemeyeceğidir. Bir nevi, güçlü güçsüz fark etmeden tüm devletlerin siber ortamda sahip olabileceği araçlarla ve diğer imkânlarla kimi zaman direkt kendileri kimi zamanda devlet dışı aktörleri arkadan destekleyerek rakip bir devlete iz bırakmadan saldırabileceği ve buna karşılık herhangi bir cezai yükümlülükle de karşılaşmayacağı bir uluslararası sistemden bahsetmek mümkün olduğundan diplomatik kaosa ve kâbusu vaki kılmaktadır. Böylelikle de bu ortamda uluslararası sistemin kurumlarına ve güven ortamına dair bir kırılma yaşanacak ve tehditlerin nereden ve ne şekilde geleceğinin belli olmaması durumu ile niyetlere güvenmeyen devletleri geri çekecek ve kendi gücünü kendisi kuracaktır.

Siber uzay bağlamında devletlerin güvenlik unsurları değerlendirildiğinde askeri, ekonomik ve siyasi boyutların ön plana çıktığı görülmekte ve dolayısıyla da dile getirilen boyutların güvenliğinin de önem arz ettiği ortaya çıkmaktadır. Savunma, bilgi sistemleri ve kritik altyapılara yönelik saldırılar devletlerin günlük yaşamına dair işlevlerini felce uğratabilme potansiyeline sahip olduğu için hem ekonomik hem de askeri ve siyasal mecralarda kaos yaratabilmektedir. Siber ortamın asimetrik güç üstünlüğü sağladığı noktasında Adams farklı ülkelerin ismini zikretmiştir. Konvansiyonel askeri gücün aksine siber ortamda ABD'nin askeri gücüne galebe çalmak isteyen ülkelerin asimetrik üstünlük elde etmek saikiyle konvansiyonel yöntemlerden ve araçlardan daha az maliyetli olan ve bir o kadar da sonuçlara etkisi olan siber silahlara erişebilme imkânını vermesi farklı güçte ülkeleri bu alanda büyük yatırımlar yapmaya sevk etmektedir. Çin'e özel vurgu yaptığı çalışmasında Adams, Pekin hükümetinin yeni ve gelişen teknolojilere muazzam yatırımlar yaptığını, ulusal savunmalarıyla eş zamanlı işleyen savaş birimleri kurduğunu ileri sürmüş, öyle ki Çin'in bu politikalarına karşılık ABD siber güvenlik konseptinde bu durumu The Great Firewall of China şeklinde yer vermiştir. Farklı yön ve boyutları ile aynı anda avantajlar sağladığı gibi öte yandan dezavantajları da barındıran bu yeni ortamda siber tehditlerin öneminin farkındalığına varan ülkeler ulusal güvenlikleri kapsamında gerekli önleyici tedbirlerini, stratejilerini, planlarını, ağlara dayalı altyapı ve organizasyonlarını revize edip yeni inşa etmektedirler.

Joseph Nye ise uluslararası ilişkilerde henüz tam olarak olgunlaşmayan siber ortamı dinamik yapısı itibariyle gelişime açık görmüş ve ulusal güvenlik stratejilerinde bu alanın yeni boyutlarıyla ele alınmasını salık vermiştir (Nye, 2011: 21-35). Çünkü ona göre de, siber ortamda fiziki altyapılardan meydana gelen ve ağlarla birlikte, ağları birbirine bağlayan fiber optik kabloları ve internet altyapılarını devlet egemenliğinin farklılaşan alt birimlerinden biri olarak görmüştür. Dolayısıyla bu alanı ulusal güvenlik çerçevesinde ciddiyetle ele alınması gerektiğini kabul eden Nye, öte taraftan alandan kaynaklanan tehditlerin niteliği, boyutları ve bunlara karşılık oluşturulacak eylem planlarını ve sonuçlarını analojik yöntemlerle geleneksel güvenlik anlayışının popülaritesinin en yüksek olduğu Soğuk Savaş döneminin kuramsal paradigmalarıyla da açıklanmasına karşı çıkmıştır. Çünkü Nye'a

göre siber ortam ile geleneksel kuramsal yaklaşımlar arasında benzerliklerden çıkarım yapma yöntemini uygulayabilmek için tarihi, tarihin paradigmalarını kavramak ve anlamak gerekmektedir. Yeni ve olgunlaşmamış dolayısıyla tarihi ve deneyimleri de yeni olan bu alana dair de bazı kuramsal fenomenleri kullanmak hatalı olacaktır (Nye, 2011).

Bu bağlamda, siber alanın ortaya çıkışı sonrası ve özellikle siber uzayın kullanımında 21. yüzyılda yaşanan artış ise ulus devletlerin tek meşru otorite olarak kabul edildiği sistemi tehdit etmektedir. Siber uzayın sanal katmanında sınırların olmayışı ve bu durumdan kaynaklı egemenlik alanlarının belirsizliği, devlet dışı aktörlerin güç kazanmasına neden olmuştur. Bu durumu güç yayılımı (power diffusion) olarak kavramsallaştıran Nye devletlerin kara, deniz ve hava boyutlarında olduğu gibi siber uzayda da bir güç olarak var olmalarına karşın, siber uzayın doğasının devletlerin tek aktör olarak bu alanda hâkim olmalarına izin vermeyeceğini belirtmiştir. Bu bağlamda siber uzayda güç, büyük devletlerden diğer devletlere ve daha da önemlisi devlet dışı aktörlere yayılmaktadır. Ortaya çıkan yeni sistem ise pre-westphalian sistemin çok aktörlü yapısı ile benzerlik göstermektedir (Ermiş, 2016). Nye'nın ortaya koyduğu bu görüş paralelinde her ne kadar siber uzayın doğası, aktör yapısı itibariyle pre-westphalian dönemle benzerlik gösterse de bu alanda aktörlerin birbirleriyle ilişki kurarken dayandığı kapasiteler farklılık göstermektedir. Çünkü siber uzayda en fazla varlığa sahip olan devletler saldırıya en açık olanlardır. Orta Çağ'da askeri anlamda en güçlü olan aktör, diğer aktörler üzerinde egemenlik kurarken, siber uzayda güçlü olan aktörün diğer aktörler üzerinde egemenlik kurması mümkün değildir. Aksine, siber uzayda güçlü olan devletin siber uzayda varlığı olmayan ama ofansif kabiliyet geliştirmiş bir aktör karşısında konvansiyonel karşılık vermesi dışında bir seçeneği yokken, ofansif kabiliyet geliştiren aktör, siber uzayda devlete büyük zarar verebilir (Ermiş, 2016).

Örneğin, siber tehditler ve savaşlarla ilgili mevcut delil olarak gösterilen Estonya, Gürcistan ve İran'a yönelik saldırıların akabinde ortaya atılan en önemli düşüncelerden biri nükleer denge dönemine atıfla caydırıcılık kavramı olmuştur. En genel ve kısa anlamda caydırıcılık karşılık verebileceği ihtimalini canlı ve gündem de tutarak rakibini belli bir davranıştan vazgeçirme politikasıdır. Daha çok Soğuk Savaş

döneminin uluslararası politikasında sürekli gündemde tutulan ve pratiğe dökülen bu kavram tarihsel süreçte de bir ülke ya da ülkeler tarafından başka ülkeleri saldırıdan ve tehditlerden caydırma amacıyla başvurmuşlardır. Soğuk Savaş sırasında da uluslararası politika da nükleer silahların devreye girmesiyle birlikte nükleer silahların kullanımı ile ilgili stratejilerden biri haline gelen caydırıcılık kavramı süper güçler arasında şekillenen güç dengesi mantığının tezahürüydü (Best vd., 2012: 243-270). Misalen, Soğuk Savaş döneminde süper güçlerden birinin rakip gücün avantajlı konum elde etmesinin bir başka deyişle de aralarındaki güç dengesinin bozulmasının engellenmeye çalışılmasının bir başka yoluydu. Bu nedenle caydırıcılık kavramı aynı zamanda güç kavramı ile doğru orantılıdır (Anders, 1998: 119-124). Arzulanan sonuçları elde etmek ve bu yolla başkalarını etkileme becerisinin olmazsa olmazı güçlü olmaktır. Ancak Nye'a göre siber ortamda diğer ortamlarda olduğu gibi büyük devletler salt bir tahakküm kuramayacaklardır. Çünkü burada ezici hâkimiyet ve güç üstünlüğünü elde edecek olan devlet aynı zamanda sistemden kaynaklı açıklıkların ve risklerin kaçınılmazlığından ve risklerin fazlalığından dolayı aslında en savunmasız ülke konumuna gelmektedir. Böylelikle bu alanda artırılacak olan güç ve kapasite ters orantılı bir şekilde karşı saldırı potansiyelini de artıracaktır. Bu durumda devletlerde saldırı kapasitesinden daha çok savunma stratejilerini geliştirme peşine düşeceklerdir.

Bir diğer taraftan nükleer strateji incelendiğinde ise durum bundan çok farklıdır. Nükleer silahların gün yüzüne çıkmasıyla imkan ve kapasiteler dahilinde sınırlı sayıda büyük gücün gerektiğinde saldırı amaçlı kullanılabilecek nükleer silahlanmaya gittiği görülmüştür. Çünkü Soğuk Savaş döneminin ideolojik kamplaşma döneminde en önemli saldırı aracı ve stratejisi nükleer kapasiteye sahip olma ve imkanlar doğrultusunda bu aracı kullanabilme potansiyeliydi. Dolayısıyla nükleer silahların ve araçların yıkıcı etkisinin de farkında olunması sebebiyle caydırıcılık cevap bulmakta ve işe yaramaktaydı. Ancak siber ortamda da başkalarının yapmak istediğine aynıyla mukabele etmek düsturu olarak tanımlanan siber caydırıcılık stratejisini bu alana uygulamak pek mümkün gözükmemektedir. Çünkü, devletlerin öncelikle bu alanda en iyi savunma saldırıdır anlayışının tersine en iyi saldırı ve strateji savunma anlayışını benimsemeleri gerekmektedir.

Hâlihazırda kimden ve ne şekilde geldiği belli olmayacak olan siber saldırılara karşı bir caydırma stratejisi de uygulanamayacağından bu noktada en muteber caydırıcılık tavrı saldırıya odaklı nükleer caydırıcılığın yerine savunmaya odaklı siber savunma anlayışı benimsenmelidir. Zaten siber ortamda savunma nitelikli bir şekilde uygulanırsa icra edilecek olan saldırıların etkisi de küçük çaplı olacaktır. Nitekim son zamanlarda devletler de siber savunma mantığı içerisinde bilgi sistemlerini hedef alabilecek saldırılara karşı hazırlıklı olmak, saldırılara karşı kurum içi politikaları ve karar destek mekanizmalarını değerlendirmek, kurumlar arası bilgi paylaşımını, haberleşmeyi ve koordinasyonu ve olası bir saldırıdan sonra geri kurtarma planlarını test etmek, tehditlere ve açıklıklara karşı farkındalık oluşturmak ve de personeli eğitmek maksadıyla çeşitli tatbikatlar ifa etmiştir (Tatar, 2011). Gerçekleştirilen tatbikatların genel başlığının olası siber saldırılara karşı (Akşam, 2015) şeklinde açıklanması yukarıda bahse konu siber savunma anlayışı önceliğini de haklı çıkarmaktadır. Çünkü yapılacak olan iyi ve geniş kapsamlı savunma stratejisi hem misilleme yapma fırsatı hem de bu alanda henüz gelişmemiş diğer tarafların da saldırılarını başlamadan sonlandırma fırsatı verecektir. Bu durum da, saldırıya aktif katılan düşman birim sayısını azaltacağından saldırıların belki de kimden geldiğinin tespitini kolaylaştıracağından ancak o zamanda iyi savunma aracılığıyla saldırı yapma imkânını sağlayacaktır.

Klasik bağlamda bahsedilen caydırıcılıktan siber uzayı farklı kılan bir diğer önemli yön de saldırının kaynağı ile ilgilidir. Örneğin Soğuk Savaş döneminde nükleer savaş ihtimalinde kimlerin kimlere karşı nükleer silahları saldırı amaçlı kullanacağı belliydi. Yukarıda da kısa bir şekilde dile getirildiği üzere siber uzayda saldırının kimden geldiğini tespit ya mümkün değildir ya da çok zordur. Bu da caydırıcılığın eyleme dökülebilmesi için gereken belli ve açık düşman kimliğini ortadan kaldırdığından siber ortamda sıkça adlandırılan caydırıcılığın kime karşı yapılacağı sorusunu ortaya çıkarmaktadır. Şayet caydırıcılığın amacı düşmana niyetlendiği eylemleri yapma konusunda cesaretini kırmak ve göz dağı vermek ise öngörüler ve ihtimaller dahilinde saldırıyı kimin gerçekleştirdiği tam olarak netleşmeyen durumda herhangi bir ülkeye yönelik gerçekleştirilecek olan saldırı hedefine ulaşmış sayılmayacaktır. Aksine muhtemelen var olan düşman sayısını daha

da artıracaktır. Saldırıyı kimin gerçekleştirdiğin tespiti genelde arafta kalan bu durum aslında siber uzayın mahsülü olan devlet destekli ve menşeli saldırıları azaltabilirken bir diğer taraftan da tespit edilememezlik özelliğinden dolayı da saldırı fırsatı sunabilir.

Caydırıcılığı istisnai yapan unsurlardan bir diğeri de cezalandırıcı rolünü icra eden saldırı kapasitesinin kontrollü bir şekilde gösterimidir. Yani, caydırıcılık gücünü ispat etmek isteyen devlet tarafından saldırgan kapasitenin kontrollü olarak ifşa edilmesi, diğer devletlerin uygulayacağı politikaların oluşturulmasında bir hayli önemli paya sahiptir (Ermiş, 2015). Bu bağlamda, devletler askeri güç ve caydırıcılık kapasitelerini ifşa etmek için tatbikatları ve törenleri bunun için araç olarak kullanırken, siber uzayda ise bireyden devlete kadar farklı düzeyde ve etkide aktör konumlandığı için sber kapasite ile gösterilmesi gereken güç ve caydırıcılık mesajı hangi şekilde ve kime karşı gösterilecektir şeklinde soruları barındırmaktadır (Ermiş, 2015).

Siber uzayda caydırıcılık etkeninin muhtemel olduğunu dile getiren ancak bazı önemli soruların cevaplanmasının şerh koyan Libicki de farklı noktalara vurgu yapmıştır. Ona göre bu sorular şimdilik siber caydırıcılığın kuramsal çerçevesine dair problem oluşturan birincil derecede ve ikincil derecede cevaplanması gereken sorulardır (Libicki, 2009: 64). Buna göre birincil derecedeki sorulardan birincisi daha öncede bahsedildiği üzere saldırganın isnat edilemezliğini vurgulayan kimin yaptığını biliyor muyuz sorusudur? Çünkü hangi alanda ve hangi şartlarda olursa olsun caydırıcılığın teoride v pratikte eylem alanı bulması için tanımlanabilen bir devletin kimliğinin ispatı şarttır. Çünkü caydırıcı emeller doğrultusunda kimi zaman gerçekleştirilen misilleme ya da korkutarak cesareti kırma filini doğru rakip devlete yöneltmek gerekmektedir. Aksi takdirde bu durum hem teorik olarak caydırıcılık anlayışına zarar verdiği gibi aynı zamanda da sayıları daha da artacak düşmanların saldırılarının artmasını da beraberinde getirmektedir.

Libicki'ye göre cevaplanması gereken ikinci soru rakip devletin değerli varlıklarını tehlike altında tutulabilip tutulamadığı üzerinedir. Ona göre, caydırıcılığın hedefine ulaşması için muharebe hasar tahminin yapılması kritik derecede öneme sahiptir. Hangi hedeflerin ne derece de hassas olduğu ve bu

doğrultuda yine ne derece de zararlarının giderileceği gibi bilinmesi zor dinamikler mukabelenin ne ölçüde olmasını zorlaştırmaktadır. Çünkü mukabelede bulunurken hedef sistemlerin yapısının boyutlarının ve ölçeğinin ne derece de hasara dayanaklı olduğunun anlaşılamaması neticesinde verilen hasarın orantısız olması gerginliklerin nüksetmesine neden olur. Libicki nazarında saldırgan ya da mukabelede bulunacak kişinin muharebe hasar değerlendirmesinde göz önünde bulundurması gereken sorular; saldırının yayılıp yayılmadığı, hedeflenen sistemlerin işlevselliğini sekteye uğratıp uğratmadığı, hedeflenen sistemler karar alıcılıların kararlarını etkileyecek düzeyde bir sistem olup olmadığı ve de en önemlisi saldırının akabinde saldıranın hasar tespitinin yapılmasına en olacak olan hedef sistemin dış dünya ile iletişiminin kesilmesi durumunda ortaya nasıl bir değerlendirme konacaktır şeklindedir. Gözlemlendiği üzere siber ortamda rakip devletlerin değerli varlıkları üzerinde tehlike ya da risk altında tutma niyeti aynı zamanda caydırıcılık düzleminde mukabele ikilemlerini barındırmaktadır.

Pratiğe dökülecek olan mukabele şayet bugünkü ve yarınki misillemelere engel oluyorsa caydırıcılık da bu durumda kırılgan bir yapı oluşturacaktır. Libicki'ye göre farklı alanlarda uygulanan caydırıcılığın niteliğinde bu sorun herhangi bir problem oluşturmasa da siber uzayın yapısı gereği ardı ardına yapılacak olan saldırılar problem oluşturacaktır. Bu bağlamda da Libicki siber caydırıcılıkta olmazsa olmaz dediği üçüncü soruyu aynı türde saldırıları aralıksız olarak tekrarlayabilir miyiz? şeklinde sormuştur. Örneğin Soğuk Savaş döneminde bütün uluslararası sistemi adeta güvenliksiz hale sokan nükleer silahlanma ve bununla ilintili olarak yıkıcılığı ve korkutuculuğu ile kendinden menkul nükleer savaş olasılığını kimse tercih etmemekteydi. Çünkü bu saldırı türü araçları ve etkileri ile yok etmeye yönelikti. Öyle ki bu durum nedeniyle de hiçbir devlet bu araçları kullanmamıştır. Öte yandan siber caydırıcılıkta ise saldırılar sık sık tekrarlanabilir. bu durumda da mukabele çerçevesinde saldırganı cezalandırma niyetiyle bir den fazla saldırı yapılabilmektedir. Ancak bu durum siber uzayın diğer alanlarında ve dinamiklerinde olduğu gibi iki ucu keskin bıçak misali bir sonraki yapılacak saldırının amacına ulaşmayı engelleyebileceğinden tezatlıkları da içerebilecektir. Çünkü hedeflenen sisteme yönelik saldırılar sonrasında bir önceki saldırıdan dolayı açıklıklar ve eksiklikler

giderilebilecek ve açıklıklar da kapatılabilecektir. Bu durumda aynı türde saldırıları art arda yapma fırsatı veren siber ortam aynı zamanda mukabelede bulunulan rakibe toparlanma ve eksikliklerini giderme fırsatı verecektir.

Libicki'nin bahse konu bu üç önemli temel siber caydırıcılığa dair sorularına ilaveten ikincil derecede önem atfettiği diğer sorularda şayet mütekabiliyetlerin caydırıcı olmaması durumunda hedef tarafı silahlardan arındıracak mı? Üçüncü tarafların saldırıya müdahil olup olmayacağı? Mukabelede verilmek istenen mesajın hedef birime doğru mesajı verip vermediği? Karşı cevap vermek için bir eşik değerine sahip midir gerginlikten kaçınmak olası mıdır ve son olarak da saldırgana misilleme yapmaya değer midir? gibi cevap bekleyen sorulardan oluşmaktadır.

Elbette, nükleer ile siber teknolojinin hem kuramsal hem de pratiksel bağlamda birbirlerinden farklılıkları büyüktür. Bu nedenle de tarihsel benzerlikler yoluyla çıkarımlar yaparak siber ile nükleer teknolojiyi caydırıcılık ve tehdit bakımından karşılaştırmak tehlikeli durumlar arz edebilir. Öncelikle nükleer teknolojinin aksine siber alan yeni ve dinamik bir ortamdır. Ayrıca nükleer teknolojinin üretimi ve öğrenimi, yavaş, kimi zaman aksayan ve de tamamlanmamış bir özelliğe sahiptir. Nükleer teknolojinin popüler olduğu dönemin şartlarında ABD ile S.S.C.B. arasında yaşanan yoğun ve bir o kadar da gerilimi yüksek bir ideolojik ve siyasi rekabet şimdiki yaşanan A.B.D- Rusya ve A.B.D. Çin rekabetinden daha fazlaydı. En azından şimdiki kadar bahse konu bu devletlerarasında birbirlerine bağımlılık da yoktu. Güç dengesinin uzantısı olan nükleer denge döneminde sıfır toplamlı oyunlar ve rekabetler devlet aktörü üzerinden şekil almaktaydı. Ancak siber teknoloji ile beraber bu durum hem aktörler hem de yine bu alanla ilintili politikalar ve stratejiler bakımından değişmiştir. Siber ortam devlet ötesi suç teşkil eden aktörlere nükleer teknolojiye nazaran önemli güç elde etme fırsatları sunmuştur. Bu durumda hâlihazırda siber teknoloji öncesinde de var olan ulusal güvenliğin tanımının ve boyutlarıyla ilgili sorgulamaları artırmıştır. Ayrıca bu yeni alandan kaynaklanan ve kaynaklanacak olan ulusal güvenlik değerlerine yönelik bu devlet ötesi suç aktörlerinden kaynaklanacak olan güvensizlik ortamında devletler bundan böyle iş birliğine başvurmak zorunda oldukların farkına varacaklardır. Çünkü sıklıkla

vurgulanan alanın kendine has yapısı itibarı ile uluslararası toplumun bu yeni tehdit türüne iş birliğine gitmeden cevap vermesi mümkün gözükmemektedir.

SONUÇ

Neredeyse tarihin hiçbir döneminde sadece bir değişkenle belirlenemeyen uluslararası sistemi, değişik boyutlarda ve ölçütlerde bir çok fenomen etkileyerek gelişimine katkıda bulunmuştur. Kahır ekseriyette de bu fenomenler (devlet, egemenlik, güvenlik gibi) fiziksel olarak mevcudiyeti olmayan fakat bir tasavvurun parçaları olarak varlıklarından ya da duruşlarından söz edilen kavramlardır. Bunun nedeni de hâlihazırda uluslararası sistemin epistemolojik bir ünite arz etmesidir ve dolayısıyla sisteme dair ileri sürülecek olan tartışmalar soyutluğunda radarına yakalanacaktır. Bu sebeple semantiği üzerinde birbirinden farklı yorumlamaların olduğu bu kavramlar üzerinde oydaşmaya varılan tanımlamalardan da mahrum kalacaktır.

İşte bu sorunun en önemli muhataplarından biri de güvenlik fenomenidir. Algıda ve pratikte bidayette beşeriyetin doğa ile olan mücadelesinde ön plana çıkmaya başlayan güvenlik fenomeni akabinde tüm siyasal ve sosyal formasyonların psikolojik, sosyal, siyasal ve ekonomik yapılarında ve ilişkilerinde davranış biçimlerine etki eden bir kavram olmuştur. Bu nedenden müteşekkil güvenlik bireyden devlet düzeyine kadar tüm aktörlerin yaşamının her evresinde karşı karşıya kaldığı bir kavramdır ve bununla ilişkili olarak da varlığını devam ettirmenin hem aracını hem de amacını oluşturur. Bu durum tarihin başlangıcında algıya dayalı sosyal bir kavram olarak türeyen güvenlik kavramının bağımsız tanımlamasını zorlaştırmaktadır. Çünkü kavram zaman, mekân ve insan bağlamıyla ilişkili olarak sürekli değişime uğramıştır.

Ayrıca güvenliğin tehdit kavramıyla olan ilişkisi de yine bağımsız tanımlamayı zorlaştıran bir diğer faktördür. Çünkü tehditler kimi zaman gözlemlenebilir olgu ve olaylara dayanabilirken kimi zamanda algıya ve öngörülere dayanmaktadır. Bu nokta da, güvenlikte tehditle doğru orantılı olduğundan bizatihi güvenlik te ona göre şekillenmektedir. Bundan dolayı güvenlik kavramı her daim dinamik ve göreceli bir kavram olarak uluslar ilişkilerde yerini almaktadır.

Güvenlik kavramı her bir dönemin kendi şartlarının ve bağlamının getirilerine göre şekillendiği için dolayısıyla dönemsel ve konjonktürel bilgi türünü ortaya

çıkarmaktadır. Bu sebeple de tarihsel olarak değişken kavram olma özelliğini taşımaktadır. Dolayısıyla kavram her ne kadar genel geçer ve sabit ölçütlere göre tanımlanamasa da en azından metodolojik bağlamda tarihin süzgecinden geçerek yorumlanmayı hak etmektedir. Çünkü güvenliğin pratik olarak ne şekilde uygulandığı, sosyal ve siyasi bağlamların bu kavramı nasıl işlediği ve dönüştürdüğü ancak tarihsel metotla incelenerek ortaya konulabilir. Bununla birlikte, güvenlik kavramı haiz olduğu tehdit, risk, endişe vb. farklılaşan alt birimlerle beraber tıpkı uluslararası sistemin kendisi gibi kurgulanmaktadır. Bu sebeple birleşik kavram olarak güvenlik fenomeni tarihin hiçbir döneminde değerlerden azade olmamıştır.

Bu hususlar ışığında güvenlik fenomenine dair vurgulanması gereken nokta onun tanım olarak ne olduğundan ziyade, ona farklı zamanlarda farklı manalar yüklenerek ne olunması istendiğidir. Böylesi bir tavır da aslında güvenliğin nesnel olmadığını ve bununla ilintili olarak türetilmiş bir kavram olduğunu ön plana çıkarmaktadır.

21. yüzyılda siber merkezli yaşanan teknolojik gelişmeler devletlerin ulusal güvenliğine yönelik ortaya çıkan siber güvenlik tehditleri sayesinde ortodoks güvenlik paradigmasını yumuşatmadan da öte aşındırmıştır. Siber güvenlik tehditleri bilişim teknolojileri aracılığıyla bir toplumun iç ve dış düzenini koruma refleksini hasara uğratma gayesi barındırır. Sanal âlemden neşet eden siber güvenlik tehditleri şimdiye kadar fiziksel olgulara yönelik tehditleri ve güvenlik anlayışlarından farklı olarak fiziksel olmayan güvenlik olgusunu meydana çıkarmıştır. Estonya, Gürcistan ve İran'a yönelik ifa edilen siber saldırılarda gözlemlendiği üzere siber güvenlik tehditleri devletlerin hem fiziksel hem de kurumsal yapısına yöneliktir. Bu tehditlerin en önemli özelliği ışık hızında gerçekleştirilip, nereden geldiğinin belirgin olmamasıdır. Yani saldırının dolayısıyla düşmanın kimliği gizlidir ve dolayısıyla tehditlerin nerede, ne zaman, ne şekilde hangi hedefleri vuracağı önceden tahmin edilememektedir. Örneğin, yukarıda örnek olarak zikredilen Estonya, Gürcistan ve İran saldırılarının faillerinin kim olduğu henüz belirlenememiştir. Bu saldırıları yapanların devlet destekli olsun ya da olmasın suç örgütleri, terörist örgütler ve düşman devletler olduğu düşünülürse düşman hedefe yönelik gerçekleştirecekleri eylemlerde oldukça elverişli alan sunmaktadır.

Kendine has karakteri ile siber uzay olarak nitelendirilen bu alandan faydalanmanın diğer yöntemlere nazaran maliyetinin az olması ve buna karşılık bilgi transferini hızlı bir şekilde yerine getirmesi sağlanan avantajlardan sayılabilir. Bahse konu avantajlardan faydalanmak için de bir bilgisayar ve yazılım yeterlidir.

Her birimden aktörün rahatlıkla siber uzaydan nemalanabilmesi bu ortamın uluslararası sistemde yeni aktörler ve stratejiler geliştiren alan olma özelliğini de ön plana çıkarmaktadır. Çeşitli suç ve terör örgütlerinin siber uzayın sağlamış olduğu fırsatlar ile daha önceden erişemedikleri araçlara burada sahip olabilmesi devletler karşısında asimetrik bağlamda da avantajlar sağlamaktadır. Çünkü daha önceden hiçbir şekilde elde edemedikleri alan hâkimiyetini hem yerel hem de küresel düzeyde elde edebilme fırsatı yakalayan bu aktörler eylemlerin ifa etmede ve stratejilerinde büyük oranda bilişim teknolojilerini kullanma eğiliminde bulunarak asimetrik güç elde etmektedirler. Örneğin devletlerin su, enerji, doğalgaz vb. kritik altyapı hizmetlerini bilgi ağları üzerinden kontrol ettiği düşünüldüğünde bu durum suç ve terörist grupları için kayda değer eylem olanağı yaratırken devletler için de siber güvenlik tehditleri yaratmaktadır. Bir örnekle açıklanmak istenirse, hedef alınacak internete bağlı altyapısı neredeyse hiç olmayan Kuzey Kore'nin neredeyse tüm hizmet altyapıları ağlara bağlanmış ABD'nin Kuzey Kore için istismar edeceği bir hayli fazla hassas ve kırılgan hedefler vardır. Hem devlet dışı gruplar hem de zayıf devletler evvelden söz sahibi etkinlik kuramadıkları oyunlarda artık açıkça müdahil olabilmekteler. Dolayısıyla siber uzaydan türeyen ileri teknoloji ekonomik ve askeri olanakları artırırken öte yandan da devletlerin ulusal güvenliklerinde zaaflar yaratmaktadır. Görüldüğü üzere aslında siber uzay devletler nezdinde hem lehte hem de aleyhte koşullar yaratarak paradoksal bir platform da sunmuştur.

Küreselleşmenin artarak devam ettiği, sınırların geçirgenliğinin kolaylaştığı, ulus devletin varlığının ve yapısının irdelendiği 21.yüzyılda devlet dışı aktörler siber ortam sayesinde daha da güçlenerek ön plana çıkmışlardır. Şiddetin gösteriş biçimi ve etkinliği siber ortam vesilesiyle bu aktörler için çeşitlilik sunmuştur. Hâlihazırda küreselleşen terörizme bu ortamın yaptığı muazzam katkı sayesinde devlet dışı suç aktörleri saldırıların niteliğini de değişime uğratma şansına sahiptir. Ağlar üzerinden organize olabilen grupların geleneksel siyasi yapılara alternatif bir birim olarak

meydan okumaya başlamasıyla, geleneksel siyasi yapılar dâhilinde siyaset icra eden aktörlere de alternatif siyasi aktörler ortaya çıkmıştır. Wikileaks ve Anonymous gibi kamuoyu ile paylaşılmayan yazışma ve belgelerin internette açıklanması ve hükümetlerin bilgi işlem sistemlerini çökertmesi gibi saldırılar güvenlik tehditlerinin siber uzay denilen sanal aleme de aksettirildiğini göstermektedir. 21.yüzyılda yaygınlaşan ve aynı anda iç ve dış politika ve güvenlik meselelerinin politik ajandalarında en üst sıralarında yer alan siber güvenlik tehditleri modern güvenlik ve savunma sistemlerinin de mihengi olan fiziki sınırlar ve egemenlik tasavvurlarını da aşınıma uğratmıştır. Sınırları ve merkezi olmayan ağlara bağlı sistemsel özelliği siber ortamı güçlü olsun ya da olmasın herhangi bir devletin hâkimiyetinin altına girmeyi engellemekte olduğundan egemenlik salahiyetinin sınırlarının ne şekilde çizileceği sorunsalını yaratmaktadır.

Devletler ve devlet dışı aktörler arasında eşitleyici rol oynayan siber ortam ulus devletleri siber güvenlik tehditleri açısından aciz bırakabilmektedir. Geleneksel güvenlik anlayışına yönelik tehdit oluşturan savaş, terör ve saldırıların niteliği belirgindi. Ancak 21.y.y.'ın ileri teknolojileri artık bu kavramların formlarını içerik ve yarattığı etkiler bakımından dönüştürmüştür. Bu alandan kaynaklı savaş bir devletin ya da ulus ötesi suç aktörlerinin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak tehdit oluşturma şeklindedir. Günümüzde bu alan eşit olmayan taraflar arasında yürütülen ve savaş stratejilerinin zayıf olanın gereksinimlerine göre uyarlanan asimetrik savaş terime en uyumlu olabilecek güvenlik tehdidine örnektir.

Geleneksel güvenlik paradigmasının literatürü ile kıyaslandığında 21. yüzyılın yeni hareket alanı olan siber uzayın siber güvenlik tehditleri amaçlar bakımından birçok noktada farklılıklar arz etmektedir. Geleneksel güvenlik paradigmasının aksine siber güvenliğe yönelik tehditlerin kaynağını belirlemek çok zordur, hatta çoğu zaman imkânsızdır. Siber uzaydan neşet edecek olan tehditler ışık hızında gerçekleşir ve kahır ekseriyette bilgi ve iletişim sistemleri alanında etkili olmaktadır. Tehditler iki veya daha fazla ülke arasında gerçekleştiği gibi kişi, organize olabilen veya olamayan grup ve örgütlerle devletlerarasında da gerçekleşebilmektedir. Yine geleneksel güvenlik paradigmasında güvenliğe yönelik tehdit olan askeri araçların maliyeti yüksek olduğundan bu araçları sadece devletler

kullanabilmekteydi; ancak siber güvenliğe yönelik tehditler bilgisayarlar veya bilgisayar sistemlerinde kullanılan donanımlar ve yazılımlar aracılığıyla icra edildiğinden dolayı maliyeti düşüktür. Dolayısıyla kullanılacak araçların maliyeti düşüktür. Bu nedenle bahse konu araçların temini ve kullanımı bireyden devlete kadar her kesim için elverişlidir. Bununla birlikte siber güvenlik tehditlerinin temel karakteristiklerinde bir diğeri de saldırı belirtilerinin farkına varılamamasıdır. Bu durum da, saldırının nerede, ne kadar ve ne şekilde hasar oluşturduğunun tespitini zorlaştırmaktadır.

Gözlemlendiği üzere siber güvenlik tehditlerinin kahır ekseriyeti farklı nitelikte etmenlerle tebarüz etmektedir. Dolayısıyla bu durum siber güvenliğin sağlanmasında da aynı yaklaşımları gerekli kılmaktadır. Bir başka deyişle siber güvenlik tehditlerinin çok boyutluluğuna paralel siber güvenliğin tesisi için alınacak tedbirlerde çok boyutluluğu elzem kılmaktadır. Çünkü 21.yüzyıla değin klasikleşen güvenlik ve tehdit algılamaları ve bu tehditlerle mücadelede benimsenen yöntem ve araçlar geleneksel güvenlik paradigmasının karşısına yeni bir tehdit versiyonu olarak çıkan siber güvenlik tehditleriyle mücadelede anakronik kalmaktadır.

Hızla gelişen ve kontrol edilemeyen siber güvenlik tehditlerine yönelik güvenliği tesis etme çerçevesinde geleneksel mücadele yöntemlerinin formu değişmek zorundadır. Bu minvalde, öncelikle siber güvenlik tehditleri ile mücadele etmek için kurulması gereken mekanizma uluslararası işbirliğinin sağlanması olacaktır. Çünkü siber güvenliğin etkili olabilmesi için ağ ve kritik altyapılara yönelik tehdit, açıklık ve suiistimal edilebilirlik konusunda bilgi paylaşımı olmazsa olmazdır. Saldırının başlangıç aşamasında gözlemlenen tehdit bir üst aşamaya geçmeden paylaşılırsa etkisi en aza indirilebilmektedir.

Bunun içinde siber güvenliğin tesisi noktasında planlı strateji ve politika hamlelerinin benimsenmesi, devletlerin önce kendi içlerinde daha sonra da uluslararası ortamda eğitimini de yaygınlaştırarak farkındalığı artırması, nitelikli personel yetiştirilmesi, uluslararası merkezli siber kuruluşların inşası, Ar-Ge çalışmalarının icra edilmesi ve de özel sektöründe devreye sokularak beraber hareket edilmesi gibi adımlar ilk planda akla gelen işbirliği alanlarıdır.

Ancak sıklıkla vurgulandığı üzere siber güvenliğe yönelik tehditlerin popülerleşmeye başlamasında en önemli etmenlerden biri gayri merkezi olması ve dolayısıyla sınır tanımamasıdır. Bu durum geleneksel güvenlik paradigmasında gözlemlenen bir saldırı durumunu uluslararası hukuki mercilerde çözüme kavuşturabilme imkânını siber güvenlik anlayışında mümkün kılmamaktadır. Bu nedenle, uluslararası alanda işbirliğine dayalı ifa edilmesi gereken olmazsa olmaz hamle siber güvenliğe dair yasal mevzuatların oluşturulması olacaktır. Çünkü siber güvenliğe dair kapsamlı ve tanımlamaları net uluslararası sistemin dolayısıyla uluslararası hukukun düzenlediği bir yasal düzenleme mevcut değildir. Bu durumda, siber güvenlik tehditlerinin eyleme dönüşmüş en ciddi çıktıları olarak tarif edilen siber terör ve siber savaş gibi kavramlarla alakalı hukuki düzenlemelerin uluslararası ortamda işbirliğini sağlayıcı şekilde var olmadığı görülmektedir. Dünya genelinde birçok devletin henüz iç yasalarında siber güvenliğe dair hukuki düzenleme yapmaması; yapanlarında yasalarını uluslararası hukuk çerçevesi ile uyumlaştırmaması boşluklar yaratmış ve dolayısıyla milli siber alanlar oluşturulamamıştır.

Elbette saldırganlarının failinin isnat edilemezliği, eylemlerin somutluğunun belirsizliği, sınır aşan özellikleri, yasal ve teknik zorluklar sebebiyle hukuki kontrol mekanizmaları da siber güvenlik tehditlerine uyumlamada engel olmaktadır. Ancak siber güvenliğin tesisinde kilit rol oynayan uluslararası işbirliğinin en önemli mekanizması hukuksal çerçeve olduğu gözlemlendiğinde en azından belli başlı düzenlemelerle farkındalık yaratılarak yapıcı tedbirler almak mümkündür. Bu bağlamda göze çarpan en önemli sorun yargılama yetkisinin çözümlenmesidir. Suçun yapanı ile mağdurunun farklı ülkelerde ikamet etmeleri halinde hangi ülkelerin hukuki kaidelerinin yürürlüğe konmasını gerektirecek yargılama sorunu ile işbirliği elzemdir. Yine hukuksal zeminde ifa edilecek olan suçluların iadesi konusundaki mutabakat da siber güvenliğe yönelik önemli ortak adımlardan biri olacaktır.

Yine, siber anlaşmazlığın sonucunda ortaya çıkabilecek olan siber savaş durumları ile ilgili hukuki belirsizlikler mevcuttur. Bu bağlamda uluslararası hukukta bir savaşı başlatmayı meşru kılan bir saldırı BM anlaşması çerçevesinde bir ülkenin ülkesel bütünlüğüne karşı kuvvet kullanımı şeklinde tanımlanmıştır. Daha öz bir

ifade ile sorun yalnızca sınırları açık bir şekilde çizilmiş olan fiziksel dünyayı dikkate almıştır. Ancak alışılmışın dışındaki siber güvenlik tehditlerini içeren siber saldırılar fiziksel güç kullanmamakta, herhangi bir coğrafi alanını ve bununla ilişkili olarak yekpare devletleri içermemektedir. Dolayısıyla II. Dünya Savaşının akabinin koşullarında düzenlenen hukuki çerçeveler 21.yüzyılda farklılaşan yönleriyle siber saldırının savaşı meşrulaştıran kuvvet kullanımı çerçevesinde nasıl yer alacağı sorusuna cevap vermemektedir. Bu nokta da, NATO'nun liderliğindeki Talin'in El kitabı ve AB'nin Siber Suçlar sözleşmesi gibi hukuki çalışmalarla, milli güvenliği tehdit edecek boyutlara ulaşmış olan siber savaş ortamının çerçevesinin hızlı bir şekilde tanımlanarak var olan uluslararası hukuk kurallarının temel ilkelerini siber güvenlik hukukuna uygulamak gerekmektedir.

Bununla birlikte herhangi bir denetleyici yönetim mekanizmasının hâkimiyet kuramadığı anarşik bir sistemin insicamı ile donatılmış siber uzay ortamı kendine has karakteri ile uluslararası ilişkilerde kuramsal perspektiften de değerlendirilmeyi hak etmektedir. Çünkü güvenlik uluslararası ilişkilerde siyaset yapma ile çok yakın ilişki içinde olan bir kavramdır. Devletlerarasındaki çatışmaların temel nedeni olarak anarşik nitelikteki uluslararası sistemden hâsıl olan güvenlik-güvensizlik nosyonunu ele alanlar ile buna karşı çıkan uluslararası ilişkiler disiplin yaklaşımlarının farklılaşan boyutlarıyla siber güvenlik kavramını nasıl tartıştıklarının incelenmesi büyük önem taşımaktadır.

Bu bağlamda kendine has küreselleşen yapısı ve onu eşsiz kılan diğer özellikler itibariyle ulusal güvenlik boyutuna farklı bir mekân eklemiştir. Getirdiği sınırsız özgürlük ortamı ile aktör belirsizliği yaratan ve ulus devletleri ulus ötesi aktörler karşısında aciz bırakabilen bu yeni mekân toprak bütünlüğü, sınırların ihlal edilemezliği, egemen eşitlik ve uluslararası hukuk gibi modern uluslararası ilişkilerin mevcut temel kurallarını siyasal bir kapasite olarak dönüşüme uğratmaya namzettir. Neredeyse tüm alanlarda yeni ilke ve kurallar meydana getiren bu mekân disiplinin yaklaşımlarını inşa ettiği tüm kuram ve kavram biçimlerine dair de kuramsal ve teorik olarak farklılıkları barındırmak zorundadır. Uluslar üstü yeni bir egemenlik ağı oluşturan bu fiziksellik barındırsa da daha çok sanallığı barındıran sanal mekânın egemenlik ağının hegemonik gücü kimin elinde olacaktır? Sınır ve hüküm tanımayan

yapısıyla bu siber uzayda güç dengeleri inşa edilebilecek mi, edilecekse ne türde işbirliği inşa edilecektir? Bu yeni egemenlik ağının dahilindeki hiyerarşilerin ya da bölünmelerin ulusal sınırlar mı yoksa küresel çizgiler üzerinden mi çizilecektir? Bu bağlamda uluslararası ilişkiler teorileri kendine has anarşik ve küresellik arzeden siber uzaya dair nasıl bir kuramsal yaklaşım öne sürecektir? 1946 sonrasında yapılan düzenlemelerle çerçevesi çizilen ve mevcut haliyle dahi uluslararası arenada anlaşmazlıkları tam olarak çözemeyen uluslararası hukuk yeni siber güvenlik anlaşmazlıklarının çözümünü içeren siberin yasal boyutuna dair temel dinamik ve çerçeveleri nasıl çizecektir?

Bu hususlar ışığında yeni uluslararası çatışma alanı olarak gözlemlenebilen ve ulusal güvenliğe yönelik farklı türde tehdit oluşturan siber güvenlik tehditleri uluslararası ilişkiler teorilerinin güvenliğe kuramsal yaklaşımını da dönüşüme uğratmaktadır. Farklı siyasal ve sosyal birimler arasındaki mücadeleler yeni değildir; fakat maliyetinin düşüklüğü, anomimliği gibi unsurlar ulus ötesi suç aktörlerine asimetrik bağlamda avantaj sağlayarak geleneksel alanların aksine bu gruplara aynı zamanda sert ve yumuşak güç etmenine haiz olma fırsatı vermiştir. Siber uzayın karakteristiği türdeş olmayan aktörler arasındaki güç farkını kısmen de olsa azaltarak 21.yüzyılda küresel politika adlandırmasının tipik örneğini teşkil etmiştir. Büyük güçler tıpkı kara, deniz ve hava alanlarında olduğu gibi muhtemelen siber alanı da domine etme kudretine sahip olacaklardır. Dolayısıyla, hâlihazırda siber uzayda ulus ötesi aktörlere tek başına güç bakımından devletlerin yerine geçme olanağı sunmamaktadır. Ancak siber uzay daha önce bu gruplara ve güçlü olmayan devletlere elde edemediği imkânları sunarak asimetrik kazanımlar sağlamış ve dolayısıyla güç değişmesi ya da kayması durumlarında oyunun dişlilerinden biri olma fırsatını vermiştir.

Görüldüğü üzere enformasyon teknolojilerindeki gelişim ve bununla beraber getirdiği siber güvenlik tehditleri hâlihazırda değişime ve dönüşüme uğramakta olan geleneksel güvenlik yaklaşımlarını tüm boyutlarıyla aşınıma uğratmıştır. Geleneksel güvenlik yaklaşımının kurumsallaşmış ve yapısallaşmış katı paradigmasında güvenlik düşmanı dışarıda belli olan ve maddi kapasitelere dayalı tehditler üzerinden dar tanımlanmakta ve bu tehditleri de bertaraf etmede askeri güç kullanımına

odaklanmaktaydı. Ayrıca geleneksel güvenlik paradigması somut ve anında cevap verilebilir tehditler üzerine kurulmaktaydı.

Westphalia döneminin kahır ekseriyetinde egemen devletlerin yalnızca diğer egemen devletlerle uğraşması gerekmekteydi. Ancak 21.yüzyılın uluslararası sisteminde güvenliğe yönelik sorun olarak ortaya çıkan birçok aktör ve husus mevcuttur. Bu aktör ve hususlara katkı yapan önemli unsur olan siber uzay ve ürettiği bilgi teknolojileri ve altyapıları yeni fırsatların oluşmasına katkı yaptığı gibi pek çok yeni tehditleri de ortaya çıkararak uluslararası ilişkiler ve dünya siyasetini etkileyen bir unsur olarak güvenliğin ve tehditlerinin çoğunu uluslar ötesi karakterde olacağını mümkün kılmıştır.

KAYNAKÇA

Açıkmeşe, Sinem Akgül (2014). Küresel Güvenlik. (Editör: Evren Balta). *Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler.* İstanbul: İletişim Yayınları, 241-253.

Akgül Açıkmeşe, S. (2011). Algı mı, Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri.*Uluslararası İlişkiler,* 8(30), 43-73.

Adams, James (2001). Virtual Defense. *Foreign Affairs,* 80(3), 98-112.

Ağaoğulları, Mehmet Ali ve Köker Levent (2011). *İmparatorluktan Tanrı Devletine*. Ankara: İmge Kitabevi.

Aki Mauri Huhtinen ve Kori Laitinen (2012). Changing Security Speech and Environment: From Nations to Corporation Security (Edited By: Rulie Ryan). *Leading Issues in Informatıon Warfare and Security Research, Good News Digital Books.* (Second Edition). 65-80.

Aksu, Muharrem ve Turhan Faruk (2012). Yeni Tehditler, Güvenliğin Genişleme Boyutları veİnsani Güvenlik.*Uluslararası Alanya İşletme Fakültesi Dergisi,* 4(2), 69-80.

Akşam, (2015). Nato'da siber Tatbikat, http://www.aksam.com.tr/dunya/natodan-siber-tatbikat/haber-400214(Erişim Tarihi: 10.10.2015).

Akyeşilmen, Nezir (2015). Siber (Uluslararası(!) Düzen ve Siber Barış, http://www.ilksesgazetesi.com/mobil/koseyazisi.php?id=1581(Erişim Tarihi: 04.04.2016).

Al Jazera, (2010). http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html (Erişim Tarihi: 11.10.2015).

Alexander Yonah (1976). *International Terrorism: National, Regional and Global Perspectives* (Third Edition). New York: Praeger Publisher.

Alexander, Yonah (2002). Introduction. (Edited By: Yonah Alexander). *Combating Terörizm: Strategies of Ten Countries.* University of Michigan, 1-14.

Allen, Patrick D. And Demchak, Chris C. (2003). The Palestinian-Israel: Cyberwar.*Academıc Journal Article Military Review,* 83(2), 52.

Amalie Weber M.(2003). The Council of Europe's Convention on Cybercrime.*Berkeley Technology Law journal,* 18(1), 425-446.

Anderson, Perry (2013). *Passages from Antiquity to Feudalism.* (Third Edition), London: Verso World History Series

Anderson, Nate (2012).Confirmed: US and Israel Created Stuxnet, Lost Control of It. http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/(Erişim Tarihi: 14.12.2015).

Aning, Kwesi (2010). Security, The War on Terror, and Official Development Assistance.*Critical Studies on Terrorism,* (3)1, 7-26.

Anthony D. Lott (2005). Creating Insecurity: Realism, Constructivism, and US Security Policy. *Political Science Quarterly,* 120(3), 527-528.

Aras, Bülent ve Karakaya Rabia Polat (2008). From Conflict to Cooperation: Desecuritization of Turkeys Relations with Syria and Iran. *Security Dialogue,* 39 (5), 495-515.

Arends J. Frederik (2008). From Homer to Hobbes and Beyond-Aspects of Security in the European Tradition. (Edited By: Hans Günter Brauch et. al.).*Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century, Hexagon Series on Human and Environmental Security and Peace,* Volume:3, Berlin-Heidelberg-New York: Springer-Verlag, 263-278.

Arı, Tayyar (2013). Uluslararası İlişkiler Torileri Çatışma, Hegemonya, İşbirliği. Bursa: MKM Yayıncılık, (8.Baskı).

Arıboğan, Deniz Ülke (1998). *Kabileden Küreselleşmeye, Uluslararası İlişkiler Düşüncesi*. İstanbul: Sarmal Yayınları.

Armaoğlu, Fahir (2013).*19.Yüzyıl Siyasi Tarihi 1789-1914*. (13. Baskı). İstanbul: TimaşYayınları.

Armitage, John and Roberts Joanne (2002). *Living with Cyberspace: Technology and Society in the 21st Century*. London: Bloomsbury Academic.

Art, Robert (2005). International Dimensions of Natıonal (In) Security Concepts, Challenges and Ways Forward. Konrad Adenauer Stiftung, 9th Berlin Conference on Asıan Security(BCAS), 1-11.

Aspray, William (2011). The History of Information Science and Other Traditional InformationDomains: Models for Future Research. Libraries&The Cultural Record, 46(2), 230-248.

Ateş, Toktamış (2012). *Siyasal Tarih* (4.Baskı). İstanbul: Bilgi Üniversitesi Yayınları, 2012.

Austın J. L. (1962). *How to Do Thıngs with Words*. London: Oxford at the Clarendon Press.

Australia's Cyber Securıty Strategy(2016).https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf (Erişim Tarihi: 23.01.2016).

Aydın, Mustafa (2004). Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği.*Uluslararası İlişkiler,*1(1), 33-60.

Ayhan Gücüyener (2016). http://www.hazar.org/content/yayinlar/jeopolitik_rekabet_siber_uzaya_tasindi_1528.aspx(Erişim Tarihi: 03.04.2016).

Ayoob, Mohammed (1995). *The Third World Security Predicament: State Making, Regional Conflict, and the International System*. Emerging Global Issues, Lynne Rienner Publishers.

Bae, Young J. (2003). Information Technology and the Empowerment of New Actors in International Relations. *Journal of International and Area Studies,10*(2), 79-92.

Bal, Mehmet Ali (2003). *Modern Devlet ve Güvenlik,* İstanbul: IQ Kültür Sanat Yayıncılık.

Baldwin, David (2007). Security Studies and the End of Cold War (Edited By: Barry Buzan and Lene Hensen). *International Security,*Los Angeles:SAGE Publications, 99-120.

Balzacq, Thierry (2005). Three Faces of Securitization: Political Agency, Audience and Context.*European Journal of international Relations*, 11(2), 171-201.

Barak Azy and Suler John (2008). Reflections on the Psychology and Social Science of Cyberspace, (Edited By: Barak Azy).*Psychological Aspect of Cyberspace: Theory, Research, Applications.*Cambridge University Press.

Bayazıt, Hüseyin (2005). Teknolojik Küreselleşmenin Güvenlik ve Strateji Alanındaki Gelişmelere, Uluslararası Güvenlik ve Strateji Kuruluşlarının İşlevine ve Yapılanmasına Etkisi.Gelişen Bilgi Teknolojisi ile Güvenlik Politikası ve Stratejiler Arasında Etkileşim ve Yönlendirme Sempozyumu, 10-11 Mart 2005, İstanbul, Harp Akademileri Basım Evi.

Baylis, John (2012). The Concept of Security in Internatıonal Relatıons (Edited By: Hans Günter Brauch et. al.) *Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century, Hexagon Series on Human and Environmental Security and Peace.* Volume:3, Berlin-Heidelberg-New York: Springer-Verlag, 495-503.

Baylis, John (2011). Internatıonal and Global Security (Edited By: John Baylis, Steve Smith, Patricia Owens).*The Globalization of World Politics: An Introduction to International Relations* (5th Edition), Oxford Universıty Press, 230-246.

Benedikt Mıcheal (1991). *Introduction & Cyberspace: Some Proposals, in Cyberspace: First Steps*, London: MIT Press

Beniger, James R. (1986). *The Control Revolution: Technological and Economic Origins of the Information Society*. London: Harward University Press.

Benjamin Miller, (2001). The Concept of Security: Should it be Redefined*? Journal of Strategic Studies,*24(2), 13-42.

Bennett, Louise(2012). Cyber Security Strategy.*ITNOW*, 54 (1), 10-11.

Berner, Sam (2003). Cyber-Terrorism: Reality or Paranoia?*South African Journal of Information Management.* 5(1), 1-4.

Best, Antony, Hanhımakı, Jussı M., Maıolo Joseph A. and Schulze Kırsten E. (2012). *20.Yüzyılın Uluslararası Tarihi* (Çeviren: Taciser Ulaş Belge). Ankara: Siyasal Kitabevi

Betz, David J. and Stevens Tim (2011). CyberSpace and The State Toward a Strategy For Cyber-Power.*Oxford: Routlege Taylor & Francis*

Bewes, Wyndham A. (1993).Gathered Notes on the Peace of Westphalia of 1648. *Transactions of the Grotius Society*, 19, 61-73.

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

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

Biegel, Stuart (2003). *Beyond Our Control? Confronting The limits of Our Legal system In The Age Of Cyberspace.* The Mıt Press.

Bilgin, Pınar (2008). Critical Theory. (Edited By: Paul D. Williams). *Security Studies: An Introductıon*. New York: Routlage.

Bilgin, Pınar (2010). Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları.*Sadem Yayınları*, 8(14), 70-96.

Bilgin, Pınar Dünya Literatürü ve Uygulamasında Güvenlik Sektörü: "Devlet Merkezli" Güvenlkten "Yurttaş Merkezli", Güvenliğe Doğru mu? Yeni Güvenlik. (Derleyen: Ümit Cizre ve İbrahim Cerrah).*Güvenlik Sektörü Yönetişimi: Türkiye ve Avrupa, Güvenlik Sektörü Çalışmalar Dizisi-4*, İstanbul: Tesev, 43-61.

Blakemore, Brian and Awan, Imran (2012). *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*, London: Routledge.

Blank, Stephen J.(2003). *Rethinking Asymmetrıc Threats, Strategic Studies Institute. Strategic Studies Institute*, U.S. Army War College.

Bloch, Ernst (2002). *Rönesans Felsefesi Üzerine.*(Çeviren: Hüseyin Portakal).İstanbul: Cem Yayınevi.

BM Enformasyon Merkezi (UNIC). (2002). Saldırı'nın (Tecavüzün) Tanımı: Birleşmiş Milletler Genel Kurulu'nun 3814 (XXIX) sayılı ve 1974 Tarihli Kararı, Ankara http://www.unicankara.org.tr/doc_pdf/3814.pdf (Erişim Tarihi: 25.01.2016).

Bomse, Amy Lynne (2001). The Dependence of Cyberspace. *Duke Law Journal*, 50(6), 1717-749.

Booth, Ken (1991). Security and Emancipation. *Review of Internatıonal Strudies*, 17(4), 313-326.

Booth, Ken(1994).Security and Self Reflections of a Fallen Realist.*YCISSOccasional Paper*Number 26, 1-26.

Booth, Ken (2007).*Theory of World Security*. Cambridge: Cambridge Univerity Press.

Borger Julıan (1999).Pentagon Kept the Lid on Cyberwar in Kosovo. https://www.theguardian.com/world/1999/nov/09/balkans (Erişim tarihi: 21.02.2016).

Bostanoğlu, Burcu (2008). *Türkiye ABD İlişkilerinin Politikası*.Ankara: İmge Kitabevi.

Brown Chrıs ve Aınley Kırsten (2013). *Uluslararası İlişkileri Anlamak*. (Çeviren: Mehtap Gün Ayral). İstanbul: Sümer Kitabevi (4. Baskı).

Branco, Marcelo (2005). Free Software and Social and Economic Development. Information, Technology and the World Economy. (Edited By: Manuel Castells and Gustavo, Cardoso).*The Network Society: From Knowledge to Policiy.* Washington, DC: Johns Hopkins Center for Transatlantic Relations, 289-304.

Brauch, Hans Gunter (2012). Güvenliği Yeniden Kavramsalllaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Dörtlüsü. (Derleyenler Mustafa Aydın, Hans Günter Brauch, vd.,).*Uluslararası İlişkilerde Çatışmadan Güvenliğe.* İstanbul Bilgi Üniversitesi Yayınları. 167-196.

Bravo, Işıl Bayar (2005).Tarihin Sonu, ilerleme ve Küreselleşme Üzerine Bir İnceleme.*C.Ü. Sosyal Bilimler Dergisi,* 29(2), 125-138.

Brown Allen E. and Grant Gerald G. (2010). Highlighting the Duality of the ICT and Development Research Agenda. *Information Technology for Development,* 16(2), 96-111.

Brown, P. (1961). Religious Dissent in the Latter Roman Empire: the Case of North Africa. *The Journal of the Hisrorical Association History,*46(157), 83-101.

Brunst, Phillip W. (2009).The Role of the United Nations in the Prevention and Repression of International Terrorism. (Edited By: Wade, Marianne and Maljevic, Almir).*A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications*. SpringerLink, 51-78.

Bryant, Rebecca (1992). What Kind of Space is Cyberspace?http://www.minerva.mic.ul.ie//vol5/cyberspace.html (Erişim Tarihi: 16.03.2016)

Buchan, Russellandand Nicholas Tsagourias (2012). Cyber War and International Law. *Journal of Conflıct and Security Law*, 17, 183-186.

Buchan, Russell (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict Security Law*, 17, 212-227.

Burchill, Scot (2013). Liberalizm. (Edited By: Scot Burchill ve Andrew Lınklater vd), *Uluslararası İlişkiler Teorileri*. (Çeviren: Ali Aslan ve Mehmet Ali Ağcan), İstanbul: Küre Yayınları.

Burton, Joe (2015). NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation. *Defence Studies,* 15(4), 297-319.

Bussolati, Nicolo (2016).The Rise of Non-State Actors in Cyberwarfare, (Edited By: Jens David Ohlin, Kevin Govern, and Claire Finkelstein).Cyber War, Law and Ethics for Virtual Conflicts, *Journal of Internatıonal Criminal Justice*, 102-126.

Buzan, Barry (1983). *People, States, and Fear The National Security Problem in Internatıonal Relations*. Sussex: Wheatsheaf Books.

Buzan, Barry (2000). Changing Agenda of Military Security. (Edited By: Hans Günter Brauch et. al.).*Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century, Hexagon Series on Human and Environmental Security and Peace,* Volume:3, Berlin-Heidelberg-New York: Springer-Verlag, 553-560.

Buzan, Barry (2013). *Barış, Güç ve Güvenlik: Uluslararası ilişkilerde Çatışan Kavramlar.* (Çeviren: Özden Sarı). İstanbul: Uluslararası İlişkiler Kütüphanesi.

Buzan, Barry and Lene Hansen (2009). *The Evolution of Internatıonal Security Studies,* Cambridge: Cambridge University Press.

Buzan, Barry, Kelstrup Morten, Lemaitre Pierre and Tromer Elzbieta (1990). *The European Security Order Recast: Scenarios for the Post-Cold War Era*. Pinter Publisher

Buzan, Barry, Waver Ole and De Wilde Jaap (1998). *Security: A New Framework for Analysis,* Lynne Rienner Publishers.

Caplan, Nathalie (2013). *CyberWar: the Challenge to National Security,* Global Security Studies, 4(1), 93-115.

Carr, Jeffery (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Q'Reailly Publıshers.

Case Of The Cyber War: Kosovo Conflict (2014). TIME, http://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/ (Erişim Tarihi: 19.03.2016).

Castells, Manuel (2007). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür*. (Çeviren: Ebru Kılıç) İstanbul: Bilgi Üniversitesi Yayınları.

Castells, Manuel (2005). The Network Society From Knowledge to Policy. (Edited By: Mauel Castells and Gustavo Cardoso). *The Network Society: From Knowledge to Policy*. Washington: DC: Johns Hopkins Center for Transatlantic Relations, 3-22.

Cavelty, Myriam Dunn (2008). Cyber-Terror—LoomingThreat or Phantom Menace?The Framing of the US Cyber-Threat Debate.*Journal of Information Technology & Politics*, 4(1), 19-36.

Cebe, Özgür (2008). PKK'nın en önemli 'hacker'ı yakalandı. http://www.hurriyet.com.tr/pkknin-en-onemli-hackeri-yakalandi-10393202 (Erişim Tarihi: 10.04.2016).

Cha, Victor D. (2000). Globalization and The Study of Internatıonal Security.*Journal of Peace Research*, 37(3), 391-403.

Chang,Yu Li (2002). *Cyberspatial Cognition Approach to Thread Digital City in Physical City*. California State Polytechnic University, Pomona.

Chansoria, M. (2012). Defying Borders in Future Conflict ın East Asıa: Chinese Capabilities in the Realm of Informatıon Warfare and Cyber space.*The Journal of East Asian Affairs,*26(1), 105-127.

Chiasson, Mike W., and Davidson Elizabeth (2005). Taking Industry Seriously in Information Systems Research. *MIS Quarterly*, 29(4), 591-605.

Childe, Gordon V. (1950). The Urban Revolution. *The Town Planning Review*, 21(1), 3-17.

Choucrı, Nazlı (2012). *Cyberpolitics in Internatıonal Relatıons*. London: Cambridge, The MIT Press.

Choucri Nazli, Stuart Madnick and Jeremy Ferwerda (2014). Institutions for Cyber Security: International Responses and Global Imperatives, *Information Technology for Development*, 20(2), 1-26.

Choucri, Nazli (2013). Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences. Prepared for World Social Science Forum (WSSF) 2013 Montreal, Canada, October 13-15, 2013.

Chourou, Bechır (2008). A Regional Security Perspective From and For the Arab World(EditedBy: Hans Günter Brauch et. al.).*Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century, Hexagon Series on Human and Environmental Security and Peace.* Volume:3, Berlin-Heidelberg-New York: Springer-Verlag, 775-790.

Chris Demchak and Peter Dombrowski, Cyber Westphalia: Asserting State Prerogatives in Cyberspace. Georgetown Journal of International Affairs, International Engagement on CyberIII: State Building on a New Frontier (2013-14), 29-38.

Cilluffo, Frank J, and Pattak Paul Byron (2000). Cyber Threats: Ten Issues for Consideration. *Georgetown Journal of International Affairs*, 1(1), 41-50.

Clark, David (2010). Characterizing Cyberspace: Past, Present, and Future. ECIR Working Paper, Version 1. 2, March 12.

Clark, lan (2000). *Globalization and International Relations Theory*. New York: Oxford Press.

Clarke Rıchard ve Knake Robert K. (2010). *Siber Savaş*. İstanbul Kültür Üniversitesi.

Clarke, Richard and Rob Knake (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collıns Publısher.

Clausewitz Carl Von (1975). *Savaş Üzerine*. (Çeviren: Selma Koçak). İstanbul: Doruk Yayınları.

Clemente, Dave (2011). International Security: Cyber Security As A Wicked Problem. *The World Today*,67(10), 15-17.

Cohen, Edward S. (2001). Globalization and the Boundaries of the State: A Framework for Analyzing the Cahnging Practice of Sovereignty Governance.*An Internatıonal Journal of Policy and Administation*, 14(1), 75-97.

Cohen, Julie E. (2007). Cyberspace As/and Space. *Columbia Law Review*, 107(1), 210-256.

Cohen, Raymond (1978). Threat Perception in International Crisis. *Political Science Quarterly*, 93(1), 93-107.

Collin, Barry (1996). The Future of CyberTerrorism, Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago. http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm (Erişim Tarihi: 14.04.2016).

Commıssıon of the European Communıtıes, http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf(Erişim Tarihi: 11.10.2015).

Concıl Of Foreign Relations (2004) Terrorism: Questions and Answers: Cyberterrorism, vol. 2004, Council on Foreign Relations. http://www.cfr.org/issue/telecommunications/ri135 (Erişim Tarihi: 03.04.2016).

Conventıon on Cybercrıme(2001). European Treaty Series - No. 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf(Erişim Tarihi: 11.12.2015).

Conway, Maura (2002). Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet, *First Monday,* 7(11), 1-9.

Conway, Maura (2005). The Media and Cyberterrorism: A Study in the Construction of Reality, PaperPresented at the First International Conference on the Information Revolution and the Changing Face ofInternational Relations and Security, 23-25May 2005, Lucerne, Switzerland, available at http://se2.isn.ch/serviceengine/Files/CRN/46731/ieventattachment_file/F6C4C67B-787E-

49CD-82DD-102705970C60/en/MConway_Terrorism.pdf (Erişim Tarihi: 26.04.2016).

Conway, Maura (2008). Media, Fear andthe Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures, Working Papers in International Studies Centre for International Studies Dublin City University.

Cooper, Barry (2004). *New Political Religions, Or an Analysis of Modern Terrorism.* Columbia: University of Missouri Press.

Corrales, Javier, and Frank Westhoff (2006). Information Technology Adoption and Political Regimes. *International Studies Quarterly,* 50(4), 911-33.

Council on Foreign Relations (2004).http://www.cfr.org/search/?Ntt=cyber+terrorism&submit.x=0&submit.y=0 (Erişim Tarihi: 28.03.2016).

Cox, Christopher (2012). Cyber Capabilities and Intent of Terrorist Forces.*Information Security Journal: A Global Perspective*, 24(1-3), 31-38.

Crang, Mike, Mike Phıll and John May (1999). Introductıon. (Edited By: Crang, Mike, Mike Phıll and John May).*Virtual Geographies: Bodies, Space and Relations.* London: Routledge, 1-22.

Critical Infrastructure Sectors. (T.y.).https://www.dhs.gov/critical-infrastructure-sectors(Erişim Tarihi: 17.01.2016).

Cruz Laura (2005). Polıcy Poınt-Counterpoınt: Is Westphalıa Hıstory? *International Social Science Review*, 80(3/4) 151-55.

Curan, Kevin and Concannon Kevin (2007). Cyber Terrorism Attacks. (Edited By: Lech J. Janczewski and Andrew M.Colarik). *Cyber Warfare and Cyber Terrorizm.* London: IGI Global. 1-6.

Cybercrime: An Overview of Incidents and Issues in Canada (2014). http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm (Erişim Tarihi: 20.02.2016).

Cybercrime: an overview of incidents and issues in Canada (2014). http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm (Erişim Tarihi: 14.12.2015).

Cyber-risk 1010: What Every Business Needs to Know http://it-online.co.za/2016/07/06/cyber-risk-101-what-every-business-needs-to-know/?utm_campaign=shareaholic&utm_medium=facebook&utm_source=socialnetwork (Erişim Tarihi: 15.02.2016).

Cyberspace as a Domain In which the Air Force Flies and Fights (2006). http://www.af.mil/AboutUs/SpeechesArchive/Display/tabid/268/Article/143968/cyberspace-as-a-domain-in-which-the-air-force-flies-and-fights.aspx (Erişim Tarihi: 23.02.2016).

Czossek Christian, Rain Ottid and Anna Maria Taliharm (2013). Estonıa After The 2007 Cyber Attacks: Legal Strategic Organizational Changes in Cyber Security. (Edited By: Matthew Warren).*Cyber Warfare and Terrorism.* 1(1), 24-34.

Caporaso, James A. (2000). *Continutiy and Change in the Westphalıan Order.* Oxford: Blackwell Publishers.

Caşın, Mesut Hakkı (2015). Genel Çerçevesi ile Kritik Altyapıları Koruma Politikaları. (Editör: Mesut Hakkı Caşın). Uluslararası Kritik Enerji Altyapı Güvenliği: Yeni Tehditler ve Fırsatlar.*Hazar Strateji Enstitüsü*.5-17.

Coughlan, Shane M. (2003). Is There a Common Understanding of What Constitutes Cyber Warfare? The University of Birmingham http://opendawn.com/ewar/docs/dissertation/dissertation.pdf (Erişim Tarihi: 30.03.2016).

Çifçi, Hasan (2013). *Her Yönüyle Siber Savaş.* Ankara: Tübitak Popüler Bilim Kitapları.

Dağ, Ahmet Emin (2009). *Uluslararası İlişkiler ve Diplomasi Sözlüğü.* (3.Basım). İstanbul: Ağaç Kitabevi Yayınları.

Davis Jessica M. (2008). From Kosovo to Afghanistan: Canada and Informatıon Operatıons. Canadian Military Journal. http://www.journal.forces.gc.ca/vo6/no3/informat-01-eng.asp (Erişim Tarihi: 11.03.2016)

De Mesquita Bruno (2000). Popes, Kings and Endogenous Institutions: The Concordat of Worms and the Origins of Sovereignty. *International Studies Review*, 2(2), 93-118

Dedeoğlu, Beril (2014). *Uluslararası Güvenlik ve Strateji.*(3.Baskı). İstanbul: Yeni Yüzyıl Yayınları.

Deibert, Ron (2015). The Geopolitics of Cyberspace After Snowden, Current History. http://www.currenthistory.com/Deibert_CurrentHistory.pdf (12.24.2015).

Deibert, Ronald J. (2013). *Parchment, Printing, and Hypermedia: Communication and World Order Transformation.*Columbia University Press, 2013.

Denning Dorothy (2001). Is Cyber Terror Next?http://essays.ssrc.org/sept11/essays/denning.htm (Erişim Tarihi: 01.13.2016).

Denning, Dorothy (1999). Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy. (Edited By: John Arquilla ve David Ronfeldt).*Networks and Netwars, Rand Cooperatıon,* 239-288.

Denning, Dorothy (1999). *Informatıon Warfare and Security*. New York: Addison –Wesley

Denning, Peter J. (1989). The Science of Computing: The ARPANET after Twenty Years. *American Scientist*, 77(6), 1-13.

Department of Defence Dictionary of Military and Associated Terms (Joint Publications 1-02). (2010). http://www.dtic.mil/cdn/404w.html(Erişim Tarih: 15.08.2015).

Derian, James Der (2000). Virtuous War/Virtual Theory.*International Affairs*, (76)4, 771–788.

Dieter Fleck (2013). Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict Security Law*, 18(2), 331-351.

Dodge Martın (1999). The Geographies of Cyberspaces, Centre for Advanced Spatial Analysis. Working Paper. Centre For Advanced Spatıal Analysıs working Paper Series, University College London.

Dodge, Martın ve and Rob Kıtchın (2000). *Mapping Cyberspace*. London: Routledge.

Doğan, Nejat (2004). Machiavellism, Kantıan Deontology, and the Melian Dialoge: A reflection on Morality and the Use of Force. *A.Ü. Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 44(1). 65-75.

Don, Bruce (1999). Revolutionary Adaptations: Science and Technology in International Relations. *Harvard International Review*,21(3), 42-46.

Donnelly, Jack (2013). *Realizm. Uluslararası ilişkiler Teorileri.* (Çeviren: Ali Aslan ve Mehmet Ali Ağcan). İstanbul: Küre Yayınları,49-80.

Donnely, Jack (2013). Eleştirel Teori, (Edited By: Scot Burchill ve Andrew Lınklater vd), *Uluslararası İlişkiler Teorileri*. (Çeviren: Ali Aslan ve Mehmet Ali Ağcan), İstanbul: Küre Yayınları

Dougherty, James E., Jr Robert L. Pfaltzgraff (2001). *Contending Theories of International Relations A Comprehensive Survey* (Fifth Edition), New York: Longman.

Drezner, Daniel W. (2004). The Global Governanceof the Internet: Bringing the State Back In.*Political Science Quarterly*, 119(3), 477-498.

Dunn, Myriam Cavelty (2008). *Cyber Security and Threat Politics, US Efforts to Secure the İnfornation Age.* London: Routledge Taylor and Francis Group.

Dunne, Robert (2009). *Computers and the Law An Introduction to Basic Legal Principles and Their Application in Cyberspace,* New York: Cambridge University Press.

Eco, Umberto (2015). *OrtaÇağ.* (Çeviren: Leyla Tonguç Basmacı). İstanbul: Alfa Yayınları.

Edwards Dave (2010). Robust ICSs Critical for Guarding Against Cyber Threats. *Journal American Water Works Association,*102 (11), 30-33.

Ege, Börteçin (2012). *Siber Savaşlar Bilişimin Karanlık Yüzü*.Ankara: Bilim ve Teknik.

Ellen O'Connell Mary (2012). Cyber Security Without Cyber War.*Journal of Conflict Security* Law, 17(2): 187-209.

Elman Colin and Miriam Fendius Elman (2001). Negotiationg Internatıonal History and Politics. (Edited By: Elman Colin and Miriam Fendius Elman). *Bridges and Boundaries: Historians, Political Scientists and the Study of International Relations,* Cambridge, Mass. The MIT Press, 1-36.

Emerald M. Archer (2014).Crossingthe Rubicon: Understanding Cyber Terrorism in the European Context.*The European Legacy,*19(5), 606-621.

Emma Rothschild (1995). What Is Security? *The MIT Press on Behalf of American Academy of Arts & Sciences*, 124 (3), 53-98.

Eran, Oded (2009). Operation Cast Lead: The Diplomatic Dimensio.*Strategic Assessment*. Volume 11(4), 13-17.

Ergil, Doğu (1992). Uluslararası Terörizm.*Ankara Üniversitesi SBF Dergisi*, 47(3), 139-143.

Erhan, Çağrı (2003). Küresellesme Döneminin Tehditlerıyle Mücadele**.** http://docplayer.biz.tr/1678779-Kuresellesme-doneminin-tehditleriyle-mucadele.html(ErişimTarihi: 03.01.2016).

Eriksson, Johan and Giampiero Giacomello (2006).The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review / Revue Internationale de Science Politique,* 27(3), 221-244.

Ermiş, Uğur (2015). https://siberbulten.com/makale-analiz/siber-uzay-ve-ulus-devlet-egemenliginin-yeniden-sorgulanmasi/ (Erişim Tarihi: 21.04.2016).

Ermiş, Uğur (2015). Siber Uzayda Caydırıcılık Üzerine, https://siberbulten.com/makale-analiz/siber-uzayda-caydiricilik-uzerine/ (Erişim Tarihi: 12.04.2016).

Ermiş, Uğur (2016). Siber Uzay Güçler Dengesini Değiştiriyor. https://siberbulten.com/makale-analiz/siber-uzay-gucler-dengesini-degistiriyor/ (Erişim Tarihi: 02.05.2016).

F. Roy Bridge and Roger Bullen (1980).*The Great Powers and the European States System 18I5- 1914*. London: Longman.

Farhat, Seema ve Mir Annice Mahmood (1966). Globalisation, Information Technology, and Economic Development. Papers and Proceedings PART II Twelfth Annual General Meeting of the Pakistan Society of Development Economists Islamabad, 14-16 December. 35(4), The Pakistan Development Review, 1019-1033.

Farnham, Barbara (2003). The Theory of Democratic Peace and Threat Perception.*International Studies Quarterly,*47(3), 395-415.

Farr Jason (2005). Poınt: The Westphalia Legacy and the Modern Natıon-State. *International Social Science Review*, 80(3/4), 156-159

Finer, Samuel (1975). State and Nation Building In Europe: The Role Of the Military. (Edited By: Charles Tilly).*The Formation of National States in Western Europe*. London: Princeton University Press, 84-163.

Flemming, P. and Stohl, M. (2000). Myths and Realities of Cyberterrorism. Office of International Programs and The Center for Education and Research in Information Assurance and Security CERIAS, Purdue Unıversity, http://www.comm.ucsb.edu/faculty/mstohl/Myths%20and%20Realities%20of%20Cyberterrorism.pdf (Erişi Tarihi: 22.02.2016).

Floyd, Rita (2007). Towards a Consequentialist Evaluation of Security: Bringing Together the Copenhagen and the Welsh Schools of Security Studies. *Review of International Studies,* 33(2), 327-350.

Follath Erich and Holger Stark (2009). The Story of 'Operation Orchard', How Israel Destroyed Syria's Al Kibar Nuclear Reactor. http://www.jmhinternational.com/news/news/selectednews/files/2009/11/20091103_SpiegelOnline_TheStoryOfOperationOrchard.pdf(Erişim Tarihi: 21.01.2016).

Ford, Christopher (2010). The Trouble with Cyber Arms Control. *The New Atlantis,* (29), 52-67.

Forsyth, Murray (1979). Thomas Hobbes and the External Relations of States. *British Journal of International Studies,* 5 (3), 196-209.

Foucalt Mıcheal (2009). *Security, Territory, Population: Lectures at the College de France. 1977-1978.* New York: Picador.

Freeland, Richard M. (1979). *The Truman Doctrine and the Origins of McCarthyism: Foreign Policy, Domestic Politics, and Internal Security. 1946–1948.* New York: Knopf.

Freyer, Hans (2014). *Sanayi Çağı.* (Çeviren: Bedia Akarsu ve Hüseyin Batuhan). DoğuBatı Yayınları, 2014.

Friedman Jonathan and M.J. Rowlands (1978). Notes Toward an Epigenetic Model of Evolution of Civilization. (Edited By: Jonathan Friedman and M.J. Rparsonowlands). *The Evolution Systems*. 201-276.

Gabriel Weimann (2004).Cyberterrorism: How Real Is the Threat?Unıted State Institute of Peace. Special Report, 119.

Gaddis, John Lewis and Nitze Paul (1980). NSC 68 and the Soviet Threat Reconsidered. *International Security*, 4(4), 164-76.

Galtung, Fredrick (2000). A Global Network to Curb Corruption: The Experience of Transparancy Internatıon. (Edited By: Ann M. Florini, Nihon Kokusai Koryu Senta). *Third Force, The Rise of Transnational Civil Society*. Carnegie Endowment for International Peace, 17-49.

Galtung, Johan (1964). An Editorial. *Journal Of Peace Research*, 1(1), 1-4.

Galtung, Johan (1969). Violence, Peace, and Peace Research.*Journal of Peace Research*, 6(3), 167-191.

Galtung, Johan (1984). Twenty Five Years of Peace research: Ten Challenges and Some Response. Journal of Peace Researc, 22(2), 1-48.

Galtung, Johan (1996). *Peace by Peaceful Means: Peace Conflict, Development and Civilization*. London: Sage and PRIO.

Gartzke, Erik (2013). The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth. *International Security*, 38(2), 41–73.

Gay, Gale H. (2011). Vulnerabilities in Cyber Security Mean Opportunities, Too. *U.S. Black Engineer & Information Technology,* 35(4), 28-30.

Geers Kenneth (2008). Cyberspace and the Changing Nature of Warfare. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ (Erişim Tarihi: 22.02.2016).

Geers, Kenneth (2011). Sun Tzu and Cyber War, Cooperative Cyber Defence Centre of Excellence (CCD COE). https://ccdcoe.org/sites/default/files/multimedia/pdf/Geers2011_SunTzuandCyberWar.pdf (Eriim Tarihi: 08.01.2016).

George, Jim (1995). Realist Ethics, Internatıonal Relatıons and Postmodernism: Thinking Beyond Egoism-Anarchy Thematıc. *Millenium: Journal of Internatıonal Studies,* 24(2), 195-223.

Ghanea-Hercock, R. (2012). Why Cyber Security is Hard. *Georgetown Journal of International Affairs*, 81-89

Gıbson, William (1995). *Neuromancer*. London: Harper Collins Publishers.

Giacomello, Giampiero and Fernando Mendez (2001). Cuius Regio Eius Religio, Omnium Spatium? State Sovereignty In The Age Of the Internet.*Informatıon Security*, 7, 15-27.

Giacomo Luciani (1998). *The Economic Content of Security*. Journal of Public Policy, Cambridge University Press, 8(2), 151-173.

Giddens, Anthony (2010).*Üçüncü Yol- Sosyal Demokrasinin Yeniden Dirilişi*. (Çeviren: Mehmet Özay).İstanbul: Birey Yayınları.

Giddens, Anthony(2014).*Modernliğin Sonuçları*. (Çeviren: Ersin Kuşadil).İstanbul: Ayrıntı Yayınları.

Giles, David (2006). Constructing Identities in Cyberspace: The Case of Eating Disorders. *British Journal of Social Psychology*. 45, 463–477.

Gilpın, Robert (1981). *War and Change In World Politics*.Cambridge: Cambridge University Press.

Gjelten, Tom (2010). Shadow Hadow Wars: Debating Cyber 'Disarmament'.*World Affairs*,173(4), 33-42.

Gleditsch, Nils Petter (1993).The Most-Cited Articles in JPR. *Journal of Peace Research* 30(4), 445-49.

Goertz, Gary and Dahl F. Paul (1992). *Territorial Change and International Conflict*. London- New York: Routledge.

Goetschel, Laurent (1999). *Security in a Globalized World: Risk and Oppurtinities*. Baden Baden: Nomos.

Goldsmith, Jack (2013).How Cyber Changes the Laws of War.*European Journal of Internatıonal Law,* 24(1), 129-138.

Goldstone, Jack A. (1991). States Making Wars Making States Making Wars. *Contemporary Sociology*, 20(2), 176-78.

Gordon ve Ford (2003). Cyberterrorism? Symantec Security Response, Whıte Paper,http://www.symantec.com/avcenter/reference/cyberterrorism.pdf(Erişim Tarihi: 24.12.2015).

Gordon, Woo (2014).Kritik Enerjı Altyapıları için Terör Risk ve Tehdit Değerlendırmeleri. (Editör: Mesut Hakkı Caşın).*Hazar Strateji Enstitüsü*, 36-43.

Gorman, Sean P. (2006). A Cyber Threat to National Security? (Edited By: Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O.

Michel-Kerjan). *Seeds of Disaster, Roots of Response.* Cambridge: Cambridge University Press, 239-257.

Grieco, Joseph (1988). Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism. *International Organization*, 42(3), 485-507.

Gross, Leo (1948). The Peace of Westphalia, 1648-1948.*American Journalof International Law*, 42(1), 20-41.

Gücüyener, Ayhan(2015). Kritik enerji Altyapılarına Yönelik Gerçekleşmiş Siber Saldırılara İlişkin Bir Değerlendirme. (Editör: Mesut Hakkı Caşın). Uluslararası Kritik Enerji Altyapı Güvenliği: Yeni Tehditler ve Fırsatlar.*Hazar Strateji Enstitüsü.*18-39.

Gürcan, Metin (2011). Bir Önceki Savaş İçin Hazırlanmak: Değişen Küresel Güvenlik Ortamının Geleneksel Savaş Olgusuna Etkisi.*Bilge Strateji: Jeopolitik, Ekonomi-Politik ve Sosyo-Kültürel Araştırmalar Dergisi*, 3(5), 127-178.

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

Gürsoy, Barış (2003). Uluslararası Güvenliğin Bir Boyutu Olarak Askeri Alanda Devrim Tartışması.*Avrasya Dosyası Güvenlik Bilimleri Özel*, 9(2).

Haas jonathan (1982). *The Evolution of the Prehistoric State.* New York: Columbia University Press.

Hackers and What They are Into (2015). https://ohitsmerivera.wordpress.com/tag/20-and-robert-lyttle/(Erişim Tarihi: 29.11.2015).

Haigh, Thomas (2013). The History of Information Technology. *Annual Review of Information Science and Technology,*45(1), 431-487.

Hansen Lene and Helen Nissenbaum (2009). Digital Disaster, Cyber Security, and the Copenhagen School.*International Studies Quarterly*, 53(4), 1155-1175.

Hansen, James Lowry, Paul B. Meservy Rayman and McDonald, Dan (2007). *Genetic Programming for Prevention of Cyberterrorism Through Dynamic and Evolving Intrusion Detection*. Decision Support Systems, 43(4), 1362-1374.

Hariff, Shaheen (2016). *Confronting Cyber-Bullying.* Cambridge: Cambridge University Press.

Harman, Chris (2015). *Halkların Dünya Tarihi.*(Çeviren: Uygur Kocabaşoğlu), İstanbul: Yordam Kitap.

Hathaway, Melissa E. and Alexander Klimburg (2012). Preliminary Considerations: On National Cyber Security. (Edited by: Alexander Klimburg).*National Cyber Security Framework Manual*. *NATO Cooperative Cyber Defence Centre of Excellence*, 1-43.

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., and Spiegel, J. (2012). The Law of Cyber-Attack.*California Law Review,*100(4), 817-885.

Heidenreich, Brianna and David H. Gray (2013). Cyber-Security: The Threat of the Internet.*Global Security Studies,* 4(3), 17-26.

Held David ve McGrew Anthony (2008). *Küresel Dönüşümler*. Ankara: Phoneix Yayınevi.

Held, David Mcgrew Anthony, Goldblatt David and Perraton Jonathan (1999). *Global Transformatıons: Politics, Economics and Culture.*California: Stanford University Press Cambridge

Helga Haftendorn (1991). The Security Puzzle: Theory-Building and Discipline- Building in International Security.*International Studies Quarterly*, 35(1), 3-17.

Heller, Celia Stropnicka (1985). *Structured Social Inequality*. London: Collier-Macmillan.

Henkoğlu, Türkay ve Bülent Yılmaz (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği* 27,(3) 451-471.

Herrera, Geoffery (2002). The Politics of Bandwidth: International Political Implications of a Global Digital Information Network. *Review of International Studies,* 28(1), 93-122.

Herrington Lewis and Richard Aldrich (2013). The Future of Cyber-Resilience in an Age of Global Complexity.*Politics,* 33(4), 299–310.

Herz, John (1976). Technology, Ethics, and International Relations. *Social Research*,43(1), 98-113.

Herzog, Stephen (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Strategic Security in the Cyber Age* 4(2), 49-60.

Heylighen, Francis (2008). Complexity and Self-organizatıon. (Edited By: B Meyers and M j Maack, M.N.).*Encyclopedia of Library and Informatıon Sciences, Taylor and Francis and Oxford*.Volume: 2, 1215-1224.

Heylighen, Francis and Joslyn Cliff (2001). Cybernetics and Second-Order Cybernetics. (Edited By: R.A. Meyers).*Encyclopedia of Physical Science & Technology*. (Thırd Edition), New yok: Academic Press.

Heywood, Andrew (2013). *Küresel Siyaset*. (Çeviren: Nasuh Uslu ve Haluk Özdemir). Ankara: Adres Yayınları.

Himma, Kenneth Einar (2007). A View of Cyberterrorism Five Years Later. Internet Security; Hacking, Counterhacking, and Society. Sudbury, MA: Jones and Bartlett. http://www.dtic.mil/cgi- bin/GetTRDoc?AD=ADA484928(Erişim Tarihi: 21.02.2016)

Hindistan ve Pakistan Arasındaki Gerilim siber Savaşa Dönüştü. (2013). http://www.aksam.com.tr/teknoloji/hindistan-ve-pakistan-arasindaki-gerilim-siber-savasa-donustu/haber-217007 (Erişim Tarihi: 08.03.2016)

Hobbes, Thomas (2001). *Leviathan.* (Çeviren: Semih Lim).İstanbul: Yapı Kredi Yayınları.

Hobden Stephen (1998). *International Relations and Historical Sociology. Breaking Down Boundaries.* Londra: Routladge.

Hobsbawm, Erıc (2013). *İmparatorluk Çağı 1875-1914.* Ankara: Dost Kitabevi.

Hobson John M. and George Lawson. (2008). What is History in International Relations. *Millennium: Journal of International Studies,* 37/2, 415-435.

Hollis, David (2011).Cyberwar Case Study: Georgia 2008.*Swalls Wall Journal,*639(2), 1-10.

Hollis, Duncan B. (2015). Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack? (Edited By: Jens David Ohlin, Kevin Govern and Claire Finkelstein). *Cyber War: Law and Ethics for Virtual Conflicts. Oxford University Press*, 129-156.

Hough, Perter (2004). *Understanding Global Security.* (Third Edition). London: Routledge.

Hua, Jian and Bapna Sanjay (2012). How Can We Deter Cyber Terrorism?*Information Security Journal: A Global Perspective.* 21(2), 102-114.

Hughes, Rex (2009). Nato In Cyberspace: Digital Defences. *The World Today* 65(4),19-21.

Hughes, Rex (2010). A Treaty for Cyberspace.*International Affairs* 86(2), 523–541

Hunter Alan ve Cheng Lui (2008). China and The New International Security Agenda. (Edited By: Hans Günter Brauch et. al.).*Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century. Hexagon Series on Human and Environmental Security and Peace.* Volume:3, Berlin-Heidelberg-New York: Springer-Verlag, 839-854.

Huysmans, Jef (1998). Security! What Do You Mean? From Concept to Thick Signifier. *European Journal of International Relations,* 4(2), 226-255.

Ikenberry, G. John (1986). The State and Strategies of International Adjustment. *World Politics* 39(1) 53-77.

Indıa and Pakistan in Cyber War (2010). http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html(Erişim Tarihi: 15.03.2016).

IŞID Siber Ordu Kuruyor. (2016). https://siberbulten.com/strateji-guvenlik/isid-siber-ordu-kuruyor/ (Erişim Tarihi: 02.09.2016).

Işıklı, Ali (2011). Kritik Altyapı Güvenliğine Yönelik Özgün Çözümler: Sanal HavaBoşluğu Siber Güvenlik Çalıştayı, Türkiye Noterler Birliği Konferans Salonu,Söğütözü, Ankara, Bilgi Güvenliği Derneği http://www.iscturkey.org/ calistay/1/images/stories/siberguvenlik.rar (Erişim Tarihi: 09.04.2016).

Jenkins, Brian (1978). International Terrorism: Trends and Potentialities. *Journal of International Affairs*, 32(1), 115-123.

Jiang, Bin and Ferjan Ormeling (1999). *Mapping Cyberspace; Visualising, Analysıng and Explorıng Vırtual Worlds.* London: Centre for Advanced Spatial Analysis University College.

John Arquilla and David Ronfeldt (1993). Cyberwar Is Coming! *Comparative Strategy,* 12(2), 141–165.

John Richard (2011).Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield.*Journal of Computer and Informatıon Law*, 29 (1), 1-29.

John Rollins and Clay Wilson (2007). Terrorist Capabilities for Cyberattack: Overview and Policy Issues, *CRS Report for Congress*. 1-28.

John, Herz (1950). İdealist Internatıonalism and the Security Dilemma.*World Politics*, 2(2). 157-180.

Jon Oltsik (2009). Russian Cyber Attack on Georgia: Lessons Learned? Network Worldhttp://www.networkworld.com/article/2236816/cisco-subnet/russian-cyber-attack-on-georgia---lessons-learned-.html (Erişim Tarihi: 13.01.2015).

Jones, Grannt D. And Kautz Robert R. (1981). Issues in the Study of New World State Formation. (Edited By: Grant D. Jones and Robert R. Kautz).*The Transition to Statehood in the New World. The Transition to Statehood in the New World.* Cambridge: Cambridge University Press, 3-36

Jorgensen, Dale W. ve Khuong M. Vu (2005). Information, Technology and the World Economy, (Edited By: Manuel Castells and Gustavo, Cardoso).*The*

Network Society: From Knowledge to Policiy. Washington, DC: Johns Hopkins Center for Transatlantic Relations,171-224

Josan, Andrei and Cristina (Covacı) Voıcu (2015). Hybrid Wars in the Age of Asymmetric Conflicts.*Review of the Air Force Academy*, 1(28), 49-52.

Joseph Jonathan (2010). The International as Emergent: Challenging Old and New Orthodoxies in International Relations Theory. (Edited By: Jonathan Joseph ve Colin wight).*Scientific Realism and Internatıonal Relatıons,* London: PalgraveMacmillian, 51-68.

Joseph M. Grieco (1988). Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism. *International Organization*, 42(3). 485-507.

Jovi, John (1998). *Games, Threats and Treaties: Understanding Commitments in Internatıonal Relatıons.* London: Pınter London.

Junio, Timothy J. (2013). How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate.*Journal of Strategic Studies*, 36(1), 125-133

Kalay, Güler (2013). Terör ve Terörizm.http://www.politikadergisi.com/okur-makale/teror-ve-terorizm (Erişim Tarihi: 18.04.2016).

Kallberg, Jan and Bhavani Thuraisingham (2014). After the War on Terror How to Maintain Long-range Terrorist Deterrence.*Journal of Policing Intelligence and Counter Terorism*, 9(1), 19-31.

Kant, Immanuel (1960). *Ebedi Barış Üzerine Felsefi Deneme*. (Çeviren: Yavuz Abadan ve Seha L. Meray).Ankara: Ajans Türk Matbaası.

Kant, Immanuel, and Kroeger A. E. (1882). Anthropology of Immanuel Kant. *The Journal of Speculative Philosophy*, 16(1), 47-52.

Karagül, Özkan (2015). Bilgi Teknolojileri ve Uluslararası ilişkilerde Fırsat-Tehdit Paradoksu. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 10(1), 115-126.

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

Kay, Sean (2004). Globalization, Power, and Security. *Security Dialogue*, 35(1), 9-25

Keagan, John (2007). *Savaş Sanatı Tarihi*. (Çeviren: Selma Koçak). İstanbul: Doruk Yayınları.

Kegley, Charles (2004). *World Politics. Trends and Transformation*, Newyork: Wadsworth,

Kennedy, Paul (2009). *Büyük Güçlerin Yükseliş ve Çöküşleri 16.Yüzyıldan Günümüze Ekonomik Değişim ve Askeri Çatışmalar*. (Çeviren: Birtane Karanakçı).Ankara: Türkiye İş Bankası Kültür Yayınları.

Keohane, Robert (1984). *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton University Press.

Keohane, Robert O. And Joseph S. Nye (1987). Power and Interdependence. *International Organization,* 41(4), 725-753.

Keyman E. Fuat (2014). Küreselleşme. (Editörler: Şaban Kardaş ve Ali Balcı). *Uluslararası İlişkilere Giriş.* İstanbul: Küre Yayınları

Kibaroğlu, Mustafa (2002). 11 Eylül Ardından Strateji, Tehdit ve Caydırıcılık. Foreign Policy, http://www.mustafakibaroglu.com/sitebuildercontent/sitebuilderfiles/Kibaroglu-11EylulArdndanStratejiTehditCaydiricilik-22dec01.pdf (Erişim Tarihi: 02.09.2016).

Koepsell, David R. And William Rapaport (1995). The Ontology of Cyberspace: Preliminary Questions and Comments on "The Ontology of Cyberspace". Presented at the Tri-Staet Philosophical Association Meeting, ST. Bonaventure university, 22 April 199. This document is SUNY Bualo Department of Computer Science Technical Report 95-25 and SUNY Bualo Center for Cognitive Science Technical Report 95-09.

Korns, Stephen W and Kasternburg, Joshua E. (2008-09). Georgia's Cyber Left Hook. *Parameters*, 60-76.

Kostopoulos, George K. (2008). Cyberterrorism: The Next Arena of Confrontation. *Communications of the IBIMA*, 6(25). 165-169.

Kozlowski, Andrzej(2014). Comparatıve Analysıs of Cyberattacks on Estonıa, Georgia and Kyrgyzstan. *European Scientific Journal*, 3, 237-245.

Krahmann, Elle (2005). From State to Non-State Actors: The Emergence of Security Governance. (Edited By: Elke Krahmann). *New Threats and New Actors In Internatıonal Security*. Palgrave Macmillan, 3-19.

Kramer, F. (2011). Cyber Security: An Integrated Governmental Strategy For Progress. Georgetown Journal of International Affairs,http://journal.georgetown.edu/wp-content/uploads/2015/07/136_gj124_Kramer-CYBER-2011.pdf (Erişim Tarihi: 22.03.2016).

Krasner, Stephen D. (1995). Compromising Westphalia. *International Security*, 20(3),115-151.

Kratochwil, Friedrich (1986).Of Systems, Boundaries, and Territoriality: An Inquiry into the Formation of the State System. *World Politics,* 39(1), 27-52.

Langer, Ralph (2013). *To kill a Centrifuge, A Technical Analysis of What Stuxnet's Creators Tried to Achieve.* Arlington/Hamburg7Munich: The Langer Group. 3-36.

Laurie R. Blank (2014). Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Lawto Activities in Cyberspace. *Social Sciences Research Network*. 14(286), 175-201.

Lawler Peter (2008). Peace Studies. (Edited By: Paul D. Williams).*Security Studies An Introductıon.* London and New York: Routledge, 73-88.

Lebow, Richard Ned (2010). *A Cultural Theory of International Relatıons*. Cambridge: Cambridge Universty of Press.

Lee Stephen J. (2012). *Avrupa Tarihinden Kesitler 1494-1789*. (4.Baskı) Ankara: Dost Kitabevi

LeeStephen J. (2014). *Avrupa Tarihinden Kesitler 1789-1980*. (4.Baskı) Ankara: Dost Kitabevi

Leffler, Melvyn P. (1990). Natıonal Security. *The Journal Of American History*, 77(1), 143-172.

Leiner, Barry M., Cerf, Vinton G., Clark, David D., Kahn, Robert E., Kleinrock, Leonard Daniel C., Lynch, Jon Postel, G. Roberts, Larry and Wolff, Stephen, https://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf (Erişim Tarihi: 22. 03.2016).

Lessig, Lawrence. (1996). The Zones of Cyberspace. *Stanford Law Review*, 48(5), 1403-411.

Lewis, James A. (2006). Cybersecurity and Critical Infrastructure Protection, Center for Strategic and International Studies, January, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf(Erişim Tarihi: 24.12.2015).

Liang, Huigang, and Xue Yajiong (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71-90.

Libicki Martın(2009). Cyberdeterrence and Cyberwar, *RAND Corporatıon*.

Libicki, Martın C. (1998). Information War, Information Peace.*Journal of International Affairs*, 51(2), 411-428.

Light, Margot (2000). Information War. *The World Today*, 56(2),10-12.

Lind, W.S., Nighttengale, K., Schmitt, J. F, Sutton, J. W. and Wilson, G. I. (1989). The Changing Face of War, Into the Fourth Generatıon, *Marine Corps Gazette*, 73(10), 22-26.

Lindsay, Jon R. (2013). Stuxnet and The limits of Cyber Warfare. *Security Studies*, 22(3), 365-404.

Locke, John (2012).*Yönetim Üzerine İkinci İnceleme*. (Çeviren: Fahri Bakırcı). Ankara: Babil Yayıncılık.

Lourdeau, K. (2005). Testimony.https://archives.fbi.gov/archives/news/testimony/hearing-on-cyber-terrorism (Erişim Tarihi: 23.12.2015).

Lovelace, Douglas(2015).*The Cyber Threat, After September 11*. Oxford University Press.

Lukas, George (2015). *Cyber-Physıcal Attacks A Growing İnvisible Threat*. Butterworth-Heinemann.

Lynch Orla and Ryder Christophr (2012).Deadliness, Organisational Change and Suicide Attacks: Understanding the Assumptions İnherent in the Use of the Term 'New Terrorism.,*Critical Studies on Terrorism*, 5(2), 257-275.

Mabee, Bryan (2003). Security Studies and the 'Security State': Security Provision in Historical Context. *International Relations*, 17(2), 135-151.

Macdonald, Matt (2008). Constructivism,(Edited By: Paul D. Wıllıams).*Security Studies An Introductıon*. London and New York: Routledge, 59-72

Machiavelli Niccolo (2013). *Hükümdar* (Çeviren: Necdet Adabağ). İstanbul: Türkiye İş Bankası

Macrae Andrew (2005). Counterpoınt: The Westphalıa Overstatement. *International Social Science Review,* 80(3/4), 159-164.

Madge Clare and Henrietta Q'Connor (2005). Mothers in the Making? Exploring Liminality in Cyber/Space. *Transactions of the Institute of British Geographers New Series*, 30(1), 83-97.

Mallik, Amitav (2004). *Technology and Security in the 21st Century, A Demand-side Perspective.* (Sıprı Research Report: 20). New York: Oxford University Press.

Mann Micheal (2012). *İktidarın Tarihi Başlangıcından 1760'a kadar Toplumsal İktidarın Kaynakları.* Ankara: Phoenix Yayınları.

Manolopoulos, Andreas (2003). Raising 'Cyber-Borders': The Interaction Between Law and Technology.*Internatıonal Journalof Law Info Tech,* 11(1), 40-58.

Maras, Marie-Helen (2015). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning.

Marchesin, Philippe (2003). The Rise of Islamic Fundemantalism in East Africa. *African Geopolitics,* 12(1). 229-240.

Mardin, Şerif (2009).*Türkiye'de Toplum ve Siyaset.* İstanbul: İletişim Yayınları.

Martın Libicki C.(2012). Cyberspace Is Not a Warfighting Domain. I*/S: A Journal of Law and Policy for the Informatıon Society*, 8(2), 325-340.

Mathews, Jessica T. (1997). Power Shift. *Foreign Affairs*, 76(1), 50-66.

Mathews, Jessica T. (2000). The Information Revolution. *Foreign Policy*, 119, 63-65.

McCarthy, Daniel R. (2015). Power and Information Technology: Determinism, Agency, and Constructivism. (Edited By: Daniel R. McCarthy).*Power, Information Technology, and International Relations Theory The Power and Politics of US Foreign Policy and the Internet*. Palgrave Studies in International Relations, 19-42.

McCorquodale Robert, Pangalangan Raul (2001). Pushing Back the Limitations of Territorial Boundaries. *European Journal of Internatıonal Law*, (12), 5, 867-888.

McGraw, Gary (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, 36(1), 109-119.

McSweeney, Bill (1996). Identity and Security: Buzan and the Copenhagen School. *Review of International Studies,* 22(1), 81-93.

Mearsheimar, John (2001). *The Tragedy of Great Power Politics*.New York: Norton.

Mearsheimer, John (1990). Back to the Future: Instability in Europe after the Cold War. *International Security*, 15(1), 5-56.

Mearsheimer, John J. (2002). Realism, the Real World, and the Academy. (Edited By: Michael Brecher and Frank P. Harvey) Realism and Institutionalism in International Studies, Ann Arbor: The University of Michigan Press, 23-33.

Melzer, Nils (2011). Cyberwarfare and International Law, Ideas For Peace and Securities. *UNIDIR Resources*, 1-38.

MGK(2013).Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı (Uluslararası Siber Güvenlik Hukuku)http://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakk-nda-tallinn-el-kitab-uluslararas-siber-guevenlik-hukuku#(Erişim Tarihi: 07.11.2015).

Miloseviş, Nikola, Case of the cyber war: Kosovo conflict (2015).https://www.linkedin.com/pulse/case-cyber-war-kosovo-conflict-nikola-milo%C5%A1evi%C4%87(Erişim Tarihi: 11.01.2016).

Mohammed Ayoob (1995). *The Third World Security Predicament: State Making, Regional Conflict, and the International System*. Emerging Global Issues.

Morgan, Patrick M. (1992). Safeguarding Security Studies.*Arms Control*, 13(3), 464-479.

Morgenthau, J. Hans (1974). *Scientific Man vs Power Politics*, Chiago: Chiago Unıversity Press.

Morgenthau, J. Hans. (1948). *Politics Among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf Inc.

Muharrem, Balcı (2013). Savaş ve Terör, Birikimler Genç Hukuk Okumaları, http://www.muharrembalci.com/hukukdunyasi/makaleler/birikimlerI/85.pdf(Erişim Tarihi: 10.03.2016).

Murray, Andrew (2007). *The Regulation of Cyberspace: Control in the Online Environment.* New York: A Glasshousse Book. Routledge.

Mythen Gabe and Sandra Walkate, (2005). Criminology and Terrörizm Which Thesis? Risk Society or Governmentality? British Journal of Criminology Advance Access http://bjc.oxfordjournals.org/content/early/2004/12/31/bjc.azi074.full.pdf (Erişim Tarihi: 20.12.2016).

Natıonal Research Councıl (2005). *Signposts in Cyberspace*. Washıngton DC: The Natıonal Academıes Press.

National Academy of Sciences (1991). *Computer At Risk Safe Computing in the Information Age.* Washington DC: Natıonal Academy Press.

Navari, Cornelia (2008). Liberalism. (Edited By: Paul D. Wıllıams) *Security Studies An Introductıon*. London and New York: Routledge, 29-43.

Nayar, Pramod K (2004). *Virtual Worlds: Culture and Politics in the Age of Cybertechnology*. SAGE Publicatıon.

Niebuhr, Reinhold (2013). *Moral Man and İmmoral Society A Study in Ethics and Politics.* (Second Edition). Lousvılle-Kentucky: Westmınster Press.

Nissenbaum, Helen (2005). Where Computer security Meets National Security. *Ethics and Information Technology,* 7, 61–73.

Nye, Joseph Jr. (2010). *Cyber Power. Belfer Center For Science and Internatıonal Affairs*. Harward Kennedy School, Cambridge: MA.

Nye, Joseph S. (2011). Cyber Security and National Security.*Cyber Security,* NewEurope (Special Edition), Sayı Mayıs-Haziran 2011, <http://www.scribd.com/doc/56702531/Cyber-Security-2011 (Erişim Tarihi: 21.02.2016).

Nye, Joseph ve Jr and David A. Welch (2011).*Küresel Çatışma ve İşbirliğini anlamak.*(Çeviren: Renan Akaman).Türkiye İş Bankası Kültür Yayınları.

Nye, Joseph, Jr. (2011). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, Wınter-2011, 18-38.

Nye, JosephJr. (2012). The Third Annual Ernest May Memorial Lecture: Nuclear Lessons for Cybersecurity? In NYE Joseph and Scowcroft B. (Edited By: Burns Nicholas and Prıce Jonathan). *Securing Cyberspace: A New Domain for National Security*. Aspen Institute, 21-41

O'Connell Mary Ellen (2012). Cyber Security Without Cyber War.*Journal of Conflict Security Law*, 17 (2): 187-209.

O'Connell, Mary Ellen and Louise Arimatsu (2012). Cyber Security and International Law, International Law: Meeting Summary.*Chatham House*, 1-12

Ole Wæver (2008). Peace and Security: Two Evolving Concepts and Their Changing Relationship, (Edited by: Hans Günter Brauch et. al.).*Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century, Hexagon Series on Human and Environmental Security and Peace*. Volume: 3, Berlin-Heidelberg-New York: Springer-Verlag, 99-111.

O'Leary, Stephan D. (1996). Cyberspace as Sacred Space: *Communicating Religion on Computer Networks*. Journal of the American Academy of Religion,64(4), 781-808.

Osiender Andreas (2001). Sovereignty, Internatıonal Relations, and the Westfalyan Myth. *Internatıonal Organization* 55 (2), 251-287.

Owens, Richard N.(1942). What Is a Security? *The Accounting Review*, 17(3), 303-308

Öğün Mehmet Nasip ve Kaya Adem (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri*, 9(18), 145-181.

Özcan, Mehmet (2002). Siber Terörle Mücadelede Karşılaşılan Zorluklar-I. http://www.turk-internet.com/portal/yazigoster.php?yaziid=4099 (Erişim Tarihi: 03.04.2016).

Özcan, Mehmet (2004). Yeni Milenyumda Yeni Tehdit: Siber Terör, *Türk Harb-İş Dergisi*, 210, 39-40

Özcan, Mehmet, (2012). Siber Terörizm ile Klasik Terörizm Arasındaki Farklar http://tirengo.blogspot.com.tr/2012/07/siber-terorizm-ile-klasik-terorizm.html (Erişim Tarihi: 12.01.2016).

Özdemir, E. (2003). *Bilgi Savaşları.* İstanbul: IQ Kültür Sanat Yayıncılık.

Özpehlivan, Ahmet (2006). Siber terörizmle Mücadelede kolluğun Rolü, Yayımlanmamış Yüksek Lisans Tezi, *Kara Harp Okulu Savunma Bilimleri Enstitüsü*. Ankara.

Pamuk, Osman (2010). Stuxneti Özel Yapan Ne? TÜBİTAK BİLGEM http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/stuxneti-ozel-yapan-ne.html (Erişim Tarihi: 02. 02.2016)

Parker, Geoffrey (2014). *Cambridge Savaş Tarihi*. (Füsun Tayanç ve Tunç Tayanç). İstanbul: Türkiye İş Bankası Kültür Yayınları.

Parsons, Talcott (1977). *Social Systems and the Evolution of Action Theory*. New York: Free Press.

Paterson, Thomas G. (1971).*Cold War Critics: Alternatives to American Foreign Policy in the Truman Years*. Chicago: Ouadre Books.

Paul W. Schroeder (1984).The Lost Intermediaries: The Impact of 1870 on the European System. *International History Review*, 6(1), I-27.

Paulson, Kevin (2002). http://www.securityfocus.com/news/414(Erişim Tarihi: 03.12.2015).

Pazarcı, Hüseyin (2014).*Uluslararası Hukuk*. Ankara: Turhan Kitabevi

Pehlivan, Oğuz Kaan (2013). Siber Güç Kapasitesi Asimetrik Savaşın Parametreleri,http://www.analistdergisi.com/sayi/2013/10/siber-guc-kapasitesi-asimetrik-savasin-parametreleri(Erişim Tarihi: 24.01.2015).

Peter R. Neumann (2009). *Old and New Terrorism, Late Modernity, Globalization and the Transformation of Political Violence*. Cambridge: Polity Press.

Philpott, Daniel (2001). *Revolutions in Sovereignty: How Ideas Shaped Modern International Relations.* New Jersey: Princeton University Press.

Poggi, Gianfranco (1979). *The Development of the Modern State: A Sociological Introduction*. Californıa: Stanford Unıversity Press.

Polyani, Karl (2001). *The Great Transormatıon: The Political and Economic Originsof Our Time*. Boston: Beacon Press.

Potyemkin, Vladimir (2009). *Uluslararası İlişkiler Tarihi*. Cilt: 1, (Çeviren: Attila Tokatlı) İstanbul: Evrensel Basım Yayın.

Press, Larry (2000). The State of the Internet: Growth and Gaps, http://www.isoc.org/inet2000/cdproceedings/8e/8e_4.htm(Erişim Tarihi: 01.11.2015).

Press, Larry. (2000). The State of the Internet: Growth and Gaps, Proceedings of INET International Networking Conference held at Yokohama, Japan for Internet Society, Reston, Va., at http://www.isoc.org/inet2000/cdproceedings/8e/8e_4.htm (14.12.2015).

Puchala, Donald J. (2003). *Theory and History in International Relations*. New York: Routlage.

Punday, Daniel (2000). The Narrative Construction of Cyberspace: Reading Neuromancer. ReadingCyberspace Debates, *College English*, 63(2), 194-213.

Q'Brien, Kevin (2003). Informatıon Age Terrorism and Warfare. (Edited By: Thomas Mockaitis and Paul B. Rich). Grand Strategy In the War Against Terrorism. London: Frank Cass, 177-200.

Quarterman, John (1990). *The Matrix: Computer Networks and Conferencing Systems Worldwide*. Michigan University Bedford: Digital Press.

Quentin Skinner (2003). Political Philosophy (Edited by: C.B. Schimit, Q. Skinner, E. Kessler, J. Kraye).*The Cambridge History of Renaissance Philosophy* (6.Edition), Cambridge; Cambridge University Press, 389-452.

Quincy, Wright (1942). *A Study of War*. Volume:1, Chıcaho and London: The University of Chiago Press.

Rathmell Andrew (2001). Controlling Computer Network Operations. *Information&Security*, 7, 121-144.

Rathmell, Andrew (1997). Cyber□terrorism: The Shape of Future Conflict?*The RUSI Journal*,142(5).

Reed, Chris (2012). *Making Laws for Cyberspace*.Oxford: Oxford University Press.

Reed, William (2003). Information, Power, and War. *The American Political Science Review,* 97(4), 633-641.

Report on Cybersecurity and Critical İnfrascture in the America (2015). http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf (Erişim Tarihi: 05.05.2016)

Rheingold, Howard (1992). *Virtual reality: The Revolutionary Technology of Computer-Generated Artificial Worlds - and How It Promises to Transform Society*. New York: A Touchstone Book Simon & Shuster.

Richard Szafranski (1994). Neocortical Warfare? The Acme ofSkill. Military Review, 41-55, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch17.pdf (Erişim Tarihi: 03.02.2016).

Richardson, Louise (2006). *What Terrorists Want: Understanding the Enemy, Containing the Threat*. New York: Random House.

Richmond, Oliver P. (2008). *Peace in Internatıonal Relatıons*. New York: Routlage

Robert Art J.(2004). Europe Hedges Its Security Bets. (Edited By: Paul James J. And Michel Wirtz). *Balance of Power: Theory and Practice in the 21st Century*.Stanford University Press. 179-213.

Rogers M. (1999). *Pyschology of Computer Criminals, In Proceedings of the Annual Computer Securiy Instıtute Conference*. St. Louis, MO.

Rollins John and Wilson Clay (2007). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. (Report for Congress: RL33123), Congressional Research Service.

Roscini, Marco (2007). Threats of Armed Force and Contemporary Internatıonal Law. *Netherlands International Law Review*, 54(2), 229-277.

Roscini, Marco (2010). *World Wide Warfare Jus ad Bellum and the Use of Cyber Force*. Max Planck Yb United Nations L 85, 14, 85-130

Roscini, Marco (2015). Cyber Operatıons As a Use Of Force, (Edited By: N. Tsagourias and R. Buchan).*Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing, 233-254.

Rosenau James N. and David Johnson (2002). Information and Turbulence in International Politics. (Edited By: Juliann Emmons Allison). *Technology, Development, and Democracy International Conflict and Cooperation in the Information Age*.SUNY series in Global Politics, 55-78.

Rothschild, Emma (2007). *What is Security*.(Edited By: Barry Buzan and Lene Hensen). Volume: 3, International Security. Sage Library of Internatıonal Relatıons, 1-34.

Rousseau, David L., and Garcia-Retamero Rocio (2007). Identity, Power, and Threat Perception: A Cross-National Experimental Study. *The Journal of Conflict Resolution*,51,5, 744-71.

Rudolph, Christopher (2003). Globalization and Security. *Security Studies*, 13(1), 1-32.

Runciman, Brian (2015). State of Play Report Cyber Security.*ITNOW*, 57, 56-57.

Russell, Alison Lawlor (2014). *Cyber Blockades*. Georgetown University Press.

Russia, China Grow Closer With New Cyber Agreement (2015).http://www.defenseone.com/threats/2015/05/russia-china-grow-closer-ever-forge-new-cyber-agreement/112453/(Erişim Tarihi: 12.15.2015).

Sabah (2016). http://www.sabah.com.tr/teknoloji/2016/07/11/nato-siber-savasa-hazirlaniyor (Erişim Tairihi: 28.07.2016).

Sahu. Barun Kumar (t.y.). Need for an Overhaul in Investigation and Prosecution of Cyber Crimes in India, http://www.csi-sigegov.org/emerging_pdf/10_85-88.pdf (Erişim Tarihi: 11.11.2015)

Saleem Muhammad and Jawad Hassan (2009). Cyber warfare, The Truth in a Real Case, Project Report for Information SecurityCourse.https://www.ida.liu.se/~TDDD17/oldprojects/2009/projects/007.pdf(Erişim Tarihi: 30.02.2016).

Samuelson, Pamela (2001). The "New Economy" and Information Technology Policy, http://people.ischool.berkeley.edu/~hal/Papers/infopolicy.pdf (Erişim Tarihi: 11.11.2015).

Sander Oral (2012). *Siyasi Tarih, İlkçağlardan 1918'e*. (3. Baskı). Ankara İmge Kitabevi.

Sasen, Saskia, (2012). The Impact of the Internet on Sovereignty: Unfounded and Real Worries, http://www.progetto-rena.it/wp-content/uploads/2012/08/The-impact-of-the-Internet-on-Sovereignty.-Unfounded-and-real-worries.pdf(Erişim Tarihi: 02.01.2016).

Schelling, Thomas C. (1966). *Arms and Influence*. Yale University Press.

Schıavenza, Matt (2015). Russia, China Grow Closer With New Cyber Agreementhttp://www.defenseone.com/threats/2015/05/russia-china-grow-closer-ever-forge-new-cyber-agreement/112453/(Erişim Tarihi: 13.03.2016).

Schmid Alex P. and Albert J. Jongman (1988). Political Terrorism: *A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*. London: Transaction Publishers.

Schmit, Alex P. and Jongmans, Albert (1988). *Political Terrorism: A New Guide To Actors, Authors, Concepts, Data Bases, Theories, And Literature.* Amsterdam; New York: Transaction Publishers.

Schmitt, Michael (2012). Classification of Cyber Conflict.*Journal of Conflict & Security Law,* 17(2), 245–260.

Schmitt, Michael N. (2014). The Law of Cyber Warfare: Quo vadis?*Stanford Law & Polıcy Review,* 25, 269-299

Schmitt, Micheal N. (2010). *Cyber Operatıonss in ınternatıonal Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict*. Durham University Law School.

Schroeder, Paul W. (1986). The 19th-Century International System: Changes in the Structure.*World Politics*, 39(1),1-26.

Sever, Muhammd (2006). *Siber Terörizm vee Karşı Tedbirler*. Ankara: Terörizmle Mücadele Mükemmliyet Merkezi.

Shackelford Scott J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law.*Berkeley Journal of International Law*, 25(3), 192-250.

Shackelford, Scott J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations.*New York: Cambridge University Press.

Sheean, Michael (2005). *International Security: An Analytical Survey.* Lynne Rienner Publisher.

Shields Robert M. (1996). Introduction: Virtual Space, Real Histories, Living Bodies. (Edited By: Robert Shields M.).*Cultures of Internet: Virtual Space, Real Histories, Living Bodies*. London: Sage, 1-10.

Shimko, Keith L. (2013). *International Relations Perspectives, Contoversies and Readings* (4th Edition).Wadsworth: Cengage Learning.

Siber Saldırı Savaş Sebebi (2011). http://www.ntv.com.tr/dunya/siber-saldiri-savas-sebebi,o7mbQtTvykux9B9Zs9gmpQ(Erişim Tarihi: 18.10.2015)

Siboni, Gabi (2011). ProtectingCritical Assets ans Infrastructures From Cyber Attacks, *Military and Strategic Affairs*, 3(1), 93-101.

Silberglitt, Richard, Anton, Philip S., Anny Wong, David R., Bohandy, S. R. Gassman, Natalie, Jackson, Brian A., Landree, Eric, Lawrence Pfleeger, Shari, Newton, Elaine M. and Wu Felicia (2006). The Global Technology Revolution Executive Summer. (Technical Reports). RAND Corporatıon, 1-44.

Simon Rushton (2011). Global Health Security: Security for Whom? Security from What? *Political Studies*, 59(4), 779–796.

Singel, Ryan (2010). White House Cyber Czar: There is no Cyber War, Wired(3.4.2010), http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ (Erişim tarihi: 30.01.2016).

Singer P.W and Friedman Allan (2015). *Siber Güvenlik ve Siber Savaş*. Ankara: Buzdağı Yayınevi.

Singer, David, J. (1958).Threat-Perception and the Armament-Tension Dilemma. *The Journal of Conflict Resolution, Studies on Attitudes and Communication*, 2(1), 90-105.

SkocpolTheda (1979). *States and Social Revolutions: A Comparative Analysis of France, Russia and China*. Cambridge Unıversity Press.

Smith Michael Joseph (1987). *Realist Thought from Weber to Kissinger*. Baton Rouge: Louisiana State University Press.

Sodon, Ayn Embar (2002). Cyberterrorism Are We Under Siege? *American Behavioral Scientist.*45(6),1033-1043.

Sönmezoğlu, Faruk (2012). *Uluslararası Politika ve Dış Politika Analizi.*(Beşinci Baskı), İstanbul: Der Yayınları.

Spilhaus, Athelstan (1971). The Next Industrial Revolution. *Proceedings of the American Philosophical Society*, 115 (4), 324-327.

Stephanson, Anders (1998). Rethinking Cold War History. *Review of International Studies, 24*(1), 119-124

Sterling, Bruce (1985). *Minorshades: The Cyberpunk Anthology*. New York: Arbor House.

Stevens, Tim (2015). *Cyber Security, Community, Time, Cyber Security and the Politics of Time.* Cambridge: Cambridge University Press.

Stıglız, Joseph E. (2007). *Makıng Globalizatın Work*. New York and London: W.W. Norton&Company.

Strassler Robert B. (1996).*The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War.* New York: Free Press.

Strauss Leo (1987). Niccolo Machiavelli. (Edited By: Lee Strauss and Joseph Cropsey).*History of Political Philosophy* (3.Edition). Chiago: University of Chiago Press, 296-318

Stritzel, Holger (2007). Towards a Theory of Securitization: Copenhagen and Beyond.*European Journal of International Relations*,13(3), 357-383.

Suhukla Shashi (2006). Emerging New Trends of Terrorism: Challenges Before the Unıted Nations. *The Indian Journal of Political Science*, 67(1). 165-176

Sumner, James and Gooday, Graeme (2008). By Whose Standards? Standardization, Stability and Uniformity in the History of Information and Electrical Technologies. History of Technology, (Edited by: Ian Inkster). *History of Technology, Institute of Historical Research*. London: University of London. 1-15.

Susan W. Brenner (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare.*Journalof Criminal Law. & Criminology*, 97(2), 379-476.

Swith W. Thomas (1999). *History and International Realations*. Londra ve Newyork: Routlege, 1999.

Şahin, Çiğdem (2004). Türkiye için Teorik Bir Çerçeve Önerisi: Buzan'ın Güvenlik Kompleksi Teorisi. IV. Türkiye'nin Güvenliği Sempozyomu (Tarihten Günümüze Dış Tehditler). *Elazığ Fırat Üniversitesi Basımevi.*

Tabansky, Lior (2011). Critical Infrastructure Protection against Cyber Threats. *Military and Strategic Affairs*, 3(2), 61-78.

Talarico, Kathryn M. (1999). *Cyberspace Without Tears: Fundamental Approaches to the Uses of Technology in the Classroom*. Literary Linguist Computing, 14(2), 199-210.

Taliharm Anna-Maria (2010). Cyberterrorism: in Theory or in Practice? *Defence Against Terrorism Review,* 3(2), 59-74.

Tanrısever, Oktay (2014). Güvenlik (Derleyen: Atilla Eralp). *Devletler ve Ötesi. İstanbul: İletişim Yayınları*, 107-124.

Taspcott, Don Caston, Art (1993). *Paradigm Shift: The New Promise of Information Technology*. Minnesota Üniversitesi: McGraw-Hill.

Tatar, Ünal (2011). *Dünya'da ve Türkiye'de Siber Güvenlik Tatbikatları*. Ankara: Tübitak Bilgem.

Terrıf, Terry (2007). Environmental Degragation and Security. (Edited by: Richard H. Shultz, Roy Godson and George H. Quester). *Security Studies for the 21. Century.* Virginia USA: Brassey's, 257-283.

Terrıff, Terry, Croft, Stuart, James, Lucy ve Patrik Morgan (1999). *Security Studies Today*. Cambridge: Polity Press.

The Natıonal Strategy to Secure Cyberspace (2003). https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf(Erişim Tarihi: 11.01.2016).

The Oxford English Dictionary, http://www.oxforddictionaries.com/definition/english/security (Erişim Tarihi: 21.09.2015)

The UK Cyber Security Strategy (2011).https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf(Erişim Tarihi. 24.12.2015).

The UK Cyber Security Strategy 2011-2016, Annual Report (2016). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (Erişim Tarihi: 22.12.2016).

The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World (2011). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Erişim Tarihi: 11.01.2016)

The UK Cyber Security Strategy, (2016). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (Erişim Tarihi: 16.03.2015).

Theohary, Catherine A. and John Rollins W. (2015). Cyberwarfare and Cyberterrorism: In Brief, Congressional Research Service Report,https://fas.org/sgp/crs/natsec/R43955.pdf (Erişim Tarihi: 21.12.2015).

Theohary, Catherine A. and Rollins John (2011). Terrorist Use of the Internet: Information Operations in Cyberspace. *Congressional Research Service* 7-5700.

Thomas Rid and Peter McBurney (2012). Cyber-Weapons.*The RUSI Journal*, 157(1), 6-13.

Thomas Rid, "Cyber War will not Take Place in", *Strategic Studies*, V.35, I.1, 2012, s.5-32;

Thomas, Tımothy (2002). Al Qaeda and the Internet: The Danger of "Cyberplanning", *Parameters*, 112-123.

Thompson, Joseph E. (2002). Virtual Regime: A New Actor in the Geopolitical Arena. *PS: Political Science and Politics*, 35(3), 507-08.

Thukydides (2010). *Peleponnes Savaşları*. (Çeviren: Furkan Akderin). Belge Yayınları,

Tıme, (2014).Case of The Cyber War: Kosovo Conflict. http://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/ (Erişim Tarihi: 02.03.2016).

Tilly, Charles (1975). Reflections on the History of European State Making. (Edited By: Charles Tilly).*The Formation of National States in Western Europe*, London: Princeton University Press, 3-83.

Türk Dil Kurumu http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.57946e799b2b82.18248825 (Erişim Tarihi: 12.11.2015).

Ullman, Richard H. (1983). *Redefınıng Security*. International Security, 8(1), 129-153.

Ulusal Siber Güvenlik Stratejisi (2016). http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (Erişim Tarihi: 10.09.2015).

Understanding Definitions of Terrorism (2015).**http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS_ATA(2015)571320_EN.pdf** (Erişim Tarihi: 20.01.2016).

United Kingdom Terrorism Act of 2000 (2000). http://www.legislation.gov.uk/ukpga/2000/11/pdfs/ukpga_20000011_en.pdf (Erişim Tarihi: 13.02.2015).

United Natıon System Chief Executives Board for Coordination (2003). Unıted Natıons Conference on Ttrade and Development Informatıon and Communicatıon Technology Development Indices. Report. New York and Geneva.

United Nations, UN Terms, http://unterm.un.org/dgaacs/unterm.nsf/WebView/99B98BDB CBAB096185256E620052EFD3?OpenDocument (Erişim Tarihi: 08.06.2015)

Ülgen, Memduh (2003). *Asimetrik Tehdit, Konsept, NATO ve Türkiye*.Ankara: Harp Akademileri Bülteni.

Ünver Mustafa ve Canbay Cafer (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik.*Elektrik Mühendisliği*, 438, 94-103.

Ünver Mustafa, Canbay Cafer ve Mirzaoğlu A.G (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut durum ve Alınması Gereken Tedbirler.*Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı,* Mayıs 2009.

Van der Wusten, H. (1996). Galtungs Peaces. How to Deal With Various Forms of Violence. *GeoJournal,* 39(4), 405-407.

Venkatesh, Vismanatah, Morris, Micheal, G., Davis, Gordon B., and Davis, Fred (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 425-478.

Verton, Dan (2003). *Black Ice: The Invisible Threat of Cyber Terrorism*. McGraw-Hill Osborne Media.

Virtual Criminology Report (2009). Virtually Here: The Age of Cyber Warfarehttp://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_REG.pdf (Erişim Tarihi: 28.01.2016).

Visner, Samuel. (2013). Cyber Security's Next Agenda. *Georgetown Journal of International Affairs, http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13008_Visner-CYBER-III.pdf*(Erişim Tarihi: 11.04.2016).

Vorobej, Mark (2008). Structural Violence. *Peace Research*, 40(2), 84-98.

Walker, R.B.J. (1993). *Inside/Outside: Internatıonal Relatıons as Political Theory*. Cambridege University Press.

Walt, Stephan M. (1991). The Renaissance of Security Studies.*International Studies Quarterly,*35 (2), 211-239

Waltz, Kenneth (1959). *Man, The State and War: A Theoretical Analysis*. New york: Columbuia University Press.

Waltz, Kenneth (1986). Anarchic Orders and Balances of Power. (Edited By: Robert O. Keohane). *Neorealism and Its Critics*. New York: Columbia University Press, 70-130.

Waltz, Kenneth (2009). *İnsan Devlet ve Savaş Teorik Bir Analiz*. İstanbul: Asil Yayın Dağıtım

Waltz, Kenneth N. (1990). Realist Thought and Neorealist Theory. *Journal of International Affairs*, 44(1), 21-37.

Waltz, Kenneth N., (1986). Anarchic Orders And Balances Of Power. (Edited By: Robert O. Keohane). *Neorealizm and Its Critics.* New York: Colombia University Press, (98-130).

Ware, Dough G. (2016). NATO officially recognizes cyberspace as domain for war. http://www.upi.com/Top_News/World-News/2016/06/14/NATO-officially-recognizes-cyberspace-as-domain-for-war/2271465941545/ (Erişim Tarihi: 14.04.2016).

Warner, Micheal and Good, Micheal (2013). Notes on Deterrence in Cyberspace. Georgetown Journal of International Affairs, 65-72. http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13006_Warner-CYBER-III.pdf (Erişim Tarihi: 18.03.2016).

Waver Ole (2007). Securitizatisation and Desecuritisation. (Edited By: Barry Buzan and Lene Hansen).*Internatıonal Security*. Volume:3, Sage library of Internatıonal Relatıons. 66-98.

Waver, Ole (1998). Security, İnsecurity and Asecurity in the West European Non War Community. (Edited By: Emmanuel Adler and Michael Bannet). *Security, Communities*. Cambridge: Cambridge University Press.

Waver, Ole (2011). Politics, Security, Theory. *Security Dialogue,* 42(4-5), 465-480.

Webb, Stephen A. (2009). Vision of Excess; Cyberspace, Digital Technologies and New Cultural Politics, Information.*Communicatıon & Society,* 1(1), 46-69.

Webster, William H. Borchgrave, Arnaud D. Gallagher, Patrick R. Cilluffo, Frank J., Berkowitz, Bruce. and Lanz, Stephanie (1998). Cybercrime… Cyberterrorism...Cyberwarfare,… Averting an Electonic Waterloo, Centre for Strategic and International Studies (CSIS), (Report No: 89206). Washington, DC.

Weımann Gabriel (2005). Cyberterrorism: The Sum of All Fears? Studies in Conflict & Terrorism.*Routledge: Taylor and Francis*, 28, 129–149,

Weiman, Gabriel (2006). *Terror on the Internet.*Washington: United Sates Institute of Peace Press.

Weimann Gabriel (2005). The Theatre of Terror. *Journal of Aggression, Maltreatment&Trauma*, 9 (3-4).

Weimann, Gabriel (2004). How Modern Terrorism Uses the Internet, United States Institute of Peace Special Report (Repor No: 116). Washington DC www.usip.org/sites/default/files/sr116.pdf (Erişim Tarihi: 13.12.2015).

Weimann, Gabriel (2011). Cyber-Fatwas and Terrorism, *Studies in Conflict & Terrorism*,34(10), 765-781.

Weimann, Gabriel, (2004).Cyberterrorism How Real Is the Threat? Unıted States Institute of Peace, 2004, Special Report.

Weiss, Charles, (2003). New Tools and New Challenges. *Georgetown Journal of International Affairs*,4(2), 107-110.

Weiss, Charles, (2005). Science, Technology and İnternational Relations.*Technology in Society,*27(3), 295–313

Wenger, Andreas (2001). The Internet and the Changing Face of International Relations and Security. (Edited By: Andreas Wenger).*The Internet and the Changing Face of International Relations and Security*. Information & Security, I&S Monitor, Volume: 7, 3-8.

Wentz, Larry (2002). Introductıon and Background. (Edited By: Larry Wentz).*Lessons From Kosovo: The KFOR Experience*. CCRP Publication Series.

What is a Script Kiddie? **http://www.pctools.com/security-news/script-kiddie/** (Erişim Tarihi: 03.02.2016).

Wheatcroft, Geoffrey. (2011). Once Upon a Time in Westphalia. *The National Interest*, 115, 10-17.

Whittaker, Jason (2004). *The Cyberspace Handbook*. London: Routledge, Taylor&Francis.

WikiLeaks Stages 'diplomatic 9/11' (2010). http://www.euractiv.com/section/public-affairs/news/wikileaks-stages-diplomatic-9-11/(17.10.2015).

Wilkinson, Paul (2011). *Terrorism Versus Democracy: The Liberal State Response*. (Third Edition). New Yok: Routledge.

William A. Owens, Kenneth W. Dam, Herbert S. Lin (2009). *Technology, Policy,Law, and Ethics Regarding U.S. Acquisition and Use of CyberattackCapabilities, Committee on Offensive Information Warfare, National ResearchCouncil*, Washington DC.: The National Academies Press,

Williams Howard, Moorhead Wright and Tony Evans (1996). *Uluslararası İlişkiler ve Siyaset Teorisi Üzerine Bir Değerlendirme*.Ankara: Siyasal Yayınevi.

Williams, M. J. (2009). *NATO, Security and Risk Management From Kosovo to Kandahar*. London: Routledge Taylor Francis.

Williams, Marc, (1989). Transnationalism and Interdependence, (Edited By: Marc Williams)*Internatıonal Relations in the Twentieth Century A Reader*. New york University Press, 241-274.

Williams, Michael C. (1996). Hobbes and ınternatıonal Relatıons: A Consideratıon. *Internatıonal Organization,* 50(2), 213-236.

Williams, Michael C. (2003). Words, Images, Enemies: Securitization and International Politics.*International Studies Quarterly*, 47(4), 511–531.

Williams, Michael C. (2006). The Hobbesian Theory of International Relations: Three Traditions, (Edited By: Beate Jahn).*Classical Theory in International Relations*. (1. Edition). Cambridge: Cambridge University Press, 253-276.

WillsDavid Barnard and Debi Ashenden, Securing Virtual Space: Cyber War, Cyber Terror, and Risk.*Space and Culture*, 15(2), 110-123.

Wohlforth, William C. (2008). Realism. (Edited by: C.REus-Smith ve D.Sindal). *Oxford Handbook of İnternational Relations*. New York: Political Science 131-147.

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

World Islamic Front (1998). Jihad against Jews and Crusade. http://fas.org/irp/world/para/docs/980223-fatwa.htm (Erişim Tarihi: 11.02.2016).

Yalvaç, Faruk (2014). Devlet. (Derleyen: Atilla Eralp). *Devlet ve Ötesi* (8.Baskı). İstanbul: İletişim Yayınları,15-53.

Yayla, Mehmet (2013). Hukuki Bir Terim Olarak Siber Savaş. Türkiye Barolar Birliği Dergisi. 104, 177-202.

Yergin, Daniel(1990). *Shattered Peace: The Origins Of The Cold War And The National Security State*. (Revised edition). Penguin Books.

Yurdusev, Nuri (2006).*Thomas Hobbes and International Relations: From Realism to Rationalism*.Australian Journal of International Affairs, 60(2), 305-321.

Zacher Mark W. and Matthew Richard A. (1995). Liberal Internatıonal Theory: Common Needs, Divergent Strands. (Edited by: Charles W.Kegley, Jr). *Contraversies in International Relations Theory, Realism and the Neoliberal Challenge*. New york: St. Martin's Press, 102-121.

Zarakol, Ayşe (2011). What Makes Terrorism Modern? Terrorism, Legitimacy, and the International System.*Review of International Studies.* 37(5). 2311-2336.

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

Zhao, Shanyang (2005). The Digital Self: Through the Looking Glass of Telecopresent Others, Symbolic Interaction.*Society for the Study of Symbolic Interaction*, 28(3), 387–405.

http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/(Erişim Tarihi: 18.09.2015).

http://infoscape.org/publications/cyberspace98.pdf (Erişim tarihi: 16.03.2016)

http://www.af.mil/AboutUs/SpeechesArchive/Display/tabid/268/Article/143968/cyberspace-as-a-domain-in-which-the-air-force-flies-and-fights.aspx(Erişim Tarihi: 22.03.2016).

http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html(Erişim Tarihi: 11.11.2015).

http://www.euractiv.com/section/public-affairs/news/wikileaks-stages-diplomatic-9-11/(Erişim Tarihi: 12.01.2016).

http://www.hurriyet.com.tr/pkknin-en-onemli-hackeri-yakalandi-10393202(Erişim Tarihi: 14.11.2015).