T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANA BİLİM DALI

KÜRESELLEŞME SÜRECİNDE DEĞİŞEN GÜVENLİK ALGISI: SİBER GÜVENLİK ÖRNEĞİ

Soner ÇELİK
1440220502

DOKTORA TEZİ

Danışman
Prof. Dr. Muharrem GÜRKAYNAK

ISPARTA, 2021

TEZ SAVUNMA SINAV TUTANAĞI

T.C.

SÜLEYMAN DEMİREL ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

YEMİN METNİ

Doktora tezi olarak sunduğum "**KÜRESELLEŞME SÜRECİNDE DEĞİŞEN GÜVENLİK ALGISI: SİBER GÜVENLİK ÖRNEĞİ**" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim.

Soner ÇELİK

08.07.2021

T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ ÇALIŞMASI ORİJİNALLİK RAPORU
BEYAN BELGESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

ÖĞRENCİ BİLGİLERİ	
Adı-SOYADI	**SONER ÇELİK**
Öğrenci Numarası	**1440220502**
Enstitü Ana Bilim Dalı	**ULUSLARARASI İLİŞKİLER ANABİLİM DALI**
Programı	**AVRUPA BİRLİĞİ ÇALIŞMALARI**
Programın Türü	**( ) Tezli Yüksek Lisans (x) Doktora**
Danışmanının Unvanı, Adı-SOYADI	**Prof. Dr. Muharrem GÜRKAYNAK**
Tez Başlığı	**Küreselleşme Sürecinde Değişen Güvenlik Algısı: Siber Güvenlik Örneği**
Turnitin Ödev Numarası	**160401185**

Yukarıda başlığı belirtilen tez çalışmasının a) Kapak sayfası, b) Giriş, c) Ana Bölümler ve d) Sonuç kısımlarından oluşan toplam 223 sayfalık kısmına ilişkin olarak, 10/06/2021 tarihinde tarafımdan Turnitin adlı intihal tespit programından Üniversitemiz Lisansüstü Eğitim ve Öğretim Yönergesininin 14 üncü maddesinde yer alan filtrelemeler uygulanarak alınmış olan ve ekte sunulan rapora göre, tezin/dönem projesinin benzerlik oranı;

Kaynakçalar hariç, alıntılar dahil, 10 kelimeden daha az örtüşme içeren metin kısımları hariç;

% 14'tür.

Danışman tarafından uygun olan seçenek işaretlenmelidir:

(x) Benzerlik oranları belirlenen limitleri aşmıyor ise;
Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylarım.

( ) Benzerlik oranları belirlenen limitleri aşıyor, ancak tez/dönem projesi danışmanı intihal yapılmadığı kanısında ise;

Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylar ve Uygulama Esasları'nda öngörülen yüzdelik sınırlarının aşılmasına karşın, aşağıda belirtilen gerekçe ile intihal yapılmadığı kanısında olduğumu beyan ederim.

Gerekçe:

Benzerlik taraması yukarıda verilen ölçütlerin ışığı altında tarafımca yapılmıştır. İlgili tezin orijinallik raporunun uygun olduğunu beyan ederim.

05/08/2021

Prof. Dr. Muharrem GÜRKAYNAK

(ÇELİK, Soner, *Küreselleşme Sürecinde Değişen Güvenlik Algısı: Siber Güvenlik Örneği,* Doktora Tezi, 2021)

ÖZET

Güvenlik olgusu, geçmişten günümüze kadar üzerinde sürekli tartışılan bir kavram olmuştur. Özellikle ulus devlet yapılarının meydana çıkması ile güvenlik kavramı sürekli bir değişim içerisine girmiştir. Günümüzde, her alandaki değişimin hızlı bir şekilde artması ve özellikle 20. yüzyılda küreselleşme, bilim ve teknoloji alanındaki gelişmeler, akademi literatüründe yer alan diğer kavramlarda olduğu gibi, güvenlik kavramı tanımında da değişime yol açmıştır.

Özellikle Soğuk Savaş sonrası dönemde, "tehdit" tanımlaması, düşman tanımlamasından çok daha önemli hale gelmiştir. Önceki dönemlerin aksine, klasik "düşman" nitelendirmesi büyük oranda geçerliliğini yitirmiş, güvenliğe yönelik algılamalar ve politikalar açısından tehdit tanımı ve tehditler ile mücadele yaklaşımı ön plana çıkmıştır. Tüm bu gelişmelerin sonucu olarak; terörizm, organize suç örgütleri, siber saldırılar, konvansiyonel ve kitle imha silahlarının yaygınlaşması, çevresel tehditler, kitlesel göç gibi tehditler; ulusal ve uluslararası güvenliğe yönelmiş tehditler arasında gösterilmektedir. Çalışmada, ortaya çıkan yeni güvenlik anlayışına yönelik önemli tehditlerden biri olan siber tehditler, siber uzay ve siber güvenlik konularına değinilecek olup kavramsal ve kuramsal zeminde tanımlamalar yapılmaya çalışılacaktır. Ardından, günümüz dünyasında yaşanan siber saldırılar ve gelişmeler sosyal bilimler açısından dikkate alınarak siber güvenliğin ulusal ve uluslararası güvenliğe etkisinin incelemesi yapılacaktır. Buradan hareketle kişisel, kurumsal ve ulusal düzeyde alınabilecek tedbirlere dair öneriler ortaya konmaya çalışılacaktır.

Çalışmada yapılacak analizler, uluslararası ilişkiler teorilerinden, derinleştirilmiş ve genişletilmiş bir güvenlik tanımı yapmaya çalışan Kopenhag Okulu bağlamında ele alınacaktır. Bu bakış açısıyla geleneksel güvenlik yaklaşımının görmezden geldiği siber güvenlik, siber saldırılar ve siber tehditler gibi konularda modern güvenlik çalışmalarına katkı yapılabileceği düşünülmektedir.

Anahtar Kelimeler: Küreselleşme, Güvenlik, Siber Güvenlik.

(ÇELİK, Soner, *Changing Security Perception In The Globalization Process: The Example of Cyber Security*, Ph. D. Thesis, 2021)

ABSTRACT

The term of security, has been consistently discussed as a case of human beings until today. Especially with the formation of nation-state structures, the concept of security has undergone a constant change. The rapid change in all parts of the world today has led to a change in the definition of security as well as in the concepts of globalization, science and technological developments in the twentieth century, as well as in all the concepts of the academia literature.

Especially in the post-Cold War period, the concept of "threat" became more important than the concept of the enemy. Contrary to the previous periods, the concept of classical "enemy" has lost its effectiveness in large scale and the approach to combat threat definitions and threats has come to the forefront in terms of security. As a result of these events; international terrorism, organized crime organizations, cyber attacks, the spread of conventional and weapons of mass destruction, environmental threats and mass migration; threatened national and international security threats. The study will focus on cyber threats, cyberspace and cybersecurity issues that are one of the major threats to the new security approach, and will try to define the conceptual and theoretical ground. Then, we will examine the effects of cyber security on national and international security by taking into consideration the cyber attacks and events in the world today in terms of social sciences. From here, we will try to put forward suggestions that can be taken at personal, institutional and national level.

Analyzes to be carried out in the study will be dealt with in the context of the Copenhagen School, which tries to make a deepened and expanded definition of security from international relations theories. From this point of view, it is considered to contribute to modern security studies such as cyber security, cyber attacks and cyber threats, which traditional security approach ignores.

Key Words: Globalization, Security, Cyber Security.

İÇİNDEKİLER

İKİNCİ BÖLÜM
GÜVENLİK ALGISINDAKİ DEĞİŞİM

ÜÇÜNCÜ BÖLÜM
SİBER TEHDİTLER VE SİBER SAVAŞIN HUKUKSAL ANALİZİ

DÖRDÜNCÜ BÖLÜM
DÜNYADA SİBER TEHDİTLERE KARŞI YAPILAN FAALİYETLER

BEŞİNCİ BÖLÜM
TÜRKİYE'DE SİBER TEHDİTLERE KARŞI YAPILAN FAALİYETLER

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
ADY	: Ağ Destekli Yetenek
AFSC	: Hava Kuvvetleri Uzay Komutanlığı
ARGE	: Araştırma Geliştirme
ASAL	: Askere Alma Dairesi
ASEAN	: Güneydoğu Asya Uluslar Birliği
BİT	: Bilgi ve İletişim Teknolojileri
BM	: Birleşmiş Milletler
BMGK	: Birleşmiş Milletler Güvenlik Konseyi
CENTO	: Merkezi Antlaşma Teşkilatı
CERT	: Bilgisayar Olaylarına Müdahale Ekibi
CIA	: Merkezi Haber Alma Servisi
CSS	: Eleştirel Güvenlik Yaklaşımları
CSSL	: Siber Güvenlik Hizmet Hattı
CTOC	: Ulusaşan Organize Suçlarla Mücadele Konvansiyonu
ÇHC	: Çin Halk Cumhuriyeti
DoS	: Hizmet Dışı Bırakma
DDoS	: Dağınık Hizmet Dışı Bırakma Saldırıları
DTÖ	: Dünya Ticaret Örgütü
DPT	: Devlet Planlama Teşkilatı
FBI	: Federal Araştırma Bürosu
FSB	: Federal Güvenlik Servisi
GRU	: Ana İstihbarat İdaresi
IEA	: Uluslararası Enerji Ajansı
IMF	: Uluslararası Para Fonu
IMPACT	: Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği
ITU	: Uluslararası Telekomünikasyon Birliği
KİS	: Kitle İmha Silahları
NATO	: Kuzey Atlantik Antlaşması Örgütü
NICP	: NATO Endüstri Siber Ortaklığı
NO.	: Numara
NSA	: Ulusal Güvenlik Ajansı
OECD	: Ekonomik Kalkınma ve İşbirliği Örgütü
PLA	: Çin Halk Kurtuluş Ordusu
RF	: Rusya Federasyonu
s.	: Sayfa
SÇH	: Silahlı Çatışma Hukuku
SEATO	: Güneydoğu Asya Anlaşması Örgütü

SOME	: Siber Olaylara Müdahale Ekibi
ss.	: Sayfa Aralığı
SVR	: Dış İstihbarat Servisi
SGK	: Siber Güvenlik Kurulu
TDK	: Türk Dil Kurumu
TR-BOME	: Türkiye Bilgisayar Olayları Müdahale Ekibi
TÜBİTAK UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Ensttüsü
USCYBERCOM	: ABD Siber Komutanlığı
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
UYAP	: Ulusal Yargı Ağı
vb.	: ve benzeri

TABLOLAR DİZİNİ

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

ÖNSÖZ

Doktora eğitim süreci boyunca yolumu aydınlatan, bilgi birikimi ve tecrübeleriyle akıl hocalığı yapan saygıdeğer danışmanım Prof. Dr. Muharrem GÜRKAYNAK'a, tez çalışmalarımın izlenmesinde ve yönlendirilmesinde değerli katkılarından dolayı Tez İzleme Komitesi Üyeleri Prof. Dr. Mehmet AKTEL ile Dr. Öğr. Üyesi Adem Ali İREN'e, savunma jürimde yer alan ve yorumlarıyla gelecek çalışmalarım için destek olan Doç. Dr. Ali Burak DARICILI ve Dr. Öğr. Üyesi Merve SEREN YEŞİLTAŞ'a, en içten teşekkürlerimi sunar ve saygılarımı iletirim.

Ayrıca, doktora eğitimi almam için beni isteklendirmekle kalmayıp yönlendiren ve çalışmalarım boyunca her türlü destekleriyle beni hiçbir zaman yalnız bırakmayan, sabır gösteren değerli eşime ve aileme sonsuz teşekkür ederim.

GİRİŞ

Çalışmanın konu başlığı, "Küreselleşme Sürecinde Değişen Güvenlik Algısı: Siber Güvenlik Örneği" şeklinde seçilmiştir. Araştırma problemimiz ise "Güvenlik algısındaki değişimin küreselleşme kavramı ile ilişkisi, yeni güvenlik anlayışına yönelik tehditler bağlamında ortaya çıkan ve giderek önemi artan "siber güvenlik" örneği üzerinden açıklanabilir mi?" olarak belirlenmiştir.

Küreselleşen dünya düzeni içerisinde teknolojik gelişmelerde yaşanan baş döndürücü hızla beraber güvenlik algısında ciddi değişimler yaşanmış ve gelişmelere paralel olarak güvenliğin yeni boyutlarının ve güvenlik alanında yeni risk/tehditlerin ortaya çıkmasına sebep olmuştur. İki kutuplu dünya düzeninde Soğuk Savaş dönemi boyunca düşmanın, tehditlerin belli olduğu ve gösterilecek reaksiyonların öngörülebildiği şartlardan, küreselleşmenin de tesiriyle uluslararası platformda kendini gösteren öngörülemez, karmaşık ve süratle değişen bir ortama dönüşüm yaşanmıştır. Bu gelişmeler çerçevesinde güvenlik kavramını belirli kalıplara oturtmak, tanımını yapmak, tüm tarafların üstünde mutabık kalabileceği hudutlarını çizmek çok zor hatta neredeyse imkânsız hale gelmiştir.

Zaman içerisinde güvenlikte esas alınan ulus devlet anlayışının ötesinde bireylerin, toplulukların da bulunduğu geniş bir kümeye geçiş yaşanmıştır. Teknolojik gelişmelerle birlikte klasik askeri tehdit/risklerin ötesinde zamanı, şiddeti, kaynağı, biçimi, sorumlusu, hukuksal çerçevesi belli olmayan, iç içe geçmiş, karmaşık tehditlerin yeni rekabet alanı tüm dünya olarak kendini göstermiş ve çok boyutlu bir konuma yükselerek bambaşka bir güvenlik kavramını ortaya çıkarmıştır.

Özellikle ABD'de yaşanan 11 Eylül 2001 olayının ardından kendini gösteren asimetrik tehdit ve asimetrik güvenlik anlayışı ile beraber; düzensiz göç, çevresel konular, kitle imha silahlarının yayılması, yeni teknolojilerin getirdiği zorluklar, organize suç örgütleri, siber güvenlik gibi kavramlar güvenliğe ilişkin önlem alınması gereken konular arasına girmiştir. 11 Eylül saldırısı sonrasında yaşanan gelişmeler düşman kavramı yerine tehdit kavramının, tanımının ve tehditlerle mücadeleye ilişkin alınacak tedbirlerin ön plana çıkmasına neden olmuştur.

Yeni güvenlik ortamında yaşanan gelişmelerle ortaya çıkan yeni risk ve tehditlerin arasında özellikle siber güvenlik ve siber ortamda yaşanan problemler biraz daha öne çıkmaktadır. Bilgisayar ve internetin hayatın her alanına yerleşmesi, kullanımının her geçen gün katlanarak ivmelenmesi, kritik altyapı/tesis/sistemlerin idaresinin ve kontrolünün bilgisayarlarla yapılması, artık herkesin cebinde bir bilgisayar taşıması sebebiyle siber tehditlerin tesirleri devletlerden bireylere kadar çok geniş bir spektrumda herkes için hayati öneme haiz bir konuma yükselmiştir.

Devletlerin siber uzayın doğal bir aktörü haline dönüşmesiyle beraber, siber suçların etki alanı basit siber eylemlerden ülkeler arasında oluşabilecek muhtemel siber savaşlara kadar kendini göstermiştir. Siber suç, siber terörizm, adi siber eylemler, siber müdahale, siber saldırı ve siber savaşlara karşı milli güvenliğin tesis edilmesi maksadıyla birçok ülke, uluslararası kurum/kuruluşlar tarafından siber konularla alakalı politika, hukuk, strateji ve işbirliği belgeleri hazırlanmıştır.

Ayrıca, bilgi teknolojilerinin güvenliğin kaderini değiştirmedeki kilit rolü yeni bir harekât alanının doğmasına sebep olmuştur. Kara, deniz, hava ve uzaydan sonra beşinci bir boyut olarak açılan bu yeni harekât alanı siber uzay olarak adlandırılmıştır.

Ülkeler siber tehdit ve siber savaşla mücadelede yeni harekât ortamına uyum sağlamak için teşkilat yapısından hukuki mevzuata, eğitimden teknik konulara kadar çok geniş bir perspektifte değişikliğe gitme ihtiyacı duymuştur. Ancak gösterilen tüm gayretlere rağmen henüz siber uzayın güvenliği ile ilgili atılan adımlar yeterli seviyeye ulaşmamış olup birçok boşluğu içinde barındırmaktadır.

Çalışmanın birinci bölümünde, küreselleşme, güvenlik ve siber güvenlik konuları kavramsal çerçevede ele alınmıştır. Bu bölümde güvenlik ve siber güvenlik konularına eğilerek, güvenlik kavramını epistemolojik olarak şekillendiren uluslararası ilişkiler teorilerinin kuramsal ana argümanları ele alınmıştır. Geleneksel güvenlik anlayışı içinde yer alan idealist, realist ve eleştirel teorilere yer verilmiştir. “Siber güvenlik, siber uzay, siber saldırı ve uluslararası ilişkiler disiplini arasındaki ilişki nasıl kurulabilir? Bu disiplinle çalışılması mümkün müdür?” sorularına cevap aranmaya çalışılmıştır.

Çalışmanın ikinci bölümünde Soğuk Savaş döneminden itibaren, güvenlik algısında meydana gelen değişime odaklanılarak, değişen güvenlik algısında ortaya çıkan yeni risk ve tehditleri ile güvenlik algısını şekillendiren kavramlar detaylı bir şekilde

incelenmiştir. Güvenlik algısındaki değişim, yapısal ve ideolojik faktörler ile tehditler esas alınarak incelenmiştir.

Çalışmanın üçüncü ve dördüncü bölümde, siber güvenliğin uluslararası güvenliğe ve hukuksal mevzuata etkisinin incelenmesinin, günümüz dünyasında yaşanan siber eylemleri anlamak açısından önemli bir yer tutmasından hareketle aşağıda yer alan bazı temel soruların cevapları aranmaya çalışılacaktır;

Bu çerçevede aktörler kimlerdir? Siber güvenlik denilirken kimin güvenliği kastedilmektedir? Devletler siber uzayda yeni oyuncular mıdır? (*new comers*) Siber uzayın kapsamı nedir? Siber uzay anarşik yapıda mıdır? Siber uzay merkezi var mıdır? Son dönemlerde yaşanan önemli siber vakalar ve bu vakaların uluslararası güvenlik algısı içerisinde doğurdukları sonuçlar nelerdir? Siber güvenliğin hukuki çerçevesi nedir? Siber saldırılar uluslararası hukuk çerçevesinde meşru müdafaa ve kuvvet kullanımı hakkını doğurmakta mıdır? Siber uzayın yönetişim sorununun uluslararası-ulusal güvenlik boyutuna etkisi nedir? Uluslararası kurum/ kuruluşlar ile ülkelerin siber güvenlik konusunda attığı adımlar nelerdir?

Çalışmamızın beşinci bölümünde ise siber güvenlik konusu Türkiye bağlamında ulusal güvenlik çerçevesinde tahlil edilmiştir. Bu kapsamında siber tehditlere yönelik yasal düzenlemeler ve teşkilatlanma yapısı incelenmiş, ulusal siber güvenlik politikaları anlatılmaya çalışılmıştır.

Son olarak, sonuç ve değerlendirme bölümünde ise, elde edilen bütün bulgulardan yola çıkarak, siber güvenliğin uluslararası ilişkiler düzleminde kullanılmaya başlaması ile uluslararası ve ulusal politikaları derinden değiştirmesinin önemini ortaya koyan değerlendirmeler yapılmıştır. Elde edilen bulgulardan hareketle kişisel, kurumsal ve ulusal/uluslararası düzeyde alınabilecek tedbirlere dair öneriler ortaya konularak bir model önerisi yapılmıştır.

Yapılan çalışmamızın nihai amacı ise, küreselleşme kavramını tarihsel perspektif, etkileri ve küreselleşme yaklaşımlarını da içerecek şekilde açıklayarak, güvenlik tanımının teorik içerik ve tarihsel boyut çerçevesinde neden ve nasıl değiştiğini ve değişen bu güvenlik algısıyla beraber ortaya çıkan yeni risk ve tehditleri analiz etmektir.

İlave olarak farklı bakış açıları ve Uluslararası İlişkiler teorileri ile ulusal ve uluslararası bir güvenlik sorunu haline gelen "siber güvenlik" ve "siber uzay" konularının

daha anlaşılabilir hâle getirmek için kavramsal ve kuramsal zeminde tanımlamalar yaparak, siber tehditlerin ve siber güvenliğin önemini ortaya çıkarmaktır.

Ayrıca siber güvenlik konusunda özellikle hukuki mevzuat açısından boşlukları belirleyerek, siber saldırıların hukuki sonuçlarının neler olabileceğini ve bu sonuçların güvenlik algısına etkilerini saptamak, Türkiye'de, siber tehdit, siber uzay ve siber güvenlik konularında kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlardaki durumu ortaya koyarak konu hakkında farkındalık yaratmak, siber tehditlerin ve siber güvenliğin ulusal ve uluslararası güvenliğine etkisini inceleyerek, bu konuda az sayıda bulunan literatürdeki güvenlik çalışmalarına katkı sağlamak ve elde edilen bulgulardan hareketle kişisel, kurumsal ve ulusal/uluslararası düzeyde alınabilecek tedbirlere dair öneriler ortaya koyarak bir model önerisi sunmaktır.

Çalışmamız; Türkçe literatürde siber güvenliğe ilişkin bilgi eksikliğinin giderilmesi ve konuya ilişkin kavramların ortaya konarak belli bir standart getirilmesi ve özelde güvenlik algısı ile siber konusunun birleştirilerek konunun hukuki çerçevesini de içerecek şekilde detaylandırılması açısından önem arz etmektedir. Ayrıca, Türkiye'de siber güvenlik ve siber uzay alanının incelenmesi ile Türkiye'nin uluslararası ilişkiler literatüründe eksik olan önemli bir alana katkıda bulunması, söz konusu kavramların devlet davranışları ve algısı üzerine etkisinin uluslararası ilişkiler teorilerinden Kopenhag Okulu bakış açısıyla ele alınacak olması bağlamında kendine has nitelikler barındırmaktadır. Dünyada yeni sayılabilecek bir güvenlik tehdidi olan siber tehditlere karşı uluslararası kurum/kuruluşlar ile ülkelerin ulusal güvenliğine olan etkilerinin örneklerle incelenmesi, günümüze kadar bu tehdide karşı alınan ve gelecekte alınması gereken tedbirlerin ortaya konulması açısında da farklı bir katkı sunmaktadır. Netice olarak siber güvenliğe yönelik bir model önerisi sunması, siber güvenliğe yönelik farkındalığın artırılmasına katkı sağlaması, siber tehditlerin siber harekât ortamındaki etkilerinin ve sonuçlarının ortaya konması açısından önemli ve özgün olduğu değerlendirilmektedir.

Tez çalışmasının kapsamı, konu bağlamında yeni güvenlik anlayışının tehdit türlerinden biri olan siber güvenlik ve siber tehditler olarak sınırlandırılmış, zaman bağlamında ise, özellikle Soğuk Savaş ve 11 Eylül 2001 sonrası dönemden günümüze kadar gerçekleşen olaylar ve gelişmeler incelenmeye çalışılmıştır. Çalışmamız tarih

aralığı olarak 1990 ile 2020 yılları arasındaki dönemi kapsamaktadır. Bu tarih aralığının seçilmesinin esas olarak iki nedeni bulunmaktadır. Birinci neden, güvenlik politikası ve yapılanması olan Soğuk Savaş düzeninin sona ermiş olmasıdır. Soğuk Savaş'ın son bulması ile gerek uluslararası sistem açısından gerekse de devlet düzeyinde yeni güvenlik politikalarına ve yapılanmalarına geçiş süreci başlamıştır. İkinci neden ise, 1990'lardan itibaren küreselleşmenin temel boyutlarının devletlerin güvenlik algıları üzerindeki etkisinin görünür hale gelmesidir.

Siber güvenlik olgusunun çalışma kapsamında ele alınış biçimine ilişkin olarak ise, siber güvenliğin çoğunlukla bilgisayar odaklı enformasyon teknolojilerine ve uygulamalarına vurgu yapan "teknik boyutu" ile uluslararası ve ulusal güvenlik kaygıları üzerinden siyasal ve hukuksal uygulamalara vurgu yapan "sosyal boyutu" arasında ciddi bir ayrım bulunmaktadır.

Bir ülkenin ulusal güvenliğini bütüncül bir şekilde sağlamakla sorumlu olan üst düzey güvenlik karar alıcılarının; nasıl ki terörle mücadele kapsamında başvurulabilecek asimetrik çatışma ya da örtülü operasyon biçimleri konusunda uzmanlık seviyesinde teknik derinliğe sahip olmaları beklenilemez ise, bilgisayar ve enformasyon teknolojileri alanında da benzeri bir uzmanlık beklentisi içerisinde bulunulmaması gerekmektedir.

Siber güvenliğin teknik boyutunun çok daha derin ve karmaşık olmasının yanı sıra söz konusu boyut çoğu zaman akademik kuruluşların ve özel sektörde faaliyet gösteren firmalarının alanları ile de kesişmektedir. Dolayısıyla gerek tümüyle teknik mahiyette olması ve gözlem yapma yoluyla tam olarak kavranamayacak bir karakter taşıması, gerekse de kamu ve özel sektörün karma bir faaliyet alanı oluşturması nedeniyle; siber güvenliğin "teknik boyutu" bu çalışmada çok sınırlı tutulmuştur. Ancak siber konusunun belki de güvenlik anlayışı içerisinde en önemli konularından birini teşkil eden hukuki mevzuat kısmı çalışmaya detaylı bir şekilde dâhil edilmiştir.

Diğer yandan açık kaynaklarda konuya ilişkin çok farklı iddialar, vakalar ve olaylar yer almasına karşın siber konusunun içerisinde barındırdığı belirsizlik ve spekülasyona açık olması nedeniyle çalışmada sadece öne çıkmış, özellikle uluslararası arenada ciddi gündem olmuş, bilinen ve nispeten kabul edilen olaylar üzerine durulmuş, kısmen gündeme az oturan ve belli seviyeyi geçemeyen olaylar ve iddialar kapsam dışında tutulmuştur.

Çalışmamız, bir durum ve olgu tespiti niteliğinde olup, küreselleşme ve özellikle 11 Eylül 2001 saldırıları sonrasında, yeni güvenlik anlayışına yönelik tehditler bağlamında ortaya çıkmış ve giderek önem kazanmış olan "siber güvenlik" kavramının genel bir resmini ortaya koymaya çalışmaktadır. Çalışmamızda, araştırma modeli olarak "ilişkisel" araştırma modeli kullanılmış, küreselleşme ve güvenlik algısı değişiminin ilişkisi siber güvenlik örneği üzerinden açıklanmaya çalışılmıştır.

Herhangi bir tez çalışması için veri toplamada en önemli süreç, ''Ayrıntılı Planlama'' yapabilmektir. Bilimsel değer taşıyacak bir eserde, veri toplanması için planlı ve programlı bir süreç gerekmektedir. Toplanan tüm veriler, bir plan çerçevesinde içeriklerine göre sınıflandırılarak; tez çalışmasının amacı doğrultusunda hareket edilmiştir. Bu kapsamda analiz edilen verilere bağlı kalınarak başlıklar, alt başlıklar oluşturulmuştur.

Çalışmamızda olgusal veriler, yazılı ve elektronik kaynaklardan yararlanabilmek maksadıyla literatür taraması yapılarak elde edilmiştir. Öncelikle yayınlanmış ulusal ve uluslararası kitap ve makalelerde literatür taraması yapılmış, çeşitli kurum ve devletlerin yaşadığı tecrübeler dikkate alınarak, gelişmiş ülkelerin yazmış olduğu ulusal siber güvenlik ile ilgili politika ve strateji belgeleri ile daha önce hazırlanmış tezler incelenmiştir.

BİRİNCİ BÖLÜM

KAVRAMSAL VE KURAMSAL ÇERÇEVE

1. KAVRAMSAL ÇERÇEVE

1.1. Küreselleşme Kavramı

Küreselleşme (*Globalization)* Anglosakson geçmişli bir kelime olup İngilizcede ise "arz küresi, dünya" anlamına gelen "*globe*" kelimesinden türetilmiştir ve en basit ifade ile "dünya çapında olmak ya da dönüşmek" manasına gelmektedir (Özpınar, 2003:7). Türkçede "*globalization*" veya "*globalizm*" kelimesinin karşılığı olarak kullanılan küreselleşme kavramı üzerinde herkesin mutabık kaldığı, görüş birliği sağlanmış net bir tanım bulunmamakta ve farklı disiplinler çerçevesinde konu hakkında birçok tanımlama yapılmaktadır (Olgun, 2006:143). Küreselleşme çok boyutlu, karmaşık ve farklı disiplinleri ilgilendiren birçok konuyu etkilediği için sade, tek ve tüm çevrelerce kabul gördüğü bir tanımlamayı yapmak oldukça güçtür (Solmaz, 2014: 91).

Küreselleşmenin siyasi alanda dolaşıma girmesi, 1980'li yıllarla birlikte Thatcher ve Reagan tarafından temsil edilen yeni muhafazakâr anlayışın iktidar dönemlerine rastlamıştır. 1990'lı yıllara gelindiğinde ise artık küreselleşme söylemi her yanı kaplamıştır (Aktel, 2003: 6). Kavramın tanımlanmasında üzerinde uzlaşılmış bir görüş yoktur. Kavram küreselleşme taraflarınca (aşırı küreselleşmeciler) olumlu, karşıtlarınca (şüpheciler) olumsuz değerlendirilmektedir.

Küreselleşme taraftarlarına göre, küresel piyasa önceki dönemlere göre çok daha gelişkin durumda ve ulusal sınırları yıkıp geçmekte, uluslar egemenliklerini, siyasetçiler de olayları etkileme yetenekleri kaybetmektedir. Küreselleşme karşıtlarına göre ise, küreselleşme refah devletini yok edecek minimal devleti amaçlayan çevrelerin kullandığı bir devrimdir (Aktel, 2003: 12-15).

Küreselleşme, 1980'lerden başlayarak, yoğunlukla da 80'lerin sonlarından itibaren totaliter yönetimlerin ortadan kalkmasını müteakip büyülü bir kavram olarak

akademisyenlerin, basın yayın kuruluşlarının, ekonomistlerin, askerlerin ve politikacıların diline pelesenk olmuş bir kelime haline gelmiştir (Kartal, 2007: 253).

Her alanda yoğun olarak kullanılmasına karşın küreselleşme kavramının ciddi bir geçmişi bulunmamaktadır. Dünya genelinde yapılan bir taramada 1979 senesine kadar bu kavrama ilişkin referans neredeyse yokken, 2001 senesinde gösterilen atıflar 57 binin üstüne çıkmıştır. Bir tanım olarak küreselleşme, artan akışkanlıkları ve insanların, nesnelerin, mekânların, bilginin büyüyen çok yönlü akıntıları ile bunların karşılaştığı ve yarattığı yapıları içeren gezegen çapındaki bir süreç ya da bir dizi süreçtir…" şeklinde ifade edilmiştir (Ekinci, 2019:3).

En yaygın ifadesiyle küreselleşme, ürünlerin, hizmetlerin, üretim unsurlarının, teknolojinin ve sermaye kaynaklarının, bölgeler, ülkeler arasında kısıtsız bir şekilde rahatça dolaşabildiği, tüm bu kavramların her geçen gün daha da bütünleştiği bir süreci tanımlamaktadır (Aktaş, 2007: 10).

Özünde küreselleşme finans unsurlarının rahatça dolaşımı ve ticaretin önündeki zorlukların ortadan kaldırılmasını belirtmektedir. Bilgi ve iletişim konuları başta olmak üzere teknoloji alanında yaşanan gelişmeler, küreselleşmenin önündeki engellerin kaldırılarak, tüm dünyaya yerleşmesinin en önemli sebebi haline gelmiştir (Danışoğlu, 2004: 38).

Son dönemlerde literatürde birçok disiplin tarafından geniş bir spekturumda ele alının küreselleşmeye herkes tarafından değişik manalar yüklenmekte ve bu yolla kavram ekonomik, siyasi ve sosyo-kültürel birçok problemin nedeni, neticesi ve/veya son çözümü olarak değişik anlayışlarla kendini göstermektedir (Demir, 2001: 74).

İktisat yönünün ön planda olduğu tanımlarda küreselleşme, iktisadi tüm konuların dünya genelinde iç içe geçmesi ve birbiri ile irtibatlanması şeklinde açıklanmaktadır. Bu anlayış çerçevesinde kavram tüm unsurların birbiri ile bağımlı olarak bir bütünün parçasını oluşturduğu iktisadi ve politik bir yapı olarak değerlendirilmektedir. Küreselleşmeyi emperyalizmin bir parçası olarak ele alan araştırmacılar, kavramı iktisadi ve siyasi tarafları olan derin bir mazinin, tarihsel geçmişin neticesi olarak ele almaktadır (Solmaz, 2014: 92).

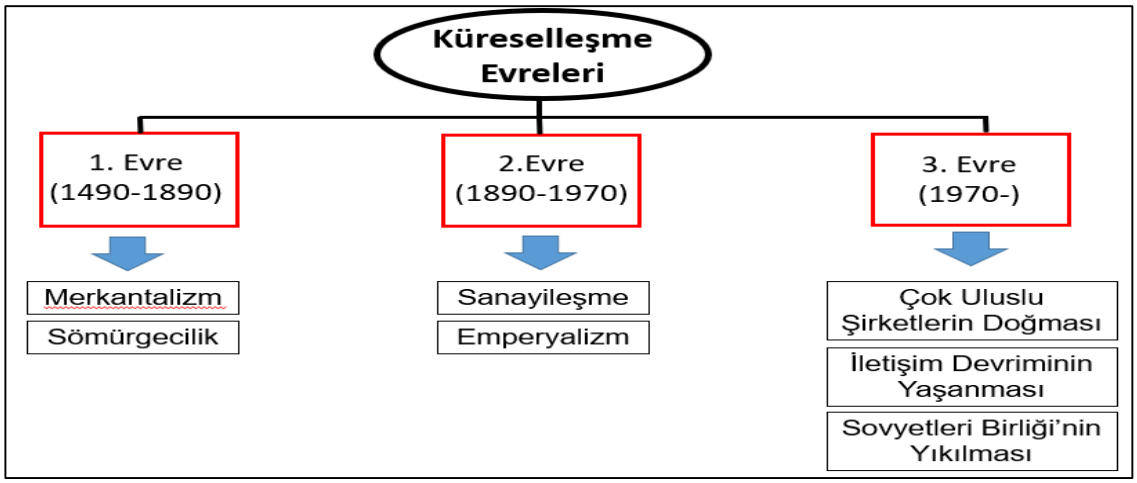
Uluslararası Para Fonu (IMF) tarafından "teknolojinin hızlı ve geniş bir alana yayılması, uluslararası sermaye, mal ve hizmetlerin sınır ötesi ticaretinin çeşit ve hacminin artmasından kaynaklanan ve ülkelerin dünya çapında artan ekonomik bağımlılığı" olarak açıklanmaktadır (Özerkmen, 2004: 135).

Yakın dönemde sosyal bilimciler tarafından yoğun olarak ele alınan küreselleşme, ulus kimlik anlayışının, hudut ve ekonomilerin ortadan kalktığı ve bu konuların büyük oyun kurucular tarafından yeniden tespit edilmesi olarak tanımlanmaktadır (Kısacık, 2019: 5).

Kavram özünde ekonomik bir süreçtir ve bu sürecin önündeki tüm sınırların, zorlukların ortadan kaldırılmasıdır. Sovyetler Birliğinin yıkılması ve Almanya'daki meşhur Berlin Duvarı'nın ortadan kaldırılması gibi tarihsel sembolik önemi bulunan olaylar neticesinde gittikçe kuvvetlenen ve dünyaya hâkim bir görüş olarak gücü katlanmıştır. Bu hâkim görüşün felsefesinde rekabet ortamının sağlanması, eldeki imkânlardan en iyi şekilde istifade edilmesi ve dünyanın refah seviyesinin yükseltilmesi bulunmaktadır (Danışoğlu, 2007: 217).

1.1.1. Küreselleşmenin Tarihsel Arka Planı

Bu kavramın geçmişini çok eskilere dayandırarak, insanoğlunun dünyaya yayılmasına kadar götüren teoriler olmakla birlikte, beş yüzyıl evvelinde kapitalist dünya düzeninin meydana gelmesiyle kendini gösteren kompleks süreçler serisinin bir devamı olarak görenler veya küreselleşmeyi son kırk-elli seneyle kısıtlayan düşünceler de bulunmaktadır (Steger, 2013:38-9; Waters, 2001:6-7). Yapılan çalışmada tarih öncesi ve modern öncesi dönem dikkate alınmayarak (Güleş, 2014:20) küreselleşme son beş yüzyıllık süreç kapsamında ele alınmış ve bugün üçüncü dönemini yaşayan küreselleşmenin evreleri Şekil 1'de sunulmuştur.



Şekil 1. Küreselleşme Evreleri

Kaynak: (Sarahan, 2018: 6)

Birinci küreselleşme 1490 senesinde merkantilizmin tesiriyle kendini göstermiş ve sömürgecilikle neticelenmiştir. İkinci küreselleşme 1890 senesinde sanayileşme, onun sebep olduğu ihtiyaçlar neticesinde belirmiş ve sömürgecilik evrim geçirerek emperyalizme geçiş yaşanmıştır. Son olarak üçüncü küreselleşme 1970 senesinde çok uluslu firmaların kurulması, 1980'li yıllarda teknoloji ile beraber iletişim çağına geçilmesi ve 1990 senesinde Sovyetler Birliği'nin dağılması ile ABD'nin tek küresel güç olarak kalması sonucunu göstermiştir.

- **1. Evre:** 6 safhada ele alınmakta olup safhalar Şekil 2'de sunulmuştur. Liberalizm ve milliyetçiliğin kuvvetli akımlar olmasına rağmen, Amerika ve Avrupa hariç çok geniş bir tesir oluşturamamıştır. Endüstri inkılabında bu iki akım bir araya gelerek Avrupa coğrafyasını ciddi seviyede değiştirmiştir. Devrimin getirisi olarak sömürgecilik vasıtasıyla dünyaya genişlemiştir (Sarahan, 2018:7).

Şekil 2. Küreselleşme Evresi

Kaynak: Sarahan, 2018:7

- 2. Evre: Küreselleşmede, denizler ve denizcilik ehemmiyetli bir konuma gelmiş, burada sağlanan üstünlük sayesinde kara medeniyetleri güçlerini yitirmiştir. Coğrafi keşiflerle Avrupa'nın elde ettiği kolay başarılar efsane haline gelerek, 20. yüzyıla kadar karşısında durulamayan bir Avrupa hissi oluşturmuştur. Bu şekilde küreselleşme periyodunda savaşçı Avrupa düşüncesi uluslararası sistemin ana karakterini meydana getirmiştir (Sander, 2016:143).

Bu safhada sanayileşme itici kuvvet şeklinde ifade edilmiştir. Sanayi devrimi, uluslararası, geniş ve emniyetli pazarların bulunmasını bir ihtiyaç haline getirmiştir. Sömürgeciliğin evirildiği emperyalizm, bu vaziyetin bir neticesi olarak değerlendirilmiştir.

- 3. Evre: Sanayi inkılabı ile birlikte iletişim teknolojileri alanında meydana gelen devrim niteliğindeki ilerlemeler küreselleşmede anahtar görev almıştır. Bazı araştırmacılar 18. yüzyıldan 19. yüzyılın ortasına kadar olan sanayi alanındaki ilerlemeyi "teknolojik devrim" olarak ele almaktadır (Sander, 2016:209).

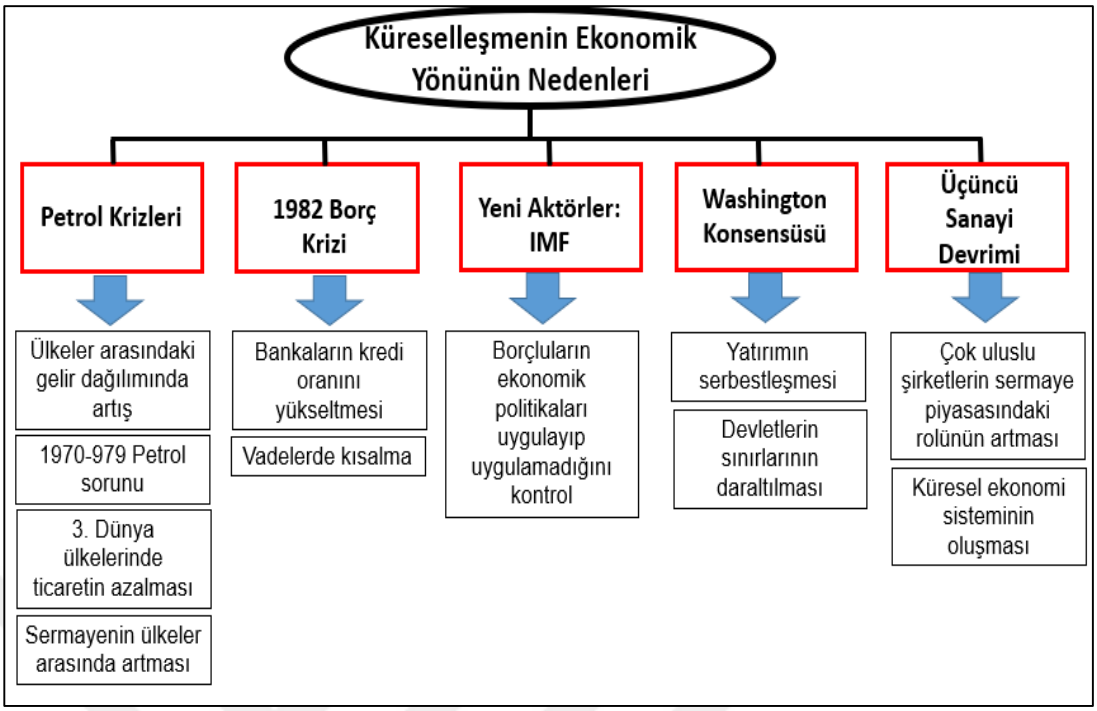
Sanayi inkılabıyla, sermaye birikimi ve üretim artmış, bu çerçevede sosyal ve politik hayatta dönüşümler görülmüştür. Yaşanan bu dönüşüm çerçevesinde çok uluslu şirketler kendini göstermiş ve Sovyetler Birliği'nin yıkılması gibi ciddi olaylar yaşanmıştır.

1.1.2. Küreselleşmenin Etkilediği Başlıca Alanlar

1.1.2.1. Ekonomik Alana Etkisi

Teknolojideki devrim niteliğindeki değişimler çerçevesinde serbest piyasa sistemindeki ivmelenme sonucunda, ürün, hizmet ve finans hareketlerinde evrim yaşanmıştır. Küreselleşmenin ekonomi alanına yansıttığı unsurlar genel olarak; (1) sermayenin dolaşım hızı, (2) sosyolojik durumun gelişmiş devletleri olumsuz etkileyecek şekilde değişmesiyle meydana gelen emek gücünün seyyaliyeti ve üretimdeki etkisi, (3) ihracatın artması ve birbirine irtibatlı hale gelmesi biçiminde kategorize edilebilmektedir. 21.yy.'da birbirine bağımlılık temeline oturtulan serbest ticaret anlayışı, devletleri karşılıklı çıkarları çerçevesinde karar olmaya sevk etmektedir. Ülkelerin her geçen gün birbirine daha da irtibatlı duruma gelmesi, global olarak ihracatın yükselmesine neden olmaktadır (Ekinci vd., 2002: 1015).

Küreselleşmenin referans noktasını oluşturan ekonomi diğer yandan bu kavramın itici kuvvetini de oluşturmaktadır. Küreselleşmenin ekonomik yönünün nedenleri Şekil 3'de sunulmuştur.



Şekil 3. Küreselleşmenin Ekonomik Yönünün Nedenleri

Kaynak: (Gögen, 2013:117-134)

1.1.2.2. Siyasi Alana Etkisi

Küreselleşme, uluslararası ilişkilerin artması, fikirsel, ideolojik farklılıklarla kutupların kaldırılması sonucunu meydana getiren bir süreçtir (Erbay, 1997:26).

Ülkelerin günümüzdeki sosyal yapılarının ana siyasal yönetim şekli olarak ele alınan ulus-devlet anlayışı genel olarak, müşterek bir kimlik anlayışı ile topluma yönelik ortak çıkar ve mefkûre birliği içerisinde birbirine kenetlenmiş bireylerden oluşan ulus ötesi bir siyasal hareket olarak ifade edilmektedir. Küreselleşme ile beraber ulus devlet kavramı etkisini yitirmeye başlamış ve gücünü uluslararası kuruluşlara kaptırmaya başlamıştır. Bu manada küreselleşmenin siyasal etkisi, hudutların bir devlete ülkesinde kayıtsız egemenlik tesis etme kuvvetinin azaltılması, karşılıklı etkileşimin ön plana çıkması, ırk, dil, etnik kimlik gibi semboller üzerine oturtulan ulus devletin fonksiyonlarının farklılaşarak, uluslararası kurum/kuruluşların daha etkin olması şeklinde de ifade edilmektedir (Çelik, 2012: 69). Siyasal etkide bölgesel seviyede çok taraflı organizasyonların ve antlaşmaların sayısının fazlalaştığı görülmektedir (Çalışır, 2009: 21).

Küreselleşmenin siyasal tesirleri ile beraber devlet, halk ve kişilerin arasındaki münasebetlerin tekrar tarif edilmesi gereksinimi kendini gösterirken, ulus-devletin gücü sarsılmış, devletin etkin ve çerçevesi belli bir yapıya ulaştırılması zarureti ciddi biçimde gündeme gelmeye başlanmıştır (Aktel, 2001: 199).

Bu kapsamda küreselleşmeyi destekleyen çalışmalarda hâlihazırda etkin olan ulus-devlet kavramının tesirinin azaldığı, değişime uğradığı ve küresel bir yönetim anlayışının kendini gösterdiği savunulmaktadır. Ulus-devlet kavramını yerinden edecek küresel anlayış yenidünya düzeni olarak da ifade edilmekte olup, ulus-devletlerin kuvvetlerini azaltmaktadır (Özyurt, 2005:67).

Bunun yanında, ekonomik amaçlarla kendini gösteren bölgesel bütünleşme girişimleri zamanla, ortak yönetişim organları olan gevşek siyasi federasyonlar biçimine evirilmiştir. Örneğin, başlangıçta kömür ve çeliğe ilişkin konularla temeli atılan Avrupa Birliği (AB) zaman içerisinde bambaşka bir konuma yükselmiştir (Çalışır, 2009: 22).

Netice olarak, küreselleşmenin siyasi boyuttaki tesirleri ulus devlet anlayışının ele alınması ve değişimi kapsamında kendini göstermektedir. Küreselleşme ile birlikte daha önce ifade edildiği gibi ürün, finans piyasası ve emek üzerindeki serbestîyesin artması ve olumsuz faktörlerin ortadan kaldırılması ulus devletin kontrol gücünü azaltmıştır. Ciddi sermaye kuvvetine sahip uluslararası şirketlerin etkileri de ulus devlet kavramını yıpratan diğer bir faktörü oluşturmaktadır (Elçin, 2012: 14).

Küreselleşmenin siyasal etkisiyle ilişkili olarak devletlerin egemenlik kuralının ötesinde uluslararası kurum/kuruluşların ve büyük ekonomik güce sahip çok uluslu şirketlerin yükselen gücü, bölgesel ve küresel yönetişimin geleceği ile alakalı ciddi siyasi sorunların sebebini oluşturmuştur (Steger, 2006:83). Bu sorunların üstesinden gelmede ulus devlet anlayışının yeterli gelmediği ve gücünün sarsıldığı gündeme getirilmektedir.

Ayrıca, yaşanan değişimle beraber kendini gösteren terörizm, insan hakları, çevre, düzensiz göç gibi yeni risk ve tehditlerin oluşturduğu sorunların üstesinden gelmek için daha yoğun bir işbirliği yapılmaktadır. Bu manada BM, NATO, DTÖ ve IMF gibi kurum/kuruluş/örgütler ehemmiyetli rol oynamakta ve bu durum ulus devlet anlayışını etkilemektedir (King ve Kendall, 2004:146-147).

1.1.2.3. Kültürel Alana Etkisi

Literatürde sıklıkla kullanıldığı gibi dünya hızla "küresel bir köy" durumuna gelmektedir. Bahse konu değişim sosyal münasebetlerin dönüşümü ve evirilmesinde kilit görev almaktadır. Klasik toplum (aile, komşuluk vb.) anlayışının yanında, uzaklıklara karşın iletişimde güçlük yaşamayan farklı, yeni bir yapı kendini göstermektedir. Bilgi iletişim teknolojilerindeki ilerlemeler dünya çapında bir kültür anlayışının meydana gelmesinde etkin bir rol almaktadır (Turan, 2014:12).

Baş döndürücü bir dönüşümün yaşandığı dünyada, toplumsal yaşamın her konusunda değer anlayışı ve alışkanlıklar değişiklik göstermektedir. Bu süratte bir dönüşümle giyim konusundan örf adetlere, tercihlerden zevklere kadar toplumsal yaşamda pek çok konu birbirinin aynı olmaya başlamıştır (Taner, 2004: 21).

Küreselleşmenin kültür alanındaki tesiriyle yerel kültürler sosyal medya ve internet gibi iletişim araçlarının da doğal bir sonucu olarak küresel anlayışın etki alanlarına teslim olmuştur. Bazı noktalarda ise bu tesir yerel ve küresel değerlerin birbirleri ile mücadelesine de sahne olmuştur (Çelik, 2012: 69). Bu mücadele ve etkileşim sonucu olarak melez kültürler kendini göstermeye başlamıştır. Küresel kültür etkileşimi kimi zaman yerel anlayışın tekrar şekillendiği bir dönem olarak ele alınmaktadır (Uluç, 2002:90).

Küreselleşmenin kültür alanındaki tesirleri ve sonuçları, bu durumun tesirine giren mahallî kültür anlayışının kendine özel şartlarına bağlı olarak değişiklik arz etmekte ve bu zaviyeden ele alındığında ya yerel kültürü tamamıyla görmezden gelinip küresel kültüre teslim olma veya yerel kültüre sarılıp dışarısıyla münasebeti kesme biçiminde seçenekler ortaya koymaktadır. Bu iki tercihin ötesinde üçüncü bir seçenek ise iki kültür arasındaki balansı tesis ederek kişilerin kendi değer yargılarını kaybetmeden, küresel değerlere de adaptasyonunun sağlanmasıdır (Özer, 2006:240). Netice olarak, küreselleşmenin kültürel alanda kendini gösteren etkileri genel olarak (Özyurt, 2002: 112-113):

- Tüketim toplumu anlayışı ve kitle psikolojisinin öne çıkması,

- Etkileşim ile melez kültürlerin kendini göstermesi

- Yaşam biçimlerinin giderek standartlaşması,

- Global problemlerden bilgi sahibi olunması,

- Milli kültür ve kimlik anlayışının etkisini azalması olarak ifade edilmektedir.

1.1.2.4. Bilgi ve İletişim Teknolojileri Üzerine Etkisi

Küreselleşme ile belki de bu kavramın ivme kazanmasındaki başat aktör olan bilgi ve iletişim teknolojilerindeki gelişmeleri ayrı ele almak mümkün değildir. Küreselleşme bu teknolojik ilerlemelerin hem sonucu hem de nedeni olarak ele alınmaktadır. İletişim teknolojilerindeki baş döndüren ivme zaman ve mekân kavramlarının ortadan kalkmasına ve dünyanın birbirine daha da yakınlaşmasına neden olsa da, bu ivme bireyleri kültürel, politik, sosyal ve iktisadi bakımdan arzulanan suni bir sanallığa itmektedir (Çaşin, Özgöker ve Çolak, 2007:63).

Teknolojinin sağladığı olanaklarla beraber bireyler, mevcut münasebetlerini sorgulayabilmektedir. Teknolojik kabiliyetler, bireylerin şahsi seçimlerine göre mal üretimine imkân tanımaktadır. Tek düze ve toplumsal üretimden öte değişik üretimler firmaların ajandasında yerini almakta ve esnek üretime geçiş yapılmaktadır. Bu durumun sonucunda eski teknolojiler, kişilerin farklı tercihlerini temin etmekte zorluk yaşarken, modern teknolojiler ile bu durum kolaylaşmıştır (Dursun, 1998:67).

Post-Fordizm şeklinde de ifade edilen üretimin küreselleşmesi durumunda dönüm noktası olan yeni üretim şekilleriyle birlikte küçülen pazarlara ve artan rekabete uyum sağlanmış, farklı özellikli taleplere karşılık verilebilmiş, üretim mantığında, tüketici isteklerinde kurumsal düzende ciddi dönüşümler kendini göstermiştir (Eser, 1995:5).

İnsan münasebetlerinin standartları derinden etkileyen, yerel, ulusal, bölgesel ve uluslararası toplum arasındaki münasebetleri temin eden kavramın teknolojik gelişmeler olduğu anlaşılmakta olup, bu durumun neticesinde ulus devletin küresel münasebetlere hâkim olduğu endüstrileşme süreci gelişmektedir. Bu duruma ek olarak uluslararası politika döneminden ulus devletin küresel münasebetleri uluslararası kurum/kuruluşlar, firmalar ve toplumsal oluşumlarla paylaşmak mecburiyetinde bulunduğu sanayi-üstü veya uluslararası politika-ötesi bir zamana geçilmektedir (Newman, 2001:82).

1.1.3. Küreselleşmeye İlişkin Düşünsel Yaklaşımlar

Held, McGrew, Goldbatt ve Perraton tahmin edilemeyen ve karışık bir kavram olduğunu vurgulayarak küreselleşemeye ilişkin üç farklı eğilimi ele almaktadır. Bunlar: aşırı küreselleşme yaklaşımı (radikaller), küreselleşme karşıtları (kuşkucular) ve dönüşümcülerdir. Küreselleşme üzerinde uzlaşmaya varılan bir kavram olmaması, konuyu inceleyen kişinin küreselleşmeyi kendi bakış açısı ile ele alması bu tarz farklılıklara sebep olmaktadır (Yalçınkaya, Çılbant ve Yalçınkaya, 2012:5).

1.1.3.1. Aşırı Küreselleşme Yaklaşımı (Radikaller)

Bu yaklaşımda küreselleşme, modernleşmeyi, ilerlemeyi belirtmekte ve bunun yanında önü alınmaması gereken bir süreci ifade etmektedir. Radikaller bu kavramın ticareti ve sermayeyi tüm dünyaya genişleteceği, devletlerin süratli genişlemesi için ciddi imkânlar vereceği ve küresel refahı tesis edeceğini iddia etmektedir (Memiş, 2014: 146). Netice itibari ile bu akımın ana felsefesini küreselleşmeyle beraber dünya refahının yükselmesi ve ülkeler arasındaki uçurumların asgari seviyeye indirilmesi oluşturmaktadır (Hayaloğlu, Kalaycı ve Artan, 2015: 120).

Radikaller devletlerin piyasa ekonomisiyle baş edemeyeceğini ve piyasanın devletlerden çok daha fazla kuvvetli olduğunu iddia etmekte, ulus devlet anlayışı yerine küresel vatandaşlık anlayışının ön plana çıktığını ve refaha ulaşan rotanın küreselleşmeden geçtiğini ileri sürmektedir. Radikaller, piyasanın devlete nazaran gücünü ele alan neo-liberaller ve küreselleşmeyi kontrolcü kapitalizmin farklı çehresi şeklinde ele alan neo-marksistlerden meydana gelmektedir (Hablemitoğlu, 2004: 20).

Radikaller ulus-devlet anlayışının sanayi devriminin bir sonucu olduğunu ve küreselleşme ile bu anlayışın ehemmiyetini yitirdiğini belirtmektedir. Diğer bir ifade ile radikaller açısından küreselleşme ulus-devlet anlayışın bitişidir (Gönen, 2013: 120). Bu anlayışa göre küreselleşme ile ekonomi farklı bir seviyeye yükselmekte ve bu kapsamda ekonominin elde ettiği bir kuvvet gün geçtikçe ulus-devlet anlayışının etkisinden uzaklaşmaktadır (Özel, 2011: 93).

Radikaller ele alınırken üstünde durulması önem arz eden konu bu anlayışın yoğun olarak idealleri ve arzu edilen durumu ifade etmesidir. Mesela; ulus devlet

kavramının ortadan kalkacağı ve yalnız bir küresel uygarlığının olacağı gibi hususlar hâlihazırda sadece bir varsayımdır.

1.1.3.2. Küreselleşme Karşıtları (Kuşkucular)

Küreselleşme karşıtları meydana gelen olaylara şüpheyle bakmakta, refah ülkesini yok edecek küçük devleti hedefleyen anlayışın sıklıkla yararlandığı bir kavram şeklinde küreselleşmeyi tanımlamaktadır (Bozkurt, 2000: 21).

Küreselleşme karşıtları, süreci kapitalizm anlayışı ile ele almaktadırlar. Bu düşünce tarzında küreselleşmenin, asgari beş yüz sene önce keşif maksatlı olarak yapılan seyahatlerle görüldüğü ve akabinde ortaya çıkan sömürgeci kuvvetin yardımıyla geçmişten günümüze kadar uzanan kapitalizmi esas alan, kapitalizmin ilerlemesi, genişlemesini hedefleyen bir sistem tesis ettiğini iddia etmektedir (Koray, 2015:3).

Küreselleşme karşıtlarına göre bu kavram ABD odaklı olarak önümüze sunulan, yenidünya düzeninin bir unsuru ve kamuflajı olan, küresel sermayenin hâkim firmalar sistemini sağlamak için istediği sistemi dayatması olarak ifade edilmektedir. Bu kavram başta gelişmekte olan ülkelere zorla kabul ettirilmeye çalışılan bir iktisadi işgaldir (Erdoğan, 2004:26). Küreselleşme karşıtlarının en çok ehemmiyet verdikleri konuların başında, ticaretin çoğunlukla OECD ülkeleri hâkimiyetinde olduğunu ve diğer ülkelerin bu ekonomik düzende bulunmadıklarını iddia ederek bu kavram yerine "uluslararasılaşma" ifadesini tercih etmeleri gelmektedir (Zengingönün, 2004:17).

Küreselleşme karşıtları küreselleşmeye kavramına olumsuz yaklaşarak, iletişim teknolojilerinin de tesiriyle küresel adaletsizliğin ciddi bir şekilde yükselmesine neden olduğunu ileri sürmektedir (Hugh, 2000:56).

1.1.3.3. Dönüşümcüler

Çağdaş toplumları ve küresel sistemi tekrar biçimlendiren kültürel, iktisadi, siyasi ve teknolojik alandaki süratli değişimlerin temelindeki ana faktör olarak küreselleşmeyi gören dönüşümcüler, günümüz şartlarının geçmişe göre ciddi değişiklikler barındırmasına vurgu yapmaları sebebiyle bu adı almıştır (Karaca, 2007:6).

Bu anlayışın görüşleri, ulus-devlet kavramının ortadan kalkması veya küreselleşme karşıtlarında olduğu gibi küreselleşmenin bütünüyle görmezden gelinmesi değil, küresel aydınlanma fikri ile çağdaşlaşmanın sebep olduğu konuların yansımasıdır. Yukarıda izah edilen iki görüşün arasında bulunan, küreselleşmeye bakışları küreselleşme karşıtlarından öte aşırı küreselleşme taraftarlarına daha benzer olan dönüşümcüler, endüstri düzeninin ilkeleri doğrultusunda konuyu ele alarak problemi bütüncül değerlendirmede yeterli olmamalarından dolayı küreselleşme karşıtlarını ve aşırı küreselleşme taraftarlarını kritik etmektedir (Duran, 2018:21).

Bu anlayışın savunucuları ulus devletin ve milli hükümetlerin pozisyonlarını tekrar düzenlediklerini iddia etmektedir. Bu durum aşırı küreselleşme taraftarlarının ulus devletin önemini kaybettiği yönündeki görüşüne ve küreselleşme karşıtlarının da değişen bir şeyin olmadığına ilişkin görüşlerine karşı çıkmaktadır (Ekinci, 2019: 20).

1.2. Güvenlik Kavramı

Güvenlik, tarihsel gelişim süreci içerisinde her zaman karşımıza çıkarak günümüze kadar varlığını sürdürmüş ve gereksinim duyulan bir kavram olmuştur. Başlangıçta bireylerin yaşam savaşı, yırtıcı hayvanlara karşı korunma, rahat ve emniyette hissetme, risk ve tehditlerden uzaklaşma şeklinde açıklanmaktadır. Bu hali devam ettirme gayretleri ile hâlihazırda kişilerin, devletlerin refah bir şekilde, çağdaş devletler düzeyinin üzerinde, özgür, adaletli, eşit, bir risk ve tehlike duymadan hayatını devam ettirme ve çalışma arzusu benzer güvenlik yaklaşımlarının değişik düzeylerde kendini göstermiş halidir. Diğer bir ifade ile önceden güvenlik her çeşit risk ve tehlike karşısında yaşamı sürdürebilme haliyken, hâlihazırda güvenlik yine risk ve tehlike kavramlarının değişik algılanış ve düzeylerine göre tespit edilmiş emniyette olma halidir (Bedir, 2019:3).

Bireyin, halkın, çevrenin, iklimin güvenliği, ulusal güvenlik ve siber güvenlik gibi daha pek çok konuda güvenliğe ilişkin tanımlamalar yapılmaktadır. “Kimin ve neyin güvenliği”, “güvenlik nasıl tesis edilir”, “uluslararası arenada daimî güvenlik tesis edilir mi?” vb. sorular kavramın tanımının yapılmasını zorlaştırmakta ve konuya ilişkin birçok boyutu ortaya sermektedir. Devletlerarası münasebetlerde de güvenlik milli, uluslararası kurum/kuruluşlarda ve vakalarda da karşımıza çıkan bir kavramdır. Güvenlik ve amaç arasında direkt bir münasebet bulunmakta ve amaca yönelik farklı güvenlik arayışları

ortaya çıkmaktadır. Uluslararası platformda tüm öğelerin büyüklükleri ve kuvvetlerine bağlı olarak farklı güvenlik arayışı bulunmaktadır (Haser, 2018: 5).

Güvenliğe ilişkin tanımlar ele alındığında değişik açıklamalar yapılmasının iki ana sebebi bulunmaktadır. Bunlardan birincisi güvenlik, tarihi vakalara, süreçlere bağlı olarak farklılık arz etmekte ve değişik algılamalara sebep olmaktadır. İkincisi ise kavramı değerlendirme şekline (devletlerin farklılıkları, konuyu ele alan bireylerin duygu düşünce ve bakış açıları gibi) göre biçimlenmesidir. Bu noktadan hareketle güvenliğe ilişkin değerlendirmeler, görüşler ve tanımlamalar devletlerin ve oyuncuların siyasetleri, her ülkenin risk ve tehdidi ele alış şekli ve değişik kuramsal bakışlar çerçevesinde biçimlenmektedir. David Baldwin (2004)'e göre güvenliğin değişik tanımlarının yapılması iki yönden ehemmiyetli bulunmaktadır. İlk olarak farklı güvenlik politikalarını kıyaslanmasını basitleştirmek, reel politika tahliline katkı sağlamaktır. İkinci olarak da değişik fikir ve yaklaşımlara haiz olanlar içinde paydaş bir zemin tesis ederek, bilimsel irtibatı basitleştirmektedir (Baldwin, 2004:2).

Latince "*Securus*" ve İngilizce "*Security*" kelimelerinden gelen, en temel haliyle huzursuzluk ve tedirginlikten uzak bir şekilde hayatı devam ettirmek şeklinde ifade edilen güvenliği (Mesjasz, 2004:4), uluslararası ilişkiler çerçevesinde ilk kez ele alan Adam Wolfers bu kavramı muğlak bir unsur olarak kıymetlendirmiştir. Adam Wolfers'a göre güvenlik hiçbir biçimde hâlihazırdaki değerlere ilişkin bir tehdit unsurunun olmaması halidir (Wolfers, 1952:481).

Türk Dil Kurumu tarafından yayınlanan sözlükte güvenlik; "(1) Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet, (2) Devlet olarak örgütlenen bir toplumun düzen ve güvenirlik içinde bulunması durumu" şeklinde ifade edilmiştir (Türk Dil Kurumu, 2018).

Güvenlik kavramına yönelik çok farklı tanımlamalar yapılmıştır. ABD'li Barry Buzan'a göre güvenlik, tehdit ve risklerden uzak durabilmek için yapılan çaba ve gayretlerdir (Buzan, 1991:34).

Güvenlik mantığı daha ziyade güvensizlik olasılıklarının bertaraf edilmesini ortaya koymaktadır. Güvensizlik olasılıkları ise, kötü muamele, kaba kuvvetle

karşılaşma, yoksunluk ve fakirlikle yüzleşme durumudur. Güvensizlik olasılıkları tehditleri gün yüzüne çıkarır, tehditler hayata geçme ihtimaline bağlı olarak gerginlik ve korku oluşturur, her gerginlik ve korku oluşturan hal tehlikeli addedilmektedir (Dedeoğlu, 2014:29).

Güvenlik, bireylerin bir tehdit söz konusu olmadan hayatlarını sürdürme ve emniyet durumu şeklinde belirtilmektedir. Diğer yandan, "zarar veya tehlikeye karşı emniyette olma veya hissetme", "tehditlerin olmaması durumu" ya da "güvensizlik derdinin bulunmaması hali" ifadeleri de kavramın manasını vurgulamaktadır (Açıkmeşe, 2014: 241).

Uluslararası ilişkilerde güvenlik kavramının tahlili üç temel üzerinden ele alınmaktadır: Birey, Devlet ve Uluslararası Sistem. Üçlü tahlilde güvenlik anlayışı piramit mantığı içerisinde bir bağlılık arz etmektedir. Bu çerçevede uluslararası düzeyde güvenliğin tesis edilmesi otomatik olarak devletlerin ve dolayısıyla da kişilerin güvenliğine tesir edecektir (Singer, 2006: 7-16).

1.2.1. Güvenlik Kavramının Tarihsel Arka Planı

Bu kavram ifade edildiği gibi "endişeden uzak olma ve sükûnet" manasına gelmekte olup eski Romalılarca tehditten uzakta bulunmak güvenlik şeklinde yorumlanmıştır. Güvenlik, Romalılarda imparatorların muhafazasında olan yaşamların güvenliği biçiminde yorumlanan "Roma Barışı" yani "Pax Romana"yı oluşturmada anahtar rol oynamıştır (Küntay ve Elmas, 2019:196-197).

Güvenlik tarihsel perspektifte değerlendirildiğinde dini temelli mücadelelerin önemli yer tuttuğu görülmektedir. Tek tanrılı inanışlar öncesinde güvenlik kavramı; işgal etme, fethetme, ganimet öğeleri ile irtibatlı olmuş, tek tanrılı inanışlarla beraber; dini yayma merkezli cihat, haçlı seferleri gibi olaylar önem arz etmeye başlamıştır. Bir tarafta dinler arası mücadele diğer yandan Avrupa'da beliren mezhepsel savaşlar nedeniyle din kavramı uluslararası güvenliğin öğesi konumuna yükselmiştir. Din konusu hâlihazırda da güvenliğin biçimlenmesinde başat aktörlerden biri olarak karşımıza çıkmaktadır. Din kisvesi adı altında yapılan terörist eylemleri, mezhepsel mücadeleyi ve hatta dinler arası

savaşı tehdit şeklinde değerlendiren yaklaşımlar güvenliği etkilemektedir (Karabulut, 2015:43).

Güvenliğin tarihsel pozisyonu iki kademeli olarak ele alınmıştır. Romalılarca kullanılmış, tutarsızlıkları ve dini tesirleri bulunan kavram birinci basamağı meydana getirerek, Orta Çağ'ın sonlarından itibaren pozisyonunu "*certitudo*" kavramına terk etmiştir. Güvenliğin ikinci basamağı ünlü düşünce adamı Thomas Hobbes'la kendini göstermiştir. Çağdaş devletlerin amaçlarını yerine getirmeye çalışan "Süper Devletin-Leviathan" meydana gelmesi ile irtibatlandırılmıştır. Başlangıçta güvenlik kavramını açıklamak, uluslararası bir düzenin bulunmaması ve ulus devletlerin politik birer oyuncu olarak sahneye çıkmamalarından dolayı kolay olmamıştır. Bu zamanlarda sadece sınırdaş olan devletlerin etkileşimi söz konusu olmuş ve bu etkileşimin temel öğelerinden birini de güvenlik kavramı oluşturmuştur (Haser, 2018:10).

Milli güvenliğin sağlanması hususundaki analizlerde Rousseau, Machiavelli ve Hobbes gibi düşünürler kötümser bir durum ortaya koymuştur. Uluslararası arena ülkelerin, sınırdaşlarının olumsuz etkilemesi pahasına güvenliklerini tesis etmeye gayret gösterdiği katı, anarşik bir bölge olarak kıymetlendirilmiş ve ülkeler arası münasebetler devamlı olarak birbirinden yarar sağlamayı amaçlayan bir güç mücadelesi şeklinde ele alınmıştır.

Sanayi inkılabı ve 19. yüzyılda kendini gösteren yeni ham madde ve pazar bulma mücadelesi güçlü devletlerin veya güç elde etme hevesindeki devletlerin güvenliğe bakışlarını ve hudut anlayışlarını bütünüyle farklılaştırmıştır. Bu dönemde güvenlik anlayışı hudutların ötesinde güçlü devletler zaviyesinden erişilebilen her yer manasına evirilmiştir. Buradan hareketle ehemmiyetli doğal kaynakları, boğaz, kanal ve geçitleri korumak, ucuz emeği elde etmek ve bu alanları ülke toprağını savunur gibi korumak güvenlik kavramının yeni boyutunu ortaya çıkarmıştır (Dedeoğlu, 2014:25).

20. yüzyılla beraber sömürgecilik uluslararası arenada ana konuyu teşkil etmiştir. Sömürgecilik faaliyetleri devletlerarasında büyük rekabete ve bunun sonucunda da iki dünya savaşına sebep olmuştur. Yaşanan savaşlar sonrasında tüm dünya ağır bedeller ödeyerek, güvenliği direkt olarak risk altında bulunmayan ülkeler dahi yaşananlardan etkilenmiştir.

Müteakiben yaşanan Soğuk Savaş döneminde de tehdit algısı değişikliğe uğrayarak tehdide konu olan öğelerin adları, yöntemleri, seviyeleri ve süreçleri değişmiştir. Siyasal organizasyonlar, rejimler, nükleer imkânlar ve bloklaşmalar gibi farklı tehditler kendini göstermiş, bu süreçte caydırıcılığı sağlamak ön plana çıkmıştır (Gülmez ve Tahancı, 2014:226).

Sovyetler Birliğinin dağılması ve küreselleşme neticesinde uluslararası düzende çok kutuplu bir anlayışa doğru dönüşüm yaşanmış, ekonomi politikalarıyla ülke hudutları kalkmış ve ülkeler birbirleri ile devamlı etkileşim içerisine girmiştir. Öncesinde askeri gücün esas alındığı anlayış yerine iktisadi, toplumsal ve siyasi güç kendini daha fazla göstermeye başlamıştır (Aktel, 2001:194).

Değişen ve farklılaşan risk ve tehdit anlayışı çerçevesinde güvenlik de toplumları, ülkeleri ve uluslararası düzenin güvenliğini temin etmek maksadıyla genişlemiştir (Erdoğan, 2013:269).

1.2.2. Güvenlik Kavramına Düşünsel Yaklaşımlar

Uluslararası İlişkiler disiplini içinde güvenlik kavramı, üzerinde geniş teorik ve ampirik incelemeler yapılan en önemli konulardan biri olmuştur. Güvenlik konusunu ortaya çıkaran en önemli unsur tehdit algısı ve bir tehdidin varlığı olarak karşımıza çıkmaktadır. Bu bölümde güvenlik kavramına yönelik düşünsel yaklaşımlar anlatılmaya çalışılacaktır.

1.2.2.1. Realizm Yaklaşımı

Güvenlik olgusu insanlık tarihi kadar eski olmasına rağmen bu alanla ilgili yapılan akademik çalışmalar çok yenidir. Uluslararası İlişkilerin temel alanlarından biri olan güvenlikle ilgili çalışmalar İkinci Dünya Savaşı'ndan sonra ortaya konulmaya başlanmış ancak yapılan ilk çalışmalarda kavramın çerçevesi dar tutulmuş, güvenliğin askeri boyutu esas alınarak uluslararası ilişkilerin geleneksel yaklaşımlarından olan realist yaklaşıma uygun değerlendirmeler yapılmıştır.(Yılmaz, 2007:70)

1.2.2.1.1. Klasik Realizm

Uluslararası İlişkilerde etkin olarak kullanılan güvenlik kavramı, realist anlayışta meydana getirilen kuramsal araştırmalarda yoğun bir şekilde kendini göstermektedir. Bu konuda literatüründe bulunan güvenlik araştırmalarında realist yaklaşım başat bir pozisyondadır (Booth, 2012:51).

Realist yaklaşımının güvenlik kavramına ilişkin fikirsel esasları Hobbes ve Tuchidides'e kadar indirilmektedir. Fakat yoğunlukla Soğuk Savaş esnasında realist anlayışın kuramsal bir bütün şeklinde kendini göstermesiyle beraber, Uluslararası İlişkiler kapsamında devletler tarafından sürdürülen münasebetlerin güvenliğe ilişkin boyutunda geniş teorik varsayımların gündeme getirildiği anlaşılmaktadır (Frederik ve Arends, 2009:9).

Realist teori, uluslararası platformda güvenliğin ve tehditlerin ana olgusunu devlet olarak ele almaktadır (Ovalı, 2006:5). Devletleri de bireyler gibi harp eden, sinirlenen, menfaatlerine göre bir sistem isteyen, güç peşinde uğraş veren varlıklar şeklinde görmekte ve bu çerçevede uluslararası arenada tehdit altında olduklarını düşündüklerinden güvenliklerini tesis etmek ve muhasımlarını ortadan kaldırmak için faaliyetler icra ettiklerini ileri sürmektedir (Ertem, 2012:196).

Devleti ana unsur gören bir güvenlik olgusuna haiz realist kuram, uluslararası arenada faaliyetler icra eden devletlerin ilk olarak kendi hudutları içinde tehlikelerden uzak durmaları ve bunun sağlanması halinde devamlılık tesis etmek için askeri imkânlara ciddi ehemmiyet vermeleri gerektiğinin üzerinde durmaktadır (Koyuncu, 2012:119).

Realist teori esas olarak, uluslararası arenada ülkelerin anarşik bir düzende hareket ettiği, bu nedenle tek amaçlarının yaşamlarını sürdürmek olduğu ve bu durumun ise ancak askeri güç ile tesis edileceği üzerine oturtulan bir anlayıştır (Yavuz, 2009:139). Bu kapsamda teori anarşik düzendeki ortamda çatışmaları doğal olarak ele almaktadır (İşyar, 2008:33).

1.2.2.1.2. Neorealizm

Realizmle yakın özellikler arz eden bu teori kapsamında güvenliğin tesis edilememesinin sebebi uluslararası düzenin yapısı ile ilişkilendirilmektedir. Uluslararası yapı ülkelerin tavırlarına göre biçimlenen bir düzen olarak kıymetlendirilmektedir. Bu anlayışta, realizmden farklı olarak ülkelerin tavırlarının insan tabiatı ile benzerlik göstermesine değil uluslararası düzenin anarşik doğası sonucunda güvensizliğin oluştuğuna vurgu yapılmıştır (Çaman,2006:43).

Bu yaklaşımın klasik realizm ile uyum gösteren diğer bir tarafı da güvenliğin tesis edilmesinde ülkelerin güç kapasitelerini devamlı olarak yükseltmesi zaruretinin vurgulanmasıdır. Bu teoride güç güvenliğin tesis edilmesinde araç olarak ele alınmakta ve devletin varlığının devam ettirilmesi hedeflenmektedir. Bu yaklaşım uluslararası ilişkiler bağlamında realizmin belli bir olgunluğa ulaşmış şekli olarak ele alınmaktadır.

Neorealizm'in en büyük savunucusu olarak görülen Kenneth Neal Waltz'un tahlilleri dikkate alındığında realizm anlayışını kritik etmediği aksine bu yaklaşımı daha geniş bir şekilde kıymetlendirdiği görülmektedir. Kenneth Waltz'un 1960'lı yıllardaki değerlendirmeleri göz önünde bulundurulduğunda düzeni anarşik ve hiyerarşik olacak şekilde ikiye böldüğü görülmektedir (Waltz, 1979:44).

Devletlerin bireyleri kısıtlayarak güvenliği tesis etmesi, devletler açısından sonsuz bir hareket serbestisinin meydana gelmesine sebep olmaktadır. Bu kapsamda neorealist yaklaşım devlet hareketlerinin de kısıtlanabileceğini belirtmektedir. Devletin hareketlerinin kısıtlanmadığı hallerde "Güvenlik İkilemi" oluşabilmektedir. "Güvenlik İkilemi" kavramı ilk defa Hans Hermann Herz tarafından bir ülkenin güvenlik içinde olması hali başka bir ülkenin güvensizlik halinde olduğu hissine sebep olması ve bazı düşmanca tedbirler alması manasında ifade edilmiştir (Herz, 1950:157).

Teorinin ana sorunlarından biri Realist yaklaşımın savunduğu sınırsız güç artırımı ve ihtiyaç halinde gücün kısıtsız bir şekilde kullanılması olarak bilinmektedir. Bu yaklaşım yoğunluklu olarak Soğuk Savaş sürecinde sistemdeki oyuncuların askeri güç merkezli olmasına ve bu oyuncuları silahlanma rekabetine sürükleyerek güvenlik üstünde tehdit oluşturmalarına sebep olmuştur. Neorealistlerin ortaya koyduğu bu ayrım ile netice itibari ile iki senaryoda da güvenliğin tesis edilmesi uluslararası düzenin yapısıyla

ilişkilendirilmektedir. Bunun ötesinde Neorealist anlayışı esas alanların güvenlik konusuna ekonomik yönü de eklendiği görülmektedir. Kenneth Waltz güvenlik kavramının sadece askeri ve stratejik yönünün bulunmadığı, ekonomik taraflarının da bulunduğunu belirterek, kavramın geniş bir perspektifte ele alınmasını sağlamıştır (Waltz, 1993:44).

Neorealistlerin 1945-1990 seneleri arasında güvenliğe ilişkin yaptıkları araştırmalar kavramın gelişmesine fayda sağlasa da değişen ve karmaşık bir yapı arz eden risk ve tehditlerin farklı yönlerde incelenmesinde kifayetsiz kalmıştır. Düzende ne ölçüde bir gücün kâfi geleceği sorusu Neorealistleri; (1) Savunmacı (*defensive*) ve Saldırgan (*offensive*) olmak üzere ikiye ayırmıştır. Savunmacılar çoğunlukla güvenliğin, düzende yer alan oyuncuların denge halinde olmasıyla tesis edilebileceğini ifade etmektedir (Eren, 2019:11).

1.2.2.1.2.1. Savunmacı (*Defansif*) Realizm

Defansifler, yenilikçi ve değişime açık devletlerin güvenlik sorunu meydana getirebileceği anlayışıyla neorealist yaklaşımın açığını gidermeye gayret göstermiştir. Bu kapsamda anarşik sistem kaynaklı "Güvenlik İkilemi" kavramının oluşturduğu muğlaklıklara ilave olarak, "saldırı-savunma dengesi" kavramını esas almıştır. Bu kavram uluslararası düzeni ifade ederken, ülkelerin takip ettikleri askeri ve siyasi stratejilerin niçin ve ne durumda meydana geldiğini ve bunun sonucunda güvenlik ikileminin ne şartlarda kendini gösterdiğini, münasebetlerin mücadeleye mi yoksa işbirliğine mi evirileceği cevaplamaya gayret göstermektedir. Bu yönüyle defansif realistlere göre, güvenlik ikilemi kaçınılmaz olmakla beraber iş birliğine evirilme olasılığı bulunmaktadır (Açıkmeşe, 2008: 98-99).

Savunma ve saldırı dengesinde, saldırı üstün durumda ise o ülke diğerlerine nazaran avantaj tesis etmek maksadıyla saldırgan stratejiler izleyebilmektedir. Diğer bir ifade ile bir ülkenin başka bir ülkeyi işgali, silahlı gücünü yok etmesi, kendini savunmadan daha basit ise o ülke saldırmayı seçebilmektedir. Bu açıdan statükocu bir devlet dahi revizyonist bir devlete evirilebilmektedir. Dengede savunma daha üstün durumdaysa, askeri gücün imkân ve kabiliyetlerinin arttırılmasına gayret göstererek durumunu koruyacak ve saldırı ihtimalini azaltabilecektir. Bu şekilde anarşik düzenin

muğlaklığı ortadan kaldırılarak harp olasılığı azalabilmektedir. Defansta olan devlet muhtemel saldırılara yönelik hazırlıklı olmaya gayret göstermekte, bu şekilde karşı tarafın güvenliğine risk oluşturmamakta ve işbirliği olasılığı yükselmektedir (Jervis, 1978: 187-189).

Robert Jervis dengenin ana belirleyici unsurunu teknoloji olarak görmektedir. Konum, müttefiklik ilişkileri, doktrinler genel çerçevede fazla dikkate alınmamakta ve tahlil dışında bırakılmaktadır. Bu kapsamda yoğunluklu olarak askeri teknolojinin geliştirilmesi ülkeler açısından hayati önem arz etmektedir. (Jervis, 1978: 183). Diğer parametreler görmezden gelinerek yalnızca teknolojiye odaklanılması üç yönden daha akıllıcadır. Birincisi, dengeyle alakalı tüm araştırmalarda askeri teknolojiye dikkat çekilmekte ve ana unsur olarak ele alınmakta, ikincisi başka bir parametrenin kavramla bağdaşması, hâlihazır şartları daha karmaşık duruma sokarak saldırı-savunma dengesinin öngörülebilirliğini tehlikeye sokmakta ve son olarak teknolojik ilerlemelerin uluslararası düzende bir değişkenliğe haiz olması durumudur. Farklı dinler, duygu düşünceler, milliyet kavramı, iç siyaset dengeleri gibi öğeler devletten devlete farklılık arz ederken, teknoloji tüm düzeni tesir altına almaktadır (Lieber, 2000: 76-77).

Özetle dengede saldırı yönünün ağır basması durumunda güvenlik ikilemi artacak, savunma tarafı ağır basması durumunda ise iş birliği olasılığı kendini gösterecektir. Robert Jervis 1973 yılındaki İsrail-Arap harbini bu denge üzerinden tahlil etmiştir. Harp başlangıcında tank ve hava kuvvetinin saldırı üstünlüğü sağladığı değerlendirilirken, harp esnasında tanksavar ve uçaksavarlar; fiyat, kullanım rahatlığı ve imha kapasitesi açısından daha üstün konuma yükselmiş, yani savunma üstünlüğü kazanmıştır (Jervis, 1978: 198).

Savunmacı realizmde, dengede saldırı öne çıktığında savaş kendini gösterse de savunma çoğu zaman daha üstündür. Bir ülke saldırıyı ön planda tutarak, revizyonist hareket ederse kendine yönelik bir kuvvet dengesinin tesisinden çekinebilmektedir. Bu vaziyette en ideal yol dengeli bir biçimde asgari güvenliği sağlamak olacaktır (Walt, 2002: 204).

1.2.2.1.2.2. Saldırgan (*Ofansif*) Realizm

Saldırgan realizm, savunmacıda konu olan ancak dikkate alınmayan revizyonist devletlerin kurama dahil edilmesi zarureti ve neticesinde kendini göstermiştir. Teorinin öncüsü olan John J. Mearsheimer kuramı beş varsayımla kısaca ifade etmiştir (Mearsheimer, 2001: 30-31);

Birincisi, uluslararası düzen anarşiktir ancak bu düzenin kaotik veya düzensiz olduğu manasına gelmemektedir. Anarşinin esasında yönetenlerin üstünde bir gücün olmaması yatmaktadır. İkincisi, kuvvetliler normal olarak, taarruzi askeri kabiliyetler kazanmakta ve bu durum da onlara birbirlerini ortadan kaldırma imkânı sağlamaktadır. Bu durum her ülkeyi diğerine karşı muhtemel tehdit durumuna sokmaktadır. Üçüncüsü, bir ülke diğerinin kendisine ilişkin tasarrufları hakkında net emin olamamaktadır. Ancak bu durum ülkelerin açık bir biçimde düşmanca düşünceleri bulunduğu manasına gelmemektedir. Dördüncüsü, ülkeler için yaşamını sürdürmek ana gayedir. Toprak bütünlüğü ve bağımsızlığın korunması önem arz etmektedir. Ülkelerin farklı hedefleri olmakla birlikte ana hedef güvenliktir. Son olarak ise devletler rasyonel oyunculardır. Uluslararası arenanın bilincindedirler ve bu duruma uygun politikalar ortaya koymaktadırlar.

Saldırgan teoride ülkelerin güç kazanma istekleri, hegemon duruma geldiklerinde sona ermektedir. Düzende yalnızca bölgesel hegemon olmuş devletler statükocu davranabilmekte, diğer şartlarda statükocu devlete rastlanmamaktadır (Mearsheimer, 2001: 40-42).

Saldırgan anlayışta, Kenneth Waltz'ın kuramının bir kritiği şeklinde görüldüğünden, gerçekte klasik realizme bir değişiklik haricinde geri yönelme söz konusudur. Klasik realizmde devletlerin revizyonist hareket etmelerinin temelinde insan tabiatı bulunurken, saldırgan da sistemin anarşik düzeni söz konusudur. Bu kapsamda klasikler iradeci, saldırganlar yapısalcıdır (Walt, 2002: 208-209).

1.2.1.1.3. Neo Klasik Realizm

Soğuk Savaş döneminin bitmesi ile beraber neorealizm ciddi eleştiriler ile yüzleşmeye başlamıştır. Soğuk Savaşın nispi istikrarlı durumunu izah edememesi, sona

ermesini öngörememesi ve bu dönemi yeterli şekilde izah edememesi yönündeki düşünceler neorealist yaklaşıma ilişkin ana eleştirileri meydana getirmiştir. Devletlerin dışa ilişkin tavırlarını izah etmedeki kısıtlılığı nedeniyle neorealist kuramda tartışmalar yaşanmıştır (Elman, 1996:8-9). Gideon Rose 1998 senesinde kaleme aldığı makalesinde ilk kez neoklasik realizm kavramını gündeme getirerek fikrin sistematik bir hal almasını temin etmiştir (Rose, 1998:146).

Neoklasik realizm, klasik realist yaklaşımın iç dinamiklerini göz önünde bulunduran birtakım öngörülerini güncellemeye çalışırken, neorealist yaklaşımın sistem anlayışını, anarşik düzeni, nispi maddi güç gibi yapısal hususlarını da göz önünde bulundurmaktadır. Neoklasik realizm anlayışını benimseyenler, uluslararası anarşik düzende devlet üzerindeki tesirlerin mahiyetinin nispi güç dağılımının yanında, devletlerin iç dinamiklerine de bağlı olduğunu ifade etmektedir (Firoozabi ve Ashkezari, 2016:95).

Gideon Rose, neoklasik realizmin klasik realizm ve neorealizm ile olan irtibatını;

"*Neo klasik realizm bir ülkenin faaliyet alanını belirleyen ilk ve en önemli faktör o ülkenin uluslararası sistemdeki yeri ve daha da önemlisi sahip olduğu göreceli maddi güç kapasitesi tarafından belirlenir. Bundan dolayı neo-realist bir yönü vardır. Fakat, bu güç kapasitelerinin dış politika üzerindeki etkisi dolaylı (indirect) ve karmaşıktır, çünkü sistemik baskılar birim düzeyde ara değişkenler aracılığıyla dönüştürülmek zorundadır. Bu da onları neoklasik realist yapar*" ifadeleri ile açıklamıştır (Rose, 1998:146).

Bu kapsamda bu anlayış, dış politika tavırlarını diğer iki teoriye nazaran daha detaylı bir şekilde tahlil etmesine ek olarak, hem uluslararası düzenin yapısı ve iç dinamikleri hem de bunların kendi aralarındaki iç içe geçmiş etkileşimlerini ortaya koyan bir teoriyi oluşturmaktadır. Bu teoriyi diğer realist kuramlardan ayıran özellik, tahlil seviyesine bağımlı değişkenler ve bunların yanına ara değişkenleri koymasıdır. Ara değişkenler, iç siyaset, lider anlayışı, devlet organizasyonu ve gücü, politik düzen gibi birçok konuyu içermektedir (Ripsman, 2016:59).

1.2.2.2. Liberal Yaklaşımların Güvenlik Anlayışı

Gücü nispi bir kavram olarak ele alan liberal yaklaşımda "Örümcek Ağı" modeli kendini göstermektedir. Bahse konu model, iç ve dış bütün münasebetlerin örümcek ağına benzer şekilde karmaşık olarak birbiri ile irtibatlı olduğunu belirtmektedir. Liberal anlayış, oyuncu seviyesindeki sebeplerden hareketle sistem seviyesindeki neticelere odaklanmaktadır. Bütünü meydana getiren unsurlar dış politika oluşturmada değişik tesirlere haizdir (Arı, 2008:332).

Liberaller güvenliği "türetilmiş" bir kavram olarak ele alarak, tüm hususları içeren bütüncül bir tanımlamasının ortaya koyulamadığını belirtmektedir. Bireylerin ve toplulukların güvenlik yaklaşımının, onların politik tavırları ve felsefi dünya bakışlarından türediği görüşü bu durumun net bir işaretidir (Bilgin, 2010:76). Diğer taraftan güvenliğin tam olarak tanımlanamaması onun ne şekilde sağlanması gerektiği yönünde verilecek cevabı güçleştirmektedir (Booth, 2012:125).

Liberalist yaklaşımda kişilerin maddi güvenliklerinin temin edilmesi önem arz etmektedir. Realizm de tehdit merkezli olunmasına karşın liberalizmde uzlaşı prensibi öne çıkmaktadır. Bu manada liberalistlerde güvenlik, çoklu oyuncular, tehditler ve tahlil seviyeleri tarafından tesis edilen ilişkiler bütünüdür (Dedeoğlu, 2014:28).

Bu teoride devletin soyut kişinin somut olduğu öngörüsünden yola çıkarak birey merkezli toplum yaklaşımı ortaya koyulmaya gayret gösterilmiştir. Liberalistler devletin pozisyonunu en düşük düzeyde tutup devlete hakem görevi vermektedir. Kişilerin politik hayattaki ehemmiyeti fazladır. Kamuoyunda rasyonel tavırlar gösterilmesi bu yaklaşımın esasını meydana getirmektedir. Liberalizm fikir, adalet, rasyonellik, özgürlük ve mülkiyet öğelerinin üstüne oturtulmaktadır. Liberalizmde aynı kişiler gibi uluslararası düzende ülkeler hakları ve sorumlulukları açısından eşittir. Liberalistlere göre uluslararası ilişkilerin ana oyuncuları sadece devletler değil, kişiler ve sivil toplum kuruluşlarıdır (Aydın, 2014:17).

Neoliberalizmde de uluslararası düzenin tabiatı ve işbirliği hususundaki fikir ayrılıkları devam etmektedir. Bu kapsamda neoliberalist anlayış amaç ve beklentiler üzerine eğilmektedir. Neoliberalizmde rakipler içinde kimin ne kazanç elde ettiği dikkate alınmaksızın mutlak kazanç prensibi esas alınırken, ekonomi konuları kendini daha fazla

göstermektedir. Neoliberaller mücadeleleri, sistem seviyesindeki güç dağılımlarıyla tahlil etmek yerine, birim seviyesindeki oyuncularla tahlil etmektedir (Kaya, 2008:89).

Neoliberalist anlayış devletlerarası barış ve güvenliği izah etmeyi esas alan bir kuramdır Bu anlayışın kendi geleceğini belirleme prensibine atfettiği önem, sınıfların manasını yitirdiği bir durumda iç ve dış siyaset farkının ortaya koyulamayışını da ciddi şekilde etkilemiştir. 20. yüzyıldan başlayarak refah, çağdaşlaşma, çevre gibi başlıklar da en az güvenlik kavramı kadar dış siyaset davranışlarını etkilemiştir. Bu açıdan liberal anlayışına göre güvenlik konusunda işbirliğinin etkisi büyüktür ve işbirliği güvenlik endişesi oluşturduğuna inanılan birçok konunun üstesinden gelmekte ehemmiyetli bir vasıta oluşturmaktadır (Aydın, 2014:18).

1.2.1.3. Eleştirel Güvenlik Yaklaşımı

Soğuk Savaş'tan itibaren kaleme alınan güvenlik araştırmaları tahlil edildiğinde güvenliğin çerçevesinin genişlediği görülmektedir. Soğuk Savaş başlangıcında tehditler ve menfaatler kapsamında değerlendirilen güvenlik kavramı, son dönemlerinde ise yalnızca neticeler değil, sebepler de göz önünde bulundurularak güvenliğin mahiyeti genişlemiş ve "Eleştirel Güvenlik Çalışmaları- *Critical Security Studies-CSS*" kendini göstermiştir (Birdişli, 2014: 234). Özellikle barış konusunun gündeme girmesi eleştirel yaklaşımın önünün açılmasını temin etmiştir (Peoples ve Vaguan, 2010: 18). 1980'li yılların başında Robert Warburton Cox, uluslararası siyaseti çözmek maksadıyla "Problem-Çözüm Teorisi" ve "Eleştirel Teori" olmak üzere 2 kuramı ortaya atmıştır (Bilgin, 2008: 92).

Çözüm kuramı, mevcut toplumsal ve güç münasebetlerini, organize durumda olan kurum/kuruluşları olduğu gibi kabul etmektedir. Her çeşit problemle ve problemin kaynağı ile mücadele ederek problemlerin sorunsuz bir biçimde halledilmesi hedeflenir. Eleştirel teori, diğerinin aksine toplumsal ve güç münasebetlerini ve organize kurum/kuruluşları göz önünde bulundurmaz ancak bunların kökenlerini ve ne şekilde değişeceğini araştırmaktadır. Eleştirel teori münasebetleri bir bütün olarak değil ayırarak incelemektedir. Eleştirel teoride büyük resme odaklanılmaktadır (Cox, 1981: 128-130).

Robert Cox'a göre uluslararası ilişkilerin tarihsel dokusu Sovyetlerin dağılmasıyla beraber değişikliğe uğramıştır. Toplumda ve çevresel kapsamda sorunlar meydana gelmiştir. Bütün negatiflikler insan ırkının hayatını tehlikeye sokmuş ve insanoğlunun korunması ana hedef alınmıştır (Cox, 2008: 87-88).

Eleştirel kuram kapsamında güvenliğin tanımına yönelik değişik anlayışlar ileri sürülmüştür. Realizmin devlet odaklı güvenlik anlayışı kritik edilmiştir. Ken Booth'a göre, realizmin güvenlik yaklaşımı, vasıtalar ve yöntemler iç içe geçtiğinden dolayı doğru değildir. Devlet gözünde güvenliği tesis etmek hedef değil vasıtadır. Devletlerin güvenliği bağımsızlıkları ve toplumsal kimliklerle ilişkilidir (Booth, 2007: 166).

Eleştirel teoride güvenlik, klasik anlayışlara nazaran biraz daha karmaşık bir biçimde ele alınmıştır. Eleştirel teoride güvenlik kavramı dört ana öğenin üstüne oturtulmuştur. Bunlar; "güvenlikleştirme (tehdit açısından)", "derinleşme", "genişleme (güvenliğin konusunu oluşturan nesneler)" ve "özgürleşme" dir (Jones, 1999: 166).

1.2.1.4. Postmodern Güvenlik Yaklaşımı

Modernitenin farklılaştırıcı, dışlayıcı yapısına atıf yapan post modern kuram; yerli-yabancı, güçlü-zayıf, zengin-fakir, savaş-barış, batı-doğu, dost-düşman, düzen-anarşi, idealizm-realizm gibi zıtlıklar esasında meydana getirilen geleneksel uluslararası ilişkiler disiplinine itiraz etmiş ve kavramlar içindeki bu hiyerarşik düzeni kritik etmiştir (Knutsen, 2006:365-366).

Klasik güvenlik anlayışının bu zıtlıklar üstünden meydana getirildiği dikkate alındığında, post modern teorinin benzer hiyerarşik düzene göre şekillendirilmiş geleneksel güvenlik yaklaşımının ontolojik ve epistemolojik geçmişlerini tartışmaya açtığı belirtilmektedir. Bu teori tarihten gelen uygulamaları ve kalıplaşmış düşünceleri inceleyerek, klasik güvenlik literatürünü, tartışılmamış unsurlarını ve iç dinamiklerini ortaya çıkarmaya gayret etmiştir (Knutsen, 2006:364-366).

Postmodern güvenlik anlayışı, küreselleşmeyle beraber ortaya çıkan kavram ve değerlerdeki değişime vurgu yapmaktadır. Küreselleşmenin tesiriyle farklılıklar birbirine yaklaşırken çatışmalarda artış göstermektedir. Geleneksel dost düşman kavramları önceden belli çerçeveye oturtulmuşken, günümüzde bu kavramların sınırlarının

belirlenerek tarifinin yapılması güçleşmiştir. Geleneksel güvenlik teorileri bugünün şartlarını analiz etmekte ve problemlere cevap üretmekte kifayetsiz kalmış ve güvenliğin muhafaza edilmesindeki fonksiyonlarını yitirmeye başlamıştır. Özetle postmodernler; küreselleşme sonucu değişik kimliklerin yükselen bir hızla çatıştığını ileri sürmektedir. Kimliksel farklılıklar içinde bir mutabakat ortamı aranmasına karşın iletişim teknolojilerinde yaşanan ilerlemeyle beraber ötekileş(tir)menin her geçen gün belirginleştiğini ve bu belirsizlikler ortamında realist yaklaşımın geleneksel güvenliği tesis etmek adına gücünü muhafaza etmeye gayret gösterdiğini ifade etmektedir (Sandıklı ve Emeklier, 2011:33-34).

Post modern kurama göre, batı odaklı uluslararası düzen, kişinin güvenliğini tüm yönleriyle etkilemekte ve geleneksel güvenlik yaklaşımı batı anlayışını ve güvenliğini önceliklendirmektedir. Örneğin, güvenlik ajandasının tepesinde bulunan düzensiz göç konusu, hiyerarşik bir kapsamda ve ben-odaklı bir anlayışla değerlendirilmektedir. Göç alan devletlerin diğer bir ifadeyle batının güvenliğine odaklanılırken, ülkelerini terk etmek zorunda kalanların güvenliği ise ikinci plana konmakta, bunlar çok kısıtlı bir şekilde gündem yapılmaktadır. Diğer yandan, post modern teorisyenler hâlihazırdaki güvenlik çalışmalarına psikolojik bir perspektif ekleyerek kavram ve değerlerin değişik bir açıdan incelenmesini sağlamıştır. Bu kapsamda, güç, mücadele, çatışma, harp gibi kavramların bireyden ayrı düşünülmesi, kişi ve toplum güvenliğine yönelik risk meydana getirmektedir. Post modern kuramcılar, yaşadığımız bilgi ve iletişim döneminde harbin bir çeşit bilgisayar oyununa evirildiğini ifade etmektedir (Derian, 1990:187).

Bununla beraber, bilgi ve iletişim teknolojilerinde yaşanan gelişmeler neticesinde harp ve çatışmaların ötesinde her an çok farklı tehditlerle karşılaşılmaktadır. Siber ortamda yaşanan bir saldırıdan genetiği değiştirilmiş gıdalara kadar çok farklı konularda güvenliği olumsuz etkileyen tehditler kendini göstermiştir. Bu kapsamda post modern yaklaşım, muhtemel çözüm arayışlarına eğilmese de hâlihazırdaki kavramlara yönelik tarifleri ve açığa çıkmamış içsel kanunları gün yüzüne çıkarma konusundaki arayışları ile güvenlik çalışmalarında öne çıkmaktadır (Eriksson ve Giacomello, 2006: 233-234).

1.2.1.5. Feminist Güvenlik Yaklaşımı

Bu teori 1990 yılından sonra "ötekileşme sürecine direnmenin bir aracı" olarak (Keyman, 2000: 241) kendine yer bulmaya başlamış, uluslararası ilişkilerin tüm konularının bir değişim periyodundan geçirilmesi cinsiyetçi bir çerçevede değerlendirilerek, bunların özünde yer alan erkek egemen yönelimi ortadan kaldırmaya ilişkin yol alınmasına vurgu yapılmıştır (Koyuncu, 2012: 117).

Feminist yaklaşımın güvenliğe ilişkin kritikleri Uluslararası İlişkilerin teorilerden ayrı olarak değerlendirilmemektedir. Feminizmin de aynı güvenlik kavramında olduğu şekilde fikir birliğine varılmış genel bir tanımının olmaması bu iki konunun birleşimini yani feminist yaklaşımda güvenliği açıklamayı güçleştirmektedir (Stancich, 1998:125).

Güvenlik kavramı üzerine araştırmalar yapan feminist teorisyenlerin Bosna'da görülen ırza geçme vakalarını uluslararası kamuoyuna getirmeleri, erkek baskın Uluslararası İlişkiler teorilerini tartışmaya götürmüş; önce birey güvenliği olmak üzere devlet dışı bütün güvenlik konularına yönelik fikir ayrılıklarına farklı bir boyut eklemiştir. Bu anlayıştan hareketle bu teorinin güvenlik alanına en ciddi getirisi, realizmin "biz/onlar" ya da "dost/düşman" şeklindeki meydana getirdiği farklılaştırıcı güvenlik yaklaşımını cinsiyet kavramı üzerinden kritik etmesi olmuştur (Ataman, 2009:26).

Feministler, güvenlik kavramını çok yönlü bir anlayışla ele alarak, öncelikle çevresel, bedensel ve yapısal olacak şekilde bütün yönleriyle şiddetin minimum seviyeye çekilmesi olarak belirtmektedir (Tickner, 197:624). Güvenlik kavramının şiddet odaklı açıklayan feministlerin bakış açısına göre güvensizliğin temeli başta cinsiyet, zümre, sınıf ve soy olmak üzere tüm toplumsal ve yapısal adaletsizliklerin etkilerinden oluşmaktadır (Tickner, 2005:6).

Feminist kuramın güvenlik konusuna getirdiği en ciddi fayda "cinsiyet güvenliği" unsurunun dikkate alınarak kıymetlendirilmesi olmuştur. Feminist yaklaşım, devlette gücün paylaşımında güvenlikten daha çok cinsiyetleştirilen başka bir alan bulunmadığını ifade ederek kadınların, uluslararası ilişkiler disiplininin uygulamasında ve teorisinde dışarıda bırakılmasını kritik etmiştir (Terriff, 1999: 91). Kadın ve erkek ayrımında, sosyolojik öğrenilmiş tavırların esas olduğu anlayışıyla "toplumsal cinsiyet-*gender*" kavramını (Peterson ve Runyan, 1999: 5) ele alan teori, cinsel kimliklerin topluluklar

tarafından oluşturulduğuna işaret etmiştir. Devleti esas unsur gören, güvenliği de askeri esasa düşüren tanımların yerine, kişisel ve toplum güvenliği ihtiva eden müşterek güvenlik yaklaşımına geçiş kuramın tekliflerinden birini oluşturmaktadır (Peterson, 1992:31). C. Enloe, güvenliğin gerçekte devletten ziyade baskın unsur erkek egemen sistemi muhafaza ettiğini ifade etmiştir (Enloe, 1989: 31).

Ana oyuncu olarak devletin görülmesinin ötesinde güvenlikte erkeğe has bakış tarzının egemenliğine itiraz ediş bu yaklaşımın bir diğer referansı olmuştur (Gürpınar, 2016). A.J.Tickner, güvenliğe ilişkin tüm konularda cinsiyet unsurunu incelerken kadınların güvenlik konularında çok nadir olarak dikkat çektiğini ve kadının güvenlikteki durumunun dahi belli olmadığını ifade etmektedir. Güvenliğin sağlanmasının şartlarında kadının kontrolü asgari seviyededir (Tickner, 1992: 30). Bu teorinin toplumsal cinsiyet bakış açısıyla güvenlik kavramına faydası, uygulama alanında kadının pozisyonunu erkekle eşit yapmaya yönelik adımlarla beraber değerlendirilmelidir.

1.2.1.6. İnşacı Güvenlik Yaklaşımı

Bu yaklaşım, 1980 senesinden sonra uluslararası ilişkiler literatüründe kendine yer bularak her geçen gün daha da yaygınlaşan bir teoridir. Sosyolojik ve eleştirel kuramların birleşiminden hareket eden inşacılar, uluslararası siyasetin, öznelerin etkileşimi sonucu toplumsal şekilde meydana geldiğini savunur ve normları, kimlikleri ve fikirleri kıymetlendirerek uluslararası siyasetin odağına koymaktadır. Bu özelliği nedeniyle inşacı güvenlik problemlerini ve uluslararası münasebetleri değerlendirirken teorik açıdan yetersiz kalsa da güvenlik anlayışında geniş sosyolojik bir taban sunmaktadır (McDonald, 2008a: 59-60).

İnşacı güvenlik kapsamında Peter Joachim Katzenstein'in "Ulusal Güvenlik Kültürü" çalışması öne çıkmaktadır. Katzenstein, güvenliğin tanımsal yönünün yeniden çalışılmasını, Soğuk Savaş'ın bitmesiyle beraber klasik güvenlik araştırmalarının kifayetsizliğinin açığa çıkarılmasını ve ulusal güvenlik kültürüyle ilgili geniş sosyolojik bir bakış zaviyesinin geliştirilmesini savunmaktadır (Katzenstein, 1996: 13-17).

İnşacı anlayışta, ulusal güvenlik siyasetinin sebepsel argümanları "norm", "kimlik" ve "kültür" öğeleriyle ifade edilmektedir. Normlar, realistlerin aksine,

uluslararası düzende toplumu meydana getiren unsurdur (Bull, 2002: 51). Normlar belli bir kimlik adına, uygun tavırlara ilişkin ortak istekleri ortaya koymaktadır Normlar kimlikleri esas alırlar ve inşa ederler. Bunun yanında normlar, eskiden inşa edilmiş hâlihazırdaki kimliklere ilişkin tavırlar adına bize fikirsel kanıtlar vermektedir (Jepperson vd, 1996: 71-73).

Ülkelerin milli hak, menfaatleri ve güvenlik politikalarını, coğrafyalarında meydana gelen olaylar ve normlar biçimlendirmektedir (Jepperson vd, 1996: 70). Arap Baharı'nda yaşanan olaylar neticesinde coğrafyada yaşanan iç savaşlar, çatışmaların neticesinde, başta Suriye kaynaklı olmak üzere ciddi bir göçmen sorunu kendini göstermiştir. Bu kapsamda düzensiz göç, göçmen ve sığınmacı gibi konularına ilişkin araştırmalar fazlalaşarak birçok ülkenin milli güvenlik dokümanlarında bu hususlara vurgu yapılmıştır.

İnşacı teorinin güvenlik kavramına ilişkin değerlendirmesinin, milli güvenliğe yönelik diğer bir sebepsel argümanı "kimlik"tir. Kimlik kavramı bir oyuncunun çevresel unsurlar ve menfaatler arasında ehemmiyetli bir irtibat noktası olarak kendini göstermektedir. Klasik manada kimlikler, oyuncular arası köklü etkileşimlerin neticesinde bire bir tesis edilen, değişkenlik arz ederek dönüşüm yaşayan bir kavramı belirtmektedir (Jepperson vd, 1996: 77).

İnşacı teorinin milli güvenliğe ilişkin diğer bir sebepsel argümanı "kültür" dür. Kültür argümanı normlar, değer yargıları vb. bir seri kıymetlendirici kuralları olan, düzende ne çeşit oyuncuların nasıl varlıklarını sürdürdüğünü, birbirleri arasındaki münasebetlerin nasıl olduğunu açıklayan bilişsel imgeleri ortaya koymaktadır (Zengin, 2019:38).

1.3. Siber Güvenlik Kavramları

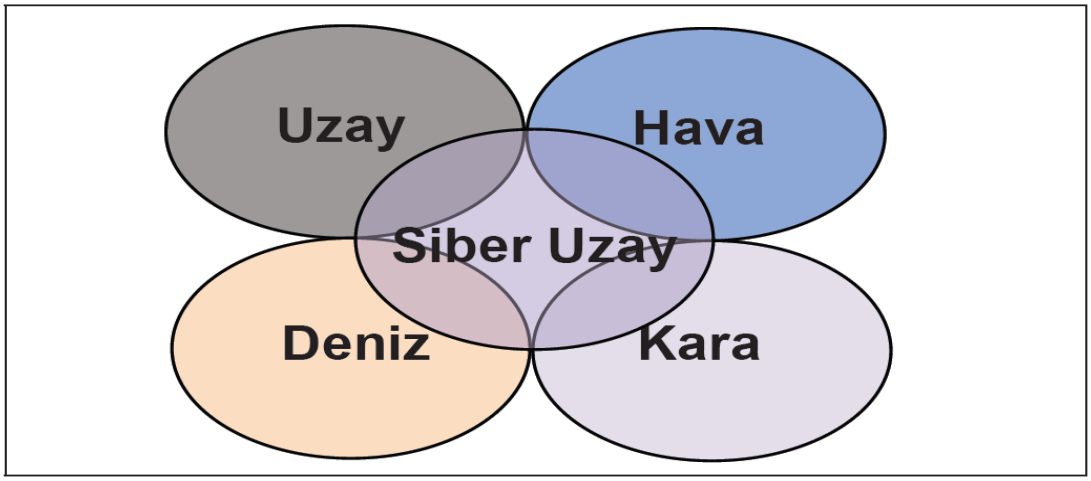
1.3.1. Siber Uzay (Alan)

Kavram ilk kez ABD'li araştırmacı William Gibson tarafından 1984 senesinde "Neu-romancer" adlı çalışmasında tanımlanmış, müteakiben kavram bilgisayar sistemleriyle direkt olarak irtibatlandırılmıştır. Siber alan internetin çok daha ötesinde bir

kavram olarak; sadece donanım, yazılım ve veriden değil ağ dâhilindeki sosyal etkileşimlerden de meydana gelmektedir. Sayısal bir ortam olarak ele alınan siber uzay, gündelik yaşamı sürdürecek her şeyi ortaya koyabilen küresel bir bilgi ağıdır. Siber alan fiziksel altyapı, bilgi, mantıksal yapılar ve insan olmak üzere dört temel kavramdan meydana gelmektedir (Sağıroğlu ve Alkan, 2018: 87).

Siber uzay, dünya ve uzay dâhil birbirine irtibatlı ya da bağımsız bilgi sistemleri altyapıları, iletişim ağları ile bilgi işlem sistemleri ve hepsini meydana getiren bütün yazılım ve donanımı kapsayan sayısal ortamdır. Birçok devlet tarafından siber uzayın tanımı milli güvenlik belgelerinde yapılmaktadır (Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016: 7).

Siber uzay bütün ağları, veri sistemlerini ve bilgi kaynaklarını küresel bir sanal sistem içinde bir araya getirmektedir. Bu kapsamda klasik kara, deniz, hava ve uzay ortamları içerisinde siber uzay (siber ortam) harekât ortamı da kendine yer bulmuştur. Siber harekât ortamı; günümüz harp anlayışına fayda sağlayacak ek bir askerî dinamik oluşturmaktadır (Çiftçi, 2013:7) (Şekil 4).



Şekil 4. Beşinci Harekât Alanı Olarak Siber Uzay

Kaynak: (Çiftçi, 2013:7)

Siber uzaydaki durum analiz edildiğinde; küresel olarak saniyede yaklaşık 8800 *tweet*, 2,9 milyon elektronik posta, Instagram'dan 955 resim atıldığı, Skype'dan 4250 görüşme ve 79000 Google taraması yapıldığı görülmüştür (İnternet Canlı İstatistikler Portalı, 2019). Bu durum Türkiye'de de benzerlik arz ederek 46 milyon internet

kullanıcısı ile Avrupa genelinde beşinci konumda bulunmaktadır. Bu istatistikler çok genel çerçevede siber uzayın ulaştığı boyutu ve etkileşim ortamını gözler önüne sermektedir (Metin, 2016: 4698).

1.3.2. Siber Tehdit

Siber tehdit; siber alanda bulunan herhangi bir fiziksel veya sanal varlığın gizlilik, bütünlük veya erişebilirliğini negatif yönde etkileyecek durumların tamamı ve bu durumlara sebep olma potansiyelidir. Siber uzayda meydana gelen istenmeyen bir açıklığı kötüye kullanma imkânı olarak da ifade edilmektedir. Siber tehdit, bir bilginin istenmeyen kişilerin eline geçmesi, bazı durumlarda ise sunulan hizmetin kısa süreli ya da bütünüyle engellenmesi, ele geçirilmesi, işlevlerini yapamaz hale getirilmesi ya da ortadan kaldırılması biçiminde gerçekleşebilmektedir (Winther, Gran ve Dahll, 2005: 371).

Ülkelerin coğrafi konumları, geçmişleri, amaçları, doğal kaynakları ve milli güvenlik yaklaşımları gibi çok farklı faktöre bağlı olarak tehdit anlayışları farklılık göstermektedir. Mesela 11 Eylül 2001'in ardından ABD tehdit algısı ve tehditle mücadele politikaları değişiklik göstermiştir. ABD'nin tehdit algısındaki değişikliğin sebepleri ise güvenlik yaklaşımlarının, imkânlarının ve tehdidi kıymetlendirme biçimlerinin farklılaşmasıdır (Küçükşahin ve Akkan, 2007: 46-47).

1.3.3. Siber Suç

Kavram en temel haliyle siber alanda işlenen suçlar olarak tanımlanmaktadır. Bu tarz durumlarda zanlı olarak bilgisayar ele alınmaktadır. Siber suçlular teknolojiyi bireysel bilgileri ele geçirmek, sırları öğrenmek ya da art niyetli hedefleri gerçekleştirebilmek için kullanmaktadır (Sağıroğlu ve Alkan, 2018: 94).

İlk önceleri klasik suç çerçevesine oturmayan ve bilgisayar ya da bilişim suçları şeklinde tanımlanan suçlar, bilgi teknolojilerinin ve internetin sosyal ve iş yaşamında genişleyerek kullanılmasıyla beraber siber suçlar olarak tanımlanmaya başlanmıştır.

Uluslararası platformları ciddi şekilde meşgul eden siber suçlar, Birleşmiş Milletler(BM) 10. Kongresinde "bilişim sistemi güvenliğini/veri işlemini hedef alan,

bilişim sistemi/ağı marifetiyle gerçekleşen kanun dışı eylemler" şeklinde tanımlanmıştır (Turhan, 2006:30-31).

2004 yılında imzalanan Avrupa Konseyi Siber Suçlar Sözleşmesi'nde ise siber suçlar; "yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekârlık ya da dolandırıcılık suçları yanında, bilgisayar ve veriye yönelik fiillere ilave olarak, bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan çocuk pornografisi, telif haklarına ilişkin ihlaller, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler" çerçevesinde ele alınmış ve kapsamı genişletilmiştir. Siber suçların büyük çoğunluğu, siber saldırı ya da harp kapsamında yer almamakta, siyasal hedefler gütmemekte ya da milli güvenlik bakımından problem oluşturmamaktadır (Yayla, 2014: 191-192).

1.3.4. Siber Terörizm

Terör eylemlerinin siber uzaydan istifade edilerek yapılması veya terör gruplarının siber uzayı vasıta olarak ele almaları şeklinde ifade edilmektedir (Krasavin, 2019). Diğer bir ifade ile siber uzay ile terör kavramlarının birleşmesidir. Siber terörizm, siyasi ya da sosyal amaçların elde edilmesi maksadıyla bir ülkeyi ya da yurttaşlarını hor görmek, korkutmak, tehdit etmek için bilgi sistemlerine, ağlara yönelik olarak siber uzayda yapılan yasalara aykırı taarruz ya da taarruz tehditlerini ele almaktadır (Denning, 2000:1).

Bu kavram, bilgi teknolojileri imkânlarının siyasi olarak güdülenmiş ulus-altı topluluk/gruplar ya da casuslar tarafından cebir, şiddet kullanmak, halkı olumsuz etkilemek ya da politikaları değiştirmek maksadıyla vasıta olarak kullanılması şeklinde açıklanmaktadır (Andress ve Winterfeld, 2011:198). Siber terörizmi ulus-altı topluluk/gruplar kullanırken, siber harp bir ülke tarafından idare edilmektedir. Problem, siber harp sebebi olarak görülecek eylemin arkasındaki ülkenin bulunmasıdır.

Teknolojik gelişmelere paralel olarak bilgi iletişim imkânlarının sağladığı kabiliyetler ve kullanıcı rakamlarındaki yükseliş art niyetlilerinde alakası cezbetmiş ve terörizm siber alana sıçramıştır. Siber terörizm, "siber uzayda, siber varlıklar kullanılarak gerçekleştirilen terör eylemleri" ve "konvansiyonel terör örgütlerinin son yıllarda

faaliyetlerini internet üzerine kaydırmaları neticesinde görülmeye başlanan siber saldırı türü" biçiminde tanımlanabilmektedir (Güngör; 2015:48).

1.3.5. Siber Caydırıcılık

Caydırıcılık bir ülke ya da grubun diğer bir ülke ya da grup tarafından kendisine karşı olabilecek askeri güç kullanımına kadar varan eylemlerden sakınması için zaruri önlemleri alması olarak ifade edilmektedir (İduğ, Çalışkan ve Güler, 2013:287).

Caydırıcılıkta vazgeçilmez iki ana kavram söz konusudur. Birincisi, muhtemel taarruz ve risklere karşı kuvvetli bir savunmaya kapasitesine sahip olmak, ikincisi ise olası bir durum karşısında herhangi bir taraftan gelen taarruza ilişkin karşılık verebilme imkân ve kabiliyetine haiz olmaktır (Haley, 2013).

Yalnızca siber güç kullanıldığında tesiri diplomatik ve iktisadi yaptırımlardan daha fazlayken, klasik ve nükleer kuvvetin tesirinden daha azdır. Netice itibari ile siber caydırıcılık tek kullanıldığında tesirli olmasının ötesinde, diplomatik, iktisadi yaptırımlar, klasik ve nükleer güçle beraber kullanıldığında daha fazla tesirli olmaktadır (Libicki, 2009: 29-30).

1.3.6. Siber İstihbarat ve Siber Casusluk

İstihbarat ve casusluk kavramları, tarihte her zaman kendine yer bulmuş, muhasım, tehdit ülke/grup/topluluğa karşın üstünlük tesis etmek maksadıyla icra edilen her türlü eylemdir. Bu kavramların ehemmiyeti zaman içerisinde hem aynı kalsa da icra yöntemleri başta teknoloji olmak üzere yaşanan gelişmelere paralel olarak farklılık arz etmiştir (Çifçi, 2013: 289).

Siber istihbarat, siber uzayda meydana gelen siber taarruz ve tehdit tahlillerini yaparak karşı taarruzlar ile bilgi elde edinilmesi olarak tanımlanmaktadır. Siber taarruzlar icra ederek ülkenin bekası için önem arz eden bilgilerin temini siber istihbaratın ana karakteristiğini meydana getirmektedir (Keleştemur, 2015: 90).

Siber casusluk, bir devletin, topluluğun, kurum/ kuruluşun, örgütün ve organizasyonun veya bireylerin kritik önemdeki bilgilerini, siber uzayda çeşitli yöntemler

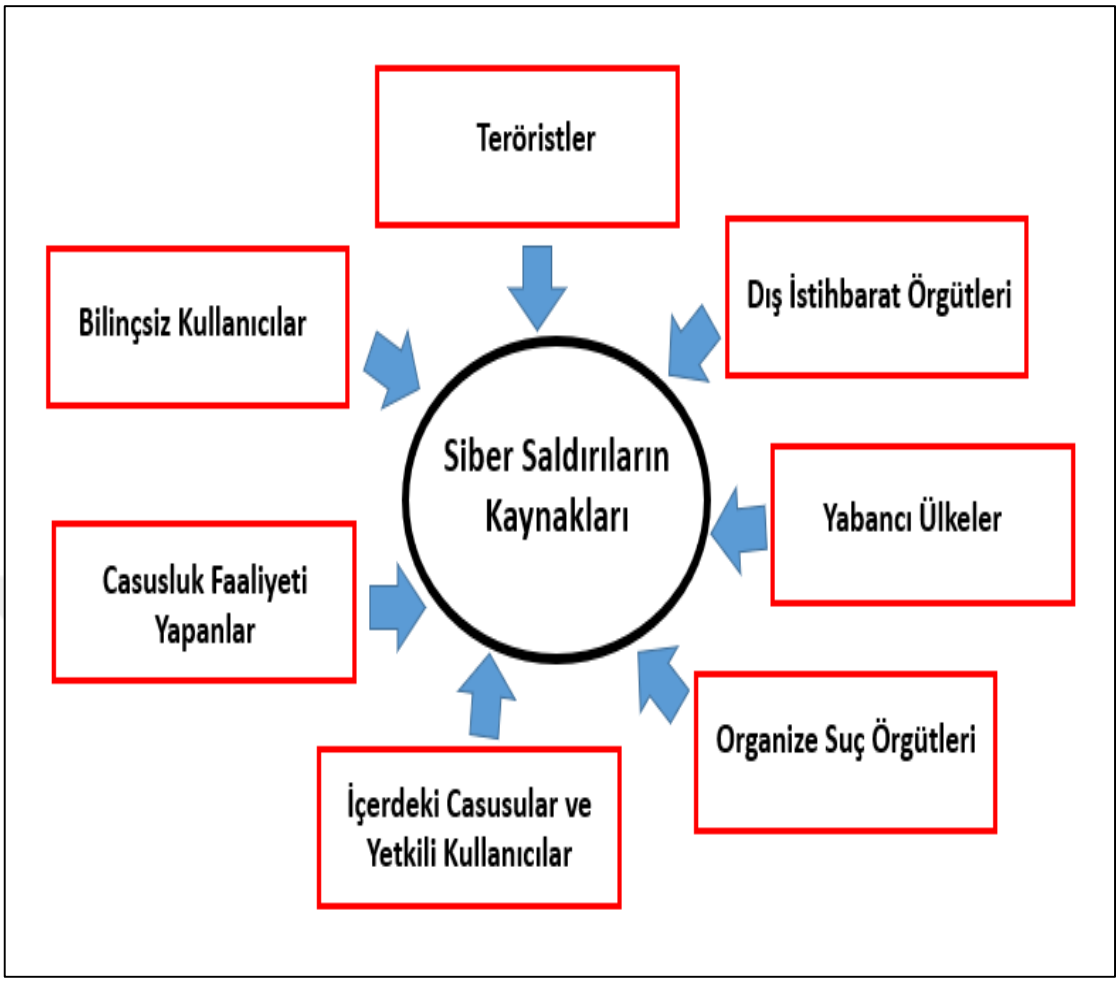
vasıtasıyla karşı tarafın haberi olmadan gizli bir şekilde temin etmektir. Bu faaliyet, kişisel ya da organize olarak maddi çıkar sağlamak amacı ile de yapılabilmektedir. Bir ülke tarafından koordineli olarak diğer bir ülkeye üstünlük sağlamak, sorun çıkarmak maksadıyla yapılan siber casusluk eylemlerinin neticeleri siber harp sebebi olabilecek kadar ileriye gidebilmektedir. Siber casusluk eylemlerinin amacında ülkeye ait gizli belgelerin yanında ticari çok gizli bilgilerde yer almaktadır. Ciddi işgücü, zaman ve sermaye ile elde edilen icatların, formüllerin korunması ve kötü niyetli bireylerin eline geçmemesi ülke bekası açısından ehemmiyet arz etmektedir. Farklı casusluk çeşitleri, uzun süredir görülse de küresel mücadele, Bilgi ve İletişim Teknolojilerinde (BİT) yaşanan ilerlemeler siber casusluk eylemlerinin sebep olduğu risk ve tehditleri ciddi manada artırmıştır (Yayla, 2014:194).

1.3.7. Siber Saldırı (Taarruz)

Siber güvenliğin ana risk ve tehdit öğesini siber saldırılar oluşturmaktadır. Siber saldırılar, bilgi ihtiva eden ağlara, bilgileri ele geçirmek, yerine yanlış bilgi koymak veya imha etmek maksadıyla icra edilmektedir. Bahse konu taarruzlar sistem, cihaz, tesis, ağ veya bunların sahip olduğu verilerin gizlilik, tamamiyet ve erişebilirliğine ya da fiziksel varlığına zarar vermek, tahrip etmek amacıyla yapılmaktadır. Başta iletişim teknolojilerinin ilerlemesi ve internetin yaygınlaşmasıyla beraber, birbirine irtibatlı sistemler siber saldırıların etki alanını büyütmüştür (O'Shea, 2003: 6).

Türkiye Ulusal Siber Güvenlik Stratejisi (2016-2019)'nde siber taarruz, "siber uzayda bulunan bilgi ve iletişim teknolojilerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi veya sistemler tarafından kasıtlı olarak yapılan işlemler" olarak tanımlanmaktadır (Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016: 7).

Siber taarruzlar ucuz, sonuçları itibariyle yıkıcı, kaynağının belirlenmesi zor, yaygın, zahmetsiz, karmaşık ve kritik altyapılara ulaşabilecek kadar etkili yöntemlerdir (Güngör, 2015:42). Siber saldırıların kaynakları Şekil 5'de sunulmuştur.



Şekil 5. Siber Saldırıların Kaynakları

Kaynak: (Çeliktaş, 2016:8)

Kenneth Geers (2010) siber saldırıları, Soğuk Savaş sürecinde ehemmiyet kazanan ve ciddi şekilde değerlendirilen "caydırıcılık kuramı" çerçevesinde tahlil etmiştir. İki küresel gücü oluşturan ABD ve Sovyetler Birliği mücadelesi klasik askeri harp mantığının ötesine geçerek psikolojik savaşa evirilmiştir. Siber taarruzlarda bu kapsamda ele alındığında ciddi bir askeri kuvvet olarak ve devletlerin nükleer teknoloji de dâhil kritik birçok bilginin çalınması ya da tahrip edilmesine kadar etki sağlayabilecektir. Caydırıcılık teorisinde, reddetme ve cezalandırma olmak üzere iki ana strateji kendini göstermektedir. Geers'e (2010) göre siber taarruzlar devletlerin sahip olduğu nükleer silahların dahi kendi ülkelerinde patlatılmasına varacak bir güce sahiptir. Bu kapsamda siber taarruzlar nükleer silahlardan dahi daha tehlikeli olabilmektedir. Bu nedenle caydırıcılık teorisinde ülkeler cezalandırma stratejisini hayata geçirmektedir (Geers, 2010:301).

1.3.8. Siber Güvenlik

Uluslararası Telekomünikasyon Birliği'nin tanımına göre siber güvenlik, siber uzayda devlet/kurum/kuruluş/bireylerin varlıklarını sürdürebilmek maksadıyla istifade edilen malzeme, strateji, güvenlik anlayışları, rehberler, risk idare usulleri, icraatlar, yönelimler, örnek uygulamalar ve teknolojilerin tamamı olarak ifade edilmektedir (Uluslararası Telekomünikasyon Birliği, 2008:2).

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber uzayda yer alan güvenlik risk/tehditlerine karşı koyabilecek biçimde meydana getirilmesini ve idame edilmesini sağlamayı hedeflemektedir. Siber güvenliğin ana amaçları bilginin erişilebilirliğini, aslına uygunluğu ve inkâr edilemezliği de dâhil olmak üzere bütünlüğünü ve gizliliğini temin etmektir (Uluslararası Telekomünikasyon Birliği, 2008:7). Siber güvenliğin ana esasları;

- Bilginin korunması,
- Bilgi bütünlüğünün, veriye ulaşımın ve bağlantı süratinin idamesi
-Sistemin işleyişinin sürdürülebilirliğinin temin edilmesidir (Atalay, 2012: 43). *CIA(confidentially- integrity- availability*)'in üç atlısı olarak ifade edilen "gizlilik, bütünlük ve erişilebilirlik" unsurları durumun önemini ortaya koymaktadır (Singer ve Friedman, 2015:57)

1.3.9. Siber Silah

Elektromanyetik spektrumu kullanmadan veya maddi bir tesir olmadan direkt olarak siber sistemleri tahrip etmek, imha etmek amacıyla yararlanılan kötü yazılım ya da metotları belirtmektedir. Siber silah ifadesi ilk olarak kötücül yazılımları zihne getirmektedir. Kötücül yazılımların Truva atlarından virüslere, botlardan solucanlara kadar çok geniş bir spekturumda çeşitleri bulunmaktadır. Metotlar da ise sahte elektronik postada, internet portalı gibi silahlar bulunmaktadır (Keleştemur, 2015; 221).

Siberin çoğu konusunda olduğu gibi siber silah tanımı ile alakalı da uluslararası bir mutabakata varılamamaktadır. Ancak siber silah genel olarak, klasik silahların bir unsuru olarak kabul edilmekle beraber kritik altyapı, bilgi ve iletişim teknolojileri ya da

bireyleri bedensel veya düşünsel olarak tesir altına almak, tehdit ya da tahrip maksadıyla kullanılan yazılım olarak tanımlanmaktadır (Rid ve McBurney, 2012: 7).

1.3.10. Siber Konusuna İlişkin Bazı Kavramların Ayırt Edici Özellikleri

Siber suç, savaş ve terör kavramları analiz edildiğinde bu unsurların bazı noktalarda benzerliklerinin bulunmasının yanında bazı noktalarda ise ciddi farklılıkların bulunduğu tespit edilmektedir. Bu kavramların meydana geliş nedenleri ve hedefleri farklılık arz etmektedir. Diğer bir ifade ile siber sözcüğü terörizm, harp ve suç kavramlarını bir sıfat olarak ele alırken temel farklılık kavramların yapısından ortaya çıkmaktadır. Bu kavramların ana özellikleri ve farklılıkları Tablo 1'de gösterilmiştir (Çakmak ve Altınok, 2009:49).

Tablo 1. Siber Suç, Siber Terör ve Siber Savaşın Temel Özellikleri ve Farklılıkları

EYLEMİN	SİBER SUÇ	SİBER TERÖR	SİBER SAVAŞ
ŞİDDETİ	AZ YOĞUN	YOĞUN	EN YOĞUN
MOTİVASYONU	KİŞİSEL KAZANÇ	SİYASİ	SİYASİ DÜŞMANIN SAVAŞMA KABİLİYETİNİ AZALTMA CASUSLUK
FAİLLERİ	BİREYLER ORGANİZE SUÇ ÖRGÜTLERİ	TERÖRİST ÖRGÜTLER	NET OLARAK BELİRLENMESE DE KAYNAKLAR DEVLET TARAFINDAN SAĞLANIR
HEDEFLERİ	KİŞİSEL HEDEFLER	KRİTİK ALTYAPILAR GÜVENLİK BİRİMLERİ HÜKÜMET KURULUŞLARI	KRİTİK ALTYAPILAR ASKERİ VE MALİ SİSTEMLER GÜVENLİK TEŞKİLATLARI
KAYNAĞI	ÜLKE İÇİNDEN VEYA DIŞINDAN	ÜLKE İÇİNDEN VEYA DIŞINDAN	ÜLKE DIŞINDAN

1.4. Günlük Hayatta Karşılaşılan Siber Saldırı Yöntemleri

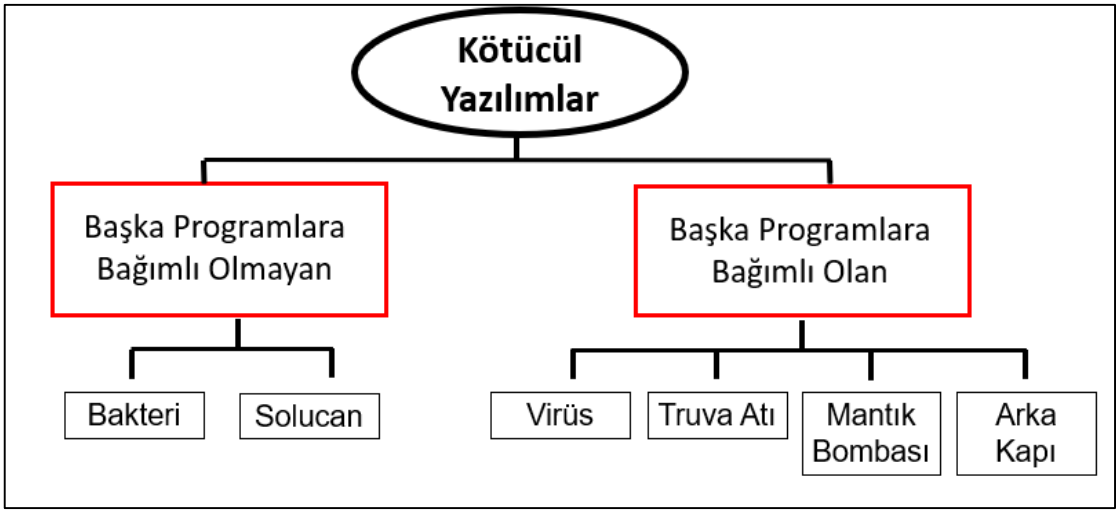
1.4.1. Hizmet Dışı Bırakma (*Denial of Service-DoS*)

Bu saldırı yöntemi hedef kullanıcıların hizmetlerden yararlanmasına mâni olmak maksadıyla yapılan taarruzlardır. Sistem veri akışını lüzumsuz işgal ederek, hizmet veremez duruma getirilmesi için yapılmaktadır. Bu yöntemde ağ bant genişliği, hafıza alanı/işlemci hızı gibi özelliklerin doyuma ulaştırılması ya da kullanıcı ile sunucu arasındaki bağlantının kesilmesi gibi metotlardan istifade edilmektedir (Carnegie Mellon Üniversitesi, 2017:1).

Bu saldırı sistem erişiminin engellenmesine ilişkin olarak en sık yapılan yöntem olarak görülmektedir. Hizmet dışına bırakmada ana hedef, yapılan taarruzlarla kurum/kuruluşun veya firmanın iletişim ağlarını felce uğratmak ve hizmet veremez hale getirmektir. Hâlihazırda bu usul genellikle çok fazla bilgisayar ile yapılmaktadır (Eren, 2017:51).

1.4.2. Kötücül Yazılımlar (Malicious Software-Malware)

Bilgi ve iletişim sistemlerine, ağlarına zarar verme, fonksiyonunu bozma, işlevini yerine getiremez hale sokma ve veri hırsızlığı gibi belli amaçlar için meydana getirilmiş bakteri, solucan, virüs, truva atı, mantık bombası ve arka kapı gibi casus yazılım silahlara verilen genel bir ifadedir. Kötücül yazılımların çeşitleri Şekil 6'da sunulmuştur (Çeliktaş, 2016:31).



Şekil 6. Kötücül Yazılımlar

Kaynak: (Çiftçi, 2013:150)

1.4.3. Yemleme (*Phishing*)

Çoğunlukla emniyetli bir internet sitesinin benzer kopyası ya da aldatmaca bir elektronik posta vasıtasıyla gerçek bir web adresi kullanıyormuş algısı oluşturarak, kanun dışı usullerle aldatılan bireyin parola, kredi kartı ve özel verilerinin çalınması şeklinde tanımlanmakta, oltalama olarak da ifade edilmektedir. Bu yöntemde art niyetli bireyler çoğunlukla elektronik postalar ile kurbanları ile iletişime geçmekte, resmi kurum/kuruluş ve firma gibi davranarak bireysel verileri ele geçirmektedir (Ulaşanoğlu ve diğerleri, 2010: 28).

Oltalama saldırıları çoğunlukla hedef sisteme ulaşabilmek maksadıyla kişinin doğasındaki bazı zayıflıklardan istifade edilmesi olarak açıklanan sosyal mühendislik taarruzları içerisinde ele alınmaktadır (Hekim, 2015: 58).

1.4.4. Yığın İleti (Spam)

Internet ortamında aynı iletinin yüksek sayıdaki kopyasının, bu tarz iletiyi alma isteğinde bulunmamış bireylere yollanması yığın ileti (spam) olarak adlandırılmaktadır. Günümüzde yığın iletiler rahatlıkla yollanabilmektedir. Yığın iletiler genellikle reklam ve satış maksatlı olmakla beraber sitemi tahrip ederek oltalama yöntemiyle kişileri dolandırmak maksatlı yollanmaktadır (Çiftçi, 2013:147).

1.4.5. Şebeke Trafiğinin Dinlenmesi (*Snifting*)

Ağ içerisinde servis sağlayıcı ile birey arasındaki veri trafiğinin izlenmesine "monitoring", bu veri akışındaki bilgilerin muhteviyatının değiştirilerek hesap, kredi kartı bilgileri gibi önemli verilerin ele geçirilmesi de "sniffing" olarak ifade edilmektedir (Çeliktaş, 2016: 39).

1.5. Siber Savaşlarda Yapılabilecek Saldırı Yöntemleri

1.5.1. İnternet Sayfalarının Ele Geçirilmesi

Başta kamu kurum/kuruluşlar ile büyük şirketler olmak üzere hedef olarak belirlenen herhangi bir web sayfasının ele geçirilerek buraya istenen mesajın bırakılmasıdır. Hedef ülke liderlerinin halk önünde zor duruma bırakmak, küçük düşürücü resimler koymak gibi saldırı metotları bu kapsamda ele alınmaktadır.

1.5.2. Dağıtık Hizmet Dışı Bırakma Saldırıları (*Distributed Denial of Service-DDoS*)

Ağ ile irtibatlı bir sunucunun faaliyetlerini kısa süreli veya tamamen sekteye uğratarak, bilgisayara ya da ağa gerçek kullanıcılarca ulaşılamamasını amaçlayan taarruz çeşidi *DoS* olarak tanımlanmaktadır. Bu tarz taarruzlarda hedef cihaz ya da sistemin, lüzumsuz isteklerle fazla yüklenmesi ve doğal isteklere yoğunluk sebepleriyle yanıt verememesi amaçlanır. *DoS* taarruzları büyük sayılarla ya da zombi şeklinde yararlanılan bilgisayarlar desteğiyle gerçekleştirildiğinde ciddi tehlike arz ederek *DDoS* şeklinde ifade edilir. *DDoS* taarruzları neticesinde en kuvvetli sistemler dahi kendini koruyamamaktadır. *DDoS* taarruzları her geçen gün daha da fazla kullanılmaktadır (Sağıroğlu ve Alkan,2018:263).

1.5.3. Gizlilik Dereceli Bilginin Ele Geçirilmesi

Gizlilik arz eden bilgilerin elde edilmesi siber casusluk olarak da adlandırılmaktadır. Kritik önemdeki ve gizli bilgilerin, bireylerden, topluluktan, muhasımdan, devletlerden, askeri, siyasi, iktisadi üstünlük tesis etmek maksadıyla kanun dışı olarak, iletişim ağları ve bilgi sistemleri vasıtasıyla elde edilmesidir. Ülke güvenliğine yönelik işlenen suçların en eski ve önemlilerinden birisi de casusluktur (Çiftçi, 2013:190).

Bu tarz faaliyetler, kişisel ya da belli bir grup tarafından maddi çıkar kazanmak veya menfaat elde etmek için yapılıyor olabilmektedir. Bir ülke tarafından organize biçimde diğer bir ülkeye zarar vermek maksadıyla yapılan siber casusluk eylemleri

duruma bağlı olarak bazı ülkeler tarafından siber harbin sebebi olarak kıymetlendirilebilmektedir (Yayla, 2013:196).

1.5.4. İnternet Üzerinden Karşı Propaganda

Bilgi iletişim teknolojilerinin yaşantımıza dâhil olmaya başladığı andan itibaren her geçen gün daha da artarak güvenlik unsurları tarafından daha ziyade propaganda maksatlı kullanıldığı bilinmektedir. Bu durumun en açık örneklerini Rusya Federasyonu(RF)-Çeçen Savaşı ve NATO'nun Kosova harekâtı oluşturmaktadır. RF ordusunun 1994 yılında Grozni'ye girdiği andan başlayarak Çeçen'ler başta internet olmak üzere tüm kabiliyetlerini kullanarak propaganda ile bilgi savaşı vermiştir. NATO'nun Kosova harekâtında yanlışlıkla bir sivil hedefi vurması karşı propaganda vasıtası olarak kullanılmış ve uluslararası kamuoyu tesir altına alınmaya çalışılmıştır (Bıçakçı, 2012:213).

1.5.5. Kritik Sistemlere Yönelik Saldırılar

Kritik altyapılar, stratejik ehemmiyeti sebebiyle siber taarruzların birincil hedefi konumundadır. Bilgi ve iletişim sistemlerindeki ilerleme ve internetin her alanda kullanılmaya başlaması kritik altyapıların kontrol sistemlerini de etkilemiştir. Fiziksel ögelerden bütünüyle izole edilmiş kontrol sistemleri, hâlihazırda bilgi ve iletişim teknolojileri vasıtasıyla idare edilebilir ve gözlemlenebilir hale gelmiştir. Son dönemlerde kritik altyapılara ilişkin siber taarruzlar giderek yaygınlaşmaktadır.

Örneğin 30 Ocak 2009'da "Conficker" virüsü Atatürk Havaalanı'nın dış hatların da kullanılan sistemleri gayri faal hale getirmiştir. TAV şirketi yaşanan olaylar neticesinde kamuoyu açıklamasıyla, yurtdışı bilet ve bagaj işlemlerinin manuel yapıldığını belirtmiştir (Şenol, 2012:14).

2010 yılında bulunan Stuxnet kötücül yazılımı İran nükleer santralini hedef alarak Stuxnet yazılımı vasıtasıyla, SCADA (*Supervisory Control and Data Acquisition*) kontrol sistemleri ile İran kritik altyapısı etki altına alınmaya çalışılmıştır (Şenol, 2016:10).

1.6. Siber Savunma Yöntemleri

Siber savunma yöntemleri yönetsel, teknolojik ve eğitim olmak üzere çok farklı boyutlarda ele alınabilmektedir. Bu üç kavram arasında bütünlük olmadığı müddetçe etkin bir siber savunmadan bahsetmek mümkün değildir. Bu yöntemlerden teknolojik unsurlar daha çok ön plana çıkmakla beraber her birinin ayrı bir ehemmiyeti bulunmaktadır. Yönetsel konular daha çok yönetimle alaka bir seri düzenlemenin ortaya konulması ve uygulanması biçiminde ifade edilmektedir. Eğitim ise kelimenin manasından da anlaşılacağı üzere bireylerin farkındalık düzeyinin ve konu hakkındaki bilgilerinin önemine işaret etmektedir. Son olarak teknolojik boyut ise başlı başına içerisinde farklı birçok konuyu ihtiva eden bir başlık oluşturmaktadır. Siber savunma yöntemlerinden teknolojik açıdan temel olarak kullanılanlar aşağıda belirtilmiştir (Yıldız, 2014:62-74).

- Kötücül yazılımlara karşı "*anti-virüs*" programlar,

- Ağ emniyeti ve yetkisiz erişimlerin önüne geçmek için "Güvenlik Duvarları-*Firewall*",

- Zararlı trafiğin kesilmesi için "Atak Önleme Sistemleri-*Instrusion Prevention System*",

- Bilginin izinsiz kurum dışına çıkarılmasını engellemek için "Veri Kaçağı Önleme Sistemleri-*Data Loss Prevention*",

- Sistemde faaliyet gösteren uygulamalar üzerindeki kusurların tespiti için "Zafiyet Tarama Sistemleri-*Vulnerability Scanner*",

- Kısıtlı kaynakların en etkin biçimde kullanılması ve en riskli sistemlere daha çok gayret sarf edilmesi için "Risk Analiz ve Önceliklendirme Sistemleri-*Risk Management System*",

- Şüpheli yazılımları ağ düzeyinde tespit ederek test sistemleri çalıştıran "Sıfırıncı Gün Zararlı Yazılım Tespit Sistemi-*Zero Day Malware Protection System, Malware Sandboxing*",

- Bilgi ve iletişim sistemlerindeki gelişmekte olan olayları gözlemleyip analiz ederek muhtemel ya da mevcut olan taarruzları "Tespit ve Önleme Sistemleri- *Intrusion Detection and Prevention)",*

- Bir ağ içindeki farklı kullanıcı düzeylerinin erişim kontrollerini denetleyen "Ağ Erişim Kontrolleri-*Network Access Controls*)",

- Şifreleme Sistemleri,

- Kimlik Doğrulama Sistemleri,

- Dağıtık ağlarda emniyetli veri aktarımı için "Sanal Özel Ağ-*Virtual Private Network*" kullanımı,

- Taarruzları tahlil etmek ve yanıltmak amaçlı "Tuzak Sistemler-*Honey Pots*"dir.

1.7. Kritik Altyapılar

Avrupa Konseyi kritik altyapıları; "zarar görmesi veya yok olması halinde, vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya kamu hizmetlerinin etkin ve verimli işleyişine ciddi boyutta olumsuz etki edebilecek fiziksel ve teknolojik tesisler, şebekeler, hizmetler ve varlıklar" olarak ele almaktadır (Avrupa Konseyi, 2008:77).

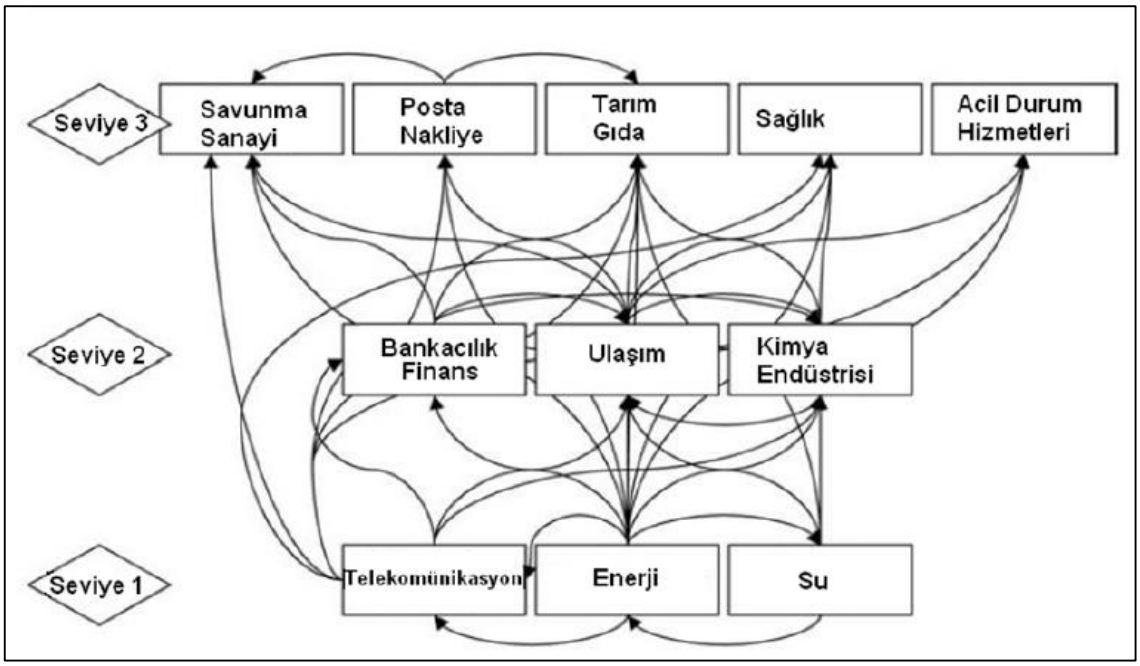
Bu kavrama ilişkin tanımlamalar devletten devlete farklılık arz edebilmekte beraber genellikle, iletişim, sağlık, ulaştırma, enerji, finans, sanayii ve ana kamu hizmetleri gibi alanlar ve bunlara ilişkin yapılar bu kavramın içinde değerlendirilmektedir. AB ve ABD tarafından Şekil 7'de sunulan listeler benzer olmakla beraber öncelik seviyesi farklı belirlenmiştir (Brunner ve Suter, 2009:531).

ABD	AB
SU	SU
GIDA	ENERJİ
SAĞLIK	ULAŞIM
ENERJİ	TARIM VE GIDA
FİNANS	KOLLUK HİZMETLERİ
ULAŞIM	BİLGİ VE İLETİŞİM
SİVİL YÖNETİM	FİNANS
BİLGİ VE İLETİŞİM	BAYINDIRLIK HİZMETLERİ
UZAY ARAŞTIRMALARI	YEREL HİZMETLER
KİMYASAL VE NÜKLEER ENDÜSTRİ	ACİL HİZMETLER
KAMU DÜZENİ VE GÜVENLİK ALANI	

Şekil 7. ABD ve AB Kritik Altyapı Listelerinin Karşılaştırılması

Kaynak: (Brunner ve Suter, 2009:531).

Kritik altyapılar olası bir siber harpte taarruzların ana hedefi pozisyonundadır. İlk olarak 1990'larda ABD tarafından ortaya atılan bu kavram her geçen gün ülkelerin gündeminde ilgi sırasını yukarılara taşımıştır. Yapılan çalışmalarda ülkenin kritik altyapıları Şekil 8'de gösterildiği gibi 3 seviyede ele alınabilmektedir (Karabacak, 2009:50). Üzerinde bulunan altyapıları besleyen ana seviye altyapılar olan birinci seviyeye yapılacak bir taarruz otomatik olarak diğer seviyeleri de etkileyecektir. Bu kapsamda telekomünikasyon, enerji ve su altyapıları önemli bir role sahiptir.



Şekil 8. Düzeylerine Göre Kritik Altyapılar

Kaynak: (Karabaca, 2009:50)

2. KURAMSAL ÇERÇEVE

2.1. Güvenlik Çalışmaları Alanında Küreselleşme Sorunsalı

Güvenlik çalışmalarının başlangıcı Soğuk Savaş olarak kabul edilse de 2. Dünya Savaşı'ndan evvel milli güvenlik stratejisi olarak harbin, yapısı, nedenleri ve tesirleri ilişkin çalışmalar yapılmıştır (Wright, 1942). Dünya savaşları arasında birinci kuşak olarak ele alınan güvenlik çalışmaları idealist yaklaşımlardan etkilenmiştir. Birinci kuşak çalışmalarda silahsızlanma, self-determinasyon, hakeme gitme ve müşterek güvenlik gibi kavramlar güvenliğin tesisinde ön plana çıkmıştır (Baldwin, 1995:119).

Güvenlik alanında yalnızca askerlerin bulunmasının kifayetsizliği 1. Dünya Savaşı'nın kötü neticeleriyle anlaşılmasını müteakip ilk defa 2. Dünya Savaşı esnasında sivillerin de askeri konularda yer alarak altın çağın ilk evresini oluşturdukları belirtilmektedir (Walt, 1991: 214).

Milli güvenliğin manasının ve içeriğinin genişletilmesine yönelik fikirler 1970'lerden itibaren teori olarak kendini göstermiş olsa da bu gayretler 2. Dünya Savaşı'nın sonundan itibaren meydana gelmeye başlamıştır. 2. Dünya Savaşı sonrası güvenlik çalışmalarında, askeri güvenliğin ötesinde dört konu daha kendine yer bulmuştur. Bunlar: ekonomik ve bireysel özgürlük gibi konular, askeri usullerle beraber askeri olmayan yöntemlerle de ulusal güvenliğin sağlanabileceği düşüncesi, güvenlik ikilemi bilincinin, askeri stratejilere riayet etme noktasında ikaz ve ihtiyat oluşturması ve iktisat, bireysel özgürlükler vb. iç dinamikler ile milli güvenlik arasındaki irtibatlara dikkat çekilmesidir (Baldwin, 1995: 122).

Güvenlik çalışmalarının ikinci kuşağını meydana getiren 1955–1965 seneleri arasındaki dönem "altın çağ" olarak tarif edilmektedir. Güvenlik çalışmaları önceki dönemin aksine dar manada güvenliği kullanarak, nükleer silahlar ve yeni teknolojilere odaklanmış, güvenlik salt askeri hususlarla çerçevelenmiştir (Rieker, 2000:4). Soğuk Savaşın tüm şiddeti ile yaşandığı bu dönemde güvenlik çalışmaları teknolojik ve ideolojik iki ana sebepten ötürü askeri odaklı olmuştur. Teknolojik olarak Sovyetler Birliği'nin nükleer konuda ABD hegemonyasını yıkması, ideolojik olarak iki ülke perspektifinden

de liberalizmin ve komünizmin karşılıklı tehdit olarak görülmesi askeri rekabete sebep olmuştur (Buzan ve Waever, 1998:8).

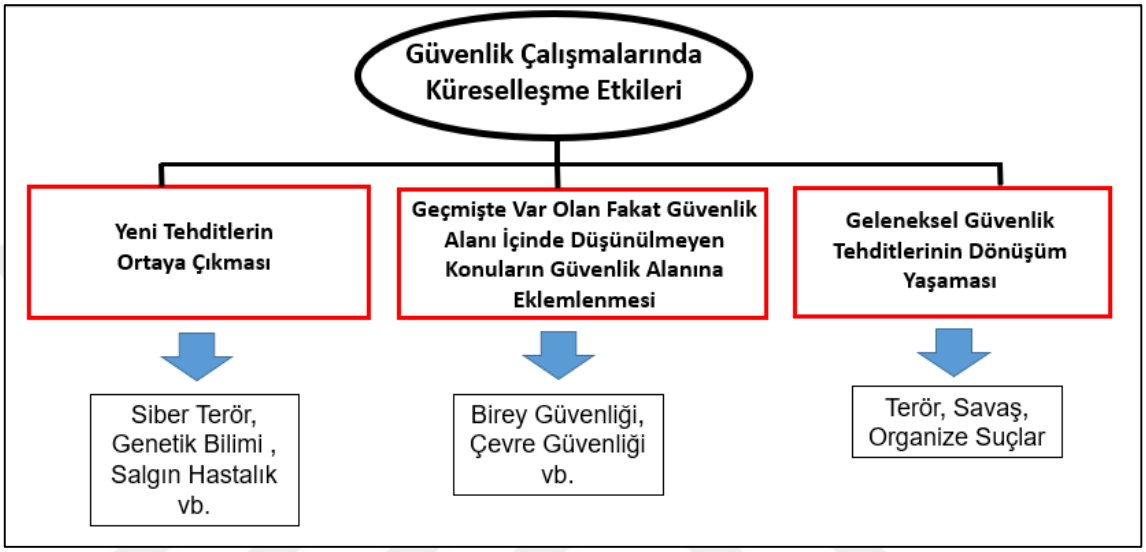
Güvenlik çalışmalarının "altın çağ" 1965 senesinde bitmiş ve gerileme dönemi kendini göstermiştir. Güvenlik alanındaki gerileme uzun sürmemiş, 1975 yılında "Rönesans" olarak nitelendirilen süreç kendini göstermiştir. Yeni siyasi problemlerin çıkması, belli kuramsal ve deneysel problemler bu dönemin oluşmasında etkili olmuştur. Özellikle 1974 yılındaki petrol sorunu batıya milli güvenlik tehditlerinin sadece askeri olmadığını ispatlamış, bu kapsamda batı yeni bir milli güvenlik literatürü meydana getirmeye başlanmıştır (Walt, 1991:216).

Güvenlik, yoğunluklu olarak Soğuk Savaş ardından ilgi cezbeden bir konu olmuştur. Soğuk Savaş'ı müteakip yaygın düşünce güvenlik konusunun popülaritesinin düşeceği şeklinde oluşmuş, ancak bu durumun aksine ilgide artış görülmüştür. Bu çalışmaların genel olarak mutabık kaldığı ana husus, güvenliğin yeni konuları ve tehditleri kapsayacak şekilde genişletilmesi zorunluluğudur (Bilgin, 2005:64).

Güvenlik anlayışı daha karmaşık, iç içe geçen bir yapı haline gelerek, ulusların hayat tarzları ve hedefleri sadece askeri/politik güçle muhafaza edilemez veya tesis edilemez durumda farklı boyutlar kazanmıştır. Bu dönemde güvenlik çalışmalarının mana ve içeriğinin genişletme fikri üç ana sebebe oturtulmuştur: neo realizmin alandaki üstünlüğünden duyulan rahatsızlık, yeni tehditlerin kapsanmasına duyulan gereksinim ve güvenlik çalışmalarını meydana gelen modern problemlerle irtibatlama isteği (Krause ve Williams, 1996:229).

11 Eylül saldırısı sonrası güvenlik araştırmaları yönünden "yeni altın çağ" şeklinde ifade edilen bir dönem olmuş ve klasik güvenlik unsurlarının tekrar başat aktör olmaya başladığı bir sürece girilmiştir. Bu kapsamda saldırı sonrası güvenlik araştırmaları, terörizmin küresel bir yön kazanması neticesinde farklılaşan niteliği ile beraber, küresel terörizmle savaşma problemini bununla sınırlı kalmamakla birlikte daha çok gündeme getirilmeye başlamıştır. Bu dönemde küreselleşmenin tesiriyle; milli güvenliğe ilişkin risk ve tehditlerin iç ve dış hudutlarının zaman geçtikçe zayıflaması, küreselleşen tehditlerin az gelişmiş devletlerin yanında refah düzeyi yüksek devletleri de içine alması güvenlik araştırmalarının sınırlarını genişletmiştir (Torun, 2012:43).

Güvenlik araştırmalarında küreselleşme süreci kendini güvenliği çok taraflı, çok yönlü ve karmaşık bir konu durumuna dönüştürmesi ile ortaya koymaktadır. Sivil toplum örgütleri gibi devlet dışı aktörleri de içermesi yönüyle çok taraflı, iktisadi, çevresel, siyasi vb. hususları da içermesi yönüyle çok boyutlu ve tehditlerin çeşitliliği, kaynağının belirsizliği vb. yönüyle de karmaşıktır. Güvenlik çalışmalarında küreselleşme etkileri özetle Şekil 9'da gösterilmiştir (Karabulut, 2009:7)



Şekil 9. Güvenlik Çalışmalarında Küreselleşme Etkileri

Kaynak: (Karabulut, 2009:7)

2.2. Uluslararası İlişkiler Teorileri ve Güvenlik

2.2.1. Güvenlikleştirme Yaklaşımları

Güvenlikleştirme kuramı, yakın dönemde çalışmalarda ciddi bir biçimde kullanılan bir yaklaşım olmuştur. Özellikle Soğuk Savaşın ardından görülen askeri darbelerin tahlil edilmesinde açıklayıcı bir kuram olarak kendini göstermektedir. O.Waever tarafından ilk kez 1995 senesinde ifade edilen güvenlikleştirme anlayışı Kopenhag Okulu gibi bazı ekollerin araştırmalarına esas oluşturmuştur. Teori inşacı bir esasa sahip olup güvenlik kavramını "söz edim-*speech act*" olarak görmektedir. Kuram kapsamında güvenlik konuları söz edimler yüzünden güvenlik tehdidi olarak inşa edilmekte ve bu şekilde inşa edilen tehditlere yönelik olağandışı tedbirlerin kullanılması meşru olmaktadır. Yönetenler olağandışı tedbirleri yürürlüğe koymak istedikleri

hususları güvenlik sorunu şeklinde ortaya koymak vasıtasıyla alınacak tedbirleri meşrulaştırma yöntemini tercih edebilmektedir (Baysal ve Lüleci, 2015: 63)

Güvenlikleştirme kavramı siyasi alandan, güvenliğe (devlet) doğru ilerlemekte (Buzan, Waever ve Wilde, 1998:23) olup "referans nesneleri-*referent objects*", "güvenlikleştiren aktörler-*securitizing actors*" ve "işlevsel aktörler-*functional actors*" olmak üzere değişik birimleri ihtiva etmektedir. "Referans nesneleri" devlet, kimlik, grup gibi varoluşsal olarak tehdide maruz kaldığı ön görülen bir kavramdır. Hükümet üyeleri ve komutalar gibi güvenlikleştirici oyuncular bir hususu güvenlikleştirmek maksadıyla söz edimi yapan kişilerdir. Oyuncular genel ilkeler, organizasyonel yapılar ve geniş kitleler üstünden yola çıkarak ana hedeflerini gizleyebilmektedir. (Buzan, Waever ve Wilde, 1998:36).

Güvenlikleştirme; bir hususun referans nesneye ilişkin olarak "varoluşsal bir tehdit" olarak belirtilmesi ve hedef topluluğun güvenlikleştirici oyuncu tarafından ikna edilmesi aşamalarını içermektedir. Hedef topluluk halktan, bürokratlara, komutanlardan siyasetçilere kadar değişiklik gösterebilmektedir (Collins, 2005:569).

2.2.1.1. Kopenhag Okulu

1990 senesinde güvenliğe farklı yönler ilave ederek genişleten ve derinleştiren Kopenhag Okulu teorisyenleri; güvenlik konusunda öznel bir fikir sistematiği oluşturmuştur (Sandıklı ve Emeklier, 2011:44). Kopenhag yaklaşımı güvenliği daha geniş bir çerçevede ele alarak; "devletin ve toplumların tehditlerden kurtulma anlayışları, rakip güçlere karşı bağımsız kimliklerini ve işlevsel bütünlüklerini koruma yetenekleri" olarak ifade etmektedir (Çomak ve Sancaktar, 2011:33). Bu ifade ile güvenliğin tahlil birimi olarak toplum ele alınmaktadır. Güvenliğin değişim süreci dikkate alındığında ulus devlet seviyesinde kendini gösteren analiz toplum ve müteakiben birey olarak genişletilmektedir. Güvenlikteki bu değişim çok taraflılığı esas alan bir yapıyı zaruri kılmaktadır.

Bu anlayışla beraber güvenlik konusunda yeni kavramsallaşmalar kendini göstermiştir. Kopenhag ekolünün Uluslararası İlişkiler bağlamında ehemmiyetli bir pozisyona sahip olan "güvenlikleştirme" kavramının kazanımına destek sağladığı ifade

edilmektedir. Ekolün lider kuramcılarından Barry Buzan güvenlikleştirmeyi somut ve objektif olarak ele almaktadır (Aydın vd., 2012).

Ekolün öncü teorisyenlerinden O.Weaver güvenlikleştirmeyi "güvenlik uygulamalarının yeniden üretilmesine yarayan meseleleri veya alanları güvenlik sorunu haline getirmek için siyasi elitler tarafından oluşturulan söylem eylemi (*Speech Act*)" şeklinde belirtmektedir (Kolasi, 2014:136). Güvenlikleştirmeyle birlikte bu ekol "güvenlik dışılaştırma-*desecuritization*" kavramına odaklanmaktadır. Güvenlik dışılaştırma ile "daha önce tehdit olarak kabul edilen şeyin artık tehdit olarak kabul edilmemesi durumu" ele alınmaktadır (Miş, 2011:349).

Okula göre bu durumda güvenlikleştirme negatif nitelendirilerek konularda "güvenlik dışılaştırma" nın zarureti ele alınmaktadır (Miş, 2011:351). Soğuk Savaş süreci güvenlik dışılaştırma konusuna iyi bir misal teşkil etmektedir. Bu süreçte kullanılan pek çok güvenlikleştirme söylemi hâlihazırda tehdit olarak görülmektedir. (Çomak ve Sancaktar, 2011:34).

Okulun literatüre başka bir katkısı ise güvenliğin çok boyutlu bir kapsamda değerlendirilmesini temin etmek olarak bilinmektedir. Bu çerçevede Buzan'ın "Security on New Framework for Analysis" adındaki araştırmasında güvenlik kavramının içeriği; (1) askeri, (2) siyasi, (3) ekonomik, (4) toplumsal ve (5) çevresel olacak şekilde beş boyutla genişletilmiştir (Kalkan Küçüksolak, 2018).

2.2.1.2. Paris Okulu

Didier Bigo ve Espeth Guild'in kaleme aldığı "Sınırların Kontrolü: Avrupa'ya ve Avrupa'da Serbest Dolaşım-*Controlling Frontiers: Free Movement into and within Europe*)" isimli araştırma ile ilk olarak gündeme gelmiştir. Bu çalışma güvenlik kapsamında Paris Okulu anlayışının teorisine bir çerçeve çizmiş ve kuruluşuna temel oluşturmuştur. Benzer şekilde J.Huysmans da "*The Politics of Insecurity: Fear Migration and Asylum in the EU*" isimli araştırmasıyla bu anlayışın içinde bulunmuştur.

Kopenhag Okulu'nda konular "dil-söylem" vasıtasıyla güvenlik meselesine dönüşmektedir. Farklı oyuncuları veya meseleleri bir grubu tehdit eder duruma getiren söylem, güvenlikleştirmeye zemin oluşturan ana unsurdur. Bu manada Kopenhag

Okulu'nun söylemlerini kısıtlı gören Bigo ve Paris Okulu bu hususlardan esinlenerek güvenliğin sıradan uygulamalar vasıtasıyla değişik mesele ve alanlara tatbik edildiğini gündeme getirmiştir. Risk ve tehditlere yönelik tedbir alınmasını, yalnızca belirli söylemlere istinat ettirmemiştir. Paris Okulu güvenlikleştirme araştırmalarında, güvenlik ve güvenliksizlikle alakalı manalandırmalara ve bu manalandırmaların oluşturduğu şartlara ve uygulamalara yönlenmesi gerektiğinin üzerinde durmuştur (McDonald, 2008b:568-570).

Güvenlikleştirmenin yalnızca söylem seviyesine düşürülmesi, bu kapsamda Paris Okulu'nun, önemli olduğunu değerlendirdiği politik ve sosyal şartların ve bu şartlarla alakalı eylemlerin esas alınmadığı durumlar kısıtlı bir görüşe tekabül etmektedir. Paris Okulu güvenlik konusunda kimlik ve benzeri kavramların meydana getirdiği şartlara ehemmiyet vermektedir (McDonald, 2008b:571).

D.Bigo'ya göre, güvenlikleştirme fiilini sadece söylemin oluşturduğu acil uygulamalar çerçevesinde ele almamak gerekmektedir. Bu yaklaşım, söylem vasıtasıyla güvenliksizleştirme fiilini uygulamanın çok zor olduğunu ve bunun için teknik kabiliyetlerin yanında, riskin tarifine ve neyin tehdit oluşturduğuna yönelik "ortak" bir görüşün resmi güvenlik unsurları tarafından tanımlanması gerektiğini ifade etmektedir (Bigo, 2006:385).

Bu yaklaşım, esas olarak güvenlik konusunu sosyal bir yapı olarak ele almaktadır. Paris Okulu, iç ve dış güvenlik hudutlarını yok saymakta, güvenlik alanı olarak ikisini de içermektedir. Soğuk Savaşın bitmesi ve Avrupa Birliği'nin kurulmasıyla birlikte milli hudutların önemini kaybetmesi, bu ayrımın kıymetini yitirmesine sebep olmuştur. Ayrıca, organize suç örgütleri hudutları aşmış, suç ve suçun kaynağı değişik ülkelerde bulunmaya başlamıştır. Bu durumda kolluk kuvvetleri hudutlara takılmış ve silahlı kuvvetler ise Soğuk Savaşın sona ermesiyle beraber, sınır ötesi harekâtlar için meşru sebepler bulmaya başlamışlardır (Bigo, 2001:93).

Okulun güvenliğe ilişkin fikirleri, "Öteki" kavramı ile alakalıdır. Öteki kavramı, halkın faaliyetleri ya da yönetim uygulamaları sonucunda dışlanan toplulukları da ihtiva etmektedir. Bigo'nun vurguladığı gibi, "güvenlik, öteki grupların üzerinde istenmeyen yan etkiler yaratabilmektedir" (Bigo, 2000:174). Bu düşünce Okulun, ortaya koyduğu

kapsamın odağında yer almaktadır. AB içerisindeki öteki toplulukları göçmenler meydana getirmektedir. Halktaki en ciddi endişe, göçmenlerin, kendilerinin bağlı olduğu yargı ve dinamiklere göçmenlerin zarar verme ihtimalleridir (Huysmans, 2006:100). Paris Okulu anlayışıysa ülke üzerinde kontrollerini kaybedeceklerinden endişe eden siyasetçilerin ve kendi geleceklerine dair endişeler taşıyan bireylerin oluşturduğu bir "gerçeklik" bulunduğu iddiasını taşımaktadır (Bigo, 2002:65).

Paris Okulu, güvenlik kavramının ne şekilde ve hangi amaçlarla kendini gösterdiğini sorgulamaktadır. Güvenliksiz, halkın terörizm ve küreselleşmenin sonucunda göstermiş olduğu reaksiyonlar neticesinde meydana gelmektedir. Farklı coğrafyalardaki değişik yorumlar, toplumun hayat sürdüğü ortamın her geçen gün yaşanamayacak derecede güvensiz bir duruma geldiğini vurgulamaktadır. Artan korku, güvensizliği ve normal olarak güvenliği hep ilk sırada tutmaktadır (Bigo, 2002:63).

Paris Okuluna göre iç ve dış biçiminde, klasik manada analiz edilen güvenliğin sınırları da farklılaşmıştır. Bu noktada göç ve göçmen konusu, netlik kazandırılması gereken hususların başında gelmektedir. Bu okulun güvenlik anlayışı, güvenlikle alakalı farklı anlayışlar bilinmesine rağmen bunların niçin geri planda kaldığını incelemekte, ele almaktadır. Siyaset alanında ve günlük yaşamda, ışıltısı fazla olmayan konular gündeme getirilmemektedir. Tüm kurum/ kuruluşların, yoğunlukta olarak da toplumda etkin grupların senelerce suçun odağını işsizlik ve göç üstüne inşa ettiklerinin altını çizmektedir. Bu unsurlar, güvenliksizle işsizlik-göç arasındaki münasebetten hareketle bir gerçeklik oluşturmaktadır. Bu kapsamda güvenliğin ne olduğunu ve tehdidin tanımını devlet belirlemektedir (Bigo, 2002:65).

2.2.2 Çevreleme Teorisi

ABD teoriyi Soğuk Savaş boyunca Sovyetler Birliği'ne yönelik olarak uzun dönemli olarak uygulamıştır. Bu açıdan, coğrafyalara ve dönemin anlayışına göre birçok değişik dış politika vasıtasının farklı oranda ve senkronize bir biçimde kullanılması ve iki süper güç arasındaki rekabetin harbe varmadan ABD'nin üstünlüğü ile neticelenmesi dikkate alındığında, tatbik edilen dış politika yöntemleri içinde kayda değer bir örnek teşkil etmektedir. Çevreleme; zararlı bir şey veya kişinin kontrol edilmesi,

kısıtlandırılması veya harbe sebep olmadan bir diğer devletin politik kuvvetinin belli sınırlar içerisinde tutulması olarak ifade edilmektedir.

Çevreleme kavramı, 2. Dünya Savaşı'nın ardından dünya sisteminin tekrar teşkil edilmesi hususunda, yoğunlukla Avrupa ve Ortadoğu'da, Sovyetler Birliği'nin elde ettiği konum ve kuvveti kullanmaması maksadıyla ABD tarafından ileri sürülen dış politika stratejisi olarak ele alınmaktadır (Rearden, 2012: 69-70). Bahse konu terimin ABD Dışişleri Bakanlığı'nda görev yapan George Frost Kennan tarafından ortaya atıldığı belirtilmektedir. Kennan, Sovyetler Birliği'nin askeri ve politik olarak uzun vadeli çevrelenmesi konusu ilk olarak 1946 senesinde bahsetmiştir (Gaddis, 2005: 4).

Başaran (2010), N.Spykman'ın kenar kuşak teorisinin temelini oluşturduğu çevreleme teorisini; "bir devletin, hayatiyet atfettiği ulusal çıkarlarının dost olmayan başka bir güç tarafından ele geçirilme ya da etki alanına alınma tehdidi altına girmesi durumunda, bu tehdidi, gerekli gördüğü bir aracı kullanarak ortadan kaldırmak amacıyla izlediği politikadır." biçiminde açıklamaktadır. Bu açıklamaya, tehdidin tesirinin genişlemesini sınırlandırarak, hedef ülkedeki yönetimin beklenen hareketlere yönlendirilmesi ve sonucunda iktisadi ve(ya) politik sistemindeki sorunlar, verimsiz organizasyon biçimi sebebiyle hedef ülke rejiminin kendiliğinden tesirsiz duruma getirilmesini temin eden dış politika stratejisi şeklinde ilaveler de yapılmaktadır (Başaran, 2010:7).

Çevrelemede, ABD'nin adımları, Sovyetler Birliği'nin İç Hilal'den kuşatılması ve bu şekilde kenar-kuşak ülkelerde komünizm rejiminin ortadan kaldırılması üstüne kurgulanmıştır. Fakat İç Hilal'de İran, Irak, Türkiye ve Pakistan'da ABD hava üslerinin tesisine karşın, Arap devletleri bu yapılanmaya katılmaya razı olmamışlardır (Emeklier ve Ergül, 2010:70).

George Frost Kennan 1946'da ABD Harp Akademisi'nde "Sovyetler Birliğinde İç Politik Güç Yapılanması" konulu ders esnasında da: *"ABD izleyeceği politikalarla, Rusya'nın uluslararası toplumun bir üyesi olarak davranışlarında ve dış politikasında öyle ikna edici ve şaşmaz model davranışlar yaratmalıdır ki, bu davranışlar en sonunda Sovyet sisteminin kalbine doğru kendi yolunu açıp hem bu ülkenin hem de Birleşmiş Milletler'in (BM) güvenlik çıkarlarıyla uyumlu değişikliklere neden olacaktır*" demiştir.

Bu konuşmasıyla, çevreleme teorisinin nihai amacının düşman devletin iç siyasal yapısında farklılıklar oluşturmak suretiyle, bahse konu ülkenin kendiliğinden uluslararası sistemin veya başat oyuncunun hedeflediği dış politikaları izlemesi olduğunu ifade etmiştir (Harlow ve Maerz, 1991: 38).

ABD'nin 2.Dünya Savaşı ardından yürüttüğü çevreleme politikasının ve ittifak oluşturma eğilimlerinin kenar kuşak kuramıyla ahenk içinde olduğu ifade edilmektedir. Bu açıdan NATO-CENTO ve SEATO gibi paktlar vasıtasıyla mihver bölge bütünüyle sarılmıştır (Davutoğlu, 2011: 105). Kennan'ın ABD'nin ulusal bağımsızlığı ve üstünlüğünün sürmesi maksadıyla ABD'ye yakın yönetimlerin olmasını bir zaruret olarak ele aldığı bölgelerde kenar kuşak olarak belirttiği alanla büyük ölçüde benzerlik göstermektedir (Gaddis, 2005: 29).

2.2.3. Gündem Belirleme Teorisi

İletişim konusundaki araştırmalar, 1960'lı senelerde davranış ve etki unsurlarına önem vermiştir. Bu dönemdeki çalışmalarda yoğunluklu olarak 1970'lerde televizyonun yaşamın bir parçası olmasıyla birlikte iletişim vasıtalarının halk ve kişi üzerinde kuvvetleri tesirleri olduğu yönündeki düşünceler kendini göstermiştir. Bu çalışmalarda esas olan öngörü medyanın fonksiyonunun yalnızca bilgi paylaşmak olmadığı bunun yanında politik karar verme ve bu kararları karşı tarafa kabul ettirme esnasında ana oyunculardan birini oluşturduğu hakikatidir (Keskin, 2012:2).

Bu dönemdeki etki esaslı araştırmaların ilk sıralarında McCombs ve Shaw tarafından 1972 senesinde ortaya konulan "Gündem Belirleme Teorisi" gelmektedir. Teoriye göre, iletişim vasıtaları kişilerin neyi düşüneceğini değil, hangi konuda düşüneceğini belirlemekte ve bu hususu da olayları sunuş şekliyle temin etmektedir (Lilleker, 2013:37). Bununla beraber teorinin özünde Walter Lippman'ın 1922 senesinde yazdığı "Public Opinion-Kamuoyu" adlı araştırması teorinin özünü oluşturmaktadır. Lippman, kişilerin etrafındaki görüntülerle kendi reel hayatı arasında bir irtibata gereksinim hissettiğini ifade etmektedir. Çalışmalarında iletişim vasıtalarının kişinin etrafındaki hakikatler ile düşüncelerindeki değişik görüntüleri meydana getirdiğini belirtmektedir (Hawks, 2002:492).

Lippman'ın çalışmalarından hareketle iletişim vasıtalarının, kişinin düşüncelerini yönlendirdiği iddia edilmektedir. Dünya da olanlar hakkında bireyleri haberdar etme misyonunu üstlenen iletişim vasıtalarının, aynı şekilde toplumun da ajandasını tespit ettiği düşüncesini odağa koyan teoridir. İletişim vasıtalarının tüm bireyleri alakadar eden problemler hakkında toplumu aydınlatması ve bu problemlere yönelik konuların da kamu önünde bir ehemmiyetinin olması düşüncesini merkeze almıştır. İletişim vasıtalarının haberleri servis ediş şekilleriyle (haberin boyutu, süresi, bulunduğu sayfa, servis edildiği zaman periyodu vb.), bazı hususlara önem verip, bazı konuları hızlı geçerek toplumun ajandasını tespit ettiği fikrine dayanmaktadır (Işık, 2014: 82).

Kuram, medya ve siyaset arasındaki bağlantıyı bu müesseselerin ajandalarındaki başlıklar kapsamında kıymetlendirerek, her iki müessesenin birbirlerine tesirini tespit etmeye gayret etmektedir. Teoriye göre: bireyler iletişim vasıtalarının alakadar olduğu konuları bilmek ve farklı vakalara gösterdikleri önem seviyesini kabullenme güdüsü göstermektedir (Terkan, 2007: 563).

McCombs ve Shaw, bireylerin yani toplumun iletişim vasıtaları ile öğrendikleri bilgileri kıymetlendirip vaka veya konuların kamuoyundaki ehemmiyetine ilişkin bir düşünce elde ederek kendi ilgi alanlarını meydana getirdikleri varsayımında bulunmaktadır (Güngör, 2011: 98). Demokrasilerde kamuoyunun rahat bir biçimde meydana getirildiği belirtilmekle birlikte baskıcı yönetimlerde ise bir biçimde yönlendirildiği ifade edilmektedir (Yüksel, 2007: 575).

İKİNCİ BÖLÜM

GÜVENLİK ALGISINDAKİ DEĞİŞİM

1. SOĞUK SAVAŞ DÖNEMİ GÜVENLİK ALGISI

1.1. İki Kutupluluk

Bu dönemin jeopolitiği; farklı ideolojilere sahip olsalar da Almanlara yönelik müttefiklik anlayışı içerisinde hareket eden ve neticede galip gelen ABD ve Sovyetler Birliği ekseninde oluşmuştur. ABD'nin bu dönemdeki dış siyasetinin ana hedefi, savaşın bitiminde oluşturulan coğrafi hudutlar içinde Sovyetler Birliği etkisinin ve kuvvetinin denetim altında tutulması biçiminde ele alınmıştır (Sempa, 2002: 67).

Bu dönemin politika üreticileri "çevreleme teorisi", "domino teorisi" ve "güç dengesi düzeni" gibi çok farklı kavramları ve teorileri literatüre kazandırmıştır. Yaşanan gelişmeler Mackinder'in Kara Hâkimiyet Teorisinin bu dönemde ehemmiyetli bir rolü bulunduğunu göstermektedir (Cohen, 2009: 28).

Sovyetler Birliği ve ABD zamanın jeopolitik durumunu teorik çerçevede ortaya koyan iki ülke olarak karşımıza çıkmaktadır. ABD iktisadi ve siyasi düşüncelerini kitlelere kabul ettirmeye gayret etmiş, bu yaklaşımın sonuca ulaşması ise tehdit faktörü olarak karşı tarafın mevcudiyetine bağımlı olarak kendini göstermiştir (Agnew, 2003: 102).

Soğuk Savaş döneminin genellikle ABD tarafından ortaya atılan kuramlar kapsamında biçimlenmesine karşın Sovyetler Birliği'nin de sosyalist dünyaya hükmetme ve komünist bir sistem meydana getirmeyi amaçlayan "Brejnev Doktrini" gibi anlayışları söz konusu olmuştur. Bu süreçte ABD tarafından uygulanan doktrinler Sovyetler Birliği'nin yayılmasının engellenerek çevrelenmesi anlayışını esas almıştır. Bu politikalardan öne çıkanlar "Truman Doktrini", "Marshall Planı" ve "Eisenhower Doktrini" çerçevesinde uygulanan çevreleme teorisi ile iki zıt kutbun ilişkilerini ilerletme çabaları yani "yumuşama-*detent*" süreci ile kendini gösteren Kissinger politikalarıdır (Balcı, 2016:111).

İki kutup arasındaki uyuşmazlıklar müttefik olmalarına rağmen daha İkinci Dünya Savaşı'nın bitmesinden hemen önce kendini göstermeye başlamıştır. Bu uyuşmazlıkların ana sebeplerinden birisi de büyük ideolojik anlayış farklılıklarından kaynaklanmıştır. İkinci Dünya Savaşı'nın sona ermesine yakın bir dönemde, Roosevelt'in yerine geçen Truman'ın Başkanlığı döneminde, ABD'nin Sovyetler Birliği ile ilişkileri ideolojik farklılıklar nedeniyle bozulmaya başlamıştır. ABD demokrasiyi ve pazar ekonomisini benimserken, Sovyetler Birliği ise baskıcı, totaliter bir anlayışla komünizmi desteklemiştir. Diğer yandan, iki kutbun özellikle Asya ve Avrupa'daki menfaat çatışmaları kutuplaşmayı daha da keskin hale getirmiştir (Miller Center of Public Affairs, 2015).

ABD'nin Truman doktrinini hayata geçirmesi ile beraber Soğuk Savaş'ın zımnen ilan edildiği kabul edilmektedir. Truman bu süreçte ABD dış siyasetinin temel düşüncelerini (History İnternet Adresi, 2019):

- Sovyetlerin komünizmin merkezi olduğu,

- Komünizmin icra ettiği faaliyetlerle ve fiili işgaller yoluyla genişlemeye çalıştığı,

- Bu taarruzlardan ülkeleri muhafaza etmek için ülkelere iktisadi ve askeri destek verilmesinin zaruri olduğu şeklinde ifade etmiştir.

Truman Doktrininin meydana getirilmesinde ciddi emeği bulunan George F. Kennan bir makalesinde; "*Sovyetler Birliği'ne karşı Amerikan politikasının uzun dönemli, sabırlı, fakat sert ve uyanık olması gerektiğini ve Rus yayılmacı eğilimlerinin çevreleme politikasıyla engellenmesi gerektiğini*" belirtmiştir (Kennan, 2003:63). Dünya düzeninin iki kutupluluk üzerine oturtulması, nükleer silahların fazlalaşması, iki farklı güçlü ve birbirine karşıt görüşün egemenlik kavgası vb. yaşanan gelişmeler, çevreleme politikasının odağına oturtulmuştur (Ikenberry, 2001:172).

Bu dönemde Sovyetler Birliği açısından öne çıkan en önemli gelişme 1968 yılında Leonid Brejnev tarafından açıklanan ve kendi ismi ile anılan "Brejnev Doktrini"dir. Brejnev, görüşlerini şu ifadelerle açıklamıştır (Armaoğlu, 2010: 688):

"Gayet iyi bilinmektedir ki, sosyalizmi inşa etmenin ortak tabii kanunları vardır ve bu kanunlardan sapma, sosyalizmden sapma neticesini verir. Sosyalizme karşı olan iç ve dış kuvvetler, belirli bir sosyalist ülkenin gelişmelerini, kapitalist sistemin tesisi yönüne döndürmeye çalışırsa, bir ülkede sosyalizme yönelik bir tehlike çıkarsa, bu aynı zamanda bir bütün olarak sosyalist milletler topluluğunun güvenliğine de yönelik bir tehlike olacaktır. Böyle bir durum, sadece o ülkenin değil, bütün sosyalist ülkeleri ilgilendiren ortak bir sorun haline gelir".

Brejnev Doktrini'nde öne çıkan ana faktör komünizme yönelik herhangi bir tehdit hissedilmesi durumunda savaş da dâhil bütün tedbirlerin alınmasına vurgu yapmasıdır. Zaten Çekoslovakya ve Afganistan müdahaleleri de bu çerçevede ele alınmıştır.

Fransızcadan geçen *detente* sözcüğü gerilimlerin azaltılması manasına gelmekle birlikte ABD Sovyetler Birliği ilişkileri açısından ayrı bir öneme sahiptir. Yumuşama-*detente* süreci 1971 yılında ABD Başkanı Nixon ile başlatılmış olup bu süreçte Dışişleri Bakanı Kissenger'ın düşünceleri öne çıkmıştır. Bu dönemde yıllarca izlenen politikalardan farklı olarak diyaloga ve işbirliğine daha açık bir tavır sergilenmiştir (Sezenler, 2009: 164).

Bu süreç genel olarak değerlendirildiğinde, iki kutuplu düzen içerisinde ABD ve Sovyetler Birliği bir güç mücadelesi içinde dünyayı kendi tesir bölgelerine göre ayırmış ve bu bölgeler iki ülke arasında da kabul görmüştür. Ancak, iki kutuplu düzende menfaatlerin geliştirilmesi ve tesir alanının arttırılması istenen yerlerde ciddi karşılaşmalar ve restleşmeler kendini göstermiştir. Buna rağmen mücadeleler genellikle iki ülkenin etkisinde bulunan ülkeler arasında yaşanmış ve doğrudan iki büyük güç arasında çatışma noktasına gelmemiştir.

1.2. Devlet Merkezli Algılama

İkinci Dünya Savaşı'nı müteakip Sovyetler Birliği ile ABD önderliğindeki iki kutup arasındaki mücadele esnasında güvenlik paradigması genel olarak realist çerçevede belirlenmiştir. İki kutuplu düzenin sürdüğü 1990 senesine kadar olan süreçte pek çok ülke tarafından esas alınan bu anlayışın ana özelliği de devlet odaklı, askeri güvenliği esas alan ve gücün arttırılmasını ön planda tutan bir felsefeye sahip olmasıdır (Baldwin, 1995:120).

Bu dönemdeki güvenlik anlayışında devletler uluslararası arenada ana oyuncular olarak karşımıza çıkmaktadır. Tarihi süreç içerisinde her çeşit oluşumun üstesinden gelen devlet kavramı, kişilerin siyasi organizasyonlarının odağında konumlanmıştır. Devlet kavramından daha önce gelen bir makam, karar mekanizması bulunmadığı gibi siyasi bağlılığın özünü oluşturabilecek ayrı bir oluşum da bulunmamaktadır. Bu nedenle kişiler ve belli kitleler gibi devlet harici oyuncuları alakadar eden hususlar ikincil derece önem arz etmekte ve alt başlık olarak ele alınmaktadır (Snyder, 2004:59).

Devletlerin tavırlarına şekil veren ana olgu açısından bazı realist kuramcılar "insan doğasına" ve bunu belirleyen ana husus olarak da "doğa durumuna" vurgu yapmıştır. Burada bireylerin tamamını belli bir çerçevede birlikte tutacak genel bir kanun bulunmamaktadır. Bu kapsamda, bireyler arasında devamlı şiddet yönelimi ve hayatını kaybetme hissi hüküm sürdüğü, tüm bireylerin kuvveti ve imkânları çerçevesinde hayatta kalabilmek maksadıyla her şeyi yapabileceği devamlı ve genel bir harp ortamı bulunmaktadır. Bu sebeple herkes hayatını muhafaza etmek, emniyet ve güvenliğini tesis etmek mecburiyetindedir (Hobbes, 2008:63-64).

Neorealist anlayış açısından da devletleri asıl sınırlayan husus uluslararası düzenin anarşik durumu, diğer bir ifadeyle oyuncular arasında üst otoriteden yoksun bir sistemdir. Karar verici üst bir otoritenin bulunmadığı yalnızca siyasi bakımdan aynı sayılan oyuncular tarafından belirlenen uluslararası düzende bir devletin pozisyonu sahip olduğu kuvvetle direkt olarak ilişkilidir. Bu düzende öne çıkan milli menfaatlerin elde edilmesi ve varlığın devam ettirilmesi diğer bir deyişle güvenliktir (Waltz, 1979:88-89).

Netice itibari ile Soğuk Savaş döneminin ana yaklaşımı realizm, realizmin sonucu olarak da bu dönemin başat oyuncuları devletler ve devletlerin hareketlerine yön veren kavramda güvenliktir. Bu kapsamda güvenlik kavramının var oluş nedeni olarak ifade edilebilecek tehdit anlayışı diğer devletler nezdinde yapılmaktadır. Sonuç olarak iç problemlerle karşılaşılsa da bunlar tehdit olarak nitelendirilmemekte ve bu sebeple tehdit olgusunun ana unsurunu hudutların ötesi oluşturmaktadır (Krahmann, 2005:10-11).

Soğuk Savaş döneminde realizmin getirdiği devlet odaklı algılamada tehdit unsuru tabiatı gereği askeri mahiyettedir. Nitekim kişilerin vefatı gibi ülkelerin ortadan kalkmasına sebep olan bu şekilde gelecekte elde edilebilecek diğer bütün kazanımları yok

eden unsur şiddettir. Asıl tehdit unsuru dışarısı olduğu için bekaya karşı oluşturulabilecek en büyük tehdit de diğer ülkelerin askeri güçlerinden kaynaklanmaktadır. Bu felsefe ile Soğuk Savaş döneminde özellikle ABD ve Sovyetler Birliği tarafından güvenliğin sağlanması için müthiş bir silahlanma yarışına girilmiş, her iki ülkede kaynaklarının ciddi bir bölümünü askeri güce ayırmıştır (Erdoğan, 2013: 268).

Bu dönemde devlet merkezli yaklaşımda, her ne kadar askeri gücün elde edilmesinde ve devamlılığın sağlanmasında iktisadi ve politik vb. farklı unsurlarda konu edilse de hiçbirisi son noktada güvenliğin tesis edilmesinde askeri imkân ve kabiliyetler kadar ehemmiyetli olmamıştır (Carr, 2001:102).

1.3. İdeolojik Rekabet

İkinci Dünya Savaşı ardından yaşanan süreçte, bir tarafta ABD'nin öncülüğünü yaptığı kapitalizm ile diğer tarafta Sovyetler Birliği'nin öncülüğünü yaptığı komünizm olacak şekilde iki farklı ideolojinin yarıştığı, mücadele ettiği bir düzen kendini göstermiştir. Sermaye ve emek konusunda iki farklı ideolojide yaşanan mücadele Soğuk Savaş'ın sona ermesine kadar olan süreçte uluslararası gündemi ciddi şekilde meşgul etmiştir (Ingulstad, 2014:2). Molla iki ideoloji arasındaki rekabeti şu şekilde ifade etmiştir (Molla, 2008:5-6):

"Özgürlüğe kavuşturulmuş, refah düzeyi yükseltilmiş aynı zamanda güvenliği sağlanmış bir Avrupa'nın nasıl oluşturulacağı konusunda ABD ve SSCB arasındaki farklı dünya görüşü ve bu sırada yaşanan gelişmeleri algılama biçimi bu rekabetin temel nedenini oluşturmuştur".

Bu süreçte iki farklı ideoloji pek çok zeminde mücadele etmiş, çok farklı olayda karşı karşıya gelmiş ve birçok kez de çatışmanın kenarından dönülmüştür. Diğer yandan, bu süreçte bu iki ideolojinin temsilcisinin rekabetinin dışında kalarak örgütlenen ve 1955 yılında ortaya çıkan "Bağlantısızlar" bloğu da uluslararası arenada kendini göstermiştir. Gelişmekte olan ülkelerin oluşturduğu bu üçüncü bloğun temel felsefesinde mücadele halinde bulunan ideolojik bloklara girilmemesi yatmaktadır. Bu üçüncü blok iç mücadeleleri sebebiyle organizasyonel bir ittifak meydana getiremese de dünyadaki

pozisyonu itibari ile önem arz etmiştir. Bu hareketin en ciddi kazanımı Batı Bloğuyla gelişim ve refah sorunlarının münazara edilmesi olmuştur (Şahin, 2015:72).

Batı demokrasileri, BM'nin oluşturulması için politik zemini tesis etmiş, kurumun ana prensipleri, meydana gelecek olayların barışçıl yollarla halledilmesine aracılık etmek şeklinde belirlenmiştir. 24 Ekim 1945 günü BM yasası geçerlilik kazanarak, yeni düzende BM, arabulucu rol ile üçüncü bir felaketin daha yaşanmaması adına sorumluluk almıştır (https://www.un.org/en/about-un/, 2019).

Sovyetler Birliği ise 1946 yılında, Balkanlar ve Orta Doğu coğrafyasında etkisini giderek daha da fazla göstermiş, bu durum ABD liderliğindeki batı demokrasisinde endişeye yol açmıştır. Sovyetler Birliği 1945-1948 seneleri arasında Doğu Avrupa'da sözde "halk demokrasileri" ismiyle göstermelik yönetimleri kullanmıştır. Bu kapsamda komünizm ilk hâkimiyetini Yugoslavya ve Arnavutluk'ta elde etmiş, müteakiben de Romanya ile Bulgaristan Sovyetler Birliği'ne tabi kılınarak 1948 yılında Prag müdahalesiyle (Doğan, 2005:72) "Demir Perde" meydana getirilmiştir (Jelavich, 2009:304).

Komünizm 'in bu ilerleyişi batı demokrasilerinde ciddi kaygılar yaratmış, güvenlik algılarında endişe meydana getirmiş ve bu dönemde iki ideoloji arasındaki mücadelenin her an bir çatışmaya dönüşme ihtimali uluslararası gündemi sürekli meşgul etmiştir. İki farklı ideolojinin meydana getirdiği bloklaşma 1949 yılında NATO'nun, 1955 yılında da Varşova Paktı'nın kurulması ile somut olarak tamamlanmıştır (Kongar, 2006:179).

2. SOĞUK SAVAŞ SONRASI DÖNEM GÜVENLİK ALGISI

2.1. Soğuk Savaş Sonrası (1990-2001)

Soğuk Savaşın sona ermesi ile bir dönüm noktası yaşanmış ve komünist rejim altındaki ülkelerde halk hareketleri görülmeye başlamıştır. Soğuk Savaş döneminde öne çıkan kavramlar yaşanan bu gelişmelerle beraber çok farklı bir boyuta evirilmiştir. Sovyetler Birliği'nde görülen bu dönüşümün temelinde Batı Bloğu ile yürütülen

mücadelede rekabet gücünün kaybedilmesi ve ekonomik anlamda yaşanan sorunlar bulunmaktadır (Brzezinski, 2000: 64).

Değişim süreci ile beraber uluslararası arenada Doğu Bloğu ile olan münasebetlerde pozitif gelişmeler yaşanmış; rekabet zemini yerini işbirliğini daha çok ön plana çıkaran bir diyalog atmosferine bırakmıştır (NATO El Kitabı, 2006:69). Diğer yandan, Sovyetler Birliği'nde yaşanan bu değişim rüzgârı birçok farklı problemi ve şiddet olaylarını da beraberinde getirmiştir. Kısıtlı imkânlar ve birçok Doğu Bloğu ülkesinde merkezi ekonomiden demokrasiye ve kapitalizme geçilmesi esnasında yaşanan güçlükler bir araya gelerek öngörülemez, karmaşık ve sürekli değişime ihtiyaç gösteren bir ortamı meydana getirmiştir (Erdoğdu, 2004:128).

Reform süreci Sovyetler Birliği'nin 1991 yılında yıkılması ile neticelenmiştir. Bu süreç uluslararası camia açısından da referans noktası olmuştur. Soğuk Savaş'ın bitmesi ile güvenlik çevrelerinde de ciddi değişimler yaşanmıştır. Yaşanan bu değişimin temelinde güç dengesinde yaşanan farklılaşma yer almıştır. Soğuk Savaş'ın sona ermesinin ardından uluslararası platformda pozitif hava kendini göstermiş olup bunun özünde uluslararası düzenin farklı bir sürece girmesi, uluslararası mekanizmaların kurularak küresel seviyede barış, istikrar, huzur ve güvenliğin sağlanabileceği ihtimali yer almıştır. Ancak, yaşanan gelişmeler ışığında bu iyimser tablonun ötesinde farklı risk ve tehditler uluslararası istikrar ve güvenliği tehdit etmeye başlamış, zaman içerisinde özellikle teknoloji alanında yaşanan gelişmelerle birlikte güvenlik olgusu iç içe girmiş çok farklı unsurları içeren, tahmin edilemeyen ve farklı bir yapı arz etmiştir (Slaughter, 2000:112).

Soğuk Savaş'ın ardından yaşanan süreci belirtmek maksadıyla kullanılan kavramlardan birisi de "Yeni Dünya Düzenidir". Bu kavramın mahiyeti tam olarak açık bir şekilde belirtilmese de dünya çapında emniyet ve güvenliğin sağlanabileceği ve iktisadi kalkınmanın tesis edilebileceği bir sisteme vurgu yapıldığı kabul edilmektedir. Meydana gelen bu düzende açık bir şekilde ortaya çıkan husus ABD'nin tek küresel güç olarak "dünyanın jandarması" rolüne bürünmeye çalışmasıdır (Carpenter, 1992:24).

ABD'nin yeni sistemdeki bu jandarma rolüne yönelik karşıt fikirler de ortaya atılmıştır. ABD tek küresel güç olarak uluslararası düzeni idare etmeye çalışsa dahi ikincil

aktörlerin bu duruma tesir edeceği ve ABD'nin adımlarını dengeleyecek şekilde hareket edeceği biçimindeki düşünceler bu öngörüye karşı ortaya atılan tezlerdir. Diğer yandan, güç dengesinin değişmesi ile ortaya çıkan düzendeki problemler, riskler ve tehditler küresel güç olsa dahi bir devletin üstesinden gelemeyeceği kadar karmaşık ve zorludur (Carpenter, 1992:24).

Sovyetler Birliği'nin dağılması sonrası süreçte uluslararası düzenin ve güvenliğin sağlanmasına ilişkin negatif düşünceler de ortaya atılmıştır. Bu kapsamda uluslararası düzenin geleceğine ilişkin farklı bir anlayış da gerçekte uluslararası düzenin kontrol dışı bir aşamadan geçtiğidir (Rubinstein, 1991:54). Bu anlayışa göre uluslararası düzenin tek bir ülke ya da kurum/kuruluş tarafından kolaylıkla yönlendirilmesi mümkün değildir. Bu düşüncelerin en önemli temsilcilerinden biri James N. Rosenau'dur. James N. Rosenau uluslararası düzenin bir karmaşa içinde olduğu ve karmaşık yapısından dolayı ileride seyredeceği durumun tahmininin kolay olmadığı fikrini ortaya atmıştır. James N. Rosenau'ya göre uluslararası düzen değişkenleri tarihte görülmediği kadar büyük ve köklü değişimler yaşamaktadır (Rosenau, 1990:9-10).

Yeni süreç, Soğuk Savaş'tan zaferle çıkan Batı Bloğu ülkelerinin siyasetlerinde de farklılıklara sebep olmuştur. Ortak düşmanın yok olmasının ardından farklı güvenlik yönelimlerine kaydıkları ve birbiri ile ilişkisi olmayan bağımsız politikaları esas almaya başladıkları ifade edilebilmektedir.

Soğuk Savaş sürecinin ardından çok uluslu firmalar ve sivil toplum kuruluşları uluslararası arenada daha serbest faaliyet gösterme imkânı bulmuştur. Bu dönemde uluslararası düzende söz konusu ülke ve devlet dışı oyuncu mevcudunda artış yaşanmıştır. Uluslararası arenada oyuncu sayısının artması, yeni sistemde güvenlik problemlerinin daha karmaşık bir yapı arz etmesi nedenlerinden birini oluşturmuştur. Bu süreçte güvenlik yaklaşımları farklılaşmaya başlamış, tehdit ve risk algıları değişerek kavramları değerlendirme biçimi değişmeye başlamıştır. Soğuk Savaş'ın ardından güvenlik kavramının mahiyeti değişmiş ve boyutları genişlemiştir. Eski sistemde tehdit olarak değerlendirilen bazı hususlar bu yapılarını kaybetmiş, bunların yerlerini küreselleşme ve teknolojik ilerlemeler nedeniyle çok farklı kavramlar ve sorunlar almıştır. Ekoloji, bulaşıcı hastalıklar, düzensiz göç, deniz haydutluğu, insan hakları, terörizm, insan

kaçakçılığı, uyuşturucu, silah kaçakçılığı, yeni teknolojiler ve siber güvenlik gibi çok farklı ve yeni problemler kendini göstermeye başlamıştır (Koçer, 2004:110).

Yeni dönemde ABD, dünyadaki konumunu ve kuvvetini korumak maksadıyla küresel ve coğrafyalara göre bölgesel stratejiler uygulamaya başlamıştır. ABD-Sovyetler Birliği'nin oluşturduğu çift kutuplu yapı yerine farklı ve çeşitli unsurların bulunduğu çok taraflı yeni bir dönem kendini göstermiştir. Farklı bir piyasa ekonomisi, demokrasi anlayışı, küresel değerler ve diplomasiyle beraber farklı askeri konseptler, stratejiler ve müttefiklik ilişkileri uluslararası arenada kendini göstermiştir (Gürlesen ve Demir, 2002:12).

Bu değişim sürecinde klasik savaş yöntemleri ve harp alanlarının yapısı farklılaşmış, kısa zamanda neticeye ulaştırılmasının mümkün olmadığı bu mücadelelerde klasik olmayan yöntem, metot ve vasıtalardan istifade edilmiştir (Kuloğlu, 2003:44). Bu karmaşık yapı içerisinde güvenlik paradigmasının manası genişlerken, tehdit merkezleri ve anlayışı belirginliğini kaybederek daha muğlak belirsiz bir duruma dönüşmüştür (Koçer, 2004:112).

Bu sürecin ardından uluslararası düzeni ve güvenlik anlayışını değerlendirirken dikkate alınması gereken ehemmiyetli bir husus da uluslararası düzende kendini gösteren bütünleşme ve ayrışma olmak üzere iki farklı eğilimdir. Bütünleşmenin görüldüğü konu küreselleşmenin de etkisiyle bölgesel birleşme eğilimleridir. Hudutların belirsizleştiği ve küresel problemlere yönelik müşterek çözümlerin dikkate alındığı bir düzene ilişkin istekler kendini göstermiştir. Diğer yandan, uluslararası düzende ayrışma çabaları da kendini göstermiştir. Etnik, mezhepsel ve dinsel kimliklerin muhafaza edilmesi bu dönemde problem alanı olarak kendini göstermiştir (Pekcan, 2007:15).

2.2. 11 Eylül 2001 Terör Saldırıları (2001-2018)

Küreselleşmenin hızlı bir şekilde yaşandığı bir dönemde 11 Eylül 2001 terör saldırılarının karşımıza çıkması ile birlikte uluslararası düzen ciddi bir dönüm noktası yaşamıştır. Terörizm yaklaşımından uluslararası düzene, risk ve tehdit algılamalarına kadar çok farklı konuda köklü değişimler yaşanmaya başlamış, asimetrik tehdit gibi çok farklı kavramlar güvenlik literatürüne girmiştir. Sebep ve neticeleri halen daha farklı

boyutlar da tartışılmaya devam eden bu olay ABD'nin gördüğü en etkili terör saldırısı olarak yerini almıştır. Bu olayı bu kadar önemli ve etkili yapan husus verdiği zarardan öte hedefin mahiyetinden kaynaklanmaktadır. Dünya Ticaret Merkezi'ne yapılan bu terörist eylemle küresel çapta iktisadi düzenin sembolü olan kurum ortadan kaldırılmıştır. Bu terörist saldırıyı bu kadar önemli yapan diğer bir konu da Soğuk Savaş sürecinin ardından görülen en büyük silahlı eylem olması ve tek küresel güç ABD'ye yönelik olarak gerçekleştirilmiş olmasıdır (Haser, 2018:44). Yaşanan olayın ardından George W. Bush "teröristlerin Amerika'ya açtığı bir savaş olduğunu, bu savaşa cevap vereceğini, bunları kimin yaptığını bulacağını ve adalete teslim edeceğini" ifade etmiştir. Bu açıklama ile tek küresel güç olan ABD tarafından başta EL Kaide olmak üzere terörizme ve teröristlere karşı açıkça harp ilan edilmiştir (Halatçı, 2006:89).

Terörist faaliyetler çok farklı alanlarda daha önceden de yaşanmış olmasına rağmen terörizm, ikiz kulelerin yıkılması ile beraber güvenlikleştirilen bir husus olarak karşımıza çıkmıştır. Bu tarihten itibaren terörizm küresel bir güvenlik problemi olarak uluslararası arenanın ajandasında ilk sıralardaki yerini almıştır. Bush yaptığı konuşmalarda Soğuk Savaş'ın ardından kendini gösteren yeni düşmanı "küresel terör" olarak hedefe koymuştur (Buzan, 1991:119).

Bu kapsamda terör kavramı devletlerin, uluslararası kurum/kuruluşların, stratejilerin ve üretilen politikaların en önemli başlıklarından biri olarak yerini almaya başlamış, terörizmle mücadele kapsamında askeri harekâtların yapılabileceği, bu konuda gerekirse yalnız hareket edilebileceği ve demokratik anlayışı tüm dünyada egemen kılmak için çaba gösterileceği ifade edilmiştir (Halatçı, 2006:97).

İkiz kulelere karşı düzenlenen bu saldırılar neticesinde terörizm ABD güvenlik yaklaşımının yeni oyuncusu olarak kendini göstermiştir. İkiz kuleler ile beraber ulus devlet kavramı tartışılmaya başlanmış, terörizm nedeniyle bu yaklaşımın tekrar biçimlendirilmesi ve manalandırılması çalışmalarına girişilmiştir. ABD'nin kendi menfaatlerine dokunmadığı sürece yaşanan olaylara karşı çıkmasını esas alan düşünce, yaşanan olayla beraber dışa açılımı esas alacak biçimde değişime uğramıştır. Milli güvenliğin tesis edilmesinin küresel terörizm nedeniyle yalnızca ülke politikaları ile değil, diğer devletlerin kendi ülkelerinde yürüttüğü stratejilerle de bağlantılı olduğu ortaya çıkmıştır. ABD tarafından Afganistan ve Irak müdahaleleri bu değişim ve anlayış

sonucu yapılmış, güvenliğin sınırların çok ilerisinden itibaren tesis edilmesi ihtiyacı çerçevesinde hareket edilmiştir (Karabulut, 2015:258).

İkiz kulelere yönelik yaşananlar asimetrik tehdit kavramı ile beraber çok farklı yeni güvenlik risk ve tehditleri gün yüzüne çıkarmış, terörizmin sebep olduğu güvenlik yaklaşımına doğru değişim yaşanmıştır. Bu sebeple saldırı büyük bir güvenlikleştirme periyoduna girilmesine neden olmuştur. Güvenlik kavramının tüm ülkeleri tesir altına alan bir problem olması sebebiyle, tüm oyuncular müşterek menfaat çevresinde bir araya gelerek müşterek güvenlik anlayışı meydana getirilmeye gayret gösterilmiştir (Haser, 2018:44).

3. YENİ GÜVENLİK ANLAYIŞININ BELİRLEYİCİ UNSURLARI

3.1. Küreselleşme Olgusu

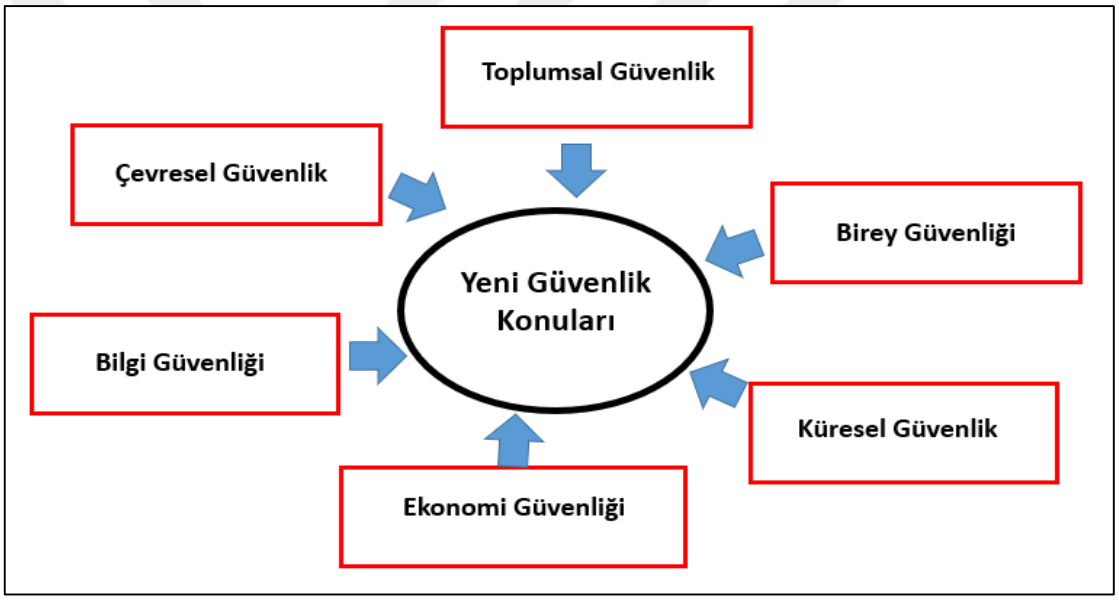
Küreselleşme olgusu üzerinde fikir birliğinin sağlandığı bir husus olarak karşımıza çıkmasa da değişim ve dönüşüm konusundaki tesirleri küreselleşmenin kabul gören en ehemmiyetli iki karakteristiği olarak karşımıza çıkmaktadır. Bu kapsamda küreselleşme yeni bir kavram olmamakla beraber özellikle Soğuk Savaş'ın sona ermesinin ardından etkisini ciddi manada göstermiş politika, iktisat ve güvenlik alanlarında devrim niteliğinde dönüşümlerin yaşanmasına sebep olmuştur (Erdoğan, 2013: 66).

Sovyetler Birliği'nin dağılmasının ardından küreselleşmenin neredeyse her konuda meydana getirdiği bu değişim rüzgârı neticesinde tehdit ve risk değerlendirmeleri farklılaşmış, çeşitlenmiş ve güvenlik anlayışının boyutları genişlemiştir. Güvenliğin genişlemesi askeri konulara ek olarak iktisadi, sosyolojik, ekolojik, siyasal, teknolojik vb. konuların da bu kavrama eklenmesi manasına gelmiştir. Diğer yandan, genişleme süreci Soğuk Savaş döneminde güvenlikte esas olan devlet kavramının ötesinde kişilerin, kitlelerin ve devlet dışı aktörlerin de güvenlik konusunda tahlil edilmesi gereken kavramlar olarak kendini göstermesine sebep olmuştur (Paris, 2001:97).

Güvenlik yaklaşımlarında kendini gösteren dönüşümün en temel nedenlerinden biri, risk ve tehdidin geleneksel pozisyonunun ötesine geçerek çok yönlü ve asimetrik bir

duruma gelmesidir. Yeni Dünya düzeni içerisinde özellikle teknolojik gelişmelerle beraber kendini gösteren yeni güvenlik ortamındaki risk ve tehditlerin biçiminin, yerinin, kaynağının, zamanının, boyutunun ve etkilerinin öngörülebilmesi neredeyse imkânsız hale gelmiş ve yeni düzende mücadele tüm dünyayı kapsayacak şekilde genişlemiştir (Genelkurmay Başkanlığı, 2007).

Yaşanan gelişmelerle beraber yeni güvenlik ortamına ilişkin birçok çalışma yapılmış ve yapılan bu çalışmalarda farklı tanımlamalarla güvenlik alanları ortaya konulmaya çalışılmıştır. Örneğin Harald Müller tarafından yapılan araştırmada yeni güvenlik konuları Şekil 10'da sunulan alanlara ayrılmıştır. Yapılan farklı çalışmalarda bu alanlara yenileri eklenmiş ya da daraltılmıştır (Müller, 2005:369).



Şekil 10. Yeni Güvenlik Konuları

Kaynak: (Müller, 2005:369)

Bu araştırmacılardan aşırı küreselleşmeci ekolü esas alanlar küreselleşmenin dünyayı daha güvenli ve emniyetli bir hale dönüştüreceğini iddia etmektedirler. Bu ekolde, küreselleşen ülkelerin problemleri barışçıl yöntemlerle sonuca ulaştıracağı ileri sürülmüştür. Nitekim bu ülkeler ekonomik münasebetleri zora sokabilecek gelişmelere engel olmaya çalışacaktır. Diğer bir ifade ile ekonomi başat aktör olacaktır (Bilgin, 2005b:178). Zamanla ekonominin başat aktör olacağı konusundaki aşır küreselleşmecilerin fikirleri haklı çıksa da bu durum güvenlik problemlerini engellemek şöyle dursun aksine körüklemiştir. Robert C. Johansen "mütekabiliyet", "eşitlik",

"sürdürülebilir çevre", "demokratikleşme" ve "silahsızlanma" olmak üzere toplam beş ilkenin uygulamaya geçirilmesi durumunda küresel güvenliğin tesis edilebileceğini ifade etmiştir (Johansen,1994:377). Bu konudaki en güncel örneği ise ABD'nin nükleer çalışmalar konusunda İran'a yaptırımlar uygularken kendi nükleer gücünün azaltılması hususunda bir şeyler yapmaması teşkil etmektedir.

3.2. Uluslararası Ekonomi

Ekonomik güvenlik diğer güvenlik çeşitleri ile ciddi bir bağlantı içerisindedir. Bunun en önemli sebebi ekonomik güvenliğin kişilerin yaşamsal gereksinimlerinden ülkelerin varlıklarına kadar büyük ve geniş perspektifte bir konu olmasıdır. Bu kavramın küresel çerçevede yapılmış bir tanımı bulunmamakla birlikte yoğunluklu olarak uluslararası ve milli anlamda mekanizmaların düzgün çalıştığı şartlar güvenli addedilmiştir (Buzan, Waver, ve Wilde, 1997: 7).

Ekonomi genel olarak mal ve hizmetlerin üretimi, tüketiciye ulaştırılması, değişimi ve ihtiyaçların giderilmesiyle alakalı faaliyetleri ihtiva etmektedir. Ekonominin güvenlikleştirilmesi kavramı ise açıklamada belirtilen sirkülasyonun sürekliliğini kapsamaktadır (Mesjasz, 2012: 241).

Hâlihazırda ekonominin uluslararası bir konumda bulunması sorunların, krizlerin sınırlarını da o seviyede genişlemiştir. Bu kavramın bütün dünyaya tesir eden neticeleri güvenlik seviyesinde de ayrışmalara gidilmesine neden olmuştur. Bu konuda güvenlik ulusal, uluslararası düzey ve devlet dışı oyuncuların (kurum/kuruluş/şirket/kişi) güvenliği biçiminde ayrım göstermektedir (Mesjasz, 2012: 242).

Ekonomik vasıtaların askeri yöntemlerin yerine ya da tamamlayıcı bir unsuru şeklinde kullanılması uluslararası ekonomi münasebetlerinin bir boyutunu meydana getirmiştir. Uluslararası ekonomik tedbirleri, hedef devlet/devletleri tedbiri hayata geçiren devletler bakımından istenen bir pozisyon veya tutuma sevk etmek maksadıyla bazı hususlardan yoksun bırakmak ya da mükâfatlandırmak şeklinde ifade etmek mümkündür (Sönmezoğlu, 2005:387).

Hâlihazırda uluslararası ekonomi anlayışı ve bu kapsamda alınan tedbirler ülkelerin önemli bir dış politika vasıtası olarak kullanılmaktadır. Özellikle küreselleşen

dünya düzeni içerisinde sermaye de küreselleşmiş ve ekonomi uluslararası bir boyuta evirilmiştir. Uluslararası ekonomi tedbirleri ceza amaçlı ya da ödüllendirici bir mahiyette olabilmekte, bu husus hem uluslararası ilişkileri hem de güvenlik durumunu etkileyebilmektedir. Uluslararası ekonominin dış politika vasıtası olarak kullanılması yakın zamanda sıklıkla karşımıza çıkan "ekonomik savaş" kavramından farklılık arz etmektedir. Ekonomik savaş, fiili bir çatışmadan ziyade şiddet barındırmayan ve muhasımın ekonomik gücünü olumsuz etkilerken kendi veya müttefikinin ekonomik gücünü arttırmaya ilişkin rekabeti tanımlamaktadır (Arı, 2008:410).

Ekonomik imkânların dış politika vasıtası şeklinde kullanımındaki istenen hedef, karşı tarafın ekonomisine doğrudan zarar vermekten öte, muhasım ülkenin politik olarak beklenen şekilde tavırlar sergilemeye yönlendirilmesidir. Bu durum, askeri kuvvet kullanımı yerine uluslararası ekonomik güçten kaynaklanan vasıtalardan istifade etmek suretiyle hayata geçirilmektedir.

Ekonominin uluslararası münasebetlerde ciddi şekilde güç elde etmesi, bu kavramın ülkelerin dış politikalarında diğer ülkeleri tesir altına alma ve yönlendirme vasıtası şeklinde kullanılmasını mümkün kılması neticesini doğurmuştur (Arı, 2008:346).

3.3. Bilgi ve İletişim Teknolojileri Devrimi

Günümüzde insanlık tarihinde görülmemiş bir süratte değişim ve dönüşüm yaşanmakta, teknoloji alanında yaşanan ilerlemeler her gün farklı bir yeniliği insanlığın hizmetine sunmaktadır. Bilgi ve iletişim teknolojilerinde kendini gösteren yenilikler yaşamın her alanında kullanılmaya başlamıştır. Özellikle internet kullanımının yaygınlaşması ile çok farklı ve yeni kavramlar hayatımıza girmiş, yeni iş imkânları kendini göstermiş ve çoğu konuda klasik yöntemler değişime uğramıştır. İnternet kullanımı küreselleşmeye ayrı bir boyut katarken, iletişim imkânlarını baş döndüren bir sürate ulaştırmış ve çok farklı bir dünya düzeninin kapılarını aralamıştır (Peker, 2010:7).

Bilgi ve iletişim teknolojilerinde kendini gösteren bu baş döndürücü sürati Bill Gates "Eğer Volkswagen firması son 25 yıl içinde bilgisayar sektörü kadar hızlı gelişmiş olsaydı bugün 500 dolara alacağımız arabalara 25 dolarlık benzin koyup dünya turu atmamız mümkün olacaktı." şeklinde ifade etmiştir (Özcan, 2010:3).

Bilişim konularında yaşanan ilerlemelerde esas unsuru "bilgi" oluşturmakta ve tüm üretim faktörlerinin önüne geçirmektedir (Koçak, 2004:1). Bilgi yüzyılı her çeşit bilginin dijital ortama aktarılmasını, yazılabilmesini ve dağıtılmasını mümkün kılan teknolojilerin gelişimini işaret etmektedir. Bilgi yaşadığı bu değişim ile fiziksel kısıtlamalardan kurtulmuştur. Elektronik iletişim şebeke ve altyapıları, verilerin kolayca farklı yerlere aktarılmasını sağlayan sanal ağlar ve internetin bahse konu teknolojilerin başat aktörleri olduğu açık bir gerçektir (Ünver, Canbay ve Mirzaoğlu, 2009:1).

Kemaloğlu (2010) kamu hizmetlerinden finans sektörüne, savunma sanayiinden sağlık sektörüne kadar hayatın her alanında kendini gösteren bu yeniliklerin bireylerin, devletlerin ve uluslararası sistemin güvenliği başta olmak üzere birçok konuya ilişkin muhtemel sonuçlarını şu şekilde özetlemiştir:

"Teknolojik gelişmelerle ilerlediğini sayan 'tarih anlayışının' sonu geliyor. Teknolojiye bağışlamadığınız etik değeri, düşmanınızdan talep edemiyorsunuz. Araçsallaşan teknolojinin temel kullanım amaçları, karlılık, tahakküm, kitleselleştirme ve kontrol oldu. Elektronik alandaki sıçramaların arkasında militarizmin kapitalizmle olan tarihi işbirliği duruyordu. Savaşlar da 'teknoloji tarihine' eşzamanlı dönüşüme uğradılar. Uygarlığın aşamalarına savaş sektörünün modernleşme aşamaları karşılık gelir. Ve sonunda bilişim ve enformasyon teknolojileriyle 'küresel köy' olan dünyamız şimdi daha tekinsiz. Günümüz 'siber savaşlar' zamanı. Bilgi çağı metafiziğiyle yüceltilen siber âlem, bir e-bomba ile alaşağı edilebilir savunmasızlıkta. Küresel düzeyde bilgi işlem ve iletişim altyapısı çökertebilir ve kişisel bilgisayarlar kullanılamaz hale gelebilir. Web sayfalarının ele geçirilmesi, hizmet dışı bırakma, enerji, iletişim, finans, güvenlik ve askeri sistemlerinin kontrolü ya da etkisizleştirme, kritik ve gizli bilgilere erişim siber saldırının hedeflerinde yer alıyor."

Yapılan değerlendirmelerden de açıkça anlaşılacağı üzere bilgi ve iletişim teknolojilerine endekslenen altyapı ve ağların her geçen gün fazlalaşması, siber ortamın tüm sektörleri içine çekmesi birçok güvenlik problemlerini, risk ve tehditleri de yanında getirmektedir (Peker, 2010:9).

Bilgi ve iletişim teknolojilerine olan bağımlılık ve siber uzayın siber saldırganların hedeflerini hayata geçirebilecekleri birçok zafiyete sahip olması, ülkelerin, bireylerin,

kitlelerin, kurum/kuruluşların, firmaların, uluslararası sistemin diğer bir ifadeyle tüm dünyanın sosyo-kültürel, siyasi, iktisadi ve askeri güvenliğini tehdit eden bir faktör oluşturmaktadır. Bu tehditlerin büyüklüğü, önemi ve yaşatabileceği problemler, bu zorluklarla mücadele edebilecek hususları ön plana çıkarmıştır (Ünver, Canbay ve Mirzaoğlu, 2009:1).

3.4. Sayıları ve Etkinliği Artan Devlet Dışı Aktörler

3.4.1. Bireyler

Modern güvenlik yaklaşımlarının temel özelliği, geleneksel anlayışta odak noktasına konan devletin yerini bireyin almasıdır. Bu anlayışta kişilerin güvenliğinin tesis edilerek muhafaza edilmesi devletin ana vazifesi olarak ele alınmaktadır. Birey güvenliği, kişilere yönelik risk ve tehditlerin tespit edilmesi, bunlardan korunması ve maruz kalındığında ise negatif tesirlerinin bertaraf edilmesi ya da asgari seviyeye çekilmesi biçiminde belirtilmektedir. Kişi güvenliği, bireylerin ana insani gereksinimlerinin karşılanması ile temel hak ve özgürlüklerin muhafaza edilmesiyle ilişkili olarak değerlendirilmektedir. Bu sebeple birey güvenliğinin bütün alanları içerdiğini ifade etmek hatalı bir bakış açısı olmayacaktır (Arman, 2011:48).

Muhafaza edici bir güvenlik yaklaşımı olan birey güvenliği, ilk önce hayatın özünü oluşturan temel hak ve özgürlükleri muhafaza etmeyi odak olarak almaktadır. Kişiler için özgürlük esas unsurdur (Çoşkun, 2003:6). Ancak, maalesef hala daha günümüzde birey güvenliğinin çoğunlukla devletler tarafından çiğnenmesi olayları yaşanabilmektedir. İki unsur arasında ciddi kuvvet eşitsizliği olduğundan, kişilerin devlete ve devletin kolluk kuvvetleri de dâhil farklı mekanizmalarına karşı korunması özgürlüğün sağlanması açısından önem arz etmektedir (Aksu ve Turhan, 2012:72). Zira yakın zamanda öncelikle insan hakları ihlaller olmak üzere kişilerin özgürlüklerinin muhafaza edilmesi için uluslararası sistem tarafından atılan adımlar ve gerektiğinde yapılan müdahaleler kişi güvenliğine verilen önemin açık bir göstergesini oluşturmaktadır (Karabulut, 2015:140-141).

Birey güvenliği, temel hak ve özgürlüklerle beraber Maslow'un ihtiyaçlar hiyerarşisi piramidinde belirttiği, hayatını devam ettirme, barınma, yeme, içme gibi ana

gereksinimlerini ve bu hususlara ilişkin tehlike durumunda kişileri korumak ve bu tehditlerle beraber birey gereksinim ve isteklerini giderebilecek süreçleri oluşturmayı amaçlayan güvenlik çalışmalarını da kapsamaktadır (Arman, 2011:49).

Küreselleşen dünya düzeninin getirdiği cinsiyet ayrımcılığı, azınlıkların ve göçmenlerin korunması, ekolojik problemlere hassasiyet, bulaşıcı hastalıklarla savaş, terörizmle mücadele, siber güvenlik, dinsel ve mezhepsel farklılıklar gibi konular da birey güvenliği ile alakalı hususlarla yakından bağlantılıdır (Şener, 2019:15).

3.4.2. Hükümet Dışı Kuruluşlar

Uluslararası sistemde ülkelerin çok ciddi tesiri altında kalmadan oluşturulan ve çok farklı alanlarda faaliyetlerini icra eden birçok organizasyonun mevcudiyetinden söz edilmektedir. Salamon hükümet dışı kuruluşları 21. yüzyılın icadı olarak nitelenmektedir (Salamon, 1997: 60). Uluslararası arenada etkin olan hükümet dışı kuruluşlar hâlihazırda sosyo kültürel yapının da önemli aktörlerinden biri konumundadır. Günümüzde demokratik anlayışın devamının sağlanması ve güvenlik konularında sivil toplumun rolünün ve etkinliğinin sürdürülmesi büyük oranda hükümet dışı kuruluşların mevcudiyeti ile doğrudan ilişkilidir (Stewart, 1997: 28).

Çoğu konuda görüldüğü gibi hükümet dışı kuruluşlar kavramı üstünde de ortak bir düşünce birliğinin ve tanımın varlığından söz etmek mümkün değildir. En genel ifadesiyle Craplet tarafından yapılan tanıma göre hükümet dışı kuruluşlar kar hedefi bulunmayan özel organizasyonlardır (Craplet, 1997: 105). Bunun yanında hükümet dışı kuruluş kavramı çoğunlukla ülkelerin karşıtı ve kar hedefi olmamanın karşılığı şeklinde ifade edilmektedir (Fernando ve Heston, 1997:12). Bir başka şekilde belirtmek gerekirse, hükümet dışı kuruluşlar dendiğinde herhangi bir devlete bağlı olmadan ve kar maksadı bulunmadan faaliyetlerini icra eden organizasyonlar akla gelmektedir. Bu kapsamda hükümet dışı kuruluşlar toplumun örgütlenme gereksiniminin, dönüşümün ve daha iyi şartlara ulaşma arzusunun dışa vurulmasıdır (Smillie, 1997: 570).

Hükümet dışı kuruluş şeklinde belirtilen bu kavramların öne çıkan özelliklerinden biri direkt olarak halkla irtibat halinde olmaları ve devletlerle herhangi bir hiyerarşik, resmi ilişkilerinin olmamasıdır (Jones, 1991:542). Hükümet dışı kuruluşların kendilerini

göstermeleri ve süratle yaygınlaşmaları ile beraber devlet odaklı siyasal organizasyonlar yerini daha çok sivil toplum odaklı yaklaşımlara bırakmaya başlamıştır. Bu kapsamda günümüzde devletlerin bir unsuru olmayan sivil toplum kavramı tüm ülkelerde süratle yayılmakta ve genişlemektedir (Salamon ve Anheier, 1997:60).

Sivil toplum kavramı başlangıçta daha ziyade "daha iyi bir toplumsal düzene kavuşmak için bireyin hak ve yükümlülüklerini düzenleyen siyasi kurumlar" (Çaha, 1994: 52) manasında kullanılırken günümüzde ülkelerin organizasyonel ve fonksiyonel yapısı haricinde olan bir bölge anlaşılmaktadır. Bununla beraber, devlet ve sivil toplum farkı ile hangi hususların vurgulanmak istendiği çoğunlukla net değildir. En genel şekilde devletin organizasyonel, hukuksal ve fonksiyonel yapısının haricinde bulunan bölgenin sivil toplumu meydana getirdiği ifade edilmektedir (Baharçiçek, 2008:299).

Hükümet dışı kuruluşlar icra ettikleri çok farklı roller ve etkinlikler ile güvenliğe çeşitli boyutlarda katkı sağlamaktadır. Hükümet dışı kuruluşlar kamuoyu oluşturma, uluslararası hukuki mevzuatın meydana getirilmesine katkı sağlama, yargısal konulara iştirak, anlaşmazlıkların barışçıl çözümü, uluslararası kurum/kuruluşlara veri sağlama ve kuralların uygulanması ile gözlemlenmesi gibi çok geniş çerçevede icra ettiği farklı faaliyetler ile güvenliğe katkı sağlamaktadır. Bu kuruluşların odak noktasını genellikle insan oluşturmaktadır (Başlar, 2005: 87).

3.4.3. Çokuluslu Şirketler

Küreselleşmeyi süratlendiren ve süreçte etkin olan başat aktörlerdendir. Küreselciler arasında dahi çok uluslu şirketlerin tanımı konusunda farklılıklar bulunmaktadır (Bolat ve Seymen, 2005:53). Aşırı küreselciler çokuluslu şirketi, koşullarda oluşan değişikliklere bağlı olarak üretimi küresel boyutta değiştirebilen firmalar olarak tanımlamaktadır. Aşırı küreselciler ülke idarelerinin çok uluslu şirketlerin yatırım yapmaları için ciddi gayret gösterdiğini ve teşvik paketlerini gündeme getirdiklerini belirtmektedir. Şüpheciler ise bu şirketlerin en büyük ve yaygın örneklerinin dahi satışlarının ve sermayelerinin kendi ülkelerinde olduğunu ve bunların uluslararası kurallara tabi küresel çapta faaliyet gösteren yerli şirketler olduklarını iddia etmektedir. Bu şirketler özellikle İkinci Dünya Savaşı'nın ardından tüm dünyada süratle genişlemiş olup günümüzde dünyadaki neredeyse tüm ülkeler çokuluslu şirketlerle irtibat

içerisine girmiştir. Küresel ticaret hacminin üçte ikilik kısmını idare eden bu firmaların küresel sermaye piyasalarının gelişiminde ehemmiyetli bir rolü bulunmaktadır (Perraton vd., 2000:19).

Çokuluslu şirketlerin, dünyanın herhangi bir yerindeki ülkenin kaynaklarından istifade edebilmesi için, bunlara sahip olması gerekmemekte, fakat faaliyet gösterdikleri ülkede kanuni firmalarla müşterek faaliyet göstermeleri gerekmektedir. Bu husus dikkate alındığında çok uluslu şirketler birçok ülkedeki faaliyetleri koordine ve denetim gücüne haiz firmalar olarak ifade edilmektedir. En yaygın ve güçlü çok uluslu şirketler bile faaliyette bulundukları sınırlar içerisindeki ulusal hukuki düzenlemelere riayet etmek durumundadır. Şirketler faaliyet gösterdikleri yerlerin hukuki mevzuatından istifade etmeye gayret gösterirken, ülkedeki firmalarla koordine içerisinde hareket ederek tüketici eğilimlerine ilişkin bilgi elde etmektedir (Dicken, 2000:50).

Çokuluslu şirketler genel olarak, merkezi belli bir ülkede bulunmasına rağmen fonksiyonlarını bir ya da daha çok ülkede merkezin koordinesindeki şubeler veya bağlı küçük firmalar vasıtasıyla belli işletme politikaları çerçevesinde idare eden şirketler şeklinde tanımlanabilmektedir (Tokol, 2001).

Küreselleşmenin süratlenmesiyle beraber çokuluslu şirketlerin faaliyet gösterdikleri konular, organizasyon yapıları, idare yaklaşımları da değişikliğe uğramaya başlamıştır. Sınır kavramı belirsizleşerek ve hatta çoğu noktada ortadan kalkarak, farklı bir boyuta evirilerek, küresel çerçevede faaliyet gösterilmeye başlanmıştır. Küreselleşmenin bu şirketlerden farklı, bağımsız değerlendirilemeyeceği ve bu kavramın iktisadi boyutumda çok uluslu şirketlerin hayati önem arz ettiği müşahede edilmektedir (Kıvılcım, 2013:13).

Çokuluslu şirketler, küreselleşmenin süratlenmesiyle beraber ciddi şekilde öne çıkmış, faaliyette bulundukları konular ve finans sistemleri gelişme kaydetmiştir. Küreselleşmenin sağladığı esneklikler; (1) yüksek seviyedeki sermayenin çok uluslu şirketler vasıtasıyla dünyanın herhangi bir noktasına kolaylıkla gönderilebilmesi, (2) bu şirketlerin emeğin veya vergilerin daha uygun olduğu bölgelere geçebilmesi, (3) internet ve etkili süratli iletişim vasıtalarının fazlalaşması, (4) elektronik ticaret örneğindeki gibi farklı pazarlama yöntemlerinin yaygınlaşması şeklinde ifade edilebilmektedir.

Bahsedilen bu konulardan güçlü çok uluslu firmalar yoğun olarak istifade edebilmektedir (Katırcıoğlu, 2008:100).

Diğer taraftan, çokuluslu şirketlerin yönetim merkezlerinin, sahiplerinin, faaliyet gösterdikleri yerlerin çok farklı ve adında da ifade edildiği gibi çokuluslu olması bazı konularda avantaj/dezavantajlar ihtiva etmektedir. Ancak çokuluslu şirketler sahip olduğu sermaye ve ticaret hacmi dikkate alındığında özellikle ekonomi güvenliği konusunda ön plana çıkmakta ve kendini göstermektedir.

3.5. Uluslararası Sistemin Tek Kutuplu Yapısı

Tek kutuplu bir düzenden söz edebilmek için, imkân ve kabiliyetler ile güç bakımından uluslararası arenada yalnız bir hegamonik gücün bulunması gerekmektedir. Bu büyük güç, kendi tercih ve menfaatlerini diğer ülkelere uygulatma kabiliyetine haiz olmalı ve uluslararası siyaseti yönlendirebilmelidir. Ancak, tüm bu hususları yerine getirirken de diğer oyunculara bağımlı olmaması gerekmektedir. Sadece böyle bir ortamda tek kutuplu (*unipolar*) düzenden söz etmek mümkündür (Güneş, 2012:83).

Bir düzenin tek kutuplu olarak addedilebilmesi için; bir ülkenin, uluslararası arenada başat aktör pozisyonunda bulunması, kuvvetinden ve etkinliğinden istifade ile uluslararası münasebetleri idare edebilmesi gerekmektedir (Efegil ve Mustafaoğlu, 2009:4). Ülkelerarası problemlerin ve uluslararası anlaşmazlıkların çözümü konusunda düzende etkin olan kuvvet, diğer ülkelerin kendi menfaatleri ve tercihlerine hizmet edecek şekilde kararlar vermesini talep edebilmekte veya bunu zorlayabilmektedir (Aydın ve Bakıncak, 2016:98).

Soğuk Savaş sürecinin sona ermesi ile birlikte ABD uluslararası düzende tek küresel güç olarak kalmış ve ayrı bir pozisyona oturmuştur. ABD'nin pozisyonu sebebiyle bu düzen "tek kutuplu sistem" olarak ele alınmıştır (Worhlforth, 1999:5). Fakat tarihsel perspektiften değerlendirildiğinde uluslararası düzende hiçbir devlet uzun dönem düzene hâkim olamamış, sistemdeki diğer devletler ile aktörler tarafından dengelenmiştir (Aydın ve Bakıncak, 2016:98).

Tek kutuplu düzen başat aktörün gözetiminde hiyerarşik bir durum arz ettiğinden dolayı sistemde etkin devletin diğerleri ile ilişkisinde istikrarlı bir işleyiş söz konusudur.

Tek kutuplu sistemin belli bir düzen sağladığı açık olmakla beraber bu durum süratli bir şekilde değişebilmektedir (Uzer, 2013:72-82). Nitekim neo realist yaklaşıma göre uluslararası düzenin anarşik yapısı nedeniyle devletler varlıklarını devam ettirebilmek için başka bir devletin öne çıkması halinde onu dengeleyecektir (Waltz, 1993:75-76).

İki kutuplu düzenin sona ermesinden sonra ideolojik çatışmalar sona erse de dünya çatışmaların daha fazla yaşandığı ve istikrarsızlıkların arttığı bir hale gelmiştir (Dilan ve Kavuncu, 2015:946). Sovyetler Birliği'nin dağılmasının ardından uluslararası ve bölgesel çapta dinsel, mezhepsel, etnik çatışmalar ile başta asimetrik tehditler olmaz üzere farklı risk ve tehditler kendini göstermiştir. İki kutuplu düzende BMGK ajandasında bulunan çatışmalara on üç barış gücü askeri görevlendirmesi yapılırken, sadece 1988-1993 senelerinde bu rakam yirmi olmuştur. Rakamlardaki bu artış dahi istikrarsız ortamın ve çatışmaların arttığının en açık göstergesidir. Tek kutuplu sistem haricinde ortaya çıkan diğer iki düzen ise "çift kutupluluk" ve "çok kutupluluk "tur. (Yılmaz, 2011:92)

4. YENİ GÜVENLİK ANLAYIŞINA YÖNELİK TEHDİTLER

4.1 Uluslararası Terörizm

Terör, Latince "*terrere*" kelimesinden türetilmiş olup "korku vermek, yıldırmak, pes ettirmek ve dehşete düşürmek" manalarına gelmektedir (Başeren, 2006:7). TDK ise terörü "yıldırı", terörizmi "yıldırıcılık" şeklinde ifade etmiştir (Türk Dil Kurumu, 2019).

Terörizmin tanımına ilişkin birbirleri ile benzerlik arz eden veya birbirinden çok farklı hususları kapsayan tanımlamalara rastlamak mümkündür. ABD terörizmi "yerel gruplar veya gizli ajanlar tarafından muharip olmayan hedeflere karşı yapılan önceden tasarlanmış, siyasi olarak motive edilen şiddet" şeklinde tanımlamıştır (Kartal, 2018:46).

NATO tarafından yapılan tanımlamada ise terörizm, "kuvvet ya da şiddetin kanundışı şekilde politik, dinî, mezhepsel, ideolojik veya çıkar maksatlı hedefleri elde etmek amacıyla devletleri veya kitleleri zorlama veya korkutmaya çalışarak, kişilere ya da mallarına karşı kullanımı veya kullanma tehdididir (NATO, 2012).

Terörün sınırları aşması, uluslararası tesirler ve neticeler meydana getirmekte; bu durumda uluslararası terörizmin oluşmasına sebep olmaktadır (Gençtürk, 2012:3). Terör

bir ya da daha fazla ülkece desteklenirse, diğer bir ülkeyi ya da uluslararası kurum/kuruluşu etkilemek maksadıyla yapılırsa, uluslararası yasal mevzuatı hedef alan eylemler icra ederse, uluslararası barış, istikrar ve güvenlik ortamına risk ve tehdit meydana getirirse, uluslararası hale gelebilmektedir (Semercioğlu, 2016:100-101).

Günümüzde uluslararası terörizmle mücadele kapsamında ülkelerin imzaladığı 12 anlaşma bulunmakta olup 2001 senesinde BMGK'nin 1373 numaralı kararıyla bu anlaşmalar tüm ülkeler açısından zorunlu hale getirilmiştir.

Bazı araştırmacılar tarafından uluslararası terörizm "gözetilen hedef, gerçekleştirilen eylemler ve kaynakları itibariyle birden fazla devleti ilgilendiren ve uluslararası sonuçlar doğuran terörist faaliyetler" olarak belirtilmiştir (Semercioğlu, 2016:100). Uluslararası terör, aynı şekilde, anlaşmalar veya uluslararası teamül hukuku açısından kabul görmüş harp kuralları ve diplomasi yöntemlerinin ötesinde yapılan şiddet içerikli kampanya ve fiilleri de ihtiva edebilmektedir (Jenkins, 1974:2).

Yapılan değerlendirmeler neticesinde uluslararası terörizmi; sınırların ötesinde, failleri çokuluslu olan, icra edilen fiilleri iki ya da fazla ülkeyi etkileyen, oluşturduğu problemlerin iki ya da fazla ülkeyi alakadar ettiği, farklı ülkelerce desteklenen ve uluslararası kurum/kuruluşları, ülkeleri ve yasaları etkileyen terör eylemleri olarak ifade etmek mümkündür.

Günümüzde bazı ülkeler tarafından terör eylemleri ve terör grupları kendi amaçlarını elde etmek maksadıyla kullanılabilmektedir. Diğer yandan, şiddet eylemleri yaygınlaşmakta ve bazı durumlarda kimi terör grupları uluslararası arenada icraatlarını başarı olarak yansıtmaya gayret göstermektedir. Barış, güvenlik ve istikrar ortamına tehdit oluşturan terör grupları yaptıkları icraatları fakir, mazlum ve mağdur kişinin yaptığı icraatlar gibi yansıtmaya çalışarak destekçi ve kamuoyu toplamaya gayret etmektedir. Bu yönüyle terör daha da fazla yayılmaya ve genişlemeye başlamaktadır. Kendi milli çıkar ve menfaatleri adına terör gruplarından, örgütlerinden istifade eden bazı ülkeler terörü tırmandırarak farklı bir boyuta taşımaktadır (Çaşin, 2008:208).

Barışı tehdit eder hale gelen terör örgütleri, eylemlerini "fakir adamın" yaptığı eylemler olarak göstererek taraftar ve destek toplamaktadır. Bu açıdan

kıymetlendirildiğinde terörizm yayılmaya başlamıştır. Kendilerini korumak adına terör yöntemlerini kullanan devletler, terör sarmalını tırmandırmakta ve terörü daha da fazla küreselleştirmektedir. Uluslararası teröre tesir eden hususları (Kartal, 2018:54):

- Teknoloji alanında yaşanan baş döndürücü gelişmeler,
- Ekonomik sorunlar, iç problemler ve çatışmalar sonucunda yaşanan düzensiz göç faaliyetleri nedeniyle eleman devşirmekteki kolaylık,
- Siyasi ve politik koşullarda görülen değişim ve dönüşümler,
- Milli ve kişisel menfaatlerin elde edilmesi adına teröre destekte yaşanan artış,
- Küreselleşmenin de etkisiyle tüm dünyada sermaye hareketlerindeki kolaylık sonucunda terörün finansal gereksinimlerinin karşılanması şeklinde sıralamak mümkündür.

4.2 Kitle İmha Silahlarının Yayılması

Kitle İmha Silahları (KİS), kişilere, binalara ve diğer kaynaklara yüksek düzeyde ve büyük oranda tahribat yaratma ve hasar verme gücüne sahip silahlardır. Çok sayıdaki insanı ve yapıyı iş yapamaz duruma getirmek ve etkilemek üzere dizayn edilmiş kimyasal, nükleer, biyolojik ve radyolojik silahlar ve maddeler KİS olarak kabul edilmektedir (NATO, 2019: 135).

KİS kelimesi ilk kez 1937 yılında Almanların İspanya'yı uçaklarla bombalamasını konu edinen bir yazıda kullanılmıştır. BM, KİS ifadesini 1947 senesinden başlayarak günümüze kadar kullanmaktadır. BM'ye göre KİS, "atomik patlayıcı silahlar, radyoaktif materyal silahları, ölümcül kimyasal ve biyolojik silahlar ve gelecekte atom bombası ve yukarıda belirtilen silahlara benzer yıkıcılık gösteren tüm silahlar"dır (Dünya Sağlık Örgütü, 2004:10).

KİS, klasik silahların birçok kez kullanılması neticesinde meydana gelen zararın tamamının ve hatta daha fazlasının yalnızca bir kere kullanılması neticesinde ortaya çıkarabilen, bununla birlikte klasik silahların meydana getiremediği taarruz sonrası negatif tesirleri de olan silahlar şeklinde ifade edilebilmektedir (Özgür, 2006: 17).

Kimyasal, biyolojik ve nükleer silahlar ciddi zarar ve hasara sebep olmaktadır. Bu yöntemin tesirleri zaman ve mekân sınırlarını zorlamakta ve çatışmaların ardından dahi

tesirler kendini gösterebilmektedir. Bu silahların kullanımında öne çıkan diğer bir olumsuzluk da sivil ve askeri hedef ayrımının yapılamamasıdır. Bu yönü itibari ile silahlı çatışma hukuku açısından da sorun teşkil etmektedir (Fındık, 2012:11).

Yapılan tanımlar çerçevesinde KİS de kendi içinde nükleer, biyolojik, kimyasal silahlar şeklinde sınıflandırılabilmektedir. Zaten 2004 yılında alınan 1540 numaralı BMGK kararı ile KİS'in terörist gruplar başta olmak üzere devlet harici aktörlerce elde edilmesinin engellenmesi amaçlanmış olup bu kararda yalnızca biyolojik, kimyasal ve nükleer silahlar KİS kapsamında ifade edilmiştir (Denk, 2011: 97).

KİS'in üç farklı çeşidini de elinde bulunduran ülke sayısı sınırlıdır. Fakat Soğuk Savaş döneminde bazı ülkeler bu kabiliyeti elde etmiştir. Bu bağlamda uluslararası platformda KİS'e sahip olanlar ve olmayanlar şeklinde iki grup otomatik olarak kendini göstermektedir. Ülkelerin felakete yol açabilecek bu silahları elde etmeye çalışmasının sebebi çoğunlukla güvenlik mülahazalarına dayandırılmaktadır. Ancak, bu durum güvenliğin tesis edilmesi bir kenarda dursun mevcut güvenlik sorunlarına başkalarını da ilave etmektedir. (Özgür, 2006: 20).

KİS'lerin terör amaçlı olarak kullanılma olasılığı bu konuyu uluslararası güvenlik ajandasının üst sıralarına konulmasına neden olmuştur. KİS'lerin teröristlerce kullanılması insanları, şehirleri, deniz ulaştırma yollarını, limanları ve kargoları kısacası uluslararası güvenliği tehdit eden önemli bir problemdir.

4.3. Deniz Haydutluğu

Deniz trafik hatlarının yoğun olduğu bölgelerde ve otorite boşluğunun bulunduğu, kontrolün zayıf olduğu alanlarda karşılaşılan deniz haydutluğu faaliyetleri halk arasında yaygın olarak kullanılan korsanlık faaliyetlerinden farklılık arz etmektedir. Deniz haydutluğu ile özel gemilerle, diğer gemilerde bulunan mürettebat ya da mallara yönelik kişisel menfaat elde etmek için açık deniz alanlarında yapılan faaliyetler ifade edilmektedir. Korsanlık da ise bu durumdan farklı olarak devlet otoritesi ile devletten alınan yetki ile bu faaliyetler yapılmaktadır (Topal, 2010:107).

Korsanlık konusuna ilişkin ilk hukuki belge 1856 Paris Deklarasyonu olup bu faaliyetler yasaklanmıştır. Müteakiben 1889 Montevideo Sözleşmesi'nde korsanlık/deniz

haydutluğunun engellenmesinin insanlığın sorumluluğunda olduğu kabul edilmiştir. 1937 tarihli Nyon Anlaşması ise Akdeniz'de tanımlanamayan saldırıları deniz haydutluğu olarak nitelendirmiştir (Keyuan, 2009: 323).

Günümüzde deniz haydutları özellikle Somali sahilleri, Malakka Boğazı ve Nijerya Körfezi'nde yoğun olarak faaliyet göstermektedir. Modern deniz haydutluğu eylemlerindeki artış esasında 2003 yılında en üst seviyeye çıkmış ama rapor edilen saldırılarda 2006-2008 yılları arasında kayda değer bir artış gözlenmiştir. Yaşanan deniz haydutluğu faaliyetlerindeki artış deniz ulaştırmasını ve dolayısıyla dünya ekonomisini olumsuz etkilemiş ve konuyu uluslararası platformlarda ciddi şekilde gündeme getirmiştir. Deniz haydutluğunun artması ile birlikte deniz güveliğinin sağlanması maksadıyla ülkeler, uluslararası kurum/kuruluşlar tarafından bahse konu bölgelerde askeri gemilerle deniz güvenlik harekâtları icra edilmeye başlanmıştır (Doğru, 2017:559).

Uluslararası Deniz Ticaret Odası Denizcilik Bürosu (International Chamber of Commerce, International Maritime Bureau-IMB) istatistiklerine göre, 2006 senesinde 239 olarak rapor edilen deniz haydutluğu ve silahlı soygun rakamları, 2007 senesinde 263'e, 2011 senesinde ise 439'a çıkmıştır (Uluslararası Denizcilik Bürosu, 2012). Bu saldırıların çoğunluğunun deniz ulaştırma yollarının önemli geçitlerinde ve petrol zengini coğrafyalarda olması, deniz haydutluğunu küresel enerji güvenliğine bir tehdit durumuna sokmuştur. Bununla birlikte, icra edilen deniz güvenlik harekâtları ve alınan tedbirler sayesinde son IMB verilerine göre, deniz haydutluğu ve silahlı soygun eylemlerinde düşüş yaşanmış olup 2019 yılında toplam 149 olay meydana gelmiştir (Uluslararası Denizcilik Bürosu, 2019).

4.4. Düzensiz Göç ve Mülteci Hareketleri

Güvenlik ortamına risk ve tehdit oluşturan önemli problemlerden biri de düzensiz göç ve mülteci hareketleridir. Bazı araştırmalar küresel göç dalgalarını belirtmekte ve etkileri çok güçlü olduğu için 21. yüzyılın "Göç Çağı" olarak adlandırılması gerektiğini ifade etmektedir. Uluslararası Göç Örgütü'ne göre; göç "bir ya da bir grup insanın ya uluslararası bir sınırı geçerek ya da bir ülke içindeki hareketi" olarak tanımlanmaktadır (Uluslararası Göç Örgütü, 2019).

Uluslararası Göç Örgütü çalışmalarında gün geçtikçe düzensiz göçmen sayısında artış yaşandığı ve çeşitli sorunlar, çatışmalar sebebiyle meydana gelen bu durumun göç alan ülkelerde gerekli tedbirlerin alınmaması durumunda farklı problemlerin çıkmasına sebep olacağını belirtmektedir. Bu problemlerin ön sıralarında düzensiz göçmenlerin bir kısmının kayıt dışı olması yer almaktadır. Sisteme kaydedilmiş göçmenler, yaş ortalamalarının yüksek olduğu ülkelerde iş gücü sağlaması nedeniyle "belirlenmiş göçmen politikaları" çerçevesinde arzu edilen bir durum oluşturmaktadır. Fakat kayıt dışı bir göçmen nüfusunun bulunması kayıt dışı bir ekonomiye ve iç güvenlik sorunlarına sebep olmaktadır (Birdişli, 2014b:135). Düzensiz göç ve mülteci sorununun, gelecek dönemde daha da artması beklenmektedir. Mark Griffiths ve arkadaşları, insanları mülteci olmaya iten nedenlerin yakın gelecekte ortadan kalkmasının söz konusu olmadığını ifade etmektedir (Griffiths, O'Callaghan ve Roach, 2013:242).

Sonuç olarak, küresel güvenlik, kamu düzeni ve ülkelerin istikrarı için tehdit oluşturmasının yanında, düzensiz göç, uluslararası ve ikili ilişkileri kötü etkilemekte ve iç ve dış politikayı güçleştirmektedir. Düzensiz göçle mücadele konusunda hiçbir ülkenin tek başına üstesinden gelemeyeceği için kaynak, geçiş ve varış ülkelerinin hem kendi içlerinde hem de uluslararası kurum/kuruluşlarla koordinasyon ve işbirliği içinde olması durumları ön plana çıkmaktadır.

4.5. Çevre Güvenliği ve İklim Değişikliği

Çevre konusu, insanoğlunun tarımla beraber yerleşik düzene geçmesi ve sanayileşme olmak üzere iki büyük dönüşümü müteakip farklı etkilerle yüzleşmiş, bu yaşananlar çevreye de tesir ederek bazı kötü tecrübe ve bozulmalara sebep olmuştur (Ponting, 2012: 45, 321).

Sanayileşmede en büyük olumsuzlukları gören çevre konusu başlangıçta belirli bir süre dikkate alınmamış ancak, çevresel değişimlerin belli seviyelere ulaşarak fark edilmesiyle beraber ehemmiyeti anlaşılmaya başlanmıştır. Soğuk Savaş döneminin çift kutuplu dünya sisteminde askeri gücü ön planda tutan güvenlik anlayışı zamanla sorgulanmış ve çevresel güvenlik ile ekonomik güvenlik gibi kavramlar güvenlik alanı içerisine dâhil edilmiştir (Allenby, 2000: 9).

Çevresel güvenlik konusuna ilişkin başlangıçta yapılan değerlendirmelerde, askeri harekâtlar neticesinde hasar gören çevrenin düzeltilmesi, sosyal tahribatlara ve mücadelelere sebep olabilecek kıtlıkların, çevresel tahribatın ve biyolojik tehlikelerin düzeltilmesini ihtiva eden insan-çevre faktörleri esas alınmıştır. Ancak, yakın dönemde bu konuya ilişkin kıymetlendirmelerde ise sınırlar ortadan kaldırılarak, birey, iktisadi, sosyal ve çevresel refahı da içeren tüm hususlar dâhil çok boyutlu bir biçimde ele alınmaya başlanmıştır (Kirchner, 2015: 1).

Konu ile ilgili fikir birliğine varılmış bir tanımlamanın bulunmadığını ifade eden Barnett, konuyu daha iyi kavramak için "çevresel güvensizlik" kavramının ele alınmasının önemini vurgulamıştır. Çevresel güvensizlik, değişimlerin sebep olduğu negatif tesirlere karşı, insanların ve kitlelerin çaresizlik durumu şeklinde belirtilmektedir. Bu durum insanların ve kitlelerin değişimlere ayak uyduramadığı veya bu değişimlerden sakınamadığı şartlarda gerçekleşen bir durumdur. Bu sebeple çevresel güvenlik, kişinin değişimi engelleme ya da bu durumlara uyum gösterme imkânıdır (Barnett, 2007: 5).

Çevre konusunun sebep olduğu sorunlar uluslararası camia için de ciddi ehemmiyet arz eden bazı problemleri beraberinde getirmiştir. Bu konuda öne çıkan problemlerden biri çevresel kötü gidişatı engellemek/azaltmak maksadıyla veya değişimlere uyum sağlamak için hangi devletlerin rol alması gerektiği ile alakalıdır. Bir başka konu ise küresel çapta görünen çevresel değişimlerin ülkeler arasındaki adaletsizliği ne ölçüde şiddetlendireceği ile alakalıdır (Page, 2000: 33). Yapılan çalışmalarda genel olarak on bir çevresel güvenlik prensibi üzerinde durulmaktadır (Spillmann ve Bächler, 1995: 136):

- Tabii kaynakların paylaşımın adaleti,
- Çevresel manada verilen hasarın yasaklanması,
- Milli, bölgesel ve küresel hususlarla alakalı rutin bilgi teatisi ve işbirliği tesisi,
- Teknik, akademik ve bilimsel konularda işbirliği yapılması,
-Uluslararası bölgelerde görülen problemlerin üstesinden gelmede barışçıl metotların kullanılması,
- Çevre konusunda uluslararası seviyede sorumluluk üstlenilmesi,
- Devam edebilir bir kalkınmanın tesis edilmesi,

- Bireylerin en iyi çevre koşullarında hayatlarını sürdürmeleri için kalitenin yükseltilmesi.

4.6. Enerji Güvenliği

Uluslararası Enerji Ajansı (IEA) tarafından bu kavram, devamlı ve uygun fiyatlı kaynakların mevcudiyeti olarak belirtilmiştir. Ancak, siyasetçiler ve bilim insanları bakış açısıyla ele alındığında enerji güvenliği başlığı çok yönlü bir kavram olarak kendini göstermekte ve değişik ülkeler açısından farklı manalar ifade edebilmektedir. Devletlerin konjonktüre ve kendi menfaatleri açısından öncelik verdiği hususlara göre enerji güvenliği konusunda farklı hususlar ön plana çıkabilmektedir (Hatipoğlu, 2019:1).

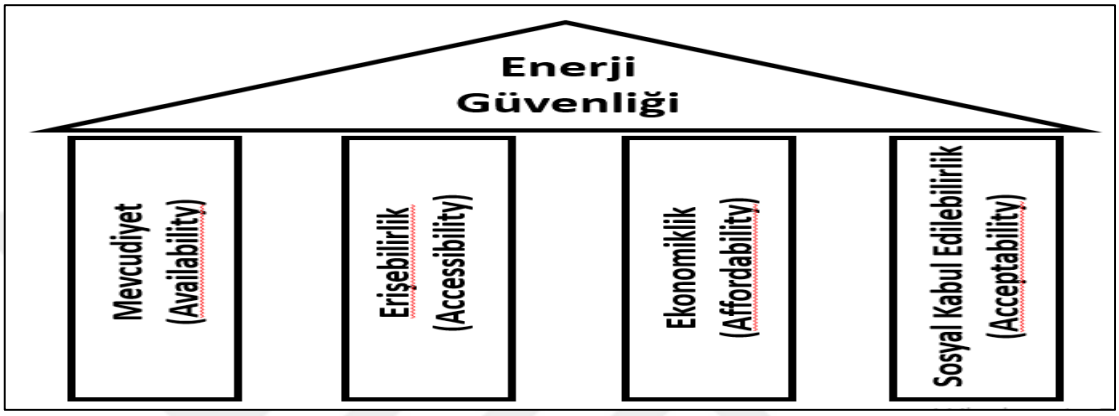
Enerji güvenliği; gereksinimin yeterli, emniyetli, ulaşılabilir bir biçimde temin edilmesi ve bu durumun devamlılığının sağlanması manasına gelmektedir. İktisadi ve sosyal refahın sağlanmasının ana ve en ehemmiyetli unsurlarından biri olan enerji arzı devletlerin öncelikli konularının içerisindedir. Gerek devamlılık ve gerekse ulaşılabilirlik bakımında enerji, gelişmekte olan ülkelerin de ajandasında ön sıralarda yer almaktadır. Diğer taraftan, mevcut kaynakların durumu ve yeni rezervlere ilişkin çalışmalara rağmen, enerji temin sürati ve paylaşım durumu da konu kapsamında gündeme gelmektedir (Göknel, 2008:67).

Enerji konusu güvenlik yönünün yanı sıra ülkenin ilerleme, sanayileşme, üretme, refah ve kalkınma ile savunma politikalarının birleşiminden oluşmaktadır. Uluslararası arenadaki başat aktörlerin ve NATO gibi ittifakların üyelerinin enerji tüketimi, ilerideki enerji gereksinimleri ve konu hakkındaki rekabetleri Soğuk Savaş sonrasından itibaren yaşanan sürecin ana öğeleri arasında bulunmaktadır. NATO bu süreçte neoliberal yaklaşım içerisinde hareket ederek 2008 yılındaki Bükreş Zirvesi'nden itibaren enerji konusuna ayrı bir önem vermiştir (NATO, 2008).

Küresel enerji güvenliğinin tesis edilmesi konusunda politik, toplumsal, iktisadi, teknolojik, askeri ve çevresel çok farklı boyutta birçok problem alanı bulunmaktadır. Rusya Federasyonu ile Batı arasındaki gerilimlerin, Ortadoğu Havzası'ndaki enerji rezervlerini veya Ukrayna gibi enerji geçiş koridorlarını etkilemesi, iklim değişikliği ve çevre konularında yürütülen görüşmelerden istenen neticelerin alınamaması ve kritik

enerji altyapılarının korunması gibi problemler enerji güvenliği konusunu daha da zorlu hale getirmektedir.

Arz edilen tüm bu hususlar enerji güvenliği ile alakalı konulardaki tüm oyuncuların bütünleşik, senkronize, işbirliği içerisinde hareket etmelerini ve stratejik tedbirler almalarını zaruri kılmaktadır (Özev, 2017:13). Asya Pasifik Enerji Araştırmaları Merkezi, enerji güvenliğini Şekil 11'de belirtilen dört temel konuda ele almaktadır.



Şekil 11. Enerji Güvenliği

Kaynak: (Hatipoğlu, 2019:2)

4.7. Salgın Hastalıklar

Küreselleşen dünya düzeni içerisinde sınırların ortadan kalkması, politik, kültürel ve ekonomik faaliyetler çerçevesinde bireylerin, ürünlerin ve hizmetlerin kolaylıkla ve yoğun bir şekilde yer değiştirmeleri salgın hastalıkları da yaygınlaştırmıştır. Bu hususlar kişisel ve kitlesel sorunlara neden olabilecek risk ve tehditlere yol açabilmektedir. Fakirlik, yetersiz kaynaklar, iç çatışmalar, ekonomik güçlükler ile tıbbi cihaz, personel ve imkânlardaki yetersizlik gibi problemler sebebiyle gelişmiş modern ülkelere göç edilmesi, göçe maruz kalan ülkelerde farklı ve büyük sağlık problemlerinin meydana gelmesine yol açabilmektedir. (Aka, 2007:123-124).

Yakın dönemde yaşanan farklı grip salgınları ve AIDS gibi salgın hastalıkların uluslararası düzende meydana getirdiği tesirler, bu konun da küresel bir risk ve tehdit oluşturulabileceğinin en açık örneklerini teşkil etmektedir. Örneğin yakın zamanda H5N1 mikrobuyla kendini gösteren kuş gribi hastalığı biyolojik terör şüphesini de arttırmıştır. Hastalığın hayvanlardan yayılarak ve küresel çapta süratli bir şekilde ölüm saçmasını

dikkat çekici bulan bazı araştırmacılar konunun hassasiyetle izlenmesini teklif etmiştir (Vogel, 2013:39-40).

Salgın hastalıkların uluslararası güvenliğe tehdit olarak algılanarak konuya ilişkin çalışmalar yapılmasının ne derece ciddi, yerinde ve isabetli bir değerlendirme olduğunun en açık örneklerinden birini de Afrika'yı tesiri altına alan Ebola teşkil etmektedir. İlk olarak yaklaşık 40 sene önce Demokratik Kongo'da görülen Ebola, 2013 senesinden itibaren tekrar yaygınlaşmaya başlamıştır. Dünya Sağlık Örgütü (WHO) istatistiklerine göre hâlihazırda yaklaşık 3 bin kişinin bu salgından dolayı hayatını kaybettiği ve küresel seviyede vakaların sayısının 6 bine ulaştığı belirtilmektedir (Milliyet Gazetesi, 2014).

Dünya çapında son 10 senelik süre zarfında 1500'den fazla bulaşıcı hastalık vakası kendini göstermiştir. Bu hastalıkların milyonlarca insana bulaşması ya da bulaşma ihtimalinin bulunması uluslararası ve ulusal güvenlikte salgın tehdidinin önemini açıkça göstermektedir (Kartepe, Ozan ve Banazılı, 2018:7).

Salgın hastalıklar bilimsel gelişmeler ve yaygın aşılama sayesinde 20. yüzyılda büyük oranda etkisini yitirmiştir. Fakat modern dünyada salgın hastalıklar başka formlarda hala insanlığın korkulu rüyası olmaya devam etmektedir. Yakın dönemde sırasıyla; SARS (2003), Kuş Gribi (2007), Domuz Gribi (2009), MERS (2012), Influenza A H7N9 (2013), Ebola (2014), ZİKA (2015) salgınları, ortaya çıkış sıklıkları ile hastalıkların 21. yüzyılda da etkili olduklarını açıkça ortaya koymaktadır. Burada dikkati çeken en önemli nokta, hastalıkların görülme sıklığındaki artıştır. Tarihsel olarak baktığımızda hemen hemen her yüzyıla denk gelen bir pandemiden söz etmek mümkündür. Oysa günümüzde salgın hastalıkların görülme sıklığı belirgin biçimde kısalmıştır. Yukarıda da belirtildiği üzere, 21. yüzyılın başında ortalama 20 yıl içinde toplam sekiz salgın ortaya çıkmış olması şaşırtıcıdır (Macar ve Asal, 2020:6).

Son olarak Aralık 2019'da Çin'in Wuhan kentinde ortaya çıkarak, kısa sürede küresel çapta bir salgına dönüşen Covid-19, uluslararası ilişkiler alanında köklü değişim ve dönüşümlere sebep olmuştur. Başta devletler olmak üzere, uluslararası sistemdeki tüm aktörler, Covid-19 krizine karşı ekonomik, siyasi ve toplumsal değişimlerin nasıl sonuçlar getireceğine ilişkin cevaplar aramaya başladılar. İlerleyen süreçte Covid-19 krizi, devletlerin gelişmişlik düzeyi ne olursa olsun kriz kaldırma kapasitelerinin zayıflığını da

ortaya çıkarmıştır. Kriz yönetiminde uygulanan politikaların başarısızlığı, her ülkenin sağlık alt yapısı ve sosyal güvenlik uygulamalarının zafiyetini gözler önüne serdiği gibi, sağlık sistemlerinin sorgulanmasına da neden olmuştur. (Macar ve Asal, 2020:8).

Önümüzdeki dönemde küresel salgın tehdidi oluşturabilecek farklı türdeki bulaşıcı hastalık virüsleri vb. pandemi türleri, iklim değişikliği gibi faktörlerin etkisiyle daha sık ortaya çıkması ve küreselleşmenin etkisiyle de uluslararası güvenliğe daha çok etkilemesi beklenildiği değerlendirilmektedir.

4.8. Sınıraşan Organize Suç ve Kaçakçılık

Küreselleşmenin beklenmeyen sonuçlarından birisi de ulusaşan organize suç grupları sayısında yaşanan artış olmuştur. Bunun nedenleri; bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle beraber karşımıza çıkan kolay uluslararası iletişim, uluslararası ticaretteki artış, gün içerisinde yapılan büyük finansal işlemlerin ve bankacılık faaliyetlerinin sağladığı ekonomik kazanç ve özellikle Sovyetler Birliği'nin dağılmasının ardından bazı ülkelerde yaşanan demokrasi hareketleri, ayaklanmalar ile büyük çaplı ekonomik sorunlardır (Ohr, 2008: 40).

Uyuşturucu, insan, küçük ateşli silahların trafiğini kapsayan ulusaşan organize suçlar ve kaçakçılık uluslararası güvenlik ortamını etkileyen önemli risk ve tehditler arasında yer almaktadır. Günümüzde organize suçların önemli bir yönünü de uyuşturucu kartellerinin kazançlarını korumak maksadıyla başvurduğu şiddet ve yolsuzluk faaliyetleri oluşturmaktadır (Birleşmiş Milletler Uyuşturucu ve Suç Dairesi, 2009).

Bu sorunu ele alan başlıca uluslararası düzenleme, Ulusaşan Organize Suçlara Karşı Birleşmiş Milletler Konvansiyonu (United Nations Convention against Transnational Organized Crime-CTOC)'dur. Konvansiyonun üç protokolü (insan ticareti, uyuşturucu ve kaçakçılık) de ulusaşan organize suçlar ve kaçakçılık hakkında hükümler belirtmektedir.

- Uyuşturucu Kaçakçılığı: Yasaklama düzenlemelerine tabi olan maddelerin küresel yasadışı ticaretidir. Uyuşturucu trafiği, kolluk uygulama tekniklerinin de kendisiyle birlikte gelişmesini sağlayacak şekilde tarih boyunca inanılmaz bir tempoda gelişmiştir. Yasadışı uyuşturucular için mevcut olan muazzam piyasa, bu yasadışı

ticaretin arkasındaki ana hareket kaynağıdır. (Birleşmiş Milletler Uyuşturucu ve Suç Dairesi, 2010a).

Küresel boyuttaki uyuşturucu tehlikesi, sosyo-ekonomik zararları bulunan, politik istikrar ve sürdürülebilir gelişmeyi sarsan, kamuoyu sağlığını, emniyetini, insanlığın refahını ve ulusal güvenliği tehdit eden bir konudur. Uluslararası sistemde bu problemlerin üstesinden gelmek maksadıyla 1972 Narkotik Uyuşturucular Üzerine Tek Konvansiyon Değişikliği ile revize edilen 1961 Narkotik Uyuşturucular Üzerine Tek Konvansiyonu ve 1988 Birleşmiş Milletler Narkotik Uyuşturucular ve Psikotropik Maddelerin Yasadışı Trafiği ile Mücadele Konvansiyon'ları bulunmaktadır.

- **İnsan Ticareti:** İnsan ticareti, ciddi bir suç ve insan haklarının ölümcül bir ihlalidir. Her yıl, erkek, kadın ve çocuk binlerce insan kendi ülkelerinde ya da diğer ülkelerde tacirlerin eline düşmektedir. Dünyadaki çoğu ülke kaynak, geçiş ve varış ülkesi olarak insan ticaretinden etkilenmektedir. Kadınlar, kız çocukları ağır işlerde çalıştırılmak, fuhuş ve zorunlu evlilik gibi istismarlar için insan ticaretine maruz kalabilmektedir. Erkekler ise borçla tuzağa düşürülerek madenlerde ve tarlalarda köleleştirilmektedir (Birleşmiş Milletler Uyuşturucu ve Suç Dairesi, 2010b).

İnsan ticareti, suç örgütlerinin oldukça yüksek finansal kaynakları ile "yatırımlarını" çeşitlendirebilmeleri sebebiyle ulusaşan organize suçlarla bağlantılıdır. İnsan ticareti uluslararası olarak "kişilerin tehdit veya güç kullanımı ve zorlama yolları ile toplanması, taşınması, transferi, barındırılması, kaçırılması, dolandırılma, aldatılma, güç ve makam yetkisinin kötüye kullanılması ya da istismar amacıyla ödemelerin veya yararların kişinin bir diğeri üzerine kontrol oluşturması amacıyla alınması veya verilmesi" şeklinde tanımlanabilmektedir (Birleşmiş Milletler, 2000). İnsan ticaretiyle mücadelede küresel araçlardan birisi Ulusaşan Organize Suçlar Konvansiyonu ve bu konvansiyonu destekleyen "Kişilerin, Özellikle Kadınların ve Çocukların Ticaretini Önleme, Baskı Altına Alma ve Cezalandırma" protokolüdür.

4.9. Siber Güvenlik

Siber güvenlik genel olarak internet ortamına bağlı ya da bazı hallerde internete bağlı olmasa dahi ağların, sistemlerin, yazılım ve donanım ayırt etmeden siber saldırılara

karşı muhafaza edilmesi maksadıyla kullanılan ve devamlı gelişim gösteren bir kavram olarak ifade edilmektedir (Gündüzhev, 2019:25).

Bilgi ve teknolojik gelişimlerin süratle ilerlediği günümüz güvenlik ortamında "siber güvenlik" çok önemli bir konumda bulunmakta ve her geçen gün önemi daha da artmaktadır. Uluslararası arenada önemli bölgesel aktörlerden biri olan NATO, 2010 yılında yayınladığı Stratejik Konseptinde yeni oluşan güvenlik ortamının tanımlaması yapmıştır. Bu tanımda ilk kez siber tehditlerden bahsedilerek ve siber saldırıların ülke yönetimleri, ekonomisi, ulaşım ve tedarik ağı ve diğer kritik altyapıları üzerinde daha büyük zararlara yol açan ve daha organize bir mahiyete büründüğü ifade edilmiş ve siber güvenlik kavramına vurgu yapılmıştır (NATO Stratejik Konsept, 2010:11).

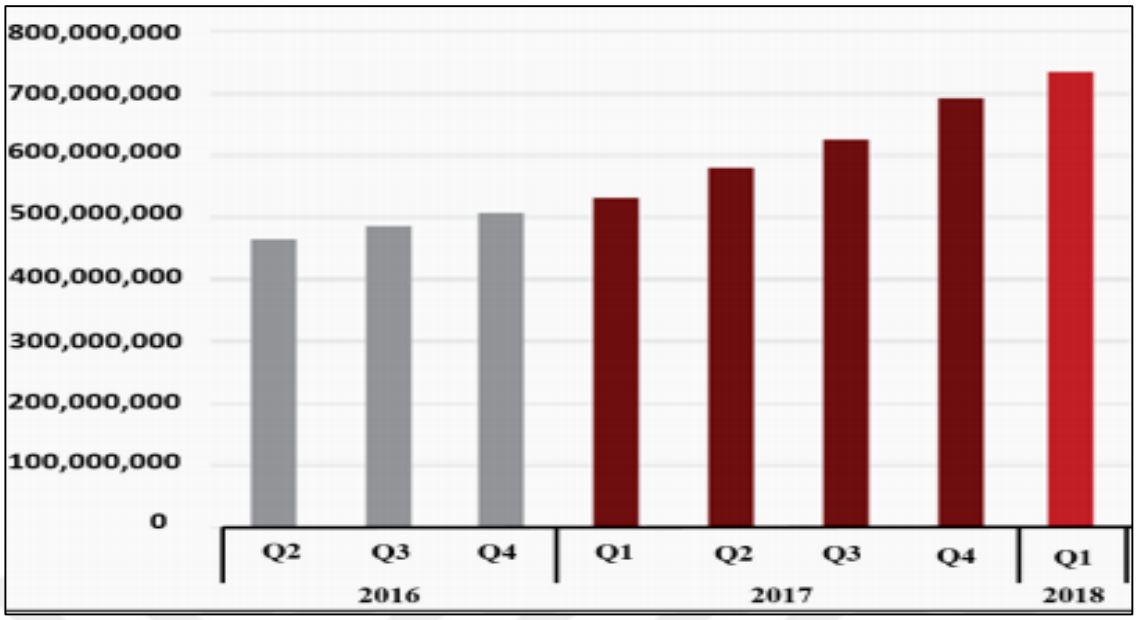
Dünya Ekonomik Forumu tarafından 2018 senesinde hazırlanan Küresel Risk Raporu'nun ana kısmını siber güvenlik ve siber uzaya ilişkin konular meydana getirmektedir. Siber ataklar yaşanabilirlik bakımından ilk beş küresel risk ve tehdit sınıfında ilk defa 2012 senesinde kendine yer bulmuştur. Raporda doğal afetlerden iklim değişikliğine çok farklı başlıklarda birçok konunun değerlendirilmesine rağmen siber konusunun kendine ön sıralarda yer bulması konunun kritik önemini açık bir şekilde ortaya koymaktadır. Raporda belirtilen risk ve tehditler Şekil 12'de sunulmuştur.

Şekil 12. 2012-2018 Arasında Yaşanabilirlik Açısından İlk 5 Küresel Risk ve Tehdit

Kaynak: (Küresel Risk Raporu, 2018:6)

Raporda kendine üçüncü sıradan yer bulan siber saldırılar ve dördüncü sırada yer bulan veri hırsızlığı, işsizlik, su krizi, düzensiz göç gibi birçok sorunu geride bırakarak kritik altyapılara zarar verilmesinden günlük hayatı durdurmaya kadar hayati konulara kumanda ettiğinden siber güvenlik konusunun önemine dikkat çekilmiştir.

McAfee tarafından 2018 yılında yayınlanan raporda da benzer şekilde siber güvenlik konusuna vurgu yapan birçok dikkat çekici veriye işaret edilmiştir. 2016 ve 2018 seneleri arasındaki kötücül yazılımların durumunun kıyaslandığı Şekil 13'deki veriler dikkate alındığında yükselişin ne boyutlara ulaştığı ve siber saldırıların ne kadar artabileceği görülmektedir. Diğer yandan, kullanıcı ile firmalar yönüyle bireysel verilerin korunması ile firmaların maddi zararları ve itibar kayıpları konularında hangi seviyelere ulaşabileceği anlaşılmaktadır.



Şekil 13. Toplam Kötücül Yazılım

Kaynak: (McAfee Tehdit Raporu, 2018: 16).

Sonuç olarak, siber güvenlik konusunun ekonomiden askeri konulara, politikadan kişisel verilerin korunmasına, finans sisteminden kamu hizmetlerinin yürütülmesine kadar hayatın her alanında yer alması bu konuyu yeni güvenlik ortamının risk ve tehditleri arasında ön plana çıkarmaktadır. Yakın dönemde hazırlanan çalışmalarda bu durumu açıkça ortaya koymaktadır.

ÜÇÜNCÜ BÖLÜM

SİBER TEHDİTLER VE SİBER SAVAŞIN HUKUKSAL ANALİZİ

1. SİBER TEHDİTLERİN SİBER SAVAŞA DÖNÜŞMESİ

Siber ortamdaki bireysel ve kurumsal bilgilere ilişkin güvenlik ihlal eden her çeşit saldırı siber tehdit olarak ifade edilmektedir. Zararlı yazılımlardan virüslere, truva atlarından kişisel bilgilerin ele geçirilmesine kadar icra edilen her türlü faaliyetler siber tehditlere örnek olarak gösterilebilmektedir (Şahinaslan, 2013:3).

Klasik tehditlerle siber ortamda karşımıza çıkan tehditler birbirinden ciddi farklılıklar arz etmektedir. Bu farklılıkların özünde ise hiç şüphe yok ki siber ortamdaki tehditlerin önceden belirlenme kapasitesinin ve ölçütlerinin sınırlı olması yatmaktadır. Siber ortamdaki baş döndürücü hız bu tehditlerin en büyük silahlarından birini oluşturmaktadır. Siber tehditleri farklı kılan bir diğer özellik de maliyettir. Çok düşük bir maliyet ve ucuz enstrümanlarla siber alanda gerçekleştirilen bir taarruz karşı tarafa ciddi zarar verebilmekte ve bedeller ödetebilmektedir. Mesela yapılacak bir saldırının neticesinde, günlük hayatta yaşanacak aksaklıklar ve bunun maliyetinden tutun da, bir ülkenin seçimlerine müdahale edilmesine kadar gidebilecek geniş spekturumda etkiler ve zararlar söz konusu olabilecektir (Gürkaynak ve İren, 2011: 265).

Siber ortamdaki baş döndürücü hız, gizlilik, belirsizlik, düşük maliyet, yüksek etki ve bilgi teknolojilerindeki hızlı ilerlemeyle birlikte teknolojinin hayatın her alanında daha yoğun yer alması neticesinde ticari ve/veya politik farklı düşüncelerle siber saldırıların sayısının da yükseldiği görülmektedir. Yakın dönemde "I Love You", "Nimda", "MyDoom" isimli virüsler vasıtasıyla yapılan saldırılar neticesinde 24,8 milyar dolarlık bir zarar meydana getirilmiştir. 2008 senesinde istihbarı amaçlarla kullanılan ve Rusya, İran, Belçika ve Suudi Arabistan başta olmak üzere pek çok ülkeye nüfuz eden "Regin" virüsü 2014 senesinde ancak bulunabilmiştir (Yılmaz, Ulus ve Gönen, 2015: 137-138).

Siber konular hâlihazırda ciddi bir şekilde dünya gündeminde en ön sıralardaki konumunu korumakta ve ülkeleri etkilemeye devam etmektedir. Siber ortam daha önce de ifade edildiği gibi sadece askeri hedeflere yönelik olarak kullanılmamakta, aynı zamanda sivil hedeflere yönelik olarak hatta politik amaçların elde edilmesine ilişkin

olarak da kullanılmaktadır. Birçok araştırmacı tarafından daha siber savaş konusunun başlarında olunduğuna, önümüzdeki kısa dönemde bu kavramın ne şekilde ciddi dönüşümler göstereceğine ilişkin birçok öngörü yapılmaktadır (Mazanec, 2015:48).

Teknolojide yaşanan baş döndürücü gelişmelere paralel olarak askeri silah, sistem ve teçhizatlar da ağ destekli yetenekten, uydu haberleşmesine, muhabere sistemlerinden bilgi aktarım sistemlerine kadar çok geniş bir spekturumda siber tehditlere açık durumdadır. ABD Ulusal İstihbarat Eski Direktörü Amiral McConnell "Siber savaş, potansiyel ekonomi ve psikolojik etkiler açısından nükleer zorlukları yansıtmaktadır" ifadeleri ile siber tehdide ilişkin durumun önemini açıkça ortaya koymuştur (McConnell: 2010).

Tüm alanlarda olduğu gibi savunma sanayii de hemen hemen her alanda BİT'leri yoğun olarak kullanmaktadır (ENISA, 2011:1). BİT imkânlarının ortadan kaldırılması veya işlevlerini yerine getiremez duruma düşürülmesi sadece askeri alanla sınırlı kalmadan sosyal hayatı da olumsuz etkileyecek şekilde kötü sonuçlar doğurabilmektedir. Siber tehditler, BİT'lerden istifade edilerek üretilmiş, tamamen farklı ve yeni saldırı türlerinin harekât alanında ortaya çıkmasına sebep olmaktadır. Siber harekât ortamında;

- Siber uzay içinde bulunan varlıklar,

-Varlıklarda meydana gelen açıklıklar/ zafiyetler,

- Siber uzayda bulunan unsurların zafiyetlerden istifade etmeyi amaçlayan aktörler,

- Siber uzayda etkin bir şekilde istifade edilen yöntemler ana elemanlar olarak kıymetlendirilmektedir (Tablo 2).

Tablo 2. Siber Harekât Ortamı Elemanları

VARLIKLAR	AÇIKLIKLAR/ ZAAFİYETLER	AKTÖRLER	YÖNTEMLER
- Kritik Altyapılar - Komuta Kontrol Sistemleri - Ağ Tabanlı Yetenekler - İnsansız Sistemler - Bilgisayar Donanımları - Yazılımlar	- Yazılım Tabanlı Güvenlik Açıklıkları - Konfigürasyon Zayıflıkları - Ağ Güvenliği Açıklıkları	- Yabancı Ülke Silahlı Kuvvetleri - İstihbarat Örgütleri - Terörist Gruplar - Organize Suç Örgütleri - Bilgisayar Korsanları - Kurum İçi İşbirlikçiler - Hacktivistler	- Hizmet Dışı Bırakma - Zararlı Yazılım Bulaştırma - Tuzaklı Donanım Satma/ Yerleştirme - Siber Casusluk - Sosyal Mühendislik

Siber harp ortamının tesir ettiği ve hayati ehemmiyeti bulunan unsurların ilk sırasında günlük hayatın doğal bir parçası olan enerji ve su üretim/dağıtım, haberleşme, ulaşım, gaz ve petrol boru hatları gibi kritik altyapıların kontrol sistemleri yer almaktadır. Çok basit bir yazılımla, kısa süre içerisinde ve çok düşük bir maliyetle bir muhasım kritik altyapı sistemi etkisiz hale getirilerek ciddi zararlar verilebilmekte, günlük hayat ciddi şekilde olumsuz etkilenebilmekte ya da daha da ileriye giderek bir felakete yol açılabilmektedir.

Yakın dönemde yaşanan bazı gelişmeleri (2007-Estonya, 2008-Gürcistan) müteakip, ülkeler, uluslararası kurum/kuruluşlar ile başta NATO, siber harbi gündemlerinde ön sıraya çekmiştir. 1990'larda sadece bilgisayar sistemleri güvenliği çerçevesinde ele alınan siber güvenlik konusu, 11 Eylül saldırını müteakip asimetrik savaş kavramının oturmasıyla beraber Estonya ve Gürcistan vakalarının ardından ciddi ve yaygın bir şekilde gündem oluşturmuştur (Gökpınar, 2009:3). NATO kapsamında değerlendirildiğinde, hâlihazırda kolektif savunmanın bir unsuru olan siber kabiliyetlerin gündeme getirilmesi politik açıdan kırılgan bir konu olmasına karşın sonuç itibari ile kaçınılmaz bir hal arz edecektir (Lewis, 2015:2).

Diğer taraftan, siber savunma, taarruzun tam tersi olarak kritik sistemlere ilişkin yapılan saldırıları tespit etmek, korumak ve kontrol altına almak maksadıyla gerekli tedbirlerinin alınması şeklinde ifade edilmektedir. Yaşanan gelişmeleri ve bunun yanında taarruzi yeteneklerin sağladığı üstünlükleri göz önünde bulunduran pek çok ülke hem

savunma hem de saldırı siber imkân ve kabiliyetlerini geliştirmeyi savunma planlama ve bütçelerine ithal etmiştir. BM Silahsızlanma Enstitüsü tarafından yapılan çalışmada;

- 193 üye ülkenin 114'ünde ulusal siber güvenlik programının bulunduğu,
- Bu programlardan 47'sinde silahlı kuvvetlere siber tehditlere karşı rol verildiği,
- 67'sinin sadece sivil programlarla yetindiği,
- En büyük askeri harcamayı yapan ilk 15 ülkenin 12'sinin sabit siber harp birimlerinin olduğu,
- Bunların arasında 10 ülkenin siber saldırı imkânının bulunduğu ya da geliştirdiği,
- RF, İngiltere, Fransa, ABD ve ÇHC'nin siber imkân ve kabiliyetler açısından en ön sırada yer aldığı görülmüştür (Birleşmiş Milletler Silahsızlanma Enstitüsü, 2013:1).

Aynı şekilde Uluslararası Telekomünikasyon Birliği (ITU) tarafından 2018 yılında ülkelerin resmi verilerine dayanılarak yapılan Siber Güvenlik Çalışmasında;

- Dünya nüfusunun yarısından fazlasının çevrimiçi olduğu (3,9 milyar kişi) ve bu oranın 2023 yılında yüzde 70'ler seviyesine ulaşacağı,
- Siber suçların maliyetinin 2020 sonuna kadar yaklaşık 2 trilyon dolar olacağı,
- Siber güvenliğin hukuki boyutunun uygulanmasına ilişkin ciddi boşlukların bulunduğu,
- Siber güvenliğe 54 ülkenin yüksek (Türkiye bu grupta yer almaktadır.), 53 ülkenin orta ve 87 ülkenin ise düşük önem verdiği belirtilmiştir (Uluslararası Telekomünikasyon Birliği, 2018:6).

Kara, deniz ve hava ortamında yaşanan rekabete özellikle Soğuk Savaş döneminde uzay da eklenerek dördüncü bir boyut daha eklenmiştir. Ardından 1990'larda özellikle internetin meydana getirdiği farklı bir boyut olarak siber alanda beşinci bir parametre olarak kendisini göstermiştir. Ülkelerin hemen hemen her alanda bilgi sistemlerini ve ağ yapılarını yoğun olarak kullanmasının doğal bir sonucu olarak onları siber taarruz ve savaşlara açık bir duruma getirmiştir. Özellikle küresel güç olarak ABD'nin siber alana her manada entegre olduğu, Obama'nın; siber uzayı ülkenin sinir uçları ve kontrol noktası olarak anlatmasından anlaşılabilmektedir (Beidleman, 2009: 1).

Siber uzayda harp fikrinin başlangıçta düşünce sınırlarının ilerisinde hayalî bir kavram olarak görülmüş olmasına rağmen zamanla uluslararası ilişkiler mantığı çerçevesinde bir geçerliliğin mümkün olduğu anlaşılmıştır. Uluslararası ortamı anarşik

bir durumda tanımlayan realist görüş; devletlerarası sorunların giderilmesinde, ülkelerin üstünde bir yapı, güç olmaması sebebiyle çatışmaların doğal olduğunu belirtmektedir. Siber ortamda bulunan aktörlerin (özellikle devletlerin) üzerinde ve onları tümüyle kontrol eden bir gücün olmaması dikkate alındığında siber ortamda da anarşik bir yapının olduğu kıymetlendirmeleri yapılmaktadır. Bu durum devletlerarasındaki ilişkilerin ve mücadelenin her an küçük çaplı çatışmadan savaşa uzanacak kadar geniş perspektifte bir dönüşümün önünü açmaktadır. Günümüzde aktörler tarafından halen daha resmi olarak açıkça ifade edilip kabul edilmese de siber harp olarak isimlendirilebilecek birçok sistematik saldırının yapılması, bu vaziyeti ortaya koyar mahiyettedir (Keskin, 2017:291).

Burada karşımıza çıkan en önemli hususlardan biri siber taarruzun harp olarak ele alınmasında iki veya daha fazla devletin arasında meydana gelme zorunluluğudur. Ancak, yaşanan süreçte bunun sistemli bir şekilde icra edilmesi de durumu siber taarruzdan bir adım ileriye götürmektedir. Siber savaş da en az konvansiyonel savaş kadar yıkıcı hatta ondan daha etkilidir. Yaşanan vakalardan da anlaşılacağı üzere yapılan siber savaşın tesirinin klasik savaşlardan daha fazla olabilmesine karşın hâlihazırda uluslararası arenada tam bir fikir ve uygulama birliği tesis edilemediği için pek çok ülke ve uluslararası kurum/ kuruluşlar yaşanan durumları siber saldırı olarak ifade etmeyi sürdürmektedir (Gürcan, 2011: 166).

2. SİBER EYLEMLERİN KATEGORİLENDİRİLMESİ

Çalışmanın bu kısmında siber eylemlerin kategorilendirilmesini kolaylaştırmak, siber uzayda gerçekleştirilen eylemleri birbirinden ayırt etmek, incelenen vakaların siber harekât spektrumundaki konumunu canlandırabilmek ve doğru bir kıymetlendirme yapabilmek maksadıyla Şekil 14'den istifade edilmiştir (Doğru, 2016:5). Spekturumda; adi siber eylemler, siber suç ve siber espiyonaj gibi kuvvet kullanımının söz konusu olmadığı ve daha çok adli kolluk güçlerinin sorumluluk alanına giren kısmı; Siber müdahale, yine kuvvet kullanımının söz konusu olmadığı, ancak muhasımın siber ortama erişimini kısıtlama ve kısmen de olsa devletin egemenliğinin ihlal edilmesini içeren kısmı; Siber saldırı ise esas itibari ile fiziksel zararı içeren kısmı ifade etmektedir.

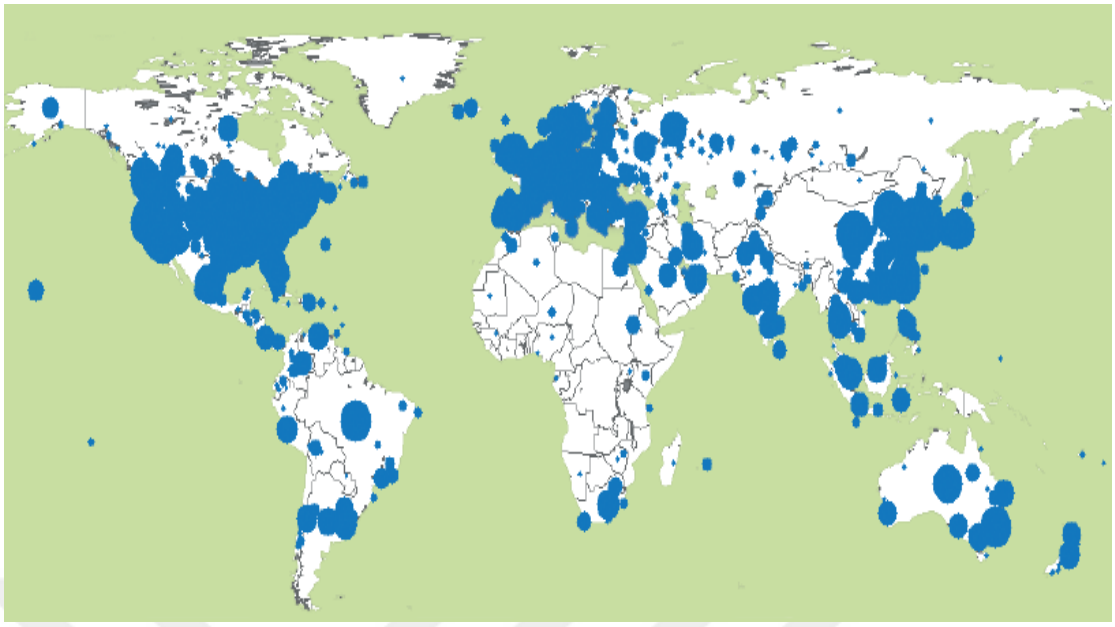
Şekil 14. Siber Harekât Spektrumu

Kaynak: (Doğru, 2016:5)

3. GEÇMİŞTE YAŞANAN ADİ SİBER EYLEMLER

3.1 Siber Suç Örnekleri

- **Slammer Zararlı Yazılımı**: 2003 senesinde bireysel kullanıcıların hedef alındığı eylemlerden farklı bir tehditle karşılaşılmıştır. Önemli firma/kurum/kuruluşların servis sağlayıcılarını hedefe koyan "Slammer" isimli bilgisayar solucanı Microsoft SQL Server 2000 programındaki boşluktan istifade edilerek meydana getirilmiştir. Söz konusu programın servis sağlayıcılar içerisinde kullanıcı elektronik postalarına ihtiyaç göstermeden yayılması özelliğini kullanan "Slammer" bu şekilde en süratli yayılan virüs olarak kendine yer bulmuştur. (Şekil 15) Virüsten en çok etkilenen Güney Kore'de 12 saat boyunca internet hizmeti verilememiştir. Virüsten doğrudan etkilenmeyen ülke ve firmalar sistemlerini belli bir dönem çevrim içi olarak kullanmak durumunda kalmıştır (Moore, 2003:33).



Şekil 15. Slammer Virüsünün Otuz Dakika İçerisinde Etkilediği Bölgelerin Gösterimi

Kaynak: (Moore, 2003:34)

- **Conficker Zararlı Yazılımı:** "Conficker" ya da "Downup", "Downadup" ve "Kido" şeklinde ifade edilen bilgisayar solucanı ilk Ekim 2008'de görülmüştür. Microsoft Windows işletim sistemini hedefe koyarak, Windows'un bir açığından istifade ile yayılmıştır. 16 Ocak 2009 tarihinde F-Secure tarafından, "Conficker" solucanının yaklaşık 9 milyon bilgisayara bulaştığı ifade edilmiştir (Larkin, 2009).

- **Flame Zararlı Yazılımı:** "Flame", casusluk amaçlı ve hedefe ilişkin saldırı yapabilmek için dizayn edilmiş, karmaşık bir taarruz vasıtası olarak kullanılmış ve 2012 yılında tespit edilmiştir. Arka kapı, truva atı ve solucan gibi değişik türlerin özelliklerini içeren bir yapıdadır. Özellikle Ortadoğu coğrafyasında üniversiteler başta olmak üzere akademik kuruluşlar ile özel sektörü hedefe koymuş, İran, Lübnan, Suudi Arabistan ve Suriye'de etkili olmuştur. "Flame" ile Skype görüşmeleri ve bilgisayar kamera görüntüleri kaydedilmiştir. Bazı araştırmalarda "Flame"in hedef kitlesinin Ortadoğu coğrafyası ve GMT+2 saat diliminde olan ülkeler olduğu ifade edilmektedir. İlk olarak elektronik postalar ile oltalama yöntemi veya çeşitli web adreslerine yerleştirilen zararlı yazılımların indirilmesi vasıtasıyla yayılan bu yazılım 2 yıl boyunca tespit edilememiştir (Enein, 2017:17).

3.2. Siber Casusluk Olayları

İngilizce "*cyber espionage*" olarak ifade edilen siber casusluk; siyasi, askeri, politik, ticari ve kişisel maksatlarla birey, kurum/ kuruluş veya ülkelerin bilgi sistemlerine yasadışı olarak girerek karşı tarafın müsaadesi olmadan hassas, gizli bilgi/belge ve sırlarının ele geçirilmesi olarak tanımlanmaktadır (Çiftci, 2017; 9)

Başlangıçta zararlı yazılımlar vasıtasıyla kullanıcı bilgisayarlarına girerek kişisel hesapların, şifrelerin elde edilmesiyle yapılırken zamanla boyut değiştirerek askeri sırlardan politikaya ve ekonomiye kadar uzayan geniş bir spekturumda üstünlük elde etmek için kullanılmaya başlanmıştır. Sistematik ve doğru şekilde yapılan siber casusluk siber harp öncesinde muhasıma karşı avantajın ele geçirilmesini temin edebilmektedir (Keleştemur, 2015; 162).

Bütün siber eylemlerde olduğu gibi casuslukta da temel sorunlardan birisi devlet destekli casusluk, kurumsal casusluk ya da bireysel sıradan hackerlık olup olmadığı konusundaki muğlaklıktır (Schaap, 2009:141). Bu çerçevede kıymetlendirilen bazı vakalar aşağıda sunulmuştur.

- **Titan Yağmuru:** ABD askeri kurum/kuruluşlara ait bilgisayarlar 2003 senesinde Çin kaynaklı olduğu değerlendirilen bir seri koordineli siber casusluğa maruz kalarak, 10-20 Tb'lık veri çalınmıştır. Yapılan çalışmalarda siber eylemlerin üç sene sürdüğü, merkezin Çin'in Guangdong şehri olduğu ve kullanılan yöntemler itibari ile ordu kaynaklı olduğu değerlendirilmiştir (Türkay, 2013:1193).

- **GhostNET:** Özellikle diplomatlar, dışişleri bakanlıkları ve büyükelçilikler gibi devletlerarası ilişkilerin yönetildiği kurumları hedef alan siber casusluk ağı olarak ortaya çıkmıştır. Yapılan yoğun çalışmalar sonucunda bugüne kadar 103 ülkede 1295 bilgisayara sızdığı belirtilen bu ağın merkezinin ÇHC olduğu bulunmuştur. GhostNET tüm altyapısının ÇHC'de bulunmasına, icra edilen faaliyetlerin ÇHC merkezli olmasına karşın, ÇHC hükümetinin bu casusluğu icra ettiğine ilişkin kesin bir bilgi bulunmamakta ve yetkililer tarafından suçlamalar kesin bir dille reddedilmektedir (Peker, 2010:65).

- **Aurora Operasyonu:** Google tarafından 2010 senesinde hem kendilerini hem de bazı şirketleri hedef alan oldukça karmaşık, koordineli bir dizi siber casusluk

olaylarına maruz kalındığı açıklanmıştır. Siber casusluğun ÇHC merkezli olduğu ve bazı şirket bilgilerinin sızdırıldığı ifade edilmiştir. Yapılan siber eylemlerle internet tarayıcısı Internet Explorer'da yer alan ve virüs karşıtı programlar tarafından tespit edilemeyen yöntemlerle sistemlerine sızıldığı belirtilmiştir (Schwartz,2013).

McAfee tarafından yapılan açıklamada ise Aurora Operasyonu'nun Google ve en az 20 farklı firmayı giriş noktası olarak ele alıp, casus yazılım ile bu firmalardan istifade ettiği belirtilmiştir. Hedef kullanıcıların bilgisayar ağlarından uzaktaki sunucuya kadar firma bilgileri ele geçirilmiştir (Kara, 2013:30).

- Wikileaks: 2006 senesinde ismini kaydettiren Wikileaks elinde birçok ülkeye ait 1,2 milyon gizli belge olduğunu açıklayarak 2007 senesinden itibaren belgeleri kamuoyu ile paylaşmaya başlamıştır. Siber casusluğun önemli vakalarından birini teşkil eden Wikileaks küresel çapta ses getirmiştir (Yayla, 2014: 194). Bu belgelerin açıklanmasını önlemek maksadıyla Wikileaks adresine yönelik saldırılar gerçekleştirilmiş, ancak "Anonymous" isimli hacker grubu tarafından destek maksatlı Mastercard, Paypal, Visa ve farklı adreslere karşı saldırılar başlatılmıştır (The Guardian Haber Sitesi, 2010).

- JSF (Joint Strike Fighter) Verilerinin Çalınması: Türkiye'nin de proje ortağı olduğu beşinci nesil savaş uçağı projesi olan F-35 veya diğer adıyla JSF (Joint Strike Fighter) uçaklarına ilişkin bilgilerin 2009 senesinde ÇHC tarafından ABD savuma sanayii dev şirketi Lockheed Martin'den siber casusluk faaliyetleri ile ele geçirildiği iddia edilmiştir. ÇHC siber istihbarat elemanları tarafından uçağa ilişkin bakımdan elektronik sistemlere kadar tüm planların ele geçirildiği belirtilmektedir (Yıldız, 2014:50).

4. SİBER MÜDAHALE ÖRNEKLERİ

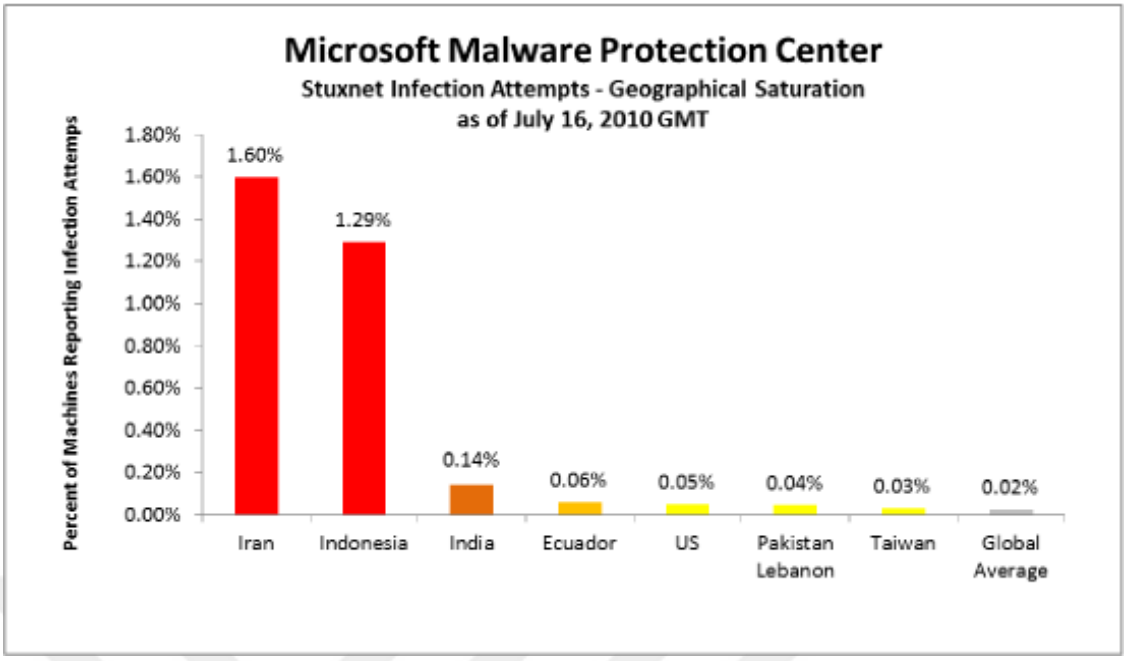
4.1. Stuxnet Vakası

En çok gündeme gelen siber müdahale son dönemlerde adından yoğun olarak söz ettiren Stuxnet adlı zararlı bir yazılım ile yapılmıştır. Bazı araştırmacılar tarafından sistemlere girerek dışarıya veri aktarımı için kapı açan bir truva atı olarak ele alınırken bazıları tarafından ise sistemlere sızarak büyük yıkımlar yapan bir solucan olarak

değerlendirilmektedir. Özellikle sanayii tesislerin kontrol sistemlerini hedefe alan Stuxnet'in Batılı devletler tarafından İran'ın nükleer programına zarar verme odaklı geliştirildiği ortaya atılmaktadır. Stuxnet'in amacı barajlar, petrol platformları, enerji santralleri ve diğer sanayi tesislerinin kontrolü için kullanılan SCADA sistemlerine sızıp fiziksel kontrol sistemlerinin çalışma biçimini değiştirmektir. Bu tarz kontrol sistemleri daha ziyade askeri üsler, kritik altyapılar, enerji santralleri, petrol boru hatları ve havaalanları gibi risk seviyesi yüksek, güvenliğin ön planda olduğu sistemlerde kullanılmaktadır (Yalçın, 2019:64).

İran, Stuxnet'in sadece görevlilerin bilgisayarlarına yayıldığını ve 30 bin bilgisayarın zarar gördüğünü belirtmiştir. Stuxnet saldırısı, siber müdahalenin etkisini gösteren temel vakalardan biridir. Solucan, İran'ın ürettiği 9.000'den fazla santrifüjden sadece 3 bin 700 tanesini çalışır durumda bırakmıştır (Ataç, 2019:12).

Siber güvenlik uzmanları tarafından Stuxnet üzerinde yapılan analizlerin neticeleri ve elde edilen bilgiler çerçevesinde yazılımın çok karmaşık bir yapı arz etmektedir. Aynı zamanda konusunun uzmanı belli bir ekip çalışmasının ortak bir ürünü olduğu, SCADA teknolojisine ilişkin kritik bilgilerin kullanıldığı, arkasında ciddi bir sermaye kaynağının bulunduğu gibi dikkat çekici bulgular da söz konusudur. Stuxnet'in, hedefi ve kendini gösterdiği coğrafya bakımından basit bir saldırı olmadığı kıymetlendirilmektedir. Şekil 16'da net bit şekilde görüldüğü gibi en çok etkilenen sistemler İran üzerinde yoğunlaşmaktadır (Industrial Ethernet Book, 2017).



Şekil 16. Stuxnet Virüsünden Etkilenen Ülkeler

Kaynak: (Industrial Ethernet Book, 2017)

Stuxnet, bugüne kadar bilinen en gelişmiş siber müdahaledir. ABD tarafından 2009 senesinde gerçekleştirildiği iddia edilen müdahalenin, İran'ın Natanz şehrindeki nükleer zenginleştirme programını hedef aldığı düşünülmektedir. Stuxnet siber harekât ortamında belirlenmiş hedefleri tesir altına almak için dizayn edilmiş yeni nesil bir at-unut sistemi olarak değerlendirilmektedir (Özbek, 2019:16).

Diğer yandan, New York Times gazetesinde 15 Ocak 2011 tarihinde basılan bir yazıda söz konusu zararlı yazılımın ABD ve İsrail uzmanlarınca ortak mesai ile oluşturulduğu iddia edilmiştir. İran nükleer programında kullanılan teknolojiye ilişkin teknik istihbarata gereksinim duyulması, yazılımın meydana getirilmesinde gelişmiş programlama ve test usullerinin kullanılması ve yazılımın hayat bulması için tesislere bireysel erişim sağlama zorunluluğu, iddiaları haklı çıkaracak nedenler olarak gösterilmiştir (Broad, Markoff ve Sanger, 2011).

4.2. İnternet Trafiği Değiştirme

2010 senesinde, ÇHC Telekom firması internet akışının %15'ini 18 dakika süresince kendine kanalize etmiştir. İnternetin bel kemiğini meydana getiren *routerlar* (yönlendiriciler) ÇHÇ üzerindeki güzergâhın kendileri için en tesirli geçiş yolu olduğuna

inandırılmıştır. Başlangıçta tespit edilemeyen olay daha sonradan değişik ağların veri gecikmesini aynı anda bildirmeleri ile gün yüzüne çıkmıştır. Normal güzergâh üzerinden akması gerekli olan trafik, güzergâh değiştirerek farklı ağlar vasıtasıyla akmıştır (Cowie, 2010).

5. SİBER SALDIRI ÖRNEKLERİ

5.1. Estonya Örneği

RF'nin Estonya'ya 2007 yılında gerçekleştirdiği siber saldırı bir ülkenin diğer bir ülkeye yaptığı ilk saldırı olarak tarihe geçmiştir. RF'nin itirazlarına rağmen Estonya Parlamentosu tarafından alınan karar uyarınca Talinn'de bulunan II. Dünya Savaşı'ndaki Sovyet askerlerini ifade eden "Meçhul Asker" anıtının kaldırılması kararı sonrasında 27 Nisan 2007 tarihinde siber saldırılar başlamıştır. Saldırıların arka planında iki ülke arasındaki gerginliğin ve RF'nin NATO ittifakı ile yaşadığı mücadelenin tesiri de bulunmaktadır (Bıçakçı,2014: 121).

Saldırıların ardından Avrupa'da e-devlet sistemini en etkin şekilde kullanan Estonya'nın birçok bilgisayarı kullanılamaz duruma gelmiş, siyasi partilerden devlet kurumlarına, bankacılık sisteminden internet altyapısının çökertilmesine kadar pek çok olay yaşanmıştır. Olaya ilişkin olarak Estonya açıkça RF'yi suçlasa da nihai bir kabullenme hiçbir zaman söz konusu olmamıştır (Darıcılı, 2014:6).

Estonya devlet başkanlığı ve parlamentosu, tüm bakanlıklar, siyasi partiler, ülkedeki büyük haberleşme kuruluşlarının yarısı, en büyük 2 banka ve 2 büyük iletişim kuruluşundaki bilgisayarlar gayri faal bırakılmıştır. Estonya'da yaşamı neredeyse durduran saldırıya ilişkin olarak NATO ve AB'de alarm seviyesini yükseltmiştir. NATO siber güvenlik uzmanlarını Estonya'ya göndererek saldırının sınırlarını ve meydana getirdiği etkiyi ölçmeye çalışmıştır (Çakmak ve Altunok, 2009:121-122).

Yaşanan bu olay sınırdaş iki ülke arasında meydana gelen yerel bir vaka olmanın ilerisinde, siber saldırıların ve siber güvenlik kavramının uluslararası ilişkiler çerçevesinde de tahlil edilmesine sebep olması açısından ehemmiyet arz etmiştir. Saldırının ardından NATO ve ABD'nin oynadığı rol Soğuk Savaş döneminde uzay

mücadelesinde olduğu gibi siber uzayın yeni bir rekabet sahası olarak görülmesine neden olmuştur (Roth, 2009:14).

5.2. Orchard Harekâtı

Siber saldırılar, tek başına bir güç unsuru olarak kullanılmanın yanı sıra icra edilen bazı harekâtlarda askerî hedeflere ilişkin icra edilen klasik taarruzlarla koordineli olarak da kullanılmıştır. İsrail'in 6 Eylül 2007 tarihinde Suriye'nin kuzey bölgesindeki Deir ez-Zur'da yer alan bir nükleer tesise düzenlediği hava harekâtı, siber müşterek harekâtın en temel örneklerinden birini teşkil etmektedir. İsrail hava saldırısı öncesinde Türkiye sınırına yakın Tali al-Abuad bölgesindeki hava radar sistemlerini tesirsiz hale getirmiş, dolayısıyla Suriye, İsrail filosunu tespit edememiş, uçaklar nükleer tesise saldırarak hasarsız bir şekilde üslerine geri dönmüştür. Saldırıyı müteakip yapılan keşiflerde tesisin tamamen imha edildiği görülmüştür. Harekâtın siber kısmının İsrail'in en önemli siber birimi Unit 8200 tarafından icra edildiği açık kaynaklarda ifade edilmiştir (Sertçelik, 2015:35).

5.3. Gürcistan Örneği

Gürcistan ile Rusya arasında Güney Osetya bölgesindeki sorunlar nedeniyle 11 Ağustos 2008'de çatışmalar başlamıştır. Askerî harekât öncesinde ve harekâtla birlikte Rusya tarafından siber saldırılarda başlatılmıştır. Siber saldırılar, Gürcistan Devlet Başkanlığı resmi internet sitesi olan "www.president.gov.ge" adresindeki Başkan Saakaşvili resmi yerine Adolf Hitlerin resminin koyulması ile kendini göstermiş, müteakiben tüm ülke geneline yayılmıştır. Bu saldırıların dağıtık servis dışı bırakma saldırısı (DDoS) olduğu tespit edilmiştir. Yapılan siber saldırılarda devlet sitelerine grafiti resmi konulmuş, Rusya geleneksel savaş yöntemleriyle paralel olarak siber saldırıları birlikte yürütmüştür. Yapılan siber saldırılar incelendiğinde ABD'den çalınan kredi kartları ile Türkiye ve Rusya'dan açılan sitelerden gerçekleştirildiği görülmüştür (Bıçakcı, 2012: 219).

Gürcistan'ın CNN ve BBC dâhil birçok web sayfalarına girişi engellenmiştir. Rusya siber güvenlik uzmanları Gürcistan'a trafiği destekleyen tüm yönlendiricileri ele geçirmiştir. Dışarıdan haber almayan Gürcistan, dışarıya da elektronik posta dahi

yollayamamıştır. Derin bilgisayar bilgisine sahip olmayan kullanıcıların da saldırılara destek vermesi amacıyla yığın dosyaları dağıtılmış, böylece saldırı kaynaklarının artırılması hedeflenmiştir (Kara, 2013:49).

5.4. ABD Seçimleri Örneği

RF'nin 2016 senesinde Başkan adayı Clinton'un kampanya yöneticisi John Podesta ile seçim kampanyasına destek veren ABD Eski Dışişleri Bakanı Colin Powell'ın elektronik postalarını ele geçirerek kamuoyuna sızdırdığı ve RF'nin aktif bir biçimde seçime kendi menfaatleri doğrultusunda müdahale ettiği ileri sürülmüştür. Hatta konu bir adım daha ileri götürülerek RF tarafından yapılan hamlelerin arkasında 2012 RF seçimlerinde Beyaz Saray yöneticilerinin Putin karşıtı faaliyetleri sebebiyle bizzat Putin'in bulunduğu iddiaları basında yer almıştır (Darıcılı, 2017a: 16).

Siber saldırıların 2015 yılında başlayacak şekilde RF İç İstihbarat Örgütü (FSB) ve Askeri İstihbarat Örgütü (GRU) koordinesinde bizzat ve bunların desteklediği gruplar (Cozy Bear, Fancy Bear, The Dukes, APT-28 ve APT-29) aracılığı ile yapıldığı belirtilmiştir. Yemleme tekniği ile konuyla ilişkili kişi ve kuruluşların 60 bine yakın elektronik postası ele geçirilerek amaçlar doğrultusunda açık kaynaklara servis edilmiştir (New York Times, 2016). Yaşanan bu olaylar sonucunda;

- Demokrat Parti kampanyası olumsuz etkilenmiş,
- Üst düzey bazı yöneticiler istifa etmiş,
- Demokrat Parti'nin diğer adayının pozisyonu kuvvetlenmiş,
- Cumhuriyetçilerin eline ciddi bir argüman geçmiş,
- Seçim süresince Clinton ciddi şekilde yıpratılmıştır.

Bahse konu siber saldırılara ilişkin ABD İç Güvenlik Bakanlığı ve Federal Araştırma Bürosu (FBI) tarafından 29 Aralık 2016 tarihinde yapılan çalışmada RF olayın faali olarak açıkça suçlanmıştır. Yapılan basın açıklamalarında gündemin ötesinde RF'nin ülkedeki kamu kurum/kuruluşlarına, firmalara, üniversitelere yönelik saldırılar da planladığı ve RF'in bu saldırılarına "Grizlly Steppe" takma ismi verildiği ifade edilmiştir (ABD İç Güvenlik Bakanlığı, 2016).

Diğer yandan, FBI, Merkezi Haber Alma Servisi (CIA) ve Ulusal Güvenlik Ajansı (NSA) ortak çalışması ile 7 Ocak 2017 tarihinde basınla paylaşılan araştırmada; "Putin'in 2016 ABD Başkanlık seçim sürecinin manipülasyonu emrini bizzat verdiği iddaa edilmiştir (ABD Milli İstihbarat Direktör Ofisi, 2017:7).

Olayların ardından bazı RF diplomatları siber saldırılarla alakaları bulunduğu gerekçesiyle istenmeyen kişi ilan edilerek ülkelerine gönderilmiş, Maryland ve New York'ta bulunan iki RF temsilciliğinin kapatılmasına karar verilmiştir (Sputnik Haber Sitesi, 2017).

Son olarak, seçimlere RF müdahalesi hakkında yapılan soruşturma kapsamında FBI Eski Başkanı James Brien Comey 6 Haziran 2017'de Kongre'de vermiştir. İfadesinde; "Rusya'nın seçimlerle ilgili siber saldırı yaptığı konusunda şüphe duymadığı, Trump'ın kendisinden konuyla ilgili yapılan 'FBI soruşturmasını durdurmasını istediğini, bu kapsamda Trump'a güvenmediği için adı geçen ile yaptığı her görüşmeyi kayıt altına alma ihtiyacı hissettiğini" açıklamıştır (BBC, 2017).

Yaşanan olaylar uluslararası hukuk kapsamında genel olarak kıymetlendirildiğinde; siber casusluk, kuvvet kullanma ve meşru müdafaa, içişlerine müdahale edilmeme ilkesinin ihlali vee özel hayatın gizliliğinin ihlali gibi kavramlar karşımıza çıkmakta ve bu kavramlar da siber bağlamında halen daha literatürde yoğun bir şekilde tartışılmaktadır (Bülbül, 2018).

6. SİBER HAREKÂTIN ULUSLARARASI HUKUK AÇISINDAN ANALİZİ

Günümüzde karar vericilerin sahip olduğu en önemli güç unsuru şüphesiz bilgidir. Bilgiye sahip olan taraf, barış döneminden itibaren gücü de elinde bulundurmakta ve savaşta harekât ortamının şekillendirmesini kolaylaştırmaktadır. Devletlerin güvenliğini tehdit eden ve hedefine ulaşmada tüm sınırları zorlayan siber eylemler, güvenlik ve tehdit anlayışına yeni bir boyut getirmiştir.

Siber eylemlere yönelik uluslararası hukukta doğrudan bir hukuki düzenleme bulunmamakla birlikte,

-BM Antlaşmasının Meşru Müdafaa hakkını düzenleyen 51'inci maddesi,

-Barışa tehdit veya saldırgan hareketi tanımlayan 39'uncu maddesi,

-NATO Antlaşmasındaki saldırı kavramını tanımlayan 5'inci maddesi,

-Cenevre Sözleşmesi'nin Sivillerin Korunması ile ilgili 4'üncü bölümü,

-Cenevre Sözleşmesi Ek Protokolleri, çerçevesinde bazı konular ele alınabilmektedir.

Siviller ve sivil hedefler kavramı dikkate alındığında, siber saldırıların uluslararası hukukta çeşitli yaptırımlara maruz kalabileceği ortaya çıkmaktadır. Örneğin, meşru müdafaa kapsamında bekanın ön planda olduğu, BM Güvenlik Konseyi kararında, silahlı müdahale dâhil her türlü yaptırımın yapılacağı, Cenevre Sözleşmesine aykırılık durumunda uluslararası yargılama ile karşılaşılacağı ve NATO'nun her türlü müdahale hakkının saklı olduğu sıklıkla ifade edilmektedir (Gervais, 2012:536, Çiftçi,2017:96-97).

Siber eylemlerin hukuki yönden kategorize edilmesi hususunda farklı belirsizlikler söz konusudur. Siber eylemlerin kaynağının belirlenmesi konusu karşımıza çıkan ilk problemi oluşturmaktadır. Bu tarz durumlarda, belli merkezler tarafından dünyada farklı yerlerde bulunan köle bilgisayarlardan oluşan bir sistematik ile hedefe angaje olunmaktadır. Verilen zarar ve tesirleri bakımından incelendiğinde, siber saldırı kategorisindeki eylemlerin konvansiyonel savaşlar gibi maddi ve can kayıplarına kolaylıkla neden olabileceği görülmektedir (Güreşçi, 2019:85-86).

Savaş hukuku açısından siber saldırılar, silahlı saldırı çerçevesinde ele alındığında saldırıya maruz kalan ülkeye meşru müdafaa hakkı doğacaktır. Ancak, saldırıya maruz kalan tarafın kendisini hangi araçlarla (fiziksel silahlar veya siber savunma araçları) savunacağı hususu muğlaktır. Bu noktada kullanılan araçlardan ziyade saldırının meydana getirdiği etkinin ele alınması anahtar rol oynamaktadır (Güreşçi, 2019:88).

Çalışmanın bu kısmında mevcut uluslararası mevzuatın siber uzaya uygulanabilirliği ve yeterliliği analiz edilmekte, siber harekât spektrumunda yer alan eylemler hafiften şiddetliye doğru Silahlı Çatışma Hukuku açısından değerlendirilmektedir.

Siber savaşın mevcut uluslararası düzenlemelere bağlı olarak kıymetlendirilmesi neticesinde, askerî harekâta ilişkin kuralların siber çatışmaya uyarlanarak kısa vadeli bir netice üretilmesi halinde siber eylemlerin kendine özgü yapısından kaynaklı yorum

farklılıkları ortaya çıkabilmektedir. Siber harekât ortamının gün geçtikçe çerçevesinin ve uygulama sahalarının genişlemesiyle beraber ülkeler arasında taktik/operatif/stratejik düzeylerde rekabet alanı olacağı dikkate alındığında, siber harekâtın mevcut uluslararası düzenlemelerin geniş şekilde yorumlanarak icra edilmesi halinde ileride yeterli olmayacağı görülmektedir. (Doğru, 2016:10).

NATO Siber Savunma Mükemmeliyet Merkezi internet sitesinde bağımsız uzmanlar grubu tarafından 3 senelik bir araştırmanın neticesinde 2013 senesinde "Uluslararası Siber Güvenlik Hukuku" ve "Siber Silahlı Çatışma Hukuku" başlıklarından meydana gelen ve herhangi bir hukuksal bağlayıcılığı olmayan "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı" yayınlanmıştır (Gedik, 2018:77).

Tallinn El Kitabı ile uluslararası bağlayıcılığı olmamasına, resmi bir özellik taşımamasına karşın ciddi bir adımla "Haklı Savaş Kuramı-*jus ad bellum*" ve "Çatışma Hukuku Kuramı-*jus in bello*" kaideleri siber alana uyarlanmıştır. Kitapta genel olarak;

- Bir ülkenin egemenlik alanında yer alan siber altyapı ve faaliyetleri kontrol altında tutulabileceği,
- Bir ülkenin, kendisiyle irtibatlandırılacak bir siber eylem için uluslararası platformda hukuki sorumluluk taşıyacağı,
- Uluslararası mevzuata aykırı bir eylemden dolayı zarara uğrayan bir ülkenin, olaydan sorumlu ülkeye yönelik siber tedbirler alabileceği,
- Siber taarruzun büyüklüğü ve tesirleri yönüyle, klasik bir harekâta eşit bir tesir meydana getiriyorsa, o siber taarruzun "kuvvet kullanımı" manasına geleceği,
- Çapı ve tesirleri itibariyle silahlı saldırı olarak tanımlanan bir siber saldırıya yönelik, mağdur ülkenin meşru müdafaa hakkının bulunacağı,
- Sivil halka ve altyapılara yönelik siber taarruz yapılamayacağı,
- Çift yönlü yani hem askeri hem de sivil maksatlarla kullanılabilecek hedeflere karşı siber saldırının mümkün olabileceği,
- Bir ülkede bulunan siber altyapı vasıtasıyla siber eylemlerin kanalize edilmiş olması, bu ülkeye sorumluluğu yüklemek için kâfi gelemeyeceği,
- Bir ülkenin sınır bütünlüğüne, siyasi özgürlüğüne tehdit meydana getiren veya kuvvet kullanımı ihtiva eden veya BM'nin hedefleriyle uyum göstermeyen siber eylemlerin yasal olmayacağı,

- Küresel ve bölgesel kurum/kuruluşların, BMGK tarafından yetkilendirilmesini veya vazifelendirilmesini müteakip, siber eylemlere karşı veya siber eylemler ihtiva eden durumlarda yaptırım özelliğindeki uygulamaların kullanılabileceği ifade edilmiştir (Talin El Kitabı, 2013).

6.1. Siber Uzayın Siber Eylemlerde Kullanımı

Siber uzay, dünyaya ve uzaya yayılmış halde olan bağımsız ve/veya birbirine bağlı her türlü bilişim sistemi, teknoloji, ağ ve bilgi sistemlerini kapsayan sayısal bir ortamdır. BİT 'de yaşanan baş döndürücü gelişmelerin hem günlük hayatta bireysel olarak hem de kurumsal manada pek çok aktör tarafından her konuda kullanılması neticesinde siber ortam her türlü etkileşime açık bir alan halini almıştır (Ataç, 2019:7).

Daha önce de ifade edildiği gibi siber ortam; kara, deniz, hava ve uzaya ilave olarak beşinci muharebe sahası olarak ele alınmaktadır (Lynn, 2010: 101). Siber ortamda değişik düzeylerde farklı siber saldırılar örnek gösterilmektedir. En basit örnek olarak, kişisel verilerin ele geçirilmesini amaçlayan tek başına hareket eden hackerlar gösterilirken, en gelişmişleri arasında nükleer tesislere, kritik altyapılara, kapalı bağlantı sistemleri veya sanayii kontrol sistemlerine, finans sektörüne zarar verebilecek olanlar gösterilebilmektedir (Neuneck ve Siroli.2013:2).

Çok süratli bir şekilde kendini yenileyen bir savaş tarzı olarak ifade edilen siber savaş ortamı gün geçtikçe daha fazla genişlemektedir. Silahlı Çatışma Hukuku'nun uygulanacağı alanı tespit etmek maksadıyla, bağımsız olarak icra edilen siber saldırılar ile askeri harekâtlara destek sağlayan siber eylemleri ayırmak gerekmektedir.

2007 senesinde Estonya örneğinde yaşanan siber saldırıda, Dağıtık Servis Dışı Bırakma (DDOS) taarruzları, RF ve Estonya arasındaki siyasi anlaşmazlıkların yaşandığı bir ortamda yapılmış ve çevrimiçi verilen birçok hizmetin kullanılamaz hale gelmesine sebep olmuştur. Siyasette yaşanan gelişmeler siber uzaya taşınmıştır (Clarke ve Knake, 2011:13-15). Estonya'ya yönelik saldırı siber kabiliyetlerden öncelikli araç olarak istifade etmenin bir örneğini oluşturmaktadır.

2008 senesinde Güney Osetya meselesi nedeniyle RF-Gürcistan Savaşı öncesinde RF tarafından başlatıldığı öne sürülen siber taarruzlar, askerî harekâttan 10 gün önce 29

Temmuz 2008'de düşük yoğunluklu olarak kendini göstermiş, asıl vurucu taarruzlar RF harekâtı ile eş zamanlı olarak, koordineli biçimde ivme kazanmıştır. RF siber saldırıları askerî harekâtla koordineli yapılan ilk saldırılar olarak ele alınmaktadır. Gürcistan'a yapılan bu saldırı siber kabiliyetlerin, geleneksel askerî harekâtlarda destekleyici araç olarak kullanılmasının bir örneğidir (Zoller, 2010:5).

Aslında bu vakalar fiziksel silahlardan yararlanmadan da savaşa veya çatışmaya benzer olguların siber ortamdan kaynaklanabileceğini göstermektedir. Bu farklı çatışma türünde devletler söz konusu olabileceği gibi devlet dışı aktörler de yer alabilmektedir (Doğru, 2016:4).

6.2. Siber Eylemler ve Haklı Savaş Kuramı (*Jus Ad Bellum*)

Günümüz uluslararası düzeninde silahlı güç kullanımının yasal olarak haklı olabilmesi için bazı özellikleri taşıması ve konuya ilişkin uluslararası hukuk kaidelerine riayet edilmesi gerekmektedir. Hukuki çerçevede olmadığı takdirde eylemler haksız sayılmaktadır. Hâlihazırda uluslararası hukukta kuvvet kullanmayı ele alan ana düzenleme BM Antlaşması'dır (Başeren, 2003:46).

"*Jus Ad Bellum*" ülkenin kuvvet kullanımını ele alan uluslararası hukukun bir parçasıdır ve meşru müdafaa kavramının uluslararası hukuk bakımından esasını oluşturmaktadır. Hukuki çerçevesi BM Şartı Md.2/4'de: "Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı, gerek Birleşmiş Milletler 'in amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar." şeklinde ifade edilmektedir. Bireysel ve kolektif meşru müdafaayı düzenleyen esaslar BM Şartının 51. maddesinde ele alınmıştır.

Devlet tarafından yapılan siber eylemlere hangi hukuk kurallarının tatbik edileceğini tespit etmek için cevaplanması gereken ana soru, devlet ve muhasım arasında silahlı bir çatışmanın var olup olmadığıdır. Bu kapsamda Silahlı Kuvvetler tarafından icra edilebilecek siber harekâtın hukuksal tahlili için *Jus Ad Bellum* iyi bir referans teşkil etmektedir.

Siber uzay bir ülkenin kuvvet kullanımına ulaşmayan icraatlarına ilave olarak ölümlü ve/ veya yaralanmalı neticelere sebep olabilecek faaliyetler içinde son derece elverişlidir. Yaşamın kaybedilmesi, yaralanma veya maddi hasara neden olan siber eylemler, uluslararası mevzuat çerçevesinde silahlı saldırı veya kuvvet kullanımı olarak kıymetlendirilebilmektedir. ABD tarafından ifade edildiği şekliyle, siber eylemler basit suçlardan siber casusluğa ve en nihayetinde de maddi kayıp veya ölüme neden olan faaliyetlere kadar genişleyen bir spektrumda kendini gösterebilmektedir (ABD Siber Komutanlığı, 2011:2).

Yaygın bir şekilde siber casusluğun zarar gören ülkenin meşru müdafaa hakkını ortaya çıkaran silahlı saldırı veya müsaade edilmeyen kuvvet kullanımına dayanak sağlamadığı kıymetlendirilmektedir. Siber harekât spektrumunda "Adi Siber Eylemler" kategorisinde kıymetlendirilen salt siber casusluk ve siber suç, BM 51'inci maddesini ve diğer uluslararası hukuk düzenlemeleri içerisinde silahla karşılık verilmesini haklı çıkarmamaktadır. Netice itibari ile bu eylem basit bir hırsızlık veya başka ülkenin sistemlerine müsaadesiz giriştir.

Spektrumda yer alan siber müdahale eylemlerinin de benzer biçimde uluslararası mevzuata uygun kuvvet kullanımı sınıfına dâhil olmadığı yönündeki düşünceler literatürde ağır basmaktadır. Aynı şekilde bir ülkenin sistemlerine müdahaleyi ihtiva eden bilgi harekâtları uluslararası hukuktaki müdahale etmeme prensibini devreye sokmaktadır. Bu prensip, ülkelerin başka ülkelerin içişlerine karışmasını yasaklayan dayanak üzerine inşa edildiğinden dolayı saldırıya uğrayan ülkeler bu eylemleri BMGK'ne ileterek protesto edebilmektedir. Ancak, ABD eski Savunma Bakanı Leon Panetta'nın "Uzaktan idare edilen platformlar ve siber sistemler gibi modern araçların, savaşların yürütülüş şeklini nasıl değiştirdiğini birinci elden gördüm. Bunlar, askerlerimize, uzakta olsalar bile düşmanla çarpışma ve savaşın gidişatını değiştirme yeteneği sağlıyor" sözlerine benzer şekilde siber eylemlerin önemli neticeler ortaya koyduğu hallerde, karar vericilerin meşru müdafaa hakkını geniş çerçevede ele alması da söz konusu olabilmektedir. (Hürriyet, 2013)

Spektrumda en şiddetli konumda siber saldırılar bulunmaktadır. ABD yetkilileri tarafından yapılan açıklamalarda kendilerine yönelik yapılan siber saldırıların bir savaş eylemi olarak değerlendirileceği net bir şekilde ifade edilmektedir (Cohen, 2012). Ancak,

BM düzenlemeleri kapsamında meşru müdafaa durumunun oluşması için tespit edilen standartlar oldukça fazladır. Literatürde siber eylemin orantılı meşru müdafaayı haklı kılacak içeriği karşılaması için geniş çapta bir fiziksel hasar oluşması ve/veya ölüm/yaralanma ile neticelenmesi zarureti ortaya konmaktadır (Ruys, 2010:140).

Stuxnet vakasında yaşanan durumda İran nükleer tesislerine zarar verilmesine yönelik bir siber saldırı gerçekleştirilmiştir (Richardson, 2011:3). Bu olay bir ülkenin kritik tesislerine maddi hasar vermeyi hedefleyen bir saldırı olması açısından dikkat çekicidir. Saldırıya maruz kalan ülkenin siber ortamda icra edilen eylemleri ele alma şekli de olası bir kuvvet kullanımını meşrulaştırma adına önem arz etmektedir. Stuxnet olayında İran'ın saldırının tesirini ehemmiyetsiz olarak göstermesi eylemin meşru müdafaa hakkına dayanak olabilecek bir argüman olmasını engellemiştir.

Bazı araştırmacılar tarafından, konu etki odaklı yaklaşım çerçevesinde ele alınarak, siber uzaydaki eylemlerin tesirinin müsaade edilmeyen kuvvet kullanımına veya silahlı saldırıya eşit olup olmadığı değerlendirilerek tahlil yapılması gerektiği üzerinde durulmaktadır (Roscini, 2014:115). Aksi düşünceler olsa da siber uzaydaki bazı durumlarda *Jus Ad Bellum*'un hayata geçirilmesi geleneksel uluslararası hukuk yaklaşımı ile uyum arz etmektedir. Siber eylemin diğer bir ülkenin kritik altyapılarında maddi zarara neden olması durumunda, eylem kuvvet kullanımı olarak anlamlandırılabilmektedir. Tallinn El Kitabında ülkelerin kendi topraklarındaki siber altyapılar üzerinde egemenlik haklarının olduğu ve bunlara ilişkin saldırıların yasal olmadığı ifade edilmektedir (Schmitt, 2013:15).

Siber eylemlerin hangi düzeyde ve koşullarda meşru müdafaa durumunu oluşturabilecek bir silahlı saldırı olarak görüleceği veya siber saldırının silahlı saldırı olarak ele alınıp alınmayacağı hususu oldukça tartışmalı bir konudur. Kuvvet kullanımının yüksek seviyede yapılması ve başka ülkenin varlığını tehdit etmesi böyle bir eylemi uluslararası mevzuata göre silahlı saldırı kategorisine koymaktadır. Ancak, ne tarz eylemlerin Madde 2(4) kapsamındaki müsaade edilmeyen kuvvet kullanımı düzeyinde kıymetlendirileceği sorusu ve bu eylemin silahlı saldırı unsuru oluşturup oluşturmadığı klasik silahlar için de uluslararası analizlerin değişiklik gösterdiği bir konudur.

Pentagon, silahlı saldırılar içerisine siber silahları da dâhil ederek, BM'nin meşru müdafaa hakkına ithal edilebileceğini savunmaktadır (Radikal Ehaber, 2011). Fakat bu durumda siber saldırılara nasıl bir kanuni karşılığın verileceğini tespit etmek maksadıyla eylemin tabiatının karakterize edilmesi, ülkelerin kıymetlendirmesine kalmakta ve uluslararası düzenlemelerin uygulanmasına bundan sonra başlanmaktadır.

6.3. Siber Eylemler ve Çatışma Hukuku Kuramı (*Jus in Bello*)

Jus in Bello ülkelerin savaş sırasında uyguladığı hukuki mevzuatın tümünü kapsamakta ve kuvvet kullanımının seviyesini belirlemektedir. 1949 yılında imzalanan 4.Cenevre Sözleşmesi, ülkeler arasındaki silahlı çatışmaları ele alan ana hukuk belgeleri olarak görülmektedir. Diğer taraftan, savunma sanayiindeki yenilikler ve harekât ortamındaki dönüşümün tesiri ile bu sözleşmelere 1977 yılında iki adet ek protokol eklenmiştir (Kocatepe, 2006:5). Bu protokoller, modern harekât ortamının Uluslararası İnsancıl Hukuk çerçevesinde teknolojik yeniliklere ve değişimlere uyumunun birinci örneği olarak kabul edilmektedir. 2 numaralı Ek Protokol, uluslararası mahiyette olmayan silahlı çatışmaları ele alan ilk uluslararası düzenlemedir (Geib, 2006:758). Silahlı saldırı, uluslararası ve uluslararası olmayan saldırılar olarak 2 türde meydana gelmektedir. Uluslararası silahlı çatışmada, iki veya daha çok ülke arasında bir silahlı çatışmanın olması halinde 1949 Cenevre Sözleşmeleri, Ek Protokol-I ve La Haye Yasası uygulanmaktadır. Ancak, bir ülke ile organize silahlı grup arasındaki uluslararası olmayan silahlı çatışmada Cenevre Sözleşmeleri'nin 3. Ortak Maddesi ve bazı hallerde Ek Protokol-II uygulanmaktadır (Solis, 2012:167-168).

Siber eylemleri Silahlı Çatışma Hukuku (SÇH) çerçevesinde kıymetlendirmeden önce cevap bulunması gerekli olan ilk soru siber eylemin SÇH açısından saldırı oluşturup oluşturmadığıdır. Saldırı fiili 1. Ek Protokol 49. maddede "Saldırı veya savunmada hasıma karşı şiddet kullanma eylemleri" olarak ifade edilmektedir (Brill, 2010:210). Saldırıdan bahsedilebilmesi için şiddet eylemini ihtiva etmesi zaruridir (Schmitt, 2011:92-93). Silahlı çatışma sırasında siber eylemler "şiddet eylemleri "ne neden olabilmektedir. Siber saldırıların birincil vasıta olarak kullanıldığı hallerde saldırılar *Jus in Bello* kapsamında silahlı saldırı seviyesine gelebilmektedir. Siber eylemlerin klasik askeri harekâtlarla koordineli olarak büyük çapta bir harekâtın desteklenmesinde

kullanıldığı hallerde siber saldırı eşiği muğlak bir durum arz etmektedir. Siber eylemlerin askeri harekâta destek sağlaması durumuna örnek olarak; bilgi harekâtı kapsamında harekât alanındaki sivil halka bazı bilgilerin servis edilmesinde siber eylemlerden istifade edilmesi mümkündür. Hedefi yalnızca sivil halkı etkilemek ve askerî harekâta yardımcı olmak kapsamındaki bilgiyi servis etmek olan siber eylemlerde hukuk ihlallerinde söz edilemeyeceği kıymetlendirilmektedir.

Uluslararası hukukta silahlı çatışmanın tanımından ayrı olarak, çatışma metotlarının her şartta SÇH ile uyumlu olmak zaruridir. SÇH'ın dört temel prensibi askeri gereklilik, ayrım, orantılılık ve gereksiz acının önlenmesidir. Silahlı bir çatışma sırasında kullanılan siber eylemler diğer kabiliyetlerle aynı esaslara tabidirler.

Saldırıya maruz kalan sivil mallar için, askeri gereklilik prensibi esas alınmalıdır. Askeri gereklilik prensibi vazifeyi başarmak için zaruri olan kuvvet kullanımına müsaade etmektedir. Fakat askeri gereklilik savaş hukukunca yasaklanan diğer eylemlere cevaz vermemektedir. Sivillerin içinde bulunduğu durumlarda tahliller daha da karmaşık bir hal almaktadır. Siber eylemlerin değişik bir tarafı da saldırıya uğrayan altyapının pek çoğunun aynı zamanda sivil halkın kullanımında olmasıdır.

Saldırının sadece askeri personel ve mallara yönelik yapılmasını zaruri kılan ayrım prensibinin kıymetlendirilmesi için siber eylemlerin kaynağının devlet veya devlet dışı aktörlere dayandırılması önem arz etmektedir. Estonya olayında yaşanan siber saldırı vakası, kaynağı belirleme sorununun klasik bir örneğini teşkil etmektedir. RF olayda sorumluluğu reddetmiş ve bağımsız olarak siber araçları kullanan hackerları suçlamıştır (Clarke, 2011:15-16). Kaynağı belirleme siber eylemlerde ciddi bir sorunsal olmakla birlikte üstesinden gelinmeyecek bir durum değildir. Mevcut kabiliyetlerle siber uzayda kaynağı tespit etmeye yönelik ciddi ipuçları bulunabilmektedir. Kaynağın tespiti noktasında, uluslararası işbirliği, bilgi paylaşımı ve detaylı istihbarat siber saldırılarda da doğru neticeler göstermektedir.

Orantılılık ilkesi, hedeflerin maddi tahribatına sebep olan siber eylemlerin meşruluğunu belirlemede kritik önemdedir. Orantılılık prensibi askeri hedefin ve avantajın elde edilmesinde sivil zararda aşırıya kaçılmamasını dikte etmektedir (Brill,

2010:211). İletişim, ulaştırma ve enerji altyapıları gibi tesislerin iki taraflı kullanımı zarar durumunda sivillere tesir etmesi sebebiyle hedef olarak ele alınması oldukça zordur.

Ayrıca, siber eylemler gereksiz acıya neden olmaktan sakınmalıdır. SÇH'nun "gereksiz acının önlenmesi" prensibi savaşanlara yönelik zararın sınırsız olmamasını vurgulamaktadır. SÇH savaşanlara askeri üstünlüğün elde edilmesinin ötesinde orantısız bir biçimde hasar vermek maksadıyla dizayn edilmiş belirli harp silah araç, gereç ve metotlarını yasaklamaktadır (Solis, 2012:272). Siber araçlar ve saldırıların kendi başlarına bu yasağı görmezden gelmeleri mümkün değildir. Ancak, siber araçlar da harp sistemlerine benzer biçimde ve gereksiz acının önlenmesi prensibi çerçevesinde kıymetlendirilmelidir.

Cenevre Sözleşmelerine 1 Numaralı Ek Protokol madde 35 kapsamında tarafların harp silah ve araçlarını tercih etme hakkı sonsuz değildir. Protokol çerçevesinde çatışma halinde dahi temel uluslararası insancıl hukuk normlarına saygı vurgulanmaktadır. Gereksiz acı çekilmesine neden olabilecek teknolojilerden istifade etmek ile kullanımı durumunda uzun süreli hasara sebep olacak metotlar yasaklanmaktadır. Ayrıca, madde 57'de sivil halka ve nesnelere hasar verdirebilecek taarruzlar açık bir şekilde yasaklanmaktadır. Siber savaş araçlarından istifade edilmesi durumunda bu düzenlemeler de göz önünde bulundurulmalıdır.

Değerlendirilmesi icap eden farklı bir hususta, *Jus in Bello*'ya uygun silahlar ve çatışma metodu açısından doğrudan siber ortamın silah olarak kullanılması durumudur. Siber ortamın silah olarak kullanılmasını sınırlayan bir düzenleme yoktur. Fakat bu durum SÇH'nin ayırım, ölçülülük ve gereksiz acıların önlenmesi prensibine aykırılık teşkil etmemelidir (Doğru, 2016:9).

Siber eylemlerden istifade edildiğinde çevreye verilmesi tahmin edilen hasarın titizlikle hesaplanabilmesi, bu metotları potansiyel olarak daha geniş ölçekli fiziksel taarruzlara göre daha tercih edilebilir yapmaktadır. Buradaki önemli husus, fiziksel hasara yönelik saldırılar ve adi siber eylemlerin siber harekât spektrumunun iki farklı tarafında bulunmasıdır (Philips, 2013:75). Açık kaynaklarda gündem olan vakaların çoğu siber gücün düşük seviyede kullanımını göstermektedir. Düşmanın elindeki bilgiye sahip olmayı hedefleyen siber eylemler veya sivil halkı etki altına almayı amaçlayan bilgi

harekâtı, “kuvvet kullanımı” veya “saldırı” tanımlarındaki sınırı aşmamaktadır. Fakat her hal ve şartta bu konuda ülkeler arasında mevzuat boşluğundan ortaya çıkabilecek değerlendirme farklılıkları, BM şartı ve SÇH’ndan bağımsız askeri reaksiyonların meydana gelmesine sebep olabilecektir.

DÖRDÜNCÜ BÖLÜM

DÜNYADA SİBER TEHDİTLERE KARŞI YAPILAN FAALİYETLER

1. KÜRESEL GİRİŞİMLER

1.1. Birleşmiş Milletler

BM, 1990'ların başından itibaren bilgi güvenliği ve siber güvenlik konusunda faaliyetler yürütmektedir. Bahse konu faaliyetler, BM Genel Kurulu'nca alınan kararlarla birlikte, BM BİT Görev Gücü ve BİT ile alakalı araştırmalar yapmakla görevli BM kuruluşu olan Uluslararası Telekomünikasyon Birliğini (International Telecommunications Union- ITU) kapsamaktadır.

BM, siber ortamda ülkelerin davranış çerçevesini belirlemede belli bir pozisyona sahip uluslararası bir kuruluştur. Konuya ilişin olarak 1990'larda başlayan çalışmalar sonucunda BM 1. Komitesi tarafından 2003 senesinde Silahsızlanma Dairesi Başkanlığının koordinatörlüğünde konuya ilişin uzlaşma alanlarını tespit etmek maksadıyla üst üstte beş adet toplantı icra edilmiştir. BM tarafından "Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmelere İlişkin Hükümet Uzmanları Grubu (UN Group of Governmental Experts-GGE)" teşkil edilerek bilgi güvenliği konusunda ciddi ilerlemeler kaydedilmiş ve 2011 senesinde siber suçlar konusunda kurulan GGE, ülkelerin müşterek bir platforma buluşması için gayret göstermiştir (Korhan, 2018:52-54).

GGE, 2015 yılında "uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler" ile alakalı bir mutabakat muhtırası hazırlamıştır (Meyer, 2015). GGE'ler, BM Tüzüğü'nde belirtilen uluslararası hukuk ve ülkelerin egemenliği prensiplerinin siber ortama tatbik edildiğine işaret ederek uluslararası siber güvenlik konusunda belli bir normatif kapsam oluşturmuştur. Fakat 2017 yılında yapılan çalışmalarda RF ve ÇHC'nin uluslararası hukuk normlarının siber ortamda tatbik edilmesini kabul etmeyerek onaylamaması sonucunda 2015 senesindeki teklifler için bir uzlaşı bildirisi yayınlanamamıştır (Korzak, 2017).

BM Genel Kurulu tarafından çeşitli tarihlerde alınan siber güvenlik ile ilişkili kararlar şunlardır:

- "Bilgi Teknolojilerinin Suç Amaçlı Kötüye Kullanımı ile Mücadele" başlıklı karar üye devletlere bilgi teknolojilerinden suç maksatlı istifade edilmesine yönelik milli düzenlemelerinde lüzumlu önlemleri almalarını ve suçluların istifade edebileceği boşlukları gidermelerini tavsiye etmektedir. Kararlarda ayrıca "Avrupa Konseyi Siber Suç Sözleşmesi "ne de vurgu yapılmakta ve bahse konu düzenlemeyi siber konusunda uluslararası seviyede ehemmiyetli bir mevzuat olarak görmektedir (BM Genel Kurulu 55/63 Sayılı Kararı, 2001 ve BM Genel Kurulu 56/121 Sayılı Kararı, 2002).

- "Küresel Siber Güvenlik Kültürünün Oluşturulması" başlıklı karar bilgi ve ağ güvenliğinin tesis edilmesinde, yaklaşımlarda değişiklik yapılmasının zaruretine işaret edilmekte, küresel çapta siber güvenlik zihniyetinin meydana getirilmesi maksadıyla lüzumlu ana faktörler (BM Genel Kurulu 57/239 Sayılı Kararı, 2003);

* Farkındalık,
* Sorumluluk,
* Güvenlik ihlallerine tepki verebilme,
* Etik,
* Demokrasi,
* Risk değerlendirme,
* Güvenlik tasarımı ve uygulaması,
* Güvenlik yönetimi ve
* Yeniden değerlendirme olarak ifade edilmektedir.

- "Küresel Siber Güvenlik Kültürünün Oluşturulması ve Kritik Bilgi Altyapılarının Korunması" başlıklı karar bilgi altyapıları ile küresel çaptaki diğer kritik altyapıların birbirine olan irtibatına ve bunlara yönelik gün geçtikçe fazlalaşan risk ve tehditlere vurgu yapmaktadır. Bahse konu karar, kritik bilgi altyapılarının savunulmasında takip edilmesi gereken ilkeleri şu şekilde belirtmektedir (BM Genel Kurulu 58/199 Sayılı Kararı, 2004);

** Siber tehditler, zafiyetler ve güvenlik ihlalleriyle alakalı acil durum ikaz sistemleri oluşturulmalıdır.*

** Tüm katılımcıların kritik bilgi altyapılarının çerçevesi ve kendilerinin bunlara yönelik sorumluluğu konusunda bilgi seviyesi yükseltilmelidir.*

** Altyapıları ve bu altyapıların birbirleri ile olan bağımlılıklarını belirleyerek güvenlik seviyesi arttırılmalıdır.*

** Unsurlar arasında (kamu-özel sektör) bilgi teatisini mümkün kılan ortaklıklar meydana getirilmesi özendirilmelidir.*

** Kriz iletişim sistemleri tesis edilmeli ve sistemlerin acil hallerde kullanılabilir olması maksadıyla gerekli testler yapılmalıdır.*

** Bilgilerin ulaşılabilirliğine yönelik stratejilerin kritik bilgi altyapılarının muhafaza edilmesine duyulan gereksinimi göz önünde bulundurması sağlanmalıdır.*

** Kritik bilgi altyapılarına ilişkin taarruzların takibi kolaylaştırılmalı ve lüzumlu durumlarda temin edilen bilgiler diğer devletlerle de paylaşmalıdır.*

** Vakalara müdahale imkânlarının geliştirilmesi, devamlılık ve acil durum planlarının denenmesi maksadıyla lüzumlu eğitim ve tatbikatlar planlanmalı, paydaşların da faaliyetlere iştirak etmesi sağlanmalıdır.*

** Kritik bilgi altyapılarına ilişkin taarruzların hukuki süreçlere tabi tutulması, bahse konu işlemlerin lüzumlu durumlarda diğer ülkelerle koordinasyon içinde yürütülebilmesi temin edildikten sonra gerekli kanuni mevzuat oluşturulmalı ve sorumlu personelin yeterli eğitim seviyesine haiz olması sağlanmalıdır.*

** Kritik bilgi altyapılarının emniyetini tesis etmek maksadıyla, lüzumlu durumlarda, acil durum ikaz sistemleri kurulmalı, tehditlere, zafiyetlere ve yaşanan vakalara yönelik bilgi teatisinin sağlanması gibi uluslararası iş birliği mekanizmaları içerisinde bulunulmalıdır.*

** Milli ve uluslararası ARGE faaliyetleri ve uluslararası standartlara göre sertifiye edilmiş güvenlik teknolojilerinin kullanılması teşvik edilmelidir*.

Bahse konu bu prensipler aynı zamanda 2003 senesinde Paris'te G8 Ülkeleri Adalet ve İçişleri Bakanları tarafından kabul edilen "Kritik Bilgi Altyapılarının Korunmasına İlişkin" prensiplerdir.

1.2. Uluslararası Telekomünikasyon Birliği (ITU)'nin Çalışmaları

ITU, esas olarak BİT hakkında çalışmalar yürüten, kamu ve özel sektör kuruluşlarına gelişmekte olan BİT şebekeleri ve hizmetleri alanında küresel çapta bir

merkez sunan BM ajansıdır. ITU'nun başlıca görevleri (Bilgi Teknolojileri ve İletişim Kurumu, 2018);

- Radyo spektrumunun küresel çapta ortak kullanımını koordine etmek,
- Gelişmekte olan dünyada elektronik haberleşme altyapısının geliştirilmesini sağlamak,
- Farklı haberleşme sistemleri arasında sorunsuz bağlantılar kurulmasına imkân verecek, dünya çapında kabul gören standartlar oluşturmak,
- Siber güvenliğin sağlanması gibi güncel konularda çalışmalar yapmaktır.

Merkezi İsviçre'nin Cenevre kentinde bulunan ITU'nun ülkemizin de aralarında bulunduğu 193 devlet bazında üyesi ve 800'den fazla sektör üyesi bulunmaktadır. ITU, özellikle aşağıda özetlenen Dünya Bilgi Toplumu Zirvesi süreciyle birlikte siber güvenlik konusunda etkin rol oynamaya başlamıştır (BM Cenevre Ofisi Nezdinde Daimî Temsilciliği, 2019).

ITU tarafından yayımlanan "ITU Ulusal Siber Güvenlik Strateji Rehberi-ITU National Cyber Security Strategy Guide" dokümanında ulusal siber güvenlik stratejisi süreci gösterilmiştir. Dokümanda ortaya konan model, fonksiyonları ve faaliyetleri de içerecek şekilde üst seviye bir görünüm ortaya koymaktadır. (Wamala, 2011:5).

1.2.1. Küresel Siber Güvenlik Gündemi

ITU Genel Sekreterliği, 17 Mayıs 2007 tarihinde, bilgi toplumunda güvenliğin tesis edilmesine ilişkin uluslararası koordinasyonun nasıl sağlanabileceğine dair bir model sunan "Küresel Siber Güvenlik Gündemi"ni (Global Cybersecurity Agenda/GCA) yayımlamıştır. Temeli ulusal değerler ve menfaatlere dayandırılan siber güvenlik stratejisinin oluşumunda, "Amaçlar-Yaklaşımlar-Kaynaklar (Ends-Ways-Means)" yaklaşımı kullanılmıştır. (Ataç, 2019:22). GCA kapsamında tespit edilen beş çalışma alanı Şekil 17'de sunulmuştur.

Şekil 17. GCA Çalışma Alanları

Kaynak: (Uluslararası Telekomünikasyon Birliği, 2019)

GCA'da tespit edilen 7 stratejik hedef **(**Uluslararası Telekomünikasyon Birliği, 2007:15):

- Global seviyede tatbik edilebilir, hâlihazırdaki milli ve bölgesel düzenlemelerle çatışmayan bir siber güvenlik mevzuatının oluşturulması,

- Siber güvenlikle alakalı faaliyet gösteren milli ve bölgesel kurum/kuruluşların kurulması ve stratejilerin geliştirilmesi,

- Global seviyede kabul edilen minimum güvenlik kriterlerinin ve hem yazılımsal hem de donanımsal olarak akreditasyon planlarının yapılması,

- Uluslararası koordinasyon ve iş birliğinin tesis edilmesi maksadıyla takip, ikaz ve vakalara müdahale için küresel bir model oluşturulması,

- Global bir dijital kimlik sisteminin teşkil edilmesi ve dijital kimlik verilerinin küresel çapta kabul görmesini temin eden bir düzenin meydana getirilmesi,

- Siber güvenlik hakkındaki bilgi teatisini sağlamak maksadıyla kurumsal kapasitenin arttırılması,

- Bütün bu hususlarda uluslararası işbirliği zemininin sağlanmasıdır.

ITU Genel Sekreterliğince koordinasyonu sağlanan Siber Güvenlik Kapısı (*Cybersecurity Gateway*), kamu ve özel sektör kurum/kuruluşlarını, STK'ları, bilim camiasını, konu hakkındaki küresel/ bölgesel kuruluşları aynı zeminde buluşturan bir inisiyatiftir. (Toure, 2019).

1.2.2. Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (International Multilateral Partnership Against Cyber Threats- IMPACT) ile Yürütülen Ortak Çalışmalar

Merkezi Malezya'da bulunan ve siber güvenlik konularına yönelik olarak kapasite oluşturmayı ve arttırmayı amaçlayan küresel girişim olan IMPACT, ITU ile birlikte müşterek araştırmalar yapmaktadır. Bahse konu araştırmalar (Ünver, Canbay ve Mirzaoğlu, 2011:11):

- Siber eylemlere yönelik olarak dünyada vuku bulan olaylara ilişkin verilerin eş zamanlı olacak şekilde elde edilmesine, tahlil edilmesine ve paylaşılmasına,
- Erken ikaz ve acil durum reaksiyon sistemi meydana getirilmesine,
- Siber güvenliğin hukuki, teknik, stratejik ve siyasi taraflarıyla alakalı kapasitenin arttırılmasına yardımcı olmaktadır.

2. BÖLGESEL GİRİŞİMLER

2.1. Avrupa Konseyi Girişimleri

Uluslararası seviyede siber suçlarla mücadele konusunda gösterilen gayretlerin en önemlilerinden biri Avrupa Konseyi tarafından 2004 senesinden itibaren kullanılmaya başlanan Siber Suçlar Sözleşmesi'dir. Bahse konu Sözleşme 47 (dördü Konsey üyesi değil) devlet tarafından kabul edilmiştir (Avrupa Konseyi, 2019).

Bölgesel bir inisiyatif olarak değerlendirilen Sözleşme, siber suçlara yönelik yapılan çalışmalar arasında ehemmiyetli bir basamak oluşturmaktadır. Taraf olan ülkeler Sözleşmede suç kapsamında belirtilen durumların, milli hukuki düzenlemelerinde de suç addedilmesini ve suçların araştırılmasını temin etmek için zaruri prosedürleri sağlamayı taahhüt etmiştir. Sözleşmeyi tamamlayıcı mahiyette 2005 senesinde "Bilgi Sistemlerine Yönelik Saldırılar Konusunda Avrupa Konseyi Çerçeve Kararı" alınmıştır (Aliusta ve Benzer, 2018: 37).

2.2. Avrupa Birliği'nin Çalışmaları

AB, siber güvenlik konusuna önem vererek bu konuyu toplumun önemli bir parçası olarak görmekte ve ağ güvenliği, bireysel verilerin korunması, e-ticaret, siber

suçlar gibi farklı birçok alanda ARGE ve prosedür oluşturma çalışmaları yapmaktadır. Bu kapsamda AB Komisyonu tarafından 2013 senesinde hazırlanan Siber Güvenlik Strateji Belgesinde vizyon, dünyanın en emniyetli ve güvenli altyapısına sahip olmak maksadıyla, bireylerin haklarını kollamak ve savunmak şeklinde ifade edilmiş ve bu hususun ancak özel/kamu ilgili tüm ulusal/bölgesel/küresel kurum/kuruluş arasında yapılacak koordinasyon ve işbirliği ile sağlanacağına vurgu yapılmıştır (Avrupa Birliği Komisyonu, 2013: 19-20).

AB'de siber güvenlik konusuna ilişkin faaliyet gösteren, merkezi Atina'da bulunan bir kurum da "Avrupa Şebeke ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency – ENISA)"dır (ENISA, 2019a). 29 Mart 2014'te 2004/460/EC numaralı karar ile kurulan ENISA'nın başlıca görevleri (ENISA, 2019b):

- AB'nin tüm kurum/kuruluşlarına, ülkelerine ve iş çevrelerine bilgi güvenliği hakkında tavsiyeler vermek,

- Avrupa'da vuku bulan vakalara ve artan tehditlere yönelik veri toplamak ve tahlil etmek,

- En iyi uygulamalara ilişkin bilgi teatisine imkân tanımak,

- AB'ye yönelik siber tehditlere ilişkin risk kıymetlendirme ve risk yönetimi imkânını arttırmak,

- Bilgi güvenliği konusundaki bilinç seviyesini ve işbirliğini geliştirmektir.

Diğer taraftan ENISA, üyelerinin ve adaylarının teşkil ettiği "Bilgisayar Olaylarına Müdahale Ekiplerine (Computer Emergency Response Team-CERT)" eğitim ve teknik destek de sağlamaktadır. Türkiye'de TÜBİTAK–UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) tarafından oluşturulan TR-BOME'nin ve ulusal akademik ağ kapsamında TÜBİTAK ULAKBİM tarafından kurulan ULAK-CSIRT'nin, ENISA tarafından akreditasyonu sağlanmıştır. (BTK, 2009)

2.3. NATO

NATO'da siber güvenlik konusunda gerçekleşen en ciddi inisiyatif NCIRC (NATO Computer Incident Response Capability) projesidir. 2005 yılından beri işlevsel olarak faaliyetlerini sürdüren proje, NATO ağlarını korunmakta, siber güvenlik desteği

sağlamakta, bilgi güveliği ve altyapılarına yönelik olayları incelemekte ve aynı zamanda Acil Reaksiyon Timlerini görevlendirmektedir. (NATO, 2016:1).

Estonya bilgi sistemlerine yapılan siber taarruzlar sonucunda NATO tarafından 2008 yılında Talinn'de "Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Enter of Exellence-CCD CoE) kurulmuştur. Mükemmeliyet Merkezi siber güvenlik konusunda eğitimden teknik desteğe ARGE faaliyetlerinden danışmanlığa kadar çok geniş bir spekturumda faaliyetler icra etmektedir. Diğer taraftan, Mükemmeliyet Merkezi koordinesinde yürütülen önemli çalışmalardan birisi de 2013 senesinde bağımsız uzmanlar grubu tarafından uzun çalışmaların sonucunda yayınlanan "Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı-The Tallinn Manual on the International Law Applicable to Cyber Warfare"dır (NATO Siber Savunma Mükemmeliyet Merkezi, 2019).

NATO tarafından siber güvenlik konusundaki çalışmalar yıllar içerisinde devam etmiş, 2012 senesinde "NATO'nun Muhabere ve Bilgi Teşkilatı (NCI Agency)" içerisinde "Siber Güvenlik Hizmet Hattı (CSSL)", siber güvenliğin tesis edilmesi için gerekli bütün hayati önemdeki faaliyetlerin idare edilmesinden sorumlu olacak biçimde kurulmuştur (Çeliktaş, 2016:75).

2.3.1. NATO Stratejik Konsepti-2010

NATO tarafından 2010 senesinde yayınlanan Stratejik Konsept'te siber güvenlik konusuna ayrıca işaret edilmiş ve üzerinde durulmuştur. Konsept'te siber tehdidin geldiği noktayla ilgili; "Siber saldırılar daha sık, daha organize bir şekilde gerçekleştirilmekte ve hükümet birimleri, iş dünyası, ekonomi ve muhtemelen ulaştırma, nakil hatları ve diğer önemli altyapılar üzerinde yarattığı hasarın maliyeti daha ağır olmaktadır. Siber saldırılar, ulusal refah ve Avrupa-Atlantik refahı, güvenlik ve istikrarı tehdit eden bir eşiğe ulaşabilir. Yabancı silahlı kuvvetler ve istihbarat servisleri, her biri bu tür saldırıların kaynağı olabilecek suçluları, terörist ve/veya aşırı uç grupları organize edebilir." ifadelerine yer verilmiştir (NATO, 2010:4).

Konsept siber savunmaya ilişkin olarak da: "*Siber saldırıları önleme, belirleme, bu saldırılara karşı savunma ve saldırının ardından toparlanma yeteneğimizi daha da geliştireceğiz. Buna ulusal siber savunma imkân ve kabiliyetlerimizi geliştirmek ve*

koordine etmek için NATO planlama sürecinin kullanılması, bütün NATO birimlerinin merkezi bir siber koruma altına alınması ve NATO'nun siber farkındalığını, uyarılarını ve tepkisini, üye ülkelerle daha iyi bir şekilde entegre etmek de dâhildir." ifadelerine yer vermiştir (NATO, 2010:5).

NATO bünyesinde yapılan çalışmalar neticesinde 2011 yılı sonunda "Siber Savunma Eylem Planı" detay hususları hakkında fikir birliğine varılmış ve üye ülkeler, milli irtibat noktalarını bildirmiştir. Türkiye milli irtibat noktası olarak TÜBİTAK UEKAE bildirilmiştir (Şentürk, Çil ve Sağıroğlu, 2012:118).

2.3.2. Son Gelişmeler

2012 yılında yapılan Chicago Zirvesi'nde yayınlanan Sonuç Bildirisi'nde de devamlı gelişen ve karmaşık hale gelen siber tehditlere karşı etkin şekilde ve koordinasyon içerisinde mücadele edilmesinin önemine işaret edilmiştir (Chicago Zirve Bildirgesi, 2012).

2014 yılında yapılan Galler Zirvesi'nde ciddi bir adım atılarak siber taarruzların ittifak üyelerinin kollektif savunması çerçevesinde 5'inci maddeyi harekete geçirebileceği belirtilmiştir. Fakat üyelerin böyle bir duruma maruz kalması halinde saldırganın nasıl tespit edileceği ve verilecek karşılığın mahiyeti hakkında herhangi bir hususa yer verilmemiştir. (Galler Zirve Bildirgesi, 2014).

Ayrıca, Zirve'de NATO'nun ana vazifelerinin yerine getirilmesine kolaylık sağlayacak yeni siber eylem planı yürürlüğe girmiştir. Bu çerçevede, NATO siber risk ve tehditler ile yaşanan sorunlara yönelik özel sektörle de koordinasyonu arttıracak bir faaliyette bulunmuş ve "NATO Endüstri Siber Ortaklığı (The NATO Industry Cyber Partnership (NICP))"nın amaçları 1500 sektör temsilcisi ve politikacının katıldığı bir organizasyonda tanıtılmıştır (NATO, 2014). Müteakiben bahse konu faaliyetler düzenli olarak yapılmaya devam edilmiştir.

2016 yılında yapılan Varşova Zirvesi'nde de önceki zirvelerde olduğu gibi siber güvenlik konusu önemli başlıklardan birini oluşturmuştur. Zirve'de siber güvenlik konusunda daha fazla işbirliği ve diyalog içerisinde olunması gerektiği belirtilmiş, siber saldırıların da klasik saldırılar kadar zararlı olduğu, siber uzayın da bir harekât ortamı

olarak tanındığı, siber uzayda barış ve istikrarın tesis edilmesi için gayret gösterileceği hususlarına vurgu yapılmıştır (Varşova Zirve Bildirgesi, 2016).

2018 yılında yapılan Brüksel Zirvesi'nde siber tehditlerin her geçen gün daha hazla, karmaşık ve yıkıcı bir şekilde güvenliği tehdit ettiği bildirilmiştir. Kollektif savunma kapsamında siber savunmanın ittifakın önemli görevlerinden birisi olduğu, aynı deniz hava ve kara da olduğu gibi siber uzay ortamında da etkili bir şekilde harekât icra etme kabiliyetine sahip olunması gerektiği belirtilmiştir. Ayrıca NATO'nun durumsal farkındalığının sağlanası ve siber uzaydaki NATO harekât faaliyetlerinin koordinasyonu için Belçika'da Siber Güvenlik Harekât Merkezi kurulacağı açıklanmıştır (Brüksel Zirve Bildirgesi, 2018).

3. ÜLKELERİN SİBER GÜVENLİĞE YÖNELİK ÇALIŞMALARI

Çalışmada, "1990'ların başından itibaren ülkelerin bilgi güvenliği ve siber güvenlik konusunda faaliyetleri ve dünyada atılan adımlar nelerdir?" araştırma sorusundan hareketle, ABD, Rusya ve Çin'in siber güvenlik politikaları, resmi politika belgeleri ve ilgili literatür üzerinden incelenmiştir. Söz konusu üç ülkenin seçilme nedeni, bu ülkelerin gerek ekonomik, gerekse askeri unsurlar bakımından dünyada "başat güç" ya da başka bir deyişle "süper güç" olarak kabul edilmeleridir. Dolayısıyla, bu ülkelerin siber güvenlik politikalarının, sahip oldukları siber güvenlik donanım ve tecrübelerinin incelenmesinin, araştırma sorusuna yanıt arama sürecinde son derece anlamlı olacağı düşünülmüştür.

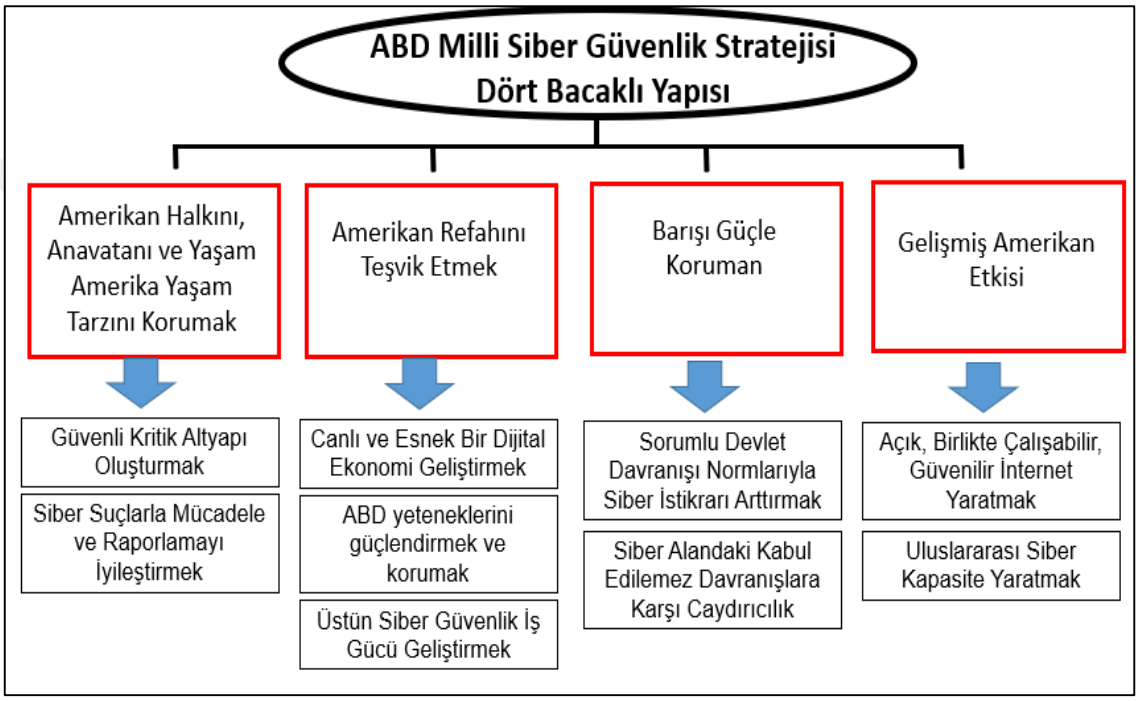
3.1. ABD Siber Yapılanması

ABD siber güvenlik konusu ile ilgili çalışmalarına 1990'lı senelerden itibaren başlamış ve özellikle 2000'li yıllardan itibaren çalışmalarını süratlendirmiştir (Wedermyer, 2012:10). Konuya ilişkin ilk kapsamlı doküman "Siber Uzay Güvenliği İçin Ulusal Strateji (The National Strategy to Secure Cyberspace)" adı altında 2003 yılında hazırlanarak siber uzayda görev alacak kurumlar belirlenmiş, müteakip dönemde konuya ilişkin farklı kurumlar tarafından çalışmalar yapılmıştır (Korhan, 2018:45).

ABD eski Başkanı Barack Obama, siber güvenlik konusunun ABD'nin yüzleştiği en ciddi ekonomik ve milli güvenlik problemlerinden biri olduğunu açıkça ifade etmesi

konunun önemini ortaya koymaktadır. (BBC, 2015). ABD'de siber güvenlik konusunda faaliyetler icra eden üç ana kurum bulunmaktadır. Bunlar; ABD Savunma Bakanlığı (United States Department of Defense), ABD İç Güvenlik Bakanlığı (The Department of Homeland Security) ve ABD Gizli Servisleri (FBI / CIA)'dir (Darıcılı, 2017a:7).

Siber güvenlik konusu ile alakalı son olarak Beyaz Saray tarafından 2018 yılı sonunda "Ulusal Siber Güvenlik Stratejisi-National Cyber Security Strategy" dokümanı hazırlanmış ve Şekil 18'de sunulan dört bacaklı bir yapı teşkil edilmiştir.



Şekil 18. ABD Milli Siber Güvenlik Stratejisi

Kaynak: (ABD Ulusal Siber Güvenlik Stratejisi, 2018)

2008 yılında ABD Savunma Bakanlığı (US Department of Defence-DoD) tarafından savaş veya silahlı çatışma halinde siber uzayın kontrol vazifesi Hava Kuvvetleri (USAF)'ne verilmiştir. Müteakiben siber uzayın kontrol sorumluluğunun yeni teşkil edilecek Siber Komutanlığa (USCYBERCOM)'na verilmesi planlanmıştır (Wedermyer, 2012). Siber Komutanlığı 31 Ekim 2010 tarihinde faaliyetlerine başlamıştır (ABD Savunma Bakanlığı, 2010:1).

3.1.1. Siber Komutanlığa Geçiş

Dünyanın en gelişmiş silahlı kuvvetlerine, silah, teçhizat, araç ve gereçlerine sahip ABD, elinde bulundurduğu bu teknolojik üstünlüğün neticesinde siber tehditlerden en çok etkilenen ülkelerin arasında yer almaktadır. Dünyanın çeşitli yerlerinde ABD askeri birimlerine ait, 88 ülkedeki 4 bin askeri üste, 15 bin iletişim ağı, 7 milyondan fazla bilgisayar olduğu ve bu altyapıyı idame ettirmek için yaklaşık 90 bin personelin istihdam edildiği ve milyarlarca dolar harcandığı ifade edilmektedir (Whitney, 2010).

Bu devasa büyüklükteki organizasyonu, dünyanın farklı coğrafyalarındaki ABD üslerine ait bilgi ve iletişim altyapılarını korumak maksadıyla 2009 yılında kurulan ve 2010 yılında tam harekât kapasitesi ile faaliyet göstermeye başlayan ABD Siber Komutanlığı, ABD Stratejik Komutanlığı altında müstakil bir alt komutanlık olarak kurulmuştur.

3.1.2. Siber Komutanlığın Görevleri

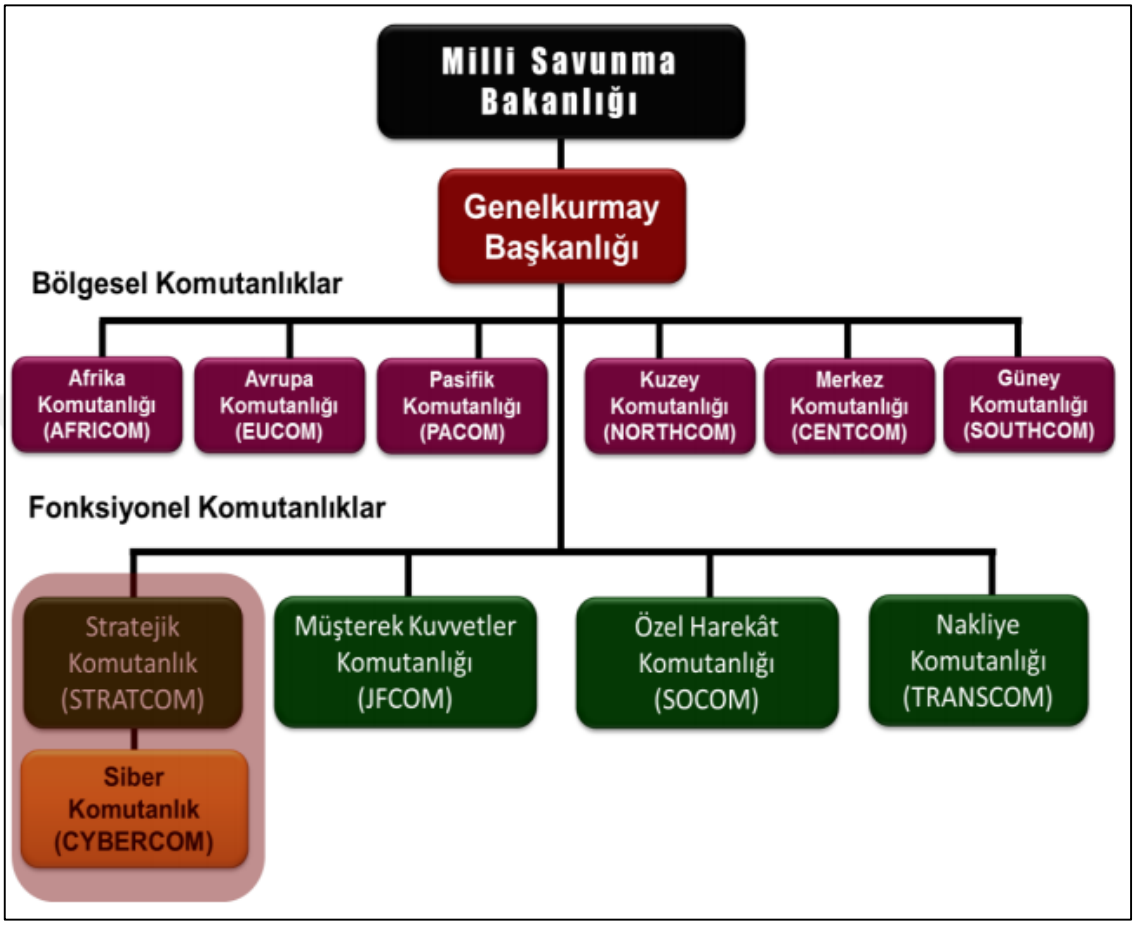
Siber Komutanlığın görevleri bilgi ağlarını korumak, siber uzaydaki askeri faaliyetleri idare etmek, siber uzayın sorunsuz bir şekilde kullanılması ve muhasım faaliyetlerinin önüne geçilmesi maksadıyla her türlü faaliyeti icra etmek şeklinde belirlenmiştir. Komutanlık siber güvenliğin tesis edilmesi maksadıyla, bilgi güvenliğine ilişkin hususları bir platformda toplayarak sinerji oluşturmayı hedeflemektedir (Jelinek, 2010). Siber Komutanlık tarafından; Bakanlık sanal ağlarının emniyetli, güvenilir ve korumalı olmasının sağlanması, siber uzaydaki tehditleri engelleyebilecek imkân ve kabiliyetlerin kazanılması ve siber uzayda icra edilecek harekâtların idaresinin merkezîleştirilmesi hedeflenmektedir (ABD Savunma Bakanlığı, 2010:1).

Siber Komutanlık bakanlığın (".mil" alanı) sanal ağlarını korumakta olup (".gov" alanı) sivil ağların güvenliği İç Güvenlik Bakanlığı (Department of Homeland Security) tarafından sağlanmaktadır.

3.1.3. Siber Komutanlığın Teşkilat Yapısındaki Durumu

ABD'nin 6'sı bölgesel ve 4'ü fonksiyonel olmak üzere toplam 10 birleşik muharip komutanlığı (Unified Combatant Command) bulunmaktadır. Siber Komutanlığı bünyesinde barındıran ABD Stratejik Komutanlığı uzay harekâtı, bilgi harekâtı, füze

savunması, komuta kontrol, istihbarat, keşif ve gözetleme ve nükleer silahlardan sorumlu komutanlık konumundadır. Siber Komutanlığın, Savunma Bakanlığı Birleşik Muharip Komutanlıklar teşkilat yapısı içerisindeki durumu Şekil 19'da sunulmuştur.



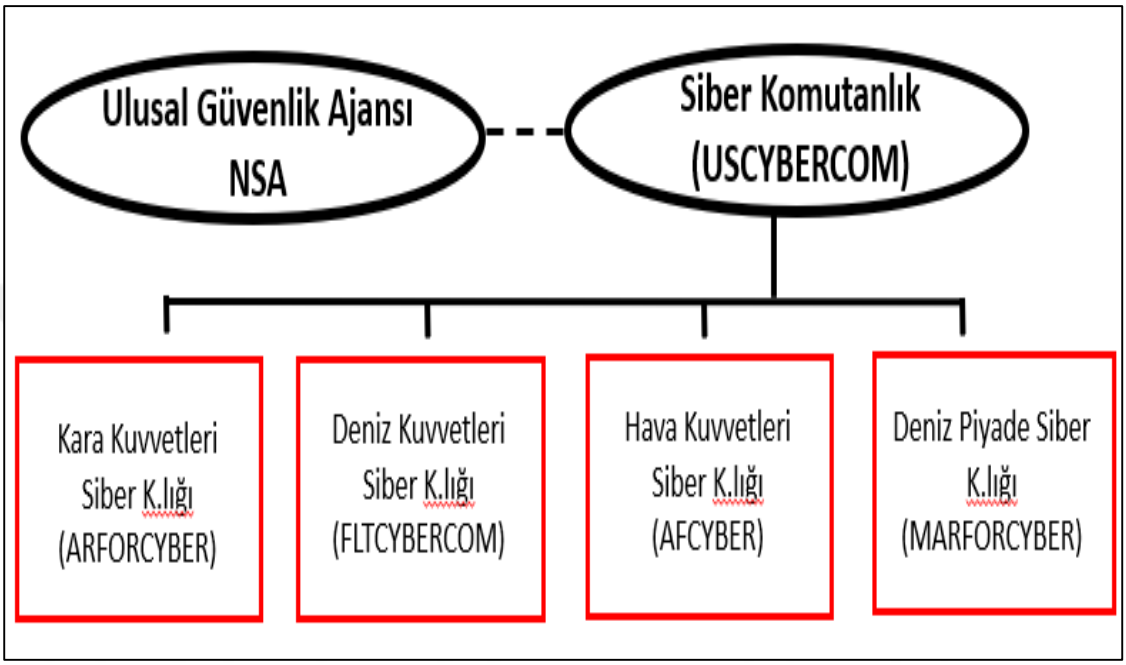
Şekil 19. ABD Siber Komutanlığının Teşkilat Yapısındaki Yeri

Kaynak: (ABD Savunma Bakanlığı, 2019)

Kurulduğu 2010 tarihinden itibaren bu teşkilat yapısı içerisinde faaliyet gösteren Siber Komutanlık, siber güvenliğin artan önemi nedeniyle 2017 yılında Savunma Bakanı'nın teklifi ve ABD Başkanı Trump'ın onayı ile Stratejik Komutanlıktan ayrılarak ayrı bir Birleşik Muharip Komutanlık olarak belirlenmiştir. Siber Komutanlık 2018 yılından yapılan törenin ardından 11. Birleşik Muharip Komutanlık olarak faaliyetlerine başlamıştır (ABD Siber Komutanlığı, 2019a).

3.1.4 Siber Komutanlık (USCYBERCOM)

ABD Siber Komutanlığını oluşturan alt unsurlar Şekil 20'de sunulmuştur. ABD'nin 11 birleşik muharip komutanlığından Siber Komutanlığın başındaki komutan, çift şapkalı olup aynı zamanda ulusal güvenlik sistemlerinin korunması ve yabancı sinyal istihbaratından sorumlu olan Ulusal Güvenlik Ajansı (NSA)'nı da yönetmektedir.



Şekil 20. ABD Siber Komutanlığı Yapılanması

Kaynak: (ABD Siber Komutanlığı, 2019a)

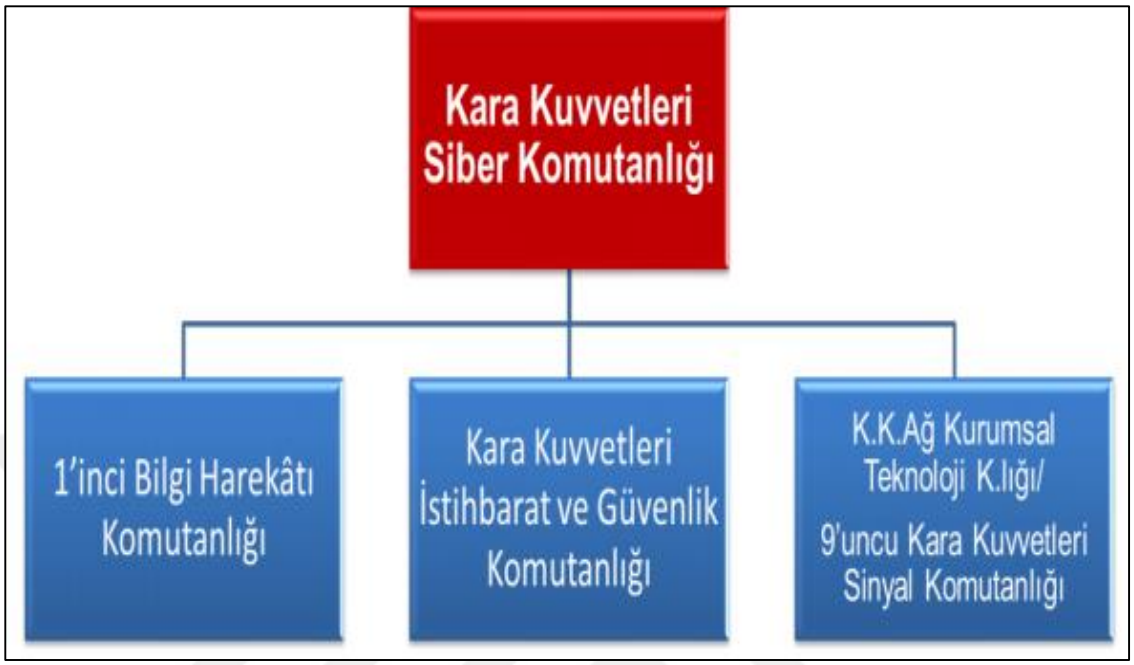
Bu komutanlık ilk teşkil edildiğinde kuvvet komutanlıklarının sadece bu komutanlığın yönlendirmesi doğrultusunda kendi ağlarını savunacağı ve işleteceği ön görülmekteydi. Ancak, siber tehdidin askerî boyutunun çeşitlilik kazanması, her kuvvetin kendine özgü güvenlik tedbirleri almasını gerekli kılmaya başlamış ve müteakiben her kuvvet süratle kendi siber yapılanmasını gerçekleştirmiştir. Bu komutanlığın altında ve siber uzayda faaliyet göstermek üzere;

- Deniz Kuvvetlerinde Siber Filo Komutanlığı,
- Deniz Piyade Komutanlığında Siber Komutanlık,
- Hava Kuvvetlerinde 16'ıncı Hava Komutanlığı,
- Kara Kuvvetlerinde Siber Komutanlık,

Teşkil edilmiş ve/veya bu müşterek yapının harekât kontrolüne tahsis edilmiştir (ABD Siber Komutanlığı, 2019b)

3.1.4.1. Kara Kuvvetleri Siber Komutanlığı

Kara Kuvvetleri Siber Komutanlığı teşkilat yapısı Şekil 21'de sunulmuştur.



Şekil 21. ABD Kara Kuvvetleri Siber Komutanlığı Teşkilat Yapısı

Kaynak: (ABD Kara Kuvvetleri Siber Komutanlığı, 2019)

1'inci Bilgi Harekâtı Komutanlığı, Kara Kuvvetleri bağlılarına ve ana komutanlıklarına bilgi harekâtına ilişkin hususlarda destek sağlamakla vazifelidir. Kara Kuvvetleri ile Savunma Bakanlığı ve diğer Kuvvet Komutanlıkları arasındaki hususların koordinasyonundan sorumlu olup büyük yetkileri bulunmaktadır (Birinci Bilgi Harekâtı Komutanlığı, 2018).

Kara Kuvvetleri İstihbarat ve Güvenlik Komutanlığı, ulusal düzeydeki karar vericiler için istihbarat, güvenlik ve bilgi harekâtı faaliyetlerini sevk ve idare eden doğrudan raporlama birimidir. İstihbarata karşı koyma, kuvvet koruma, elektronik harp ve bilgi harbinde önemli sorumluluklara sahiptir (Kara Kuvvetleri İstihbarat ve Güvenlik Komutanlığı, 2018).

Kara Kuvvetleri Ağ Kurumsal Teknoloji Komutanlığı / 9'uncu Kara Kuvvetleri Sinyal Komutanlığı Kara Kuvvetleri'nin sanal ağlarının işletilmesi ve korunmasından sorumludur. Yaklaşık 16.000 personel görev yapmaktadır (Kara Kuvvetleri Ağ Kurumsal Teknoloji Komutanlığı, 2018).

3.1.4.2. Siber Filo Komutanlığı (FLTCYBERCOM)

Siber Filo Komutanlığı, ABD Siber Komutanlığının (USCYBERCOM) Deniz Unsur Komutanlığı olarak faaliyetlerini yürütmektedir. Dönemin Deniz Kuvvetleri Komutanı tarafından verilen emir gereğince 29 Ocak 2010 tarihinde faaliyete geçen Siber Filo Komutanlığının idari kontrolü Deniz Kuvvetleri Komutanlığı Bilgi Hâkimiyeti Başkanlığı (N-2/N-6)'nda, harekât kontrolü ise Siber Komutanlıktadır (McCullough, 2011). Siber Filo Komutanlığının teşkilat şeması Şekil 22'de sunulmuştur.

Şekil 22. ABD Siber Filo Komutanlığı Teşkilat Yapısı

Kaynak: (Siber Filo Komutanlığı, 2017a)

ABD Siber Savunma Komutanlığı'nın bağlısı olarak kurulan Siber Filo Komutanlığı'nın görevi; karada ve denizde görev yapan tüm muharip unsurlara istihbarat, bilgi harekâtı, sinyal istihbaratı, kriptoloji, elektronik harp ve uzay alanlarında operasyonel destek sağlamaktır (Burgess, 2009).

Komutanlığın sorumluluğu ise, siber, elektronik harp, bilgi harekâtı ve sinyal istihbaratı kabiliyet ve görevlerini siber, elektromanyetik ve uzay etki alanlarında tam kapsamlı olarak icra etmektir. Ayrıca, ABD Deniz Kuvvetleri'nin sinyal istihbarat (SIGINT) makamı olup istihbarat bilgisinin toplanması, analiz edilmesi ve ilgili makamlara ulaştırılması sorumluluğunu da taşımaktadır. Bahse konu komutanlık bu görevlerini yaklaşık 14 bin personel ile yerine getirmektedir (Siber Filo Komutanlığı, 2017b).

3.1.4.3. Hava Kuvvetleri Siber Komutanlığı (16'ncı Hava Kuvveti Komutanlığı)

USCYBERCOM altındaki, ABD Hava Kuvvetleri'nin siber alan kuvvet ve desteğini sağlayan numaralı bir hava kuvvetidir. Önceleri, ABD Hava Kuvvetleri Siber Komutanlığı'nın altında bir birim olarak faaliyete geçirilmesi planlanmıştır. Ancak, Hava Kuvvetleri Siber Komutanlığının faaliyete geçirilmesi iptal edildiği için Hava Kuvvetleri Uzay Komutanlığı'nın bir bileşeni olarak göreve başlamıştır. Ağustos 2009 tarihinde, 16'ıncı Hava Kuvveti Komutanlığının, kurulması planlanan Hava Kuvvetleri Siber Komutanlığının bir parçası olması kararı değiştirilerek, Hava Kuvvetleri Uzay Komutanlığı (Air Force Space Command, AFSC) altında bir bileşen olması kararlaştırılmıştır (Wikipedia, 2019).

3.2. Rusya Federasyonu Siber Yapılanması

Rusya Federasyonu (RF), günümüzde siber uzayı Amerika Birleşik Devletleri (ABD) ve Çin Halk Cumhuriyeti (CHC) ile birlikte domine eden en önemli küresel güçlerden biri konumundadır. RF'nin siber kapasitesinin mahiyetini diğer iki devletten ayıran temel fark, siber uzayın sağladığı imkânları dış politik sorunlarının çözülmesi noktasında ve özellikle de komşuları ile ilişkilerinde bir baskı / yaptırım aracı olarak kullanmasıdır. RF'nin mevcut siber saldırı kapasitesi, Sovyet döneminin teknoloji mirasının da bir sonucu olarak, özellikle 2000'li yıllar ile birlikte ortaya konulan siber güvenlik ve savunma stratejileri belgeleri kapsamında geliştirilmiştir ve geliştirilmeye de devam edilmektedir.

Ulusal Güvenlik Strateji Belgesinde yeterince yer almamasına karşın, Rusya'nın siber güvenlik ile ilgili spesifik stratejiler oluşturarak belgeler yayınladığı ve dahi bu konuda ABD'den daha erken işe başladığı söylenebilecektir. Uluslararası İletişim Birliği Rusya'nın siber güvenlikle ilgili politikalarını belirleyen belgelerin 2000 yılından bu yana geliştirildiğini belirtmektedir. Bu belgeler (ITU, 2015), Rusya Federasyonu Bilgi Güvenliği Doktrini (RFBGD, 2000), Uluslararası Bilgi Güvenliğinde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi (Basic Principles for State Policy of the Russian Federation in the field of International Information Security) belgeleridir (Göçoğlu, 2017:8).

RF'de 1999 senesinde V.Putin'in başa geçmesi ile beraber, 2000 senesinde ulusal güvenlik politikası tekrar gözden geçirilmiş ve bilgi harekâtı (information operations) konusuna ağırlık verilmiştir. RF Bilgi Güvenliği Doktrini ilk kez yetkili Güvenlik Konseyine sunulmuştur (Çiftci, 2013:44).

Yapılan çalışmalar neticesinde savunma ve taarruza ilişkin bilgi harekâtı imkânları Savunma Bakanlığı altında faaliyet gösteren Elektronik Harp Birlikleri bünyesine dâhil edilmiştir. 2001 senesinde Voronezh'da ileri seviye hackerlık ve siber taarruz eğitimleri veren "Voronezh Askeri Telsiz-Elektrik Elektronik Enstitüsü" faaliyetlerine başlamıştır (Clarke ve Knake, 2011: 37).

2008 senesinde bilgi harekâtı konularına odaklanmak maksadıyla 15 000 çalışanı bulunan ve 6000 öğrenci alma imkânına sahip "Voronezh Askeri Havacılık Mühendisliği Üniversitesi" tesis edilmiştir (Özçoban, 2014:97). Diğer yandan, "Stratejik Roket Kuvveti Akademisi" altında faaliyet gösteren "Elektronik ve Bilgi Harbi Teşkilatı" bulunmaktadır. Eğitim konusuna da ayrı önem veren RF, 90'a yakın yükseköğretim kurumunda bilgi güvenliğine ilişkin olarak (Çiftci, 2013:45):

- Kriptoloji,
- Donanım ve yazılım güvenliği,
- Bilgi güvenliği organizasyonu ve ileri teknolojileri,
- Bilgi sistemlerinin bütünleşik yapıda savunulması,
- BİT sistemleri konularında dersler verilmektedir.

RF'nin siber güvenliğe ilişkin stratejisini saldırı-savunma teorisi üstünden ele alan Medvedev (2015), bu konuda faaliyet gösteren devlet kurumlarını; "Federal Güvenlik Servisi- Federal Security Service-FSB", "Dış İstihbarat Servisi-Foreign Intelligence Servisi-SVR" ve silahlı kuvvetlerin "Ana İstihbarat Servisi- Mail Intelligence Directorate-GRU" olarak tespit etmiştir (Medvedev, 2015:3). Ayrıca, RF'nin siber uzayı kullanım şeklinin savunmadan öte taarruz yaklaşımına daha yakın olduğu, savunma konusunun yalnızca yapılacak yatırımların şekillendirilmesine kumanda ettiği düşünülmektedir. (Medvedev, 2015:76-77).

RF'nin güncel savunma, dış politika ve Siber Güvenlik Strateji Belgeleri'nin temel amaçlarından biri, ülkenin enformasyon ve siber güvenliğinin sağlanmasıdır. RF,

belirtilen amaç doğrultusunda devletin siber güvenliğini sağlamaya çalışırken, siber uzayın verdiği imkânlardan azami ölçüde faydalanan ve RF hükûmetlerinin istihbarat ihtiyaçlarının yanı sıra stratejik öneme sahip teknolojik yenilikleri elde etmeye yönelik bir siber espiyonaj sistemi de kurmayı hedeflemiştir. Bu çerçevede RF tarafından birbirleriyle eş güdüm halinde çalışan her biri ortak ve farklı amaçlara yönelmiş, siber uzayı kullanma noktasında önemli imkân ve kabiliyete sahip dört istihbarat (FSB, FSO, SVR, GRU) servisi kurulmuştur.

FSB, SSCB döneminde faaliyet gösteren ÇEKA, NVD ve KGB'nin yerini alan ve iç güvenlik alanında faaliyet gösteren bir gizli servistir. Bir iç güvenlik servisi olarak FSB'nin faaliyetleri iki boyutlu olarak düşünülmelidir. FSB'nin ilk görevi ülke genelinde devlet güvenliği aleyhine sürdürülen faaliyetler hakkında istihbarat toplamaktır (Gady vd. 2010: 5). Örneğin, RF'deki ayrılıkçı Çerkez / Çeçen gruplarının, cihat yanlısı selefi veya tekfiri terör örgütlerinin veya organize suç odaklarının faaliyetlerini izlemek, takip etmek ve haklarında istihbarat toplamak FSB'nin görevidir. FSB'nin bir diğer görevi ise RF'ye yönelik olarak sürdürülmekte olan *espiyonaj* faaliyetlerine karşı koymaktır. Bu karşı koyma faaliyeti *kontr/espiyonaj* çalışması olarak adlandırılır ve RF aleyhine dış istihbarat servisler aracılığıyla sürdürülen *subversif* (yıkıcı/bölücü) bilgi operasyonların da engellenmesi amacını içerir. Bu kapsamda, RF'ye yönelik siber saldırılara karşı koymak ve temelde ülkenin siber güvenliğini sağlamak, FSB'nin görevidir (http://www.cicentre.com/?page=191, 2016). FSB'nin siber güvenlik alanındaki diğer bir sorumluluğu ise ülke genelindeki Rus vatandaşlarının ve yabancıların telekomünikasyon iletişim bilgilerinin istihbar olunan bilgiler kapsamında takip edilmesidir. Bu görev kapsamında FSB, Rus GSM ve telefon şirketlerinin yasal bir zorunluluk olarak kurmak zorunda oldukları, RF'deki internet ve analog haberleşmesini takip eden ve bir nevi denetleme sistemi şeklinde tesis edilmiş olan "Operatif Denetleme Faaliyetleri Sistemi" (System for Operative Investigative Activities / SORM)'nin kontrolünü de üstlenmiştir. FSB'nin sanayi, teknoloji ve bilişim sektörlerine yönelik espiyonaj faaliyetlerinin engellenmesi noktasında Rusya Teknik ve İhracat Kontrol Servisi (Federal Service for Technical and Export Control of Russia / FSTEC) ile de yakın işbirliği bulunmaktadır. Bu kapsamda 2004 yılında kurulan ve RF Savunma Bakanlığı bünyesinde faaliyet göstermekte olan FSTEC'nin ihracat denetim rejimini kontrol etmek suretiyle sanayi, teknoloji ve bilişim sektörlerini hedef alan espiyonaj operasyonlarına karşı koymada

önemli bir rolü bulunduğu belirtilebilir (Carr, 2011: 318). Ayrıca önemle belirtmek gerekir ki FSB, siber güvenlik alanındaki çalışmalarının yanı sıra diğer tüm faaliyetlerini SVR ile koordinasyon içinde sürdürmektedir (Staar, 2010:10).

SVR de KGB'nin devamı olarak RF'nin ülke dışındaki espiyonaj faaliyetlerini yürütmek amacıyla kurduğu dış istihbarat servisidir. SVR, RF'nin dış istihbarat ihtiyaçlarının karşılanmasında, GRU ile birlikte temel aktör konumundadır. SVR, hedef aldığı devlete yönelik askerî, siyasi, biyografik, ekonomik, sosyal, ulaştırma, iletişim, bilim ve teknoloji konularında istihbarat toplamaktadır. Siber güvenlik stratejisi açısından ise RF'nin bir ülkenin bilim ve teknoloji kapasitesini hedef alan siber casusluk operasyonlarını planlamak SVR'nin görevleri arasındadır. SVR'nin yurt dışında, Belarus, Kazakistan, Tacikistan, Ermenistan, Kırgızistan, Suriye, Küba, Vietnam ile Güney Osetya, Abhazya, Kırım ve Transdinyester bölgelerinde GRU ile birlikte ortak kullandığı elektronik ve sinyal istihbaratı toplama merkezleri de mevcuttur (Heickerö, 2015: 30-32).

GRU, Rus Genelkurmayı'na bağlı olarak faaliyet gösteren askerî istihbarat teşkilatıdır. SSCB zamanında Kızıl Ordu'ya bağlı olan GRU, RSK'nin büyüklüğü kapsamında RF'nin en geniş sayı ve kapasiteli istihbarat teşkilatıdır. GRU, askerî ve dış istihbarat konularının yanı sıra ülke güvenliği ile ilgili her alanda istihbarat toplama yetkisine sahiptir. Siber güvenlik açısından GRU'nun temel görevleri Rus askerî kapasitesini hedef alan dış servis kaynaklı siber operasyonlara karşı kontr/espiyonaj faaliyeti yürütmek ve imkân bulunması hâlinde hedef ülkenin askerî kapasitesine yönelik siber casusluk operasyonları planlamaktır (http://www.cicentre.com/?page=191, 2016). Stratejik Füze Birlikleri'nin faaliyetlerinin sürdürülmesinin yanı sıra ülkeye yönelik siber saldırılara karşı koymak üzere kurulmuş olan "Computer Emergency Response Team"lerin kontrolü de GRU'nun diğer Rus istihbarat ve güvenlik kuruluşları ile koordineli olarak gerçekleştirdiği görevler arasındadır (Heickerö, 2015: 27).

RF siber güvenlik konusunda yoğun gayret göstererek özel sektörde konunun uzmanı teknik ve akademik personel ile işbirliği içerisinde faaliyetlerini yürütmekte ve etkili siber silahlarla kuvvetli bir siber harp görüşünü esas almaktadır. Klasik yöntemlerle beraber kullanılan siber silahların, askeri imkân ve kabiliyetlerle ile harekâtın etkinliğini arttıracağı ve bu şekilde siber silahların etkili bir güç çarpanı olarak kendini göstereceği yaklaşımını benimsemiştir. RF esas aldığı bu yaklaşımını da yakın zamanda yaşanan

Gürcistan ve Ukrayna olaylarında da fiilen uygulamıştır. RF muhasımın finans, askeri, kamu ve özel iletişim ağlarına zarar verebilecek, klasik bir askerî harekât öncesinde ve harekât esnasında muhasım kritik altyapılarını gayri faal duruma sokabilecek siber imkân ve kabiliyetlere haizdir (Billo ve Chang: 2004: 107; Schaap, 2009: 139).

RF dâhilindeki kritik internet ağlarının denetimini sıkı şekilde elinde bulunduran hükümet, meclisten geçirdiği yasalarla da internet sunucularının farklı bir ülkeye ağ trafiği ile alakalı veri paylaşmasını engellemiş ve bu şekilde hükümet desteği ya da isteği ile yapılan siber eylemlere yönelik bilgi elde edilmesinin önüne geçmiştir (Çeliktaş, 2016:67).

3.3. Çin Halk Cumhuriyeti Siber Yapılanması

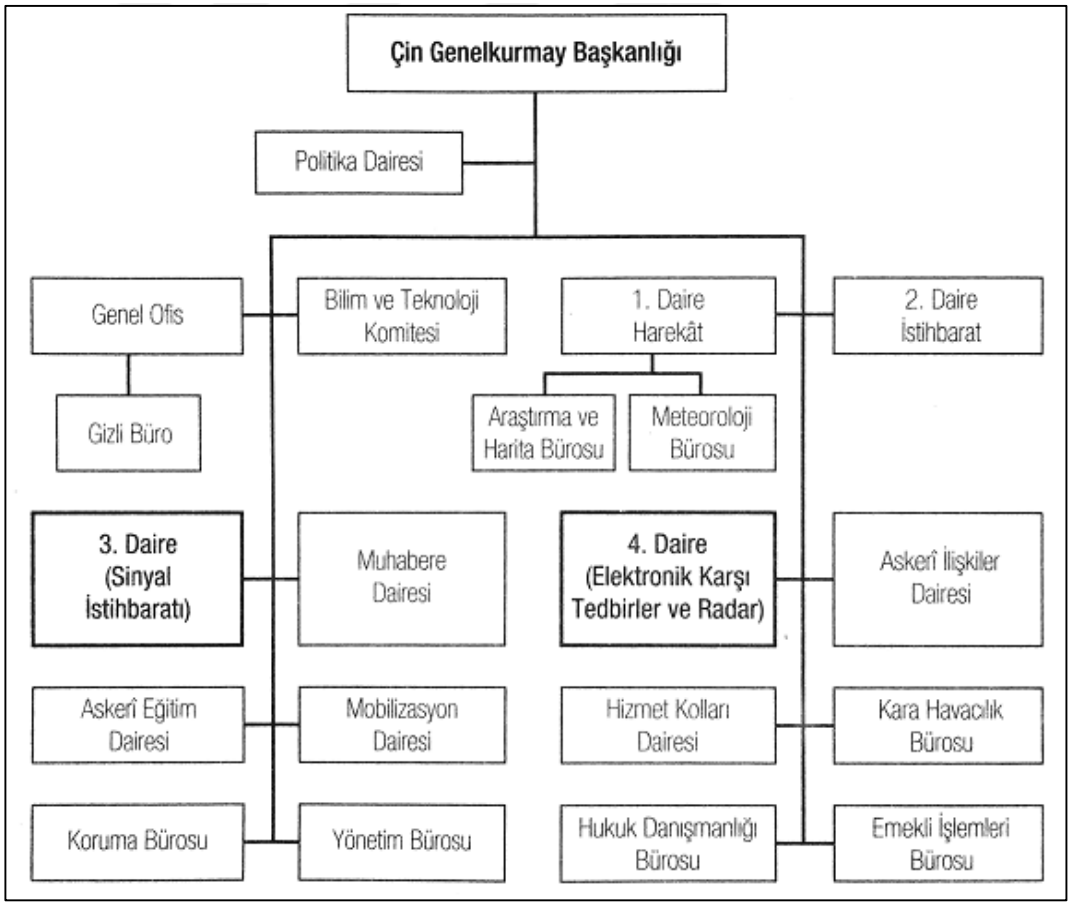
Çin'in siber güvenlikle bilgi ve iletişim teknolojilerine verdiği önemin geçmişi 20. yüzyılın sonlarına yani bu teknolojilerin ilk ortaya çıktığı zamanlara kadar dayanmaktadır. İlk olarak 1986 yılında ekonomik bilgilerin yönetimine dair küçük bir grup kurulmuştur. 2003 yılında ise siber güvenliğe dair ilk sivil belge olan Belge 27 yayınlanmıştır. Belge, kritik altyapıların korunmasına yönelik aktif bir savunma politikası oluşturmayı amaçlarken dinamik gözlemleme, gelişimi destekleme, devlet organları ve kurulan ekonomik bilgilerin yönetimi grubuyla iş birliği yaparak siber güvenlik politikalarını yönlendirmeyi amaçlamıştır (Raud, 2016: 11).

Çin'in siber güvenlik alanında yaptığı kurumsal ve hukuki düzenlemelerin geçmişi 2014 yılının biraz öncesine dayanmaktadır. Çokuluslu bir denetim şirketi olan ve dünyada bu alanda en büyük dört şirketten (Big Four) biri olan KMPG'nin yayınladığı raporda (KMPG, 2016: 5) bu düzenleme ve gelişmeler kronolojik olarak sıralanmıştır. 2014 yılından önce yapılan düzenlemeler siber güvenliğe ve sistemsel altyapıların önemine odaklanılmış, devlet tarafından oluşturulan konsey bilgisayar bilgi güvenliği prosedürleri oluşturulmuş, Kamu Güvenliği Bakanlığı (Ministry of Public Security) bilgisayar virüslerine karşı savunma ve internet için birtakım standartlar geliştirmiştir. 2014 yılında, Çin devlet başkanı Xi Jinping başkanlığında siber güvenlik grubu kurulmuş ve yapılan çalışmalar o yılki hükümet raporunda yer almıştır. 2015 yılında Çin'in ulusal kongresi olan NPC'de (Standing Committee of the National People's Congress) kamuoyu

yoklaması yapmak suretiyle halkın da görüşlerini göz önüne alarak Siber Güvenlik Kanunu tasarısını oluşturmuştur.

ÇHC askeri konseptinde siber güvenlik, büyük sermaye ayırılması ve araştırmalar yapılması gerekli olan hayati öneme haiz bir konu olarak ifade edilmiştir. Çinli idareciler ve komutanlar siber imkân ve kabiliyetlerin harp stratejilerinde ciddi asimetrik katkı sağladığına işaret etmektedir (Mulvenon, 2009:257).

ÇHC komuta kademesi tarafından 2011 senesinde siber savaş organizasyonuna yönelik olarak birtakım açıklamalarda bulunulmuş ve ÇHC ilk defa bir süper elit siber savaşçı birliğinin bulunduğunu, otuz personelden oluşan bu timin "Mavi Ordu" olarak isimlendirildiğini belirtmiştir. Yapılan açıklamalarda kurulan bu ekibin, Çin Halk Kurtuluş Ordusu (PLA)'nun sanal ağlarını olası taarruzlardan muhafaza etmek maksadıyla oluşturulduğu açıklanmıştır (Hwang, 2012: 191). ÇHC Genelkurmay Başkanlığındaki Siber Teşkilat Yapısı Şekil 23'te sunulmuştur.



Şekil 23. ÇHC Genelkurmay Başkanlığındaki Siber Teşkilat Yapısı

Kaynak: (Çiftci, 2013:42)

ÇHÇ, siyasi ve politik yapısı ile ideolojik durumu nedeniyle ülkenin savunması ile birlikte siber güvenlik konusu da çoğunlukla silahlı kuvvetlerinin kontrolüne verilmiştir. PLA organizasyonunda gösterilen üçüncü ve dördüncü daireler bilgi ve iletişim altyapısının bekasının sağlanmasıyla vazifelidir. Bahse konu daireler her üç kuvvet komutanlığının ve milis güçlerinin siber harple ilgili unsurları ile koordineli bir şekilde ÇHC hudutlarında olan bütün iletişimi denetim altında tutmaktadır (Corera, 2015:232).

Genelkurmay 3. Dairesi diğer yandan, PLA'nın kullandığı tüm bilgi sistemlerinin ve sanal ağlarının korunmasıyla da vazifelidir. Bu daire daha ziyade milli seviyedeki faaliyetlerin icrasından sorumludur. Bu Dairenin bünyesinde 12 operasyonel büro ve 3 araştırma enstitüsü bulunmakta olup siber güvenliğin geliştirilmesi maksadıyla sürekli olarak araştırma geliştirme faaliyetleri yürütmekte ve yükseköğretim kurumlarıyla da işbirliği yapmaktadır (Stokes, Lin ve Hsiao: 2011:5-7). Genelkurmay 4. Dairesi daha ziyade elektronik karşı tedbirler ve radar konularında vazifelidir. Klasik savaş mantığı içerisindeki elektronik taarruz birimi olarak faaliyetlerini icra etmektedir.

PLA bünyesinde dünyadaki en süratli süper bilgisayarları bulunmaktadır. Jiangnan Bilgisayar Teknolojileri Araştırma Enstitüsü (Jiangnan Computer Technology Research Institute) ismiyle de anılan 56'ncı Araştırma Enstitüsü Çin'deki en köklü ve büyük ARGE organizasyonudur. Çok önemli süper bilgisayar yatırımları yapmakta ve bu süper bilgisayarlarla Çin'deki diğer bilgisayar merkezlerine ve PLA bünyesindeki organizasyonlara destek vermektedir. Burada yer alan süper bilgisayarlar vasıtasıyla, diğer ülkelerin kriptolarını, karmaşık kodlarını ve şifreleme sistemlerini kırma çalışmaları yapılmaktadır (Stokes, Lin ve Hsiao: 2011:5).

ÇHC siber konusunda öncü ve lider konuma gelmek için 1900'lardan itibaren bu konuya eğilmiş ve günümüz kadar konuya ilişkin birçok doktrin ve strateji belgeleri yayınlamıştır. PLA "bilgileştirme" stratejisi çerçevesinde modernleşme programı ile BİT ve siber ortam konularında süper güç olmayı hedeflemektedir (Ventre, 2010).

ÇHC'nin hackerları çok geniş, etkin ve önemli bir siber taarruz tecrübe, birikim ve kabiliyete sahiptir. ÇHC'nin çok farklı konularda faaliyet gösteren, uzmanlaşmış geniş bir bilgisayar topluluğu bulunmaktadır. İnternet aracılığı ile birbirleri ile iletişime geçen bu topluluklar siber taarruz silahlarını da sanal ağlar üzerinden paylaşmaktadır. ÇHC'de

2011 senesinde faaliyetlerine başlayan mavi ordunun bu hackerların faaliyetini koordine etmek maksadıyla kurulduğu yönünde iddialar bulunmaktadır (Dnchey, 2011).

Ayrıca, ÇHC politik anlamda kritik bilgilerin ülke dışına çıkması ya da içeri girmesini engelleyen "Altın Kalkan" isimli meşhur bir filtreleme sistemi uygulamaktadır. Altın Kaplan sistemi "Büyük Çin Güvenlik Duvarı" olarak da anılmaktadır. Bu sistemin olası bir siber harp halinde ÇHC koruyacağı ve ciddi üstünlükler sağlayacağı açıktır. (Clarke ve Knake, 2010: 35).

BEŞİNCİ BÖLÜM

TÜRKİYE'DE SİBER TEHDİTLERE KARŞI YAPILAN FAALİYETLER

1. TÜRKİYE'DE SİBER GÜVENLİĞİN TARİHÇESİ

Türkiye'nin siber uzaya bağımlılığı incelendiğinde; sanayi tesislerinden barajlara, bürokrasi alanından hava denetim sistemlerine, hastane hizmetlerinden kritik altyapılara kadar çok farklı alanda ve sistemlerde bilgi teknolojilerine bağımlı duruma geldiği görülmektedir. Bununla beraber yakın zamanda her geçen gün artan UYAP-Ulusal Yargı Ağı, MERNİS-Kimlik Paylaşımı, ASAL-Asker Alma Dairesi, TAKBİS -Tapu ve Kadastro, MEBBİS-Öğretmen Bilgileri) ve e-Devlet uygulamaları gibi bireylere ilişkin ciddi ve önemli hususlar ihtiva eden bahse konu altyapıları ülkemiz açısından kritik altyapılar haline getirmiştir.

Türkiye'de siber konusunda farkındalığın yükselmesi, yakın dönemde ciddi siber taarruzlarla yüzleşilmesi ve siber güvenlik önlemleri ile alakalı çalışmalara yer verilmesinin gereksinim haline dönüşmesiyle beraber farklı konular üzerine yoğunlaşılmaktadır. Bu konulardan başlıcaları; siber güvenlik uygulama programları, milli bilgi güvenliği planı, milli bilgi güvenliği kapısı, hukuki düzenlemeler, siber güvenlik reaksiyon timleri ve personeli, tatbikatlar, seminerler ve silahlı kuvvetler içerisinde yapılan faaliyetler ve oluşumlar biçiminde ele alınabilir.

1.1. Siber Saldırı Örnekleri

2003 senesinde Batman Hidroelektrik Barajı'nın inşasını alan Alman Noel Şirketi yöneticileri paralarını alamadıkları sebebiyle firma bilgisayarlarını parolayla şifreleyip ülkeden ayrılmış ve neticede barajın 3 bölümünde çalışmalar durmuştur (Karabacak, 2011: 35). Bu olay özellikle kritik altyapılarda milli yazılım ve kontrol sistemlerine duyulan ihtiyacı ortaya koyması açısından önemlidir.

Bu vaka üzerine TÜBİTAK Uzay Teknolojileri Araştırma Enstitüsü tarafından başlatılan "Küçük ve Orta Ölçekli Hidroelektrik Santraller için Kontrol-Kumanda, Ölçme ve Koruma Sistemi Tasarım, Geliştirime ve Prototip Üretimi (HESKON) Projesi"

2009'da tamamlanmıştır. Proje ile baraj ve nehir türündeki hidroelektrik santral tesisleri için kontrol sistemi geliştirilmiştir. Sistemin aynı zamanda küçük ve orta ölçekli santrallerde de kullanılması amaçlanmaktadır.

30 Ocak 2009 tarihinde TÜBİTAK UEKAE içerisinde çalışmalarını devam ettiren "Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME)", bilgisayarlarda süratle yer bulan farklı bir solucan bulunduğunu zamanında uyarmış olmasına rağmen, ülkemiz havalimanlarına etkileri büyük olmuştur. TÜBİTAK tarafından uyarılan "downadup" ismindeki "networm" virüsü Atatürk Havaalanı Yurtdışı Terminali'ndeki bilgisayarları etkilemiştir. Bilet ve bagaj işlemlerinin yapıldığı SITA-CUTE sistemlerine bulaşmış ve tüm bilet ve bagaj işlemlerini elle yapılmak zorunda kalmış, birçok yolcunun bagajları havalimanında kalmıştır. Olaydan sonra TR-BOME' den yapılan duyuruda, Microsoft'un 23 Ekim 2008'de bazı Windows işletim sistemlerine tesir eden, ivedi olduğunu duyurduğu"MS08-67"numaralı güncellemeyi piyasaya sürdüğü ifade edilerek, küresel olarak 15 milyon bilgisayarı etkilediği değerlendirilen "Confickr" adlı solucanın, güncellemenin yapılmadığı bilgisayarlarda faal olduğu açıklanmıştır.

Terminal yetkilileri, "SITA-CUTE" sistemine yerleşen "downadup" ismindeki "networm" virüsü sebebiyle sistem sorunu olduğunu teyit ederek, sistemin faal hale getirilmesi maksadıyla 400 "CUTE" işlem biriminin sistemden ayrılarak virüsten arındırıldığı belirtilmiştir. Yaşanan hadise virüs kaynaklı bir siber saldırının günlük hayatın akışını da doğrudan engelleyeceğinin göstergesi olarak değerlendirilmektedir (Habertürk, 2009).

6 Haziran 2011 tarihinde, Anonymous tarafından "anonews.org" sitesinden bir duyuru yapılarak Türkiye'de internete uygulanan sansürlere karşı mücadele edileceği bildirilmiştir. Video paylaşım sitesi Youtube'da yayınlanan bir video ile Türk Hükümeti tehdit edilmiştir. Ardından 9 Haziran 2011 günü saat 18:00'de Bilgi ve İletişim Kurumu internet sitelerine saldırılar yapılmış, saat 18:15 civarında kısmi bir kesinti yaşanmış ancak öncesinde alınan tedbirler sayesinde hizmet verilmeye devam edilmiştir.

Mayıs 2015 tarihinde yaklaşık 3 gün boyunca ".gov" uzantılı internet sitelerine ve kamu personeline ait e-posta adreslerine 12 farklı ülkeden siber saldırı yapılmıştır. Saldırılarda kamuya ait internet sitelerine erişim yavaşlamış ve kamu personelinin e-posta adreslerine çok sayıda yığın e-posta geldiği tespit edilmiştir (Hürriyet, 2015).

Suriye'den havalanıp sınırlarımızı ihlal eden ve tüm uyarılara rağmen ihlale devam eden Rus uçağının Türk Hava Kuvvetleri uçakları tarafından 24 Kasım 2015 tarihinde düşürülmesinin ardından, ülkemize yapılan siber saldırılar yoğunlaşmaya başlamıştır. Siber saldırılar arasında özellikle 14 Aralık 2015 tarihinde başlayan ve üç gün süren saldırılar yoğun bir şekilde hissedilmiş, ".tr" uzantılı sitelere erişimlerde sıkıntılar yaşanmıştır. Çeşitli finansal kurum ve kuruluşlarda hizmet kesintileri yaşanmış, sistemlerin aktif hale gelmesi zaman almıştır.

Küresel ağ güvenliği kuruluşu WatchGuard, 2020 yılında Türkiye'de siber saldırıların en çok mayıs ayında gerçekleştiğine dikkat çekmiştir. WatchGuard Tehdit Laboratuvarı'ndan elde edilen verilere göre, 2020 yılında Türkiye'de gerçekleşen 1.5 milyon kötü amaçlı yazılım saldırısının yaklaşık 3'te 1'i Mayıs ayında gerçekleşmiştir. (Habertürk, 2020)

1.2. Siber Güvenlik Tatbikatları

Dünyada siber güvenlikle alakalı ortaya konan araştırmalarda milli ve milletlerarası mahiyette yapılan tatbikatlar da ciddi bir yer tutmaktadır. Bu tatbikatlar vasıtasıyla kurumsal siber güvenlik seviyesinin tespitinin ötesinde kurumlar arası/milletlerarası işbirliği imkânı ve kapasitesi de belirlenmekte ve tespit edilen veriler kapsamında düzeltme ve geliştirme çalışmaları yapılmaktadır. Bu çerçevede Türkiye'de;

-TÜBİTAK koordinatörlüğünde sekiz kamu kurum/ kuruluşunun iştiraki ile milli düzeyde ilk siber güvenlik tatbikatı olan "BOME 2008 Bilgi Sistem Güvenliği Tatbikatı", 20-21 Kasım 2008 tarihlerinde gerçekleşmiştir. BOME 2008 tatbikatı, mesai saatlerinde (09:00-18:00) gerçekleştirilmiş olup katılımcı kurum temsilcileri çalışmalara, kendi kurumlarından katılmıştır(Tatar,2008).

- TÜBİTAK ve BTK koordinatörlüğünde 41 kamu, sivil sektör ve sivil toplum kurum/ kuruluşunun iştiraki ile "Ulusal Siber Güvenlik Tatbikatı 2011(USGT-2011)", 25-28 Ocak 2011 tarihinde gerçekleştirilmiştir. Tatbikatta katılımcı kurum ve kuruluşlardan bilgi ve iletişim teknolojileri, hukuk ve halkla ilişkiler uzmanı statüsündeki 200'e yakın personel görev almıştır. Katılımcı kurumların siber saldırı durumunda verecekleri tepkileri gerçek ortamdaki ve simülasyon ortamındaki saldırılarla ölçülmesiyle kurumların hem teknik kabiliyetlerinin hem de kurum içi ve kurumlar arası

koordinasyon yetenekleri değerlendirilmiştir. Geniş katılımlı ilk siber güvenlik tatbikatı "Ulusal Siber Güvenlik Tatbikatı-2011 (USGT-2011)"Türkiye'de siber güvenlik hakkında idari, teknik ve yasal imkânın daha ileri bir seviyeye getirilmesinde, kurumlar arasında bilgi ve deneyim paylaşımına ve başta idare düzeyinde olmak üzere tüm basamaklarda bilincin meydana getirilmesinde ciddi katkılar vermiştir.

Söz konusu tatbikatta kurumların bilgi sistemleri vakalarına müdahale kabiliyetinin belirlenmesi için kurumların farklı siber güvenlik hataları durumunda gösterdikleri reaksiyonlar kıymetlendirilmiş, bu reaksiyonlar için yararlandıkları imkân ve kurumlar arası işbirliği konuları değerlendirilmiştir.

Genelkurmay Başkanlığı'nın da katıldığı tatbikatın sonuç raporuna göre, katılımcılar bakımından ciddi seviyede açıklık bulunduğu neticesi gözler önüne serilmektedir. Açıklıkların ortadan kaldırılması hususunda, bilgi sistemlerine ilişkin materyal-yazılım alımı ve aynı yatırımların yeterli gelmeyeceği, öncelikle kurum/kuruluş idarecileri olmak üzere kurum/kuruluş çalışanlarının komple bilgi güvenliği hususunda yetiştirilmesi, ek olarak bilgi güvenliği ile alakalı kurumsal iş süreçlerinin hayata geçirilmesi gerekmektedir. Sağlanan verilere çoğunlukla kıymetlendirildiğinde Türkiye'de siber güvenliğin tesis edilmesi için kısaca bilgi güvenliği yönetim sistemi, iş devamlılığı, personel kaynakları, kurum içi ve kurumlar arası iletişim ve koordinasyon konularında araştırma yapılması zarureti görülmektedir (BTK, 2019).

-BTK tarafından, siber saldırılara karşı önlemlerin alınması amacıyla 8-29 Mayıs 2012 tarihleri arasında gerçekleştirilen "Siber Kalkan" tatbikatına internet erişim hizmeti sunan ve internete erişim sağlayan elektronik haberleşme sektöründen 12 işletmeci katılmıştır (BTK,2012).

- TÜBİTAK ve BTK koordinasyonu ile 61 kamu, sivil sektör ve sivil toplum kurum/ kuruluşunun iştiraki ile "Ulusal Siber Güvenlik Tatbikatı 2013", 25 Aralık 2012-11 Ocak 2013 tarihleri arasında gerçekleştirilmiştir (TUBİTAK, 2013). 8 aşamadan oluşan tatbikatta, ilk 6 aşamada kurum ve kuruluşlara gerçek siber saldırılar düzenlenmiş; her kurum kendi sistemlerini savunurken olası açıklıklar tespit edilmeye çalışılmıştır. Tatbikatın son 2 aşamasında ise, tüm kurum ve kuruluşların katılımıyla 10-11 Ocak 2013 tarihleri arasında Ankara'da yapılmıştır.

- 15-16 Mayıs 2014 tarihlerinde İstanbul'da icra edilen "Siber Kalkan 2014 Tatbikatı"na 19 ülkeden katılım olmuştur. ITU'dan 1 temsilci, ITU-IMPACT'ten 7 kişilik teknik ekip, 17 ülkenin ulusal siber olaylara müdahale ekiplerinden 47 tatbikat katılımcısı, Yunanistan, Japonya ve İtalya'dan birer konuşmacı, ülkemizdeki kamu kurum ve kuruluşlarından, sektördeki işletmecilerden ve sivil toplum kuruluşlarından ziyaretçiler etkinliğe iştirak etmiştir. Tatbikatta ülkemiz, Bakanlık, BTK ve TÜBİTAK'tan meydana getirilen 4 kişilik bir takım ile temsil edilmiştir.

Tatbikat sonunda BTK Başkanı konuşmasında, siber vakaların ülke ekonomilerine verdiği kötü sonuçlar ifade edilerek, siber vakaların, küresel ekonomiye verdiği olumsuz tablonun maliyetinin senelik yaklaşık 1 trilyon dolar olduğu ifade etmiştir. Ayrıca, günümüzde artık sadece taarruzların türleri ve miktarının değil, süratlerinin de yükseldiğine atıf yaparak, "2013 yılında 100 Gbps üstünde yüksek bant genişlikli çok sayıda saldırı görüldü. Geçen yıl saldırı sürelerinde de artış yaşandı ve hedef alınan kurumların hizmetlerinde de ciddi kesintiler meydana geldi hem dünyada hem de Türkiye'de. Bu dönemde ABD, DDoS saldırılarına kaynaklık etmesi bakımından Çin'i geride bıraktı ancak Asya ülkeleri orantısal olarak ön planda yer almaya devam ediyor." demiştir (Hürriyet, 2014).

1.3. Siber Güvenliğe Yönelik Yasal Düzenlemeler

Mart 2000'de AB Konseyi'nce hazırlanan e-Europe+ çerçevesinde ve Lizbon Protokolü kapsamında meydana getirilen ve 9.10.2001 tarihli ve 352 numaralı Başbakanlık Genelgesiyle hayata geçirilen e-Türkiye inisiyatifinin 13 temel çalışma grubundan biri de TSK bünyesinde faaliyetleri koordine edilen Güvenlik Çalışma Grubu olmuştur (e-Avrupa Eylem Planı, 2003).

24 Temmuz 2004 tarihinde yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu, elektronik imzanın hukuki ve teknik yönleri ile kullanımını düzenlemektedir. Kanun, kâğıt ortamda yürütülen işlemlerin elektronik ortamda güvenli ve hukuki sonuç doğuracak biçimde yürütülebilmesi için büyük imkân sağlamıştır.

26 Eylül 2004 tarihinde TBMM'de kabul edilen ve 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu(TCK), kişi hak ve özgürlüklerini, kamu

düzen ve güvenliğini, hukuk devletini, kamu sağlığını ve çevreyi, toplum barışını korumak ve suç işlenmesini önlemek maksadıyla uygulanan düzenlemelerdir. Doğrudan siber güvenliğe yönelik bir kanun değildir fakat aşağıda belirtilen maddeler vasıtasıyla ilişkilidir;

Madde 124- Haberleşmenin Engellenmesi, Madde 132-Haberleşme Gizliliğini İhlal, Madde 123-Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması, Madde 134- Özel Hayatın Gizliliğini İhlal, Madde 135-Kişisel Verilerin Kaydedilmesi, Madde 136- Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme, Madde 243- Bilişim Sistemlerine Girme, Madde 244- Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, Madde 245- Banka Veya Kredi Kartlarının Kötüye Kullanılması.

DPT de "Bilgi Toplumu Stratejisi 2006 – 2010" çerçevesinde bir uygulama programı kaleme alarak bazı görevlendirmeler saptanmıştır. Türkiye'de bilgi toplumuna ulaşma anlayışı içerisinde meydana getirilen en geniş milli strateji metni olan ve 2006–2010 periyodunu içeren "Bilgi Toplumu Stratejisi Eylem Planı", 2006/38 numaralı Yüksek Planlama Kurulu Kararı ile tasdik edilmiş ve 28.07.2006'da resmi gazetede yayımlanarak hayat geçirilmiştir (Resmi Gazete, 2006).

Ulusal Bilgi Sistemleri Güvenlik Programı başlıklı 88 numaralı eylemde siber ortamdaki güvenlik risklerinin devamlı bir şekilde takip edilmesi, ikazlar yayınlanması, bu tehditlere yönelik nasıl önlemler alınabileceğine ilişkin duyurular yapılması, tehditlerin bertaraf edilmesi halinde karşı önlemlerin eş güdümünü sağlayabilecek bir "bilgisayar olaylarına acil müdahale merkezi (CERT)" oluşturulması öngörülmüştür. Ayrıca kamu kuruluşlarının ihtiyaç duyduğu asgari güvenlik düzeylerinin kuruluş ve hayata geçirilen madde bazında belirlenmesi, kuruluşların istifade ettiği sistem, program ve ağların güvenlik düzeylerinin belirlenmesi ve aksaklıkların ortadan kaldırılması yönünde teklifler yapılması amaçlanmıştır. TUBİTAK-UEKAE içerisinde bazı araştırmalar kaleme alınmış ve "Türkiye Bilgisayar Olaylarına Müdahale Ekipleri (TR–BOME)"meydana getirilmesi hususunda teknik hususlar ile kalifiye personel başlıklarında belli oranda gelişme sağlanmıştır. "NATO NCIRC (NATO Computer Incident Capability)" ile 15.12.2006'da Mutabakat Muhtırası imzalanmıştır. Bu muhtıra sayesinde NATO ve TÜBİTAK UEKAE bilgi sistemleri vakalarına müdahale hususunda ne şekilde adım atacaklarını belirlemişlerdir.

23 Mayıs 2007'de 5651 numaralı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" kabul edilmiştir. Bu yasa internet vasıtasıyla yapılan bazı suçlarla baş etmede muhteviyat, yer toplu kullanım ve erişim sağlayıcılarına bazı yükümlülükler ve vazifeler vermektedir. Bahse konu yasada tasavvur edilen erişime müsaade etmeme önlemleri, ilk başta kötü yazılımları yayan internet adreslerine ilişkin nispi bir koruyucu tedbir imkânı tesis etmektedir. Fakat hâlihazırda internet vasıtasıyla gerçekleştirilen siber taarruzlarla bilgi güvenliğine eğilen bazı tehditlerin daha değişik usullerle gerçekleştirildiği dikkate alındığında 5651 numaralı yasanın bilgi güvenliğini tesis etme açısından kısıtlı bir kabiliyet verdiği görülmektedir (Güngör, 2015:100).

10 Kasım 2008 tarihinde yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu, elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılmasına ilişkin usul ve esasları belirlenmesini amaçlamaktadır. 19 Şubat 2014 tarihli 6518 sayılı kanun ile "Siber Güvenlik Kurulu" bu kurulun görevleri 5809 sayılı kanuna eklenmiş, BTK ve işletmecilere elektronik haberleşme ile ilgili temel görevler verilmiştir.

Uluslararası işbirliğinin bir örneği olarak hazırlanan "Avrupa Konseyi Siber Suç Sözleşmesi", 10.11.2010 tarihinde Dışişleri Bakanlığınca imzalanmış olup TBMM tarafından bir takım çekincelerden dolayı onaylanmamıştır.

Resmi gazetede duyurularak hayata geçirilen 20.10. 2012 tarihli ve 28447 numaralı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" vasıtasıyla kurumsal organizasyon açısından mevcut duruma esas teşkil eden Siber Güvenlik Kurulu oluşturulmuştur. Kurul başkanlığını doğrudan Ulaştırma Denizcilik ve Haberleşme Bakanı yürütmektedir. Kurul, Dışişleri Bakanlığından Milli Savunma Bakanlığına, Kamu Düzeni ve Güvenliği Müsteşarlığından MİT'e kadar birçok kamu kurum/kuruluşun üst seviye bürokratlarından meydana gelmektedir. Sekretarya görevlerini ise UDHB uhdesinde tesis edilmiş olan Siber Güvenlik Dairesi Başkanlığı yürütmektedir.

Kurulun temel görevleri söz konusu Bakanlar Kurulu kararında detayları ile tespit edilmiştir. Bu görevler ise temelde Türkiye'nin siber güvenlik politikalarını belirlemek, yönetmek, konu kapsamındaki milli yazılım ve donanım sistemlerinin geliştirilmesini sağlamak, siber güvenlik hakkında toplumda farkındalık oluşturmak şeklinde özetlenebilir (28447 Sayılı Resmî Gazete, 2012).

Son olarak ise, 24 Kasım 2016 tarihinde kabul edilen Kişisel Verilerin Korunması Kanunu ile kişisel verilerin işlenmesinde, başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunması amaçlanmaktadır. Kanun, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyması gereken usul ve esasları belirlemektedir.

1.4. Siber Güvenlik Stratejisi ve Eylem Planları

Siber Güvenlik Kurulu'nca belirlenen "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 25 Ekim 2013 tarihli ve 28683 numaralı Resmi Gazetede duyurularak hayata geçirilmiştir (Resmi Gazete, 2013). Söz konusu strateji ile başta hayati ehemmiyete haiz kurum/ kuruluşlara yönelik olası siber taarruzların, strateji kararları ve icraat maddeleri ile beraber, engel olunması hedeflenmektedir. Bahse konu icraat maddeleri incelendiğinde, yedi temel başlık içerisinde ele alındığı görülmektedir. Bunlar;

- Hukuki Düzenlemelerin Tesis Edilmesi,
- Adli Olaylara Destek Sağlayacak Araştırmaların İdare Edilmesi,
- Milli Siber Vakalara Müdahale Organizasyonunun Tesis Edilmesi,
- Milli Siber Güvenlik Altyapısının Kuvvetlendirilmesi,
- Siber Güvenlik Konusunda Personel Eğitilmesi,
- Siber Güvenlikte Milli Teknolojilerin Oluşturulması/Kullanılması,
- Milli Güvenlik Sistemlerinin İçeriğinin Genişletilmesidir.

Planda verilen kararlarla, ülke çapında siber ortam ve bilişim sistemlerine ilişkin yapılacak olası taarruzların engellenmesi amaçlanmıştır. Zamanla bilgi teknolojilerindeki yeniliklerle beraber taarruz usullerinin farklılaşmasıyla değişik açıklıklar oluşmaktadır. Planda, bu açıklıkların asgari seviyeye çekilip milli güvenli bilgi toplumu meydana getirme konunda amaçlar belirlenmiştir. Siber taarruzların basit ve düşük maliyetle

yapılabilmesi ve sorumlunun belirlenmesinin kolay olmaması nedeniyle, öncelikli olarak eylem maddelerinde kullanıcı bilinç seviyesi ve eğitim durumu üzerinde durulmuştur.

Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı, UDHB koordinasyonunda kamu kurum ve kuruluş temsilcileri, sivil toplum yetkilileri ve özel sektör temsilcilerinden oluşturulan bir ekip tarafından hazırlanmıştır. 2016-2019 döneminde, mevcut riskleri belirlenen ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar aşağıdaki şekilde belirlenmiştir;

-Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurum tarafından denetlenmesi,

-Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması,

- Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi,

-Kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hatalar ve afetlerden korunması için düzenlemelerin yapılması,

-Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe sahip olması,

-Siber güvenlik konusunda kurum yöneticilerinin ve personelinin farkındalığının artırılması.

Belirtilen stratejik amaçlara ulaşmak için gerçekleştirilecek eylemler beş stratejik eylem başlığı altında toplanmıştır;

1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması
2. Siber Suçlarla Mücadele
3. Farkındalık ve İnsan Kaynağı Geliştirme
4. Siber Güvenlik Ekosisteminin Geliştirilmesi
5. Siber Güvenliği Milli Güvenliğe Entegrasyonu.

Son olarak Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan ‘Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023’e ilişkin 2020/15 Sayılı Cumhurbaşkanlığı Genelgesi, 29 Aralık 2020 tarihli Resmi Gazete’ de yayımlandı. Stratejik amaçlar kapsamında hayata geçirilecek her bir eylemin gerçekleştirilmesinden sorumlu ve iş

birliği yapılacak kurum ve kuruluşlar, eylem kapsamında atılacak adımlar ve eylemlerin gerçekleşme süreleri de belirlendi.

'Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020–2023' için görüşlerini paylaşan Cumhurbaşkanı Recep Tayyip Erdoğan, "Sürekli gelişim ve değişim kaydeden, yaygınlaşarak yaşamımızın ayrılmaz bir parçası haline gelen bilgi ve iletişim teknolojileri bizlere birçok imkân sunarken siber güvenlik risklerini de beraberinde getiriyor. Siber tehditlere karşı, milli güvenliğimizin önemli bir parçası olan ulusal siber güvenliğimizin sağlanması en öncelikli konulardan biri haline geldi. Ortaya çıkan ulusal ihtiyaçlarla teknolojide yaşanan gelişmeler dikkate alınarak Ulaştırma ve Altyapı Bakanlığınca, kamu, özel sektör, sivil toplum kuruluşları ve üniversitelerle iş birliği içinde 'Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020–2023' hazırlandı" dedi.

Belgede şu noktalar vurgulanmıştır: "Yapısal olarak değişen, gelişen, karmaşıklaşan ve sayıları hızla artan siber tehditler karşısında vatandaşlarımızın, kurumlarımızın, sektörlerimizin, kısacası ulusal siber ortamımızın güvenliği, ülkemizin ekonomik büyümesinde de anahtar rol oynamaktadır. Ekonomik ve toplumsal yaşantıda gözle görülür değişimlerin ortaya çıktığı ve teknolojik dönüşüm dinamiklerinin hızlandığı küresel pandemi ve sonrasına ilişkin koşullar; altyapı, yeni teknolojiler, insan kaynağı ve farkındalık açısından siber güvenlikle ilgili gereksinimleri de artırmıştır. Ulusal siber güvenlikte çıtanın her geçen gün daha da yukarıya çıkarılması güçlü ulusal stratejilerle mümkündür. Bunun için teknolojik gelişmelerin etkileri, siber tehditlerde ortaya çıkan eğilimler, ulusal ihtiyaçlar ve uluslararası uygulamalar dikkatle incelenerek hedefler ortaya kondu. Söz konusu hedeflere ulaşmak için gereksinimlerle gerçekleştirilecek faaliyetler belirlenerek çalışmalar tamamlandı."

Yerli ve milli siber güvenlik teknolojilerinin üretilmesi konusunda özel sektör tarafından gerçekleştirilen çalışmaların desteklenmesine yönelik eylemlerle de teknolojik kazanımlar artırılacak. Ayrıca siber güvenliğin doğası gereği ulusal faaliyetlerin yanında uluslararası iş birliğinin geliştirilmesi de önem arz etmekte. Bu çerçevede ikili ve çoklu iş birliklerinin artırılması ve bilgi paylaşımının geliştirilmesine yönelik çalışmalar gerçekleştirilip siber uzayda uluslararası ortak normların ve standartların oluşturulması için yürütülen faaliyetlere katkı sağlanacak. Stratejik amaçlar kapsamında hayata geçirilecek her bir eylemin gerçekleştirilmesinden sorumlu ve iş birliği yapılacak kurum

ve kuruluşlar, eylem kapsamında atılacak adımlar ve eylemlerin gerçekleşme süreleri de belirlendi. Önümüzdeki dönemde ulusal siber güvenliğin sağlanmasına ilişkin olarak gerçekleştirilecek faaliyetlerin kapsamının belirlendiği 'Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023' ile bu alanda Türkiye'nin 2023 yılı vizyonunun gerçeğe dönüşmesi hedeflenmektedir (Özkan, 2021).

2. ULUSAL SİBER GÜVENLIK TEŞKİLATLANMASI

Türkiye'nin resmi siber güvenlik kurumlarının organizasyon yapısı üç temel hedef kapsamında şekillendirilmiştir. İlk grupta yer alan kurumlar siber suçlar ile mücadele etmek ve faaliyet alanları dâhilinde istihbari faaliyetlerde bulunmak amacıyla kurulmuşlardır. İkinci grupta yer alanlar kurumlar, kritik altyapıların ve kamunun siber güvenliğinin sağlanması ve Türkiye'nin siber savunma, saldırı ve espiyonaj kapasitesini oluşturması hedeflerine odaklanmışlardır. Üçüncü grupta yer alan kurumlar ise devlet destekli özel girişimlerdir. Tüm bu organizasyon yapısının Türkiye'nin siber güvenlik politikasının oluşturulması noktasındaki hedeflerinin tespit edilmesinden ve yönetilmesinden sorumlu üst kurul ise SGK'dır (Darıcılı, 2019).

Siber suçla mücadele ve kendi faaliyet alanlarına dair istihbari faaliyet yürütme hedefine yönelen kuruluşlar, İçişleri Bakanlığı bünyesinde oluşturulan Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı (JGK) Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü'dür. İkinci grupta yer alan kurumsal yapılanmalar ise BTK, Milli İstihbarat Teşkilatı (MİT) Başkanlığı, Afet ve Acil Durum Yönetimi Başkanlığı'na (AFAD), Türk Silahlı Kuvvetleri (TSK) Siber Savunma Komutanlığı, TÜBİTAK'tır. Bu kapsamda 2008 ve 2014 yılında yapılan yasal düzenlemeler ile BTK, bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması konuları kapsamında Türkiye'nin siber savunma kapasitesinin oluşturulmasında temel işlevleri sağlayan kurumu haline gelmiştir (BTK, 2018).

Diğer yandan 2009 yılında çıkarılan bir kanunla Türkiye'de afet hallerindeki acil durum yönetimi yetkisi AFAD'a verilmiştir. Yine aynı kanuna göre afetler, teknolojik ve

doğal afetler olarak ikiye ayrılmıştır. Bu kapsamda Türkiye'nin topyekûn bir siber saldırıya karşı karşıya kalması ve bunun bir afet seviyesine ulaşması halindeki olası kriz süreci AFAD tarafından koordine edilecektir (27261 Sayılı Resmî Gazete, 2009). Ancak bu kriz yönetimin nasıl yapılacağı, hangi kurumsal yapılanmalar ve süreçler dâhilinde sürdürüleceği konusu net olarak ortaya konmamıştır.

MİT Elektronik ve Teknik İstihbarat (ETİ) Başkanlığı, 2937 sayılı MİT'in kuruluş kanununda yazan hedefleri kapsamında telekomünikasyon yoluyla elde edilen istihbaratı tespit etmek, bu şekilde tespit edilen istihbaratı analiz etmek, görüntü İstihbaratı (Imagery Intelligence / IMINT) sağlamak ve analiz etmek, kriptolu haberleşmelere hulul etmek görevleri kapsamında faaliyet yürütmektedir. Sinyal İstihbaratı Başkanlığı (SİB) ise Sinyal İstihbaratı (Signal Intelligence / SIGINT) sağlamak, hedef unsurların haberleşme ve radar iletişimine hulul etmek ve derlenen ham istihbaratı analiz etmek şeklinde görevler icra etmektedir (MİT, 2018). SİB, daha önce Genelkurmay Elektronik Sistemler (GES) Komutanlığı olarak faaliyet gösteren birimin 2012 yılında MİT'e devri ile kurulmuştur (Sabah Gazetesi, 2012). MİT'e devredilerek SİB adını alan GES Komutanlığı, NATO standartları kapsamında yıllarca TSK'nın sinyal istihbaratı ihtiyaçlarını karşılayan birimi olmuştur. Bu birim, 2012 yılında Fetullahçı Terör Örgütü (FETÖ) yapılanmalarının sızma girişimlerini engellemek amacıyla MİT'e devredilmiştir. GES Komutanlığı sahip olduğu imkân ve kabiliyetler bakımından ABD'nin Ulusal Güvenlik Ajansı (National Security Agency / NSA) ile kıyaslanabilir. NSA, ABD'nin küresel izleme, şifre çözme, veri toplama, veri analizi, sinyal toplama, çeviri ve yabancı istihbaratlara karşı istihbarat yapma amaçları için tesis ettiği müstakil bir istihbarat örgütüdür (NSA, 2018). GES'in MİT'e devredilmesi dönemin şartları kapsamında bir zorunluluktan kaynaklanmış olmakla birlikte, böylesine geniş imkân ve kabiliyete sahip bir örgütlenmenin ABD örneğinde olduğu gibi asker-sivil personel yönetimi ile müstakil bir kanuna, örgütlenmeye ve bütçeye sahip olacak şekilde, Türkiye'nin siber güvenlik stratejisinde yer almasında bizce fayda mütalaa edilmektedir. MİT'in mevcut iş yoğunluğu, yeni yapılan yasal düzenlemeler ile giderek artan yetki alanı ve hacmi dikkate alındığında, SİB Türkiye'nin milli siber güvenlik ve espiyonaj ihtiyaçlarını karşılayacak şekilde NSA örneğinde olduğu gibi müstakil bir yapı şeklinde faaliyetlerine devam etmesi daha verimli bir yaklaşım olabilecektir (Darıcılı,2019).

2.1. Ulusal Siber Güvenlik Görev ve Sorumluluk Dağılımı

Bakanlar Kurulu tarafından alınan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar 20 Ekim 2012 tarih ve 28447 sayılı Resmi Gazete ile yürürlüğe girmiştir. Bu kararla, Ulaştırma, Denizcilik ve Haberleşme bakanının başkanlığında "Siber Güvenlik Kurulu" kurulmuştur (Resmi Gazete,2015).

Kurul, siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını sağlamak amacıyla kurulmuştur. Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurumları ile üyelerinin temsil düzeyleri Bakanlar Kurulu tarafından belirlenir.

1 Kasım 2011 tarihli Resmi Gazete 'de yayınlanan, 26 Eylül 2011 tarih ve 655 sayılı "Ulaştırma Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname" kapsamında bakanlığın görevleri belirlenmiştir. Bakanlığın siber güvenliğe yönelik görevleri, 6 Şubat 2014 tarihinde kabul edilen 6518 sayılı Kanun ile 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilmiştir (Resmi Gazete,2015).

Telekomünikasyon sektörünü düzenleme ve denetleme fonksiyonunun bağımsız bir idare tarafından yürütülmesi amacıyla 4502 sayılı Kanun'la kurulan Telekomünikasyon Kurumu, 10 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile yeni bir düzenlemeye tabi olmuş ve adı Bilgi Teknolojileri ve İletişim Kurumu (BTK) olarak değiştirilmiştir (BTK,2015). Kurum, elektronik haberleşme sektörünü düzenlemek ve denetlemekten sorumludur. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezi'nin Kurulması ve Sektörel-Kurumsal SOME'lerin Oluşturulması" başlıklı 4. eylem maddesi uyarınca BTK bünyesinde USOM (TR-CERT) kurulmuştur. Mayıs 2013 tarihinde kurulan USOM, ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile kendisine ulaştırılan ihbarları da değerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi için kamu kurum ve kuruluşları ile koordinasyonu sağlamaktadır. Kurumsal SOME'ler kurumlarına doğrudan veya dolaylı yoldan yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemi almak veya aldırmak, bu tür olaylara karşı müdahale

edebilecek mekanizmayı ve olay kayıt sistemlerini kurmak, bilgi güvenliğini sağlamaya yönelik çalışmalar yapmak veya yaptırmakla yükümlüdürler.

1963 yılında kurulan TUBİTAK, Türkiye'de bilim ve teknolojiyi teşvik etme, yönlendirme ve popüleştirmeyi amaçlayan, Bilim, Sanayi ve Teknoloji Bakanlığı'na bağlı; idari ve mali özerkliğe sahip resmi bir devlet kurumudur. TUBİTAK enstitülerinden biri olan Ulusal Elektronik ve Kriptoloji Enstitüsü (UEKAE), stratejik kamu kurumlarının ihtiyaç duyduğu bilgi güvenliği ve elektronik sistem projelerini geliştirirken aynı zamanda Türkiye'nin siber güvenlik birikimine önemli katkı sağlayan bir AR-GE kuruluşudur. 2012 yılında bu yana ise TUBİTAK BİLGEM bünyesinde Siber Güvenlik Enstitüsü (SGE) olarak ayrı birim şeklinde faaliyetlerine devam etmektedir. SGE'nin etkinlikleri üç başlık altında toplanmaktadır;

-İleri siber güvenlik araştırma-geliştirme çalışmaları,

-Siber güvenlik stratejisi belirleme çalışmaları,

-Siber güvenlik çözüm projeleri ve siber güvenliğe yönelik sistem ve teknolojik ürünler.

Türk Silahlı Kuvvetleri; kara, deniz, hava ve uzay harekât alanlarının yanında, yeni bir harekat alanı olan siber ortamda yer almak maksadıyla 2012 yılında TSK Siber Savunma Merkezi Başkanlığı teşkil etmiştir. Merkezin adı 2013 yılında "TSK Siber Savunma Komutanlığı" olarak değiştirilmiştir. Komutanlık, Genelkurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanlığına bağlı olarak görev yapmakta, bünyesinde her kuvvetten personel yer almaktadır.

2.2. Ulusal Siber Olaylara Müdahale Merkezi

Siber güvenliğin sağlanması için "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar" 20 Ekim 2012 tarihli Resmî Gazetede Bakanlar Kurulu Kararı olarak yayımlanmıştır.

Bu Karar ile siber güvenliğe ilişkin program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla "Siber Güvenlik Kurulu" ("Kurul") oluşturulmuştur. Kurul bu alandaki çalışmalarını yürütmek adına bir toplantı düzenlemiş ve "Ulusal Siber Güvenlik Stratejisi ve 2013–2014 Eylem Planını" ("Eylem Planı") kabul etmiştir.

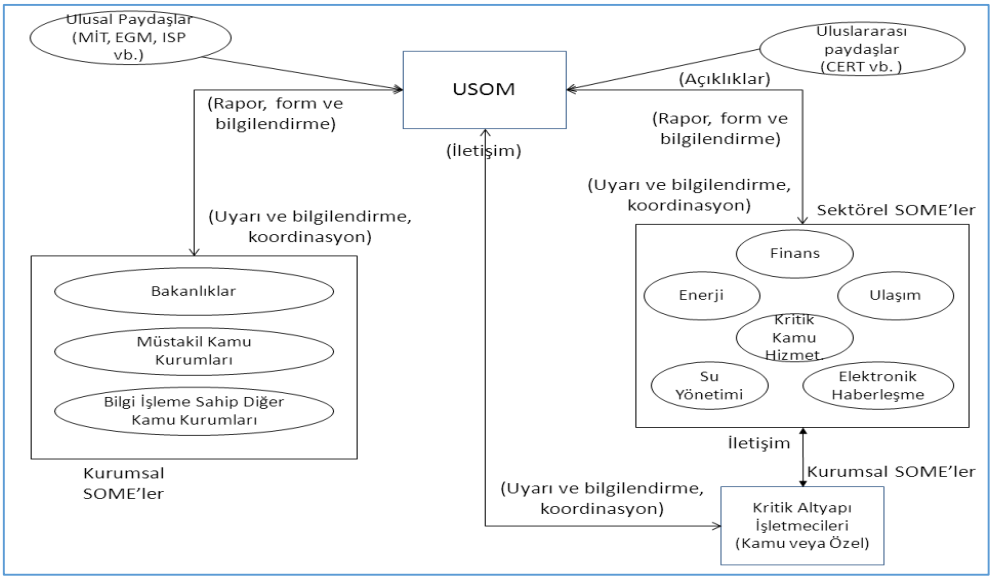
Eylem Planı uyarınca temel görevi koordinasyon ve iş birliği olan Ulusal Siber Olaylara Müdahale Merkezi ("USOM"), Telekomünikasyon İletişim Başkanlığı bünyesinde kurulmuştur. Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından hayata geçirilen USOM'un kurulma amacı şu şekilde özetlenmiştir:

– Türkiye'de siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması,

– İnternette yer alan tüm aktörler ile uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişimi sağlamak,

– Siber güvenlik olayları hakkında alarm, uyarı ve duyuru yoluyla kritik sektörlerin korunması için ulusal ve uluslararası koordinasyonun tesis edilmesi.

"Ulusal Siber Olaylara Müdahale Merkezi" vazifeleri çerçevesinde ülkemiz kaynaklı hem de yabancı menşeli siber riskleri belirleme ve bu tehditlerin önüne geçme görevlerini yapmaktadır. Bahse konu siber güvenlik faaliyetlerine yönelik ortaya konan araştırmalar kapsamında sorumlulara ilişkin olarak alarm, ikaz ve ilan işlemleri de yerine getirilmektedir. Kurulması planlanan USOM ve SOME' lerle birlikte, siber suçlara müdahalenin daha hızlı ve sistemli olması hedeflenmiştir. Sektör ve kurumlar tespit ettikleri siber tehditlerde sorumlu kuruluşlarla diyaloga geçerek milli işbirliğine katkı sağlamaktadır. Milli siber vakalara müdahale şeması içinde bulunan USOM, sektörel ve kurumsal SOME' lerin aralarındaki ilişki Şekil 24'de görülmektedir.



Şekil 24. Ulusal Siber Olaylara Müdahale Merkezi Organizasyonu

Kaynak: BTK

Yukarıdaki şekilde yer alan kavramları açıklamak gerekirse;

a) Uyarı ve bilgilendirme: Siber olay öncesinde USOM tarafından hazırlanan bülten, duyuru gibi bilgileri,

b) Koordinasyon: Siber olay esnasında USOM ve varsa bağlı olduğu Sektörel SOME tarafından yapılan koordinasyonu,

c) Rapor, form ve bilgilendirme: Siber olay öncesi, esnası ve sonrasında USOM ve varsa bağlı olduğu Sektörel SOME tarafından talep edilen ve Kurumsal SOME'ler tarafından iletilen bilgileri ifade etmektedir.

Siber olaylara müdahale edebilmek için kurulan ekibe, Siber Olaylara Müdahale Ekibi (SOME) denir. SOME'ler bilgi sistemleri güvenlik olaylarına müdahale hizmeti ile diğer önleyici ve düzeltici hizmetler veren ekiplerdir. SOME'ler ülke seviyesinde veya kurum seviyesinde kurulabilir. Kurumun tümüne merkezi olarak görevlendirilebileceği gibi belirli sayıda alt seviyelerde de oluşturulabilir. Burada önemli olan husus, koordinasyonun sağlanması ve yeterli güvenlik personelinin istihdam edilmesidir. Kurumsal SOME'lerin görevlerini, siber olay aşamalarını temel alarak 3 başlıkta incelemek gerekmektedir.

1) Siber Olay Öncesi: Kurumda bir siber olayın yaşanmadığı veya gerçekleşmediği durumda Kurumsal SOME'ler, kurum içi farkındalık çalışmalarının gerçekleştirilmesi, kurumsal bilişim sistemleri sızma testlerinin yapılması / yaptırılması ve kayıtların düzenli olarak incelenmesi çalışmalarını yapmaktadırlar.

2) Siber Olay Esnası: Kurumda herhangi bir siber olayın gerçekleştiği durumlarda, Kurumsal SOME'lerin bilgi işlem birimi, internet servis sağlayıcısı, Sektörel SOME, USOM, hukuk müşavirliği, savcılık, kolluk kuvveti ve basın müşavirliği ile birlikte iş birliği içerisinde hareket ederek ilgili siber olayı durdurma çalışmalarını aşağıdaki sırayı izleyerek yapmaktadırlar.

Olay veya olay bildirimi sonrasında Kurumsal SOME, bilgi işlem birimi ile ilgili olayın siber olay teşkil edip etmediği hakkında araştırma yapar. Olayın siber olay olduğuna karar verilirse, müdahalenin koordineli bir şekilde gerçekleştirilmesi amacıyla USOM ve ilgili Kurumsal SOME'nin varsa bağlı olduğu Sektörel SOME ile irtibata geçilerek iş birliği içerisinde hareket edilir ve müdahalede bulunulur. Eğer siber saldırı

sonucunda suç işlendiğine kanaat getirilirse ilgili adli ve idari kurumlara haber verilir. Müdahalenin gerçekleştirilmesinden yani siber olayın sona erdirilmesi sonrasında değerlendirme yapılır ve siber olay sonrası işlemler gerçekleştirilir.

3) Siber Olay Sonrası: Siber Olay Esnasında yapılması gereken işlemler tamamlandığında, siber olayın tekrarlanmasını engellemek adına aşağıdaki çalışmalar yapılır. Zaman geçirmeden olaya neden olan açıklık belirlenir ve çıkarılan dersler kayıt altına alınır.

Kurumsal SOME, siber olay ile ilgili bilgileri USOM tarafından belirlenen kriterlere uygun şekilde USOM'a ve varsa bağlı olduğu Sektörel SOME'ye gönderir ve kayıt altına alır. Olayla ilgili olarak gerçekleştirilebilecek düzeltici/önleyici faaliyetlere ilişkin öneriler kurum yönetimine arz edilir. Yaşanan siber olayların türleri, miktarları ve maliyetleri ölçülüp izlenir. Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu hazırlanır, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilir.

İnternet kullanıcıları, kolluk kuvvetleri, küresel kurum/ kuruluşlar, araştırma birimleri ve sivil sektör arasındaki işbirliği ve koordine hususları USOM tarafından yerine getirilmektedir. SOME' ler devamlı USOM ile irtibat durumundadır ve iki yönlü bilgi akışı söz konusudur. Sektörel SOME' lerse ülkedeki kritik alanların siber güvenliğinin tesis edilmesiyle vazifelidir. Kurul bünyesinde Türkiye'ye ait kritik alanlar; Ulaşım Altyapısı, Enerji, Elektronik İletişim, Sermaye Piyasası, Su İdaresi ve Kritik Kamu Hizmetleri şeklinde tespit edilmiştir. Sektörel SOME'ler kritik alanlara ilişkin düzenleyici ve kontrol edici kuruluşların içerisinde veya ilgili bakanlık uhdesinde kurulmuştur. USOM, kendisine gelen ihbarları ilk aşamasından itibaren yöneten, özel ekipleri tarafından çözüm sürecine kadar takip eden ve değerlendiren resmi bir kurumdur. Aynı zamanda ulusal ve uluslararası siber güvenlik tatbikatları düzenlenerek kamu kurum ve kuruluşlarının siber saldırılara karşı farkındalığının artırılmasına yardımcı olarak bilinçlendirme ve yönlendirme faaliyetleri sürdürmektedir.

SONUÇ VE DEĞERLENDİRME

Güvenlik kavramı tarihi perspektif içerisinde her dönem karşımıza çıkan, tüm insanlar için tesis edilmesi ve korunması önem arz eden bir konu olarak uluslararası ilişkilerin ana maddelerinden birini teşkil etmiştir. Bu nedenle devletlerin ana varlık nedeni olarak güvenlik olgusu ön plana çıkmıştır. Fakat sanayi devrimi ile kendini daha yoğun olarak gösteren BİT'lerinde yaşanan gelişmeler güvenlik konusunu hem pozitif hem de negatif olacak şekilde iki taraflı olarak etkilemiştir. Güvenlik konusu, insanların hayat tarzlarındaki değişim ile beraber farklılaşmıştır. Diğer yandan, BİT'lerinde görülen ilerlemeler, ekonomik ve sosyal şartların süratli değişimi ile beraber küreselleşme nedeniyle güvenlik konusunun tekrar tartışılması gündeme gelmiştir. Yaşanan gelişmelerin insan hayatını doğrudan etkilemesi neticesinde klasik yaklaşımlar güvenlik paradigmasını manalandırmada kifayetsiz kalmıştır.

21. yüzyılda güvenlik olgusu ve milli güvenlik yaklaşımları 2. Dünya Savaşı'nın ardından nispeten daha sınırlı bir değişimle karşılaşmıştır. Bu dönemde ulus devlet kurgusu içinde ülkeler risk, tehdit, tehlike ve düşman tanımlarını daha net bir biçimde belirtmiş ve güçleri oranında bu unsurlarla mücadele etmiştir. Ancak, özellikle 1990'lardan sonra Sovyetler Birliği'nin dağılmasının ardından küreselleşmenin daha da ivmelenmesi ile birlikte güvenlik daha geniş, belirsiz, çok yönlü, karmaşık, farklı oyuncuların rol aldığı, klasik aktörlerin ise nispeten önemini yitirdiği bir durum arz etmiştir. Bu değişimler neticesinde özellikle klasik güvenlik yaklaşımındaki düşman olgusunun yerini tehdit kavramı almıştır.

Ortaya çıkan bu yeni durum çerçevesinde günümüz şartlarında klasik kalıpların yanında ve ötesinde yeni ve farklı anlayışlara da gereksinim vardır. Hâlihazırda küreselleşmenin de tesiriyle tehdidin kaynağının belirlenerek mücadele edilmesi zorlaşmıştır. Gelişmeler çerçevesinde risk ve tehditler de küreselleşmeye başlamış, bu sebeple ülkelerin bireysel olarak üstesinden gelemeyecekleri bu problemlerle mücadele edebilmek maksadıyla güvenlik paradigmasının günümüz şartlarına uygun şekilde, geniş kapsamda ele alınması gerekmiştir.

Güvenlik anlayışının kapsamı genişlerken diğer taraftan tehdit ve risk kavramı da her geçen gün somut olma özelliğini kaybetmiştir. Küreselleşmenin doğal bir sonucu olarak sınırların belirsizleşmesi ve bu manada ortadan kalkması neticesinde milli ve uluslararası güvenlik arasındaki ayrım kalkmış, daha geçişken bir hal almıştır. Bu çerçevede güvenlik kavramının tekrar değerlendirilmesi, mevcut şartlara göre yeni riskleri de ihtiva edecek ve birey güvenliğini önceliğe alacak şekilde, eski yaklaşımların ötesinde yeni görüşleri de içerecek şekilde ele alınması gerekmiştir.

Klasik anlayışa göre devletler güvenliğin yegâne sorumlusuyken, yeni anlayışlara göre güvenlik kavramı bütün bireyler için müşterektir ve karşılıklı bağımlılık zeminine oturtulmuştur. Global risk ve tehditler bütün insanlar için söz konusu olup rekabetten öte uluslararası işbirliği, koordinasyon, diyalog ve karşılıklı bağımlılığı ön plana çıkarmıştır.

Sovyetler Birliği'nin dağılmasının ardından iki kutuplu bloklaşma düzeninin sona ermesi, devlet odaklı realist görüşün ağırlığının azalması, teknolojik gelişmelerle birlikte küreselleşme sürecinin hızlanmasına neden olmuştur. Özellikle 11 Eylül saldırılarının yaşanmasının ardından yeni güvenlik ortamında terörizm, kitle imha silahlarının yayılması, deniz haydutluğu, düzensiz göç ve mülteci hareketleri, çevre güvenliği ve iklim değişikliği, enerji güvenliği, salgın hastalıklar ve ulusaşan organize suç ve kaçakçılık ile siber güvenlik gibi risk ve tehditler kendini göstermiştir. Güvenlik paradigmasının bu şekilde çeşitlenmesi, farklılaşması ve genişlemesi ile birlikte daha önce de arz edildiği gibi klasik güvenlik anlayışı tartışılmış, bu kapsamda hem pozitivist eleştirel anlayışlar hem de Kopenhag Okulu anlayışının ortaya koyduğu fikirlerle güvenliğin yeni durumunu açıklamakta yeni görüşler ortaya konmuş ve bireyin güvenliği esas alınmıştır.

Yeni güvenlik ortamının oluşturduğu risk ve tehditler arasında, teknolojik gelişmelerin ve internetin hayatın hemen hemen her alanına girmesi ile birlikte siber güvenlik konusu bir adım öne çıkmıştır. Birçok devlet adamı ve komutan tarafından siber güvenlik konusunda yapılan açıklamalar ile yakın dönemde siber güvenlik konusunda yaşanan olaylar bu durumu açıkça ortaya koymuştur.

Hayatın her alanında kolaylaştırıcı bir unsur olarak internetin ve bilgi teknolojilerin yer alması sebebiyle askeri dışa kapalı sistemler haricinde, milli, kamusal ve özel sektör bilgi ve iletişim sistemleri ile altyapılarının birbirinde ayrılması mevcut şartlarda neredeyse mümkün değildir. Sağlık alanından finans sektörüne, eğitim sisteminden yargı sistemine, ulaştırma sisteminden savunma sanayine, enerji sektöründen haberleşme sistemine kadar hemen hemen tüm alanların birbirine entegre olması ve içi içe girmesi siber güvenlik konusunun önemini, tehdidin ulaştığı boyutu ve olası etkilerini net bir şekilde göstermektedir. Siber güvenlik konusunda yaşanabilecek bir olumsuzluğun seviyesine bağlı olarak devletin tüm unsurlarını dramatik bir şekilde etkileme ihtimali söz konusudur. Bu nedenle siber güvenlik konusu bireyin, toplumun, devletlerin ve uluslararası sistemin gündemine üst sıralardan girmiştir.

Milli güvenlik bakımından önem arz eden ve hasar alması halinde ciddi sonuçları olan kritik altyapılara yönelik siber uzaydan gelebilecek eylemlerin, binlerce bireyin istifade ettiği sistemleri ve dolayısıyla bireyin yaşamını tehdit etmeye başlaması ile siber güvenlik kaygı haline dönüşmüştür. Bu kapsamda kritik altyapıların tespit edilerek siber güvenliğine ilişkin tedbirler alınması, siber eylemlere karşı muhafaza edilmesi elzemdir.

Ülkeler açısından değerlendirildiğinde sanal ortamdan gelecek risk ve tehditler ile bunlara yönelik atılacak adımlar ve alınacak önlemlerle alakalı farklı düşünceler bulunmaktadır. Siber uzayda ülkeye yönelik yapılan taarruzlara ilişkin askeri tedbirler çerçevesinde reaksiyon gösterilmesine ulaşan, siber taarruzları harp nedeni görme anlayışının yanında, siber ortamda vuku bulun tehditlerin aynı platformda karşılık bulması gerektiğini savunan tezlerde söz konusudur.

Türkiye'de siber güvenlik farkındalığının yükseltilmesi, yakın dönemde artan şekilde siber eylemlere maruz kalınması ve bu durumun bir gereksinim olarak kendini göstermesi ile beraber; ulusal bilgi güvenliği programları, ulusal bilgi güvenliği kapısı, siber güvenlik eylem planları hazırlanmaktadır. Ayrıca hukuki mevzuat çalışmaları yapılmakta, siber güvenlik acil reaksiyon timleri ve birimleri teşkil edilmekte, siber güvenlik eğitim/tatbikatları, çalıştaylar ve konferanslar icra edilmektedir.

Siber eylemler ülkelerin milli güvenliğini tehdit etmesi yönünden farklı bir harekât alanı olarak siber uzayı karşımıza çıkarmıştır. Siber ortamda, eylemlerin kaynağını tespit etme ve süratini belirleme gibi birçok güçlük bulunmaktadır. Eylemin sorumlusunun tespitinin zor olması, eylemlerin sürati, karmaşıklığı, gizliliği karar alma süreçlerini ve mevcut karşı tedbirlerin etkinliğini zafiyete uğratabilmektedir.

Askeri çerçeveden bakıldığında siber uzay komutanların görevlerini yapabilmeleri için bilmesi, planlaması ve harekât icra etmesi gereken kara, deniz, hava ve uzaya ek beşinci bir boyut olarak karşımıza çıkmaktadır. Siber vasıtaların, silahların askeri karar vericilere sağladığı üstünlüklerden biri askeri hedeflerin tesir altına alınmasında ateş kuvveti kullanmadan düşmana asimetrik tesir oluşturabilmesi ve potansiyel olarak inisiyatifi elde bulundurmasıdır. Savunma perspektifinden değerlendirildiğinde ise askeri yeteneklerin kaybedilmemesinde önemli bir yeri olan siber uzayın muhafaza edilmesi hayati bir görev halini almıştır. Bu durumun yakın zamandaki örnekleri Gürcistan ve Estonya vakalarında yaşanmıştır.

Siber güvenliğin tesis edilmesinin önemi dikkate alındığında, siber uzaydaki eksikliklerin giderilmesi, siber eylemlere yönelik tespit, ikaz, savunma, karşı saldırı mekanizmalarının teşkil edilmesi ve koordinasyonun sağlanması maksadıyla ABD'deki yapıya benzer bir Siber Komutanlığı'nın kurulması ciddi bir üstünlük olarak karşımıza çıkmaktadır. Türkiye'de siber güvenlik konusunda icra edilen faaliyetler dünyada belirli bir seviyeye gelmiş olmasına rağmen gelişime açık olup tehdit kaynakları ve yöntemlerinin farklılık göstermesinden ötürü hiçbir zaman yeterli olarak kabul edilmeyecektir.

Siber güvenlik konusunda araştırma ve geliştirme merkezleri tarafından gereksinimlerin milli ve yerli kaynaklarla giderilmesi önem arz etmektedir. Bu çerçevede, öncelikle gereksinimler tespit edilmeli, bu gereksinimlerin milli kabiliyetlerle giderilmesi için üzerine odaklanılacak konular belirlenmelidir. Kamu kurum/kuruluşları, eğitim kurumları ve özel sektör bu ihtiyaçların giderilmesinde koordinasyon içerisinde bulunmalı ve hatta bunun bir adım ötesine geçilerek uluslararası işbirliği çalışmalarına ve programlara iştirak edilmelidir.

Siber uzaydaki eylemlerin sayısının her geçen gün artması, çeşitlenmesi ve etkilerine karşın kuvvet kullanımının en temel konusu olan meşru müdafaa doktrini çerçevesinde konumu da dâhil olmak üzere tabi olduğu hukuki düzen hali hazırda net tespit edilmemiştir. Uluslararası hukukun ve kavramların geniş manada yorumlanması ile mevcut problemlere bir şekilde çözüm üretilmektedir. Fakat siber harekât ortamının her geçen gün kapsamının genişlemesi, faaliyetlerin, uygulama alanının artması ve seçim sonuçlarını etkileme konusu da dâhil olmak üzere dünya çapında büyük etkiler oluşturabilecek örneklerin sayısının ve kapsamının gelecekte daha da fazlalaşacağı öngörülmektedir. Bu kapsamda mevcut uluslararası hukukun geniş manada yorumlanması suretiyle yapılan uyarlamaların siber eylemlerin sınıflandırılması, eşik seviyeleri ve askeri mukabele metotlarını tespit etmede kâfi gelmeyeceği kıymetlendirilmektedir.

Devletlerin BİT'lere her geçen gün daha da fazla gereksinim duyması ileride siber eylemlere ilişkin tehdidin daha da fazlalaşmasına ve kapsamının genişlemesine sebep olacaktır. Teknolojinin ve internet kullanımının her geçen gün yaygınlaşmasıyla beraber terör grupları siber uzayı kullanmaya başlamıştır. Terör örgütleri/grupları siber uzaydan propaganda ve şiddet maksatlı olmak üzere iki amaç için istifade etmektedir. Şiddet eylemlerindeki maksat hedefe zarar vermek ve imha etmektedir. Şiddet içermeyen eylemlerde ise maksat etkinliği, güvenilirliği sarsma ve maddi çıkar elde etmektir. Terör faaliyetlerinin siber uzayda vuku bulması sınırları ortadan kaldırmış ve devletlerin, uluslararası kurum/kuruluşların ve organizasyonların işbirliği içerisinde olmasını gerekli hale getirmiştir.

Siber uzaydaki tehditlerin asgari seviyeye indirilmesinde ve bertaraf edilmesinde izlenmesi gereken metotlardan birisi de eğitim faaliyetleridir. Yapılacak eğitim faaliyetleri ile farkındalık ve bilinç seviyesi yükseltilecek ve personel kaynaklı hataların en aza indirgenmesi sağlanmış olacaktır.

Siber uzaydaki tehditlerin her geçen gün daha da fazlalaşması sebebiyle bireysel ve kurumsal tüm bilgi ve iletişim cihazlarında donanımsal ve güvenlik tedbirlerinin alınması zaruret arz etmiştir. Kurum/kuruluşlar ile şirketlerde tehdit kıymetlendirmeleri yapılarak muhtemel siber eylemler karşısından uygulanacak prosedürler tespit edilmeli ve yedekleme planları yapılmalıdır.

Devletlerin siber eylemlere bakış açıları farklılık arz edebilmektedir. Bazı devletler siber uzayda daha az faaliyet gösterdiğinden, internet kullanıcı ve işlem sayısı düşük olduğundan bu alana biraz daha ilgisiz kalabilmektedir. Bazı devletler ise siber uzayı harp alanı olarak kıymetlendirmekte ve bu alandaki faaliyetlerine ayrı önem vererek diğer devletlerin zafiyetlerini, açıklıklarını belirlemeye çabalamaktadır. Bu anlayışı esas alan devletler genellikle bu konuda işbirliği ve diyaloğa kapalı şekilde hareket etmekte ve konunun muallakta kalmasını tercih etmektedir.

Siber uzayın yapısı itibari ile meydana getirdiği geniş ve kontrolsüz atmosfer alınan tüm tedbirlere karşın eylemi yapanın tespit edilmesini güçleştirmekte ve hasarın büyümesine neden olmaktadır. Siber eylemlerin hedefleri ve etkileri göz önünde bulundurulduğunda bu taarruzların bazılarının arkasında devletlerin bulunduğu değerlendirilmektedir. Diğer yandan, siber uzayda tespit edilmeden birçok siber casusluk eylemleri de icra edilmektedir. Fark edilmeden, gizlice icra edilen siber eylemler daha tehlikeli ve korkutucu olabilmektedir.

Türkiye özelinde siber güvenliğe ilişkin yapılan çalışmalar ve gelişmeler değerlendirildiğinde bazı adımların atıldığı ve konu için hâlihazırda geç olmadığı, kritik altyapı/tesislerin korunmasında, kendi teknolojilerimizin geliştirilmesinde ve bilişim uzmanlarımızın eğitilmesinde yapısal değişimler, adımlar ve stratejiler ile orta ve uzun dönemde siber güvenliğin tesis edilmesinde ilerleme kaydedilerek başarılı olunabileceği değerlendirilmektedir.

Türkiye'de siber güvenliğe yönelik farkındalık seviyesi dünyada olduğu gibi hızlı bir biçimde yükselmektedir. Bu kapsamda siber güvenliğe yönelik kanunlar dâhil bazı yasal düzenlemeler yapılmaya başlanmış, kalkınma planlarına konu edilmese de strateji ve eylem planları ortaya konmuş, bu stratejiler dâhilinde birtakım organizasyonlar ve yapılar teşkil edilmiştir. Fakat atılan bu adımların geliştirilmesi, konuya ilişkin uzman personel kaynağının yetiştirilmesi ve milli bilgi iletişim teknolojilerinin geliştirilmesine önem verilmelidir.

Şekil 25. Ulusal Siber Güvenliğin Sağlanması Süreci

Ulusal boyutta alınması gereken tedbirler Şekil 25 kullanılarak incelendiğinde;

Birinci aşamada; Türkiye siber güvenlik hususunda hâlihazır durumu değişik ülkelerin hukuki düzenlemeleri ile hem bölgesel hem de küresel araştırmalarla mukayese edilerek değerlendirilmeli ve siber güvenlik hususunda ciddi ulusal plan/ programlar ve hukuki düzenlemeler ortaya koymuş olan ülkelerden istifade edilmelidir. Bu basamakta ehemmiyetli olan husus hukuki boşlukları ve bu boşlukların yokluklarının ne şekilde ortadan kaldırılacağına yönelik mümkün olduğunca fazla değişik usul ve metot belirlemektedir.

İkinci aşamada; siber güvenlik hususunda millî yol haritamız ve ulusal kapsam modeli meydana getirilmeli ve ulusal siber güvenlik hukuki düzenlemelerimiz belirlenmelidir. Milli çerçeve model;

-Ulusal siber güvenlik stratejisi ve stratejinin tesirli bir biçimde hayat geçirilmesi,

-Hâlihazır güvenlik kanunlarının sibere uydurulması maksadıyla zaruri araştırmaların yapılması,

-Bilgi teknolojilerini hedef gören taarruzların engellenmesi, belirlenmesi, reaksiyon gösterilmesi ve asgari zayiatla geri dönüşün tesis edilmesi için zaruri yöntem ve metotların tespiti,

-Milli siber güvenlik zihniyetinin içselleştirilmesinin tesis edilmesi,

-Milli siber güvenlik planının kontrol edilmesi, kıymetlendirilmesi, gerçeklemesi ve etkinliğinin yükseltilmesi gibi konuları esas almalıdır.

Üçüncü aşamada; milli siber güvenlik araştırmalarını yürüten kurumsal yapının etkinliği sağlanmalıdır. Bu organizasyonun vazife ve sorumluluklarının yasal altyapısı belirlenmeli, personel, eğitim, istihbarat yetenekleri arttırılmalıdır. Devlet çapında sayısal ortamda savunma birimlerinin oluşturulmasının, kurumların birlikte hareket etmesinin ve bütçeden yeterli kaynağın bu konuya aktarılmasının gerekli olduğu değerlendirilmektedir. Milli Bilgi Güvenliği anlayışını idare edecek merkezi bir kuruluşun (ABD'deki NSA gibi) en kısa zamanda kurularak, tüm kurum/ kuruluşların için bağlayıcı mahiyette bir otorite olmasının, istihbaratın internetten yapıldığı günümüzde, bizleri siber taarruzlara yönelik kuvvetli kılacağı düşünülmektedir.

Dördüncü aşamada; siber aktörlerin bu kadar etkin bir biçimde uluslararası koordinasyon yaptığı bilgi çağında, siber güvenlikten sorumlu görevliler maalesef bu koordinasyon ve dayanışmayı hayata geçirememektedir. Ulusların coğrafi sınırlarının varlığı saldırganlara önemli avantaj sağlamakta ve saldırılarla mücadelede devletlerarasında işbirliğinde yeni bir anlayış oluşturma zorunluluğu ortaya çıkmaktadır. Siber saldırılar tüm uluslararası toplum için büyüyen bir endişe kaynağıdır. Siber tehdide karşı başarılı olabilmek için tüm ülkelerin ulusal gayretleri uluslararası arenada koordineli şekilde birleştirilerek bu alanda işbirliğine gidilmelidir. Ülkeler arası bu tür bir işbirliği sadece yasal düzenlemelerde yapılacak işbirliğini değil, aynı zamanda caydırıcılığı da içinde barındıran askeri işbirliğini de gerektirmektedir. Bu bağlamda Birleşmiş Milletler ve NATO iki uluslararası anahtar örgüt konumundadır.

Barışta ve savaşta bilgi ve iletişim sistemlerinin siber saldırılardan korunması ve ihtiyaç duyulduğu anda hizmet vermeye devam etmesi için atılması gereken adımlar vardır. Ülke çapında topyekûn siber ortam güvenliğinin tesis edilmesi için atılması gereken adımlar ana başlıklar olarak sıralanmıştır;

- Siber güvenliğin hukuki, teknik, idari, ekonomik, politik ve sosyal boyutlarını ele alan multidisipliner bir yaklaşım benimsenmeli ve gerekli yasal mevzuatın bu kapsamda oluşturulması gerekmektedir.
- Ülkemizin kritik altyapılarını emniyetli hale getirmek, siber tehditlere karşı koymak, siber uzaydaki imkân ve kabiliyetleri tesis etmek maksadıyla kapsamlı siber güvenlik strateji ve planları hazırlanmalı, konuların hayata geçirilmesine yönelik denetim faaliyetleri gerçekleştirilmelidir.

- Üniversitelerde ve eğitim kurumlarında siber uzay, siber savaş ve siber tehditler üzerinde araştırma programları başlatılmalı ve siber savunma anlayışı konusunda bölümler açılarak siber güvenlik derslerinin müfredatlarda yer bulması sağlanmalıdır.

- Bilgi ve iletişim sistemlerinin güvenliğini sağlayacak olan insan kaynağı, güncel güvenlik teknolojileri ve sistemleri konusunda teorik ve pratik olarak yetiştirilmeli, kamu kurum ve kuruluşlarında siber güvenlik farkındalık programları düzenli olarak uygulanmalıdır.

- Güvenliği ön plana alan bilişim sistemi yaklaşımının benimsenmesi ve sistemlerin tasarımından gerçekleştirimine kadar her aşamada, güvenli yazılım geliştirme prensipleri dikkate alınarak faaliyetler icra edilmelidir.

- Siber tehditlere devlet kurumlarının, özel sektörün veya bireylerin tek başına karşı koyabilmesi mümkün değildir. Bu kapsamda devlet ve özel sektör arasında eğitim, teknoloji desteği, istihbarat paylaşımı ve ar-ge çalışmaları gibi alanlarda işbirliği yapılmalıdır.

- Herhangi bir savaşı kazanmak için sadece savunma yeterli değildir. Bu açıdan, siber saldırı kabiliyetinin kazanılmasına yönelik adımlar atılmalı, angajman kuralları belirlenmeli ve kanunla bu faaliyetleri gerçekleştirecek kritik kurumlara görev verilmesi hususu göz önünde bulundurulmalıdır.

Son olarak, Türkiye'de siber güvenliğin sağlanması maksadıyla savunma yeteneklerini geliştirmek için yoğun gayret gösterilmektedir. Ancak, hâlihazırdaki çabalar siber risk spektrumunun dar bir kısmını kapsamaktadır. Çok boyutlu siber tehditleri en uygun şekilde bertaraf etmek için bütünsel bir yaklaşım benimsenmelidir. Yukarıda arz edilen maddeler ile yapılan tez çalışması kapsamında konunun farklı birçok yönlerini de içerecek şekilde önerilen "**Türkiye Siber Güvenlik Yönetişim Modeli**nin siber güvenliğin sağlanmasında iyi bir rehber olabileceği değerlendirilmektedir.

Türkiye Siber Güvenlik Yönetişim Modeli Önerisi

Milli Güvenlik Kurulu(MGK) tarafından "Milli Güvenlik", "Devletin milli varlığına, bekasına ve güvenliğine yönelik tehditlere karşı tedbirler almak için bölgesel ve küresel ortamın izlenerek tehdit ve fırsatların tespit edilmesi ile bu hususlara uygun siyasetin belirlenmesini ve en uygun politikaların uygulanmasını sağlayacak süreç ve

unsurlar" olarak tanımlanmaktadır (MGK,2020). Günümüz bilgi ve iletişim teknolojileri çağında bu çerçevede milli güvenliğin temel unsurları arasında yer alan askeri, siyasi, diplomatik ve ekonomik bileşenlerin yanına "siber" unsurların da ilave edilmesinin faydalı olacağı düşünülmektedir. Nitekim savunma sahası bakımından NATO'nun Temmuz 2017 tarihli açıklamasında, kara, hava, deniz ve uzaydan sonra "siber uzay" beşinci operasyonel alan olarak ilan edilmiştir (NATO, 2017). Ayrıca Aralık 2016'daki NATO toplantısında, uluslararası hukukun siber alanda da uygulanması gerektiği belirtilmiş ve 14 Aralık 2017 tarihinde, NATO'nun kolektif savunma çerçevesindeki çekirdek görevlerinden birisinin siber savunma olduğu vurgulanmıştır.

Bu minvalde ülkemizde de 2012 yılından itibaren siber güvenlik alanında benzer çalışmalar yapılmaya başlanmıştır. Yakın tarihte Cumhurbaşkanlığı, siber güvenlik alanında farklı kurumlarda yürütülen çalışmaları tek çatı altında toplamak için çalışma başlatmıştır (Hürriyet, 2017). Cumhurbaşkanı Sayın Recep Tayyip Erdoğan'ın talimatıyla başlatılan çalışmalar kapsamında, siber güvenlik altyapısının yerlileştirilmesi, durum analizi yapılması ve alınması gereken tedbirler ortaya konulacaktır. Yapılan çalışmalar neticesinde Sanayi ve Teknoloji Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu ile TÜBİTAK gibi kurumlarda ayrı ayrı yapılan siber güvenlik çalışmalarının tek çatı altında birleştirilmesi planlanmaktır. Bu kapsamda başta akademisyenler olmak üzere, bilişim uzmanlarıyla siber güvenlik otoritelerinden gelen görüş ve öneriler toplanmaktadır. Artık güvenlik denince akla sadece askeri çözümler ve önlemler gelmemekte, siber alana dair tedbirler de ön plana çıkmaktadır. Özellikle kamu güvenliğinde siber güvenliğin sağlanmasına yönelik tedbirler günümüz dünyasında daha fazla önem arz etmektedir.

Ayrıca günümüzde devletlerin güvenliği teknolojik gelişmelere doğrudan bağlıdır. Bu kapsamda, siber uzay alanındaki teknolojilere sahip olamayan devletler ciddi güvenlik zafiyetleri ile karşı karşıyadırlar. Aynı şekilde devletlerin güvenliklerini sağlama noktasında, klasik güvenlik anlayışına göre planlanmış tüm kurum ve stratejilerini etkili bir siber saldırı ve siber savunma kapasitesi yaratmak adına yeniden organize etmesi de gerekmektedir.

Günümüzde, siber güvenlik sorunsalı farklı kurumların sorumluluklarıyla kesişen çok boyutlu ve stratejik olarak ele alınması gereken bir konu haline gelmiştir. Siber uzayın ortaya çıkardığı yeni tehditlerle mücadele ve fırsatları değerlendirmek için devletin diğer aktörleri ile birlikte çalışma zorunluluk halini almış, bir yönetişim modelinin üretilmesini gerekli kılmıştır. Ulusal seviyede hazırlanacak bir siber güvenlik yönetişim modelinin küresel bir yaklaşıma sahip olması bir fırsat olarak görülmelidir. Bu ülkemizin üretmiş olduğu çözümler yoluyla küresel anlamda rolünü artıracak, uluslararası arenada farklı aktörler ile işbirliği platformları inşa edilmesini sağlayacaktır.

Siber güvenliğin tehdit ve fırsatlar anlamında milli güvenlik açısından taşıdığı kritik önem, bölgesel ve küresel uluslararası güç dengesinde oynayabileceği oyun değiştirici rolü, getirebileceği ekonomik fayda ve bunun gibi nedenlerden dolayı stratejik seviyede ele alınması gerekmektedir. Cumhurbaşkanlığına bağlı yeni bir birimin ihdas edilerek gerekli kadro desteğiyle siber güvenlik yönetişimi konusunda bir an önce harekete geçmesi, ülkemizin siber gücünü artırmada ve gerek dışarıdan gerekse içerden Türkiye'ye yönelik siber tehditlere karşı dayanıklılığın artırılması açısından önem arz etmektedir. Bu kapsamda yönetişimi sağlayacak ve gerek devlet kurumları arasında gerekse devlet-dışı aktörler ile koordinasyonu sağlayacak bir yapının **Siber Güvenlik Ofisi** düzeyinde meydana getirilecek bir kurumla yürütülmesi düşüncesi ön plana çıkmıştır.

Ülkemizin varlığını ve bekasını yakından ilgilendiren siber güvenlik meselesinin stratejik seviyede ele alınması Genelkurmay'dan Dışişleri Bakanlığına, İçişleri Bakanlığından Ticaret Bakanlığına, BTK'dan MİT'e kadar uzanan farklı kurumların iş birliği ve uzmanlığı ile ancak başarı sağlanabilecektir. Siber güvenlik yönetişiminde devlet kurumlarının eş güdümünün yanı sıra sivil toplum kuruluşları, üniversiteler ve özel sektörün iş birliğiyle oluşturacağı ekosistem Türkiye'nin teknoloji ihracatı, diplomatik etkinliği, istihbarat gücü, siber alandaki menfaatlerinin korunması gibi birçok önemli konuda ilerlemesinin yolunu açacaktır. Böylece hem olası bir saldırı durumunda hızlı aksiyon alınabilecek hem de tüm siber güvenlik birimlerinin yönetilmesi ve koordinasyonu kolaylaşacaktır. Birimlerin görev ve sorumluluklarının kesin çizgilerle ayrılması, kriz sırasındaki müdahalenin yönetilmesini kolaylaştıracaktır.

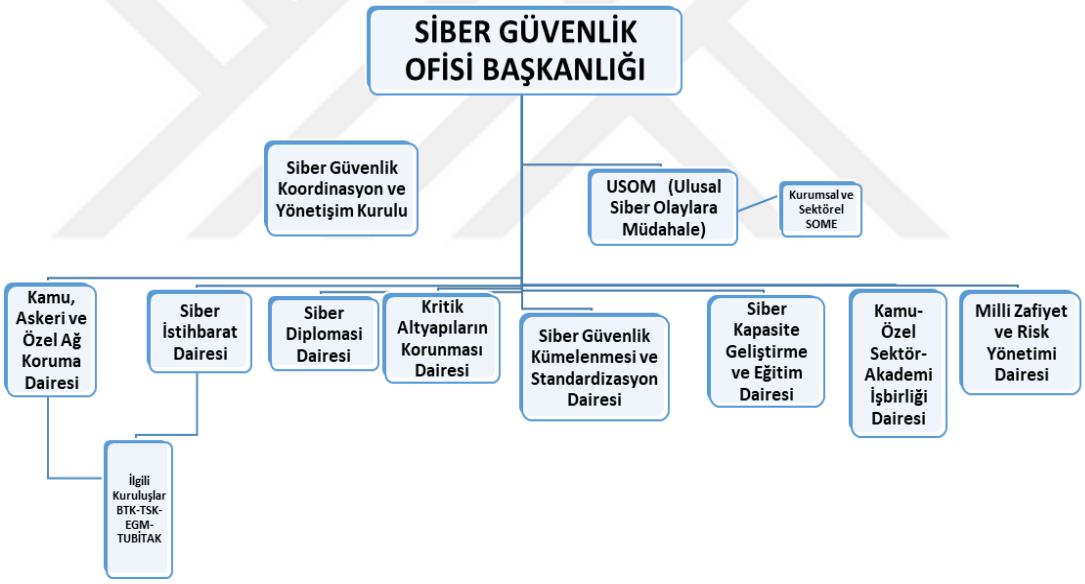
Daha önceki bölümlerde belirtildiği üzere Türkiye'nin siber güvelik sistematiğinin sürdürülmesindeki ana omurga BTK'dır. Diğer güvenlik ve istihbarat kurumları ile özel girişimler ise kendi faaliyet alanları kapsamında siber güvenlik meselesine odaklanmaktadırlar. Hâlbuki bir devletin siber savunma ve saldırı kapasitesi geliştirilmesine yönelik tüm çabaları o devletin ulusal ve uluslararası güvenliği ile ilgilidir. Bu bağlamda da bizce devletin siber güvenlik sistematiğinin işletilmesi multidisipliner bir yaklaşımla organizasyon yapısı belirlenmiş, müstakil bir güvenlik kurumu tarafından yönetilmelidir.

Türkiye'de siber güvenlik alanındaki çalışmalar, Ulaştırma ve Altyapı Bakanlığı çatısı altında yürütülmektedir. Siber güvenlik yönetişiminin bu şekilde uygulanması, birçok aksaklığa neden olabilmektedir. Ayrıca siber güvenlik alanında çalışma yürütecek kurumun hangisi olduğu ve karar alacak kurumun yetkileri kesin çizgilerle belirlenmediği için aksiyon anlamında karışıklık ortaya çıkmaktadır. Türkiye'nin 2016-2019 yılı için hedeflerinin belirlendiği Ulusal Siber Güvenlik Stratejisi Belgesinde "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması." şeklinde siber güvenlik alanında yönetimin tek bir merkezde toplanması konusuna değinilmektedir. Ancak bu konu detaylandırılmamıştır.

Netice olarak gelinen noktada Türkiye'nin devlet yönetiminde ülkenin siber güvenlik stratejisini geliştirme, siber savunma ve saldırı kapasitesine yatırım yapma konusunda bir farkındalık olduğu açıktır. Bu noktada yukarda belirtilen planlamalar ve kurumsal yapılanmalar dâhilinde bugüne kadar iyi niyetli adımlar atılmıştır. Ancak bu adımların daha da geliştirilmesi gerekmektedir. Siber uzay, uluslararası sistemde devlet için yeni bir mücadele alanıdır. Bu alanı devletler askeri kapasitelerini geliştirmek adına bir fırsat olarak okumaktadırlar. Hatta siber saldırıları dış politikada sorun yaşadıkları ülkelere karşı bir baskı yöntemi olarak kullanmaktan da çekinmemektedirler. Tüm bu rekabet ve siber çatışma süreçleri de uluslararası sistemi eskisinden daha belirsiz ve anarşik hale getirmektedir. Bu kapsamda Türkiye'de, ulusal ve uluslararası güvenliğini sağlamak adına siber güvenlik stratejisini en üst düzey planlama ve kurumsal yapılarla geliştirmek zorundadır.

Türkiye Siber Güvenlik Yönetişim Modeli(SGYM) kapsamında, siber güvenlik ve siber savunmanın başlı başına bir alan haline gelmiş olmasından dolayı, siber güvenlik alanındaki çalışmaların yönetiminden, direkt Cumhurbaşkanına bağlı yeni bir ofis konumlandırılarak **Siber Güvenlik Ofisi**'nin sorumlu olması gerektiği öngörülmekte olup önerilen yapı Şekil 24'de örnek yapılanma organizasyonu şeklinde gösterilmiştir.

Bu kapsamda bizler de güvenlik politikalarında karar alıcılara mümkün olduğunca fikir, öneri ve tavsiyelerde bulunmalıyız. Özellikle ülkemizin siber güvenlik stratejilerinin gözden geçirilerek, birçok devletin milli güvenlik belgelerinde ön sıralarda yer verdiği siber güvenlik alanında kapsam, hedefler, öncelikler, organizasyon yapısı, kaynak tahsisi, ar-ge (araştırma ve geliştirme) koordinasyonu, kamu-özel sektör iş birliği, eğitim gibi başlıklarda çözümler sunulması gerektiği düşünülmektedir.



Şekil 26. Siber Güvenlik Ofisi Örnek Yapılanma

KAYNAKÇA

ABD İç Güvenlik Bakanlığı (2016). "Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale". https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity. (Erişim Tarihi: 20.11.2019).

ABD Kara Kuvvetleri Siber Komutanlığı (2019). "About Us". https://www.arcyber.army.mil/Organization/About-Army-Cyber/ (Erişim Tarihi:25.12.2019).

ABD Milli İstihbarat Direktör Ofisi (2017). "Background to Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. https://www.dni.gov/files/documents/ICA_2017_01.pdf (Erişim Tarihi: 20.11.2019)

ABD Savunma Bakanlığı (2010). "U.S. Cyber Command Fact Sheet". https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-038.pdf (Erişim Tarihi:25.12.2019).

ABD Siber Komutanlığı (2011). "Assessing Actions Along the Spectrum of Cyberspace Operations". https://info.publicintelligence.net/USCC-CyberSpectrum.pdf (Erişim Tarihi: 18.11.2019).

ABD Savunma Bakanlığı (2019). "Combatant Commands". https://www.defense.gov/Our-Story/Combatant-Commands/ (Erişim Tarihi:25.12.2019).

ABD Siber Komutanlığı (2019a). "U.S. Cyber Command History". https://www.cybercom.mil/About/History/ (Erişim Tarihi:25.12.2019).

ABD Siber Komutanlığı (2019b). "Components". https://www.cybercom.mil/Components/ (Erişim Tarihi:25.12.2019).

ABD Ulusal Siber Güvenlik Stratejisi (2018). "National Cyber Strategy". https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Erişim Tarihi:22.12.2019).

Açıkmeşe, S.A. (2008). "Kopenhag Okulu Ve Realist Güvenlik Çalışmalarında Aktör, Tehdit ve Politika: Avrupa Güvenliği Üzerine Bir Değerlendirme". *Doktora Tezi*. Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Açıkmeşe, S.A. (2014). *Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler*. (Editör: Evren Balta) İstanbul: İletişim Yayınları.

Agnew, J. (2003). *Geopolitics: Re-visioning World Politics*. London: Routledge.

Aka, H. B. (2007). Küresel Güvenlik Bağlamında Sağlık. *Stratejik Öngörü*. Sayı:11, ss.122-126.

Akleylek, S.-Tok, Z.Y. (2011). "Siber Güvenlikte Kriptoloji". Ankara:Siber Güvenlik Çalıştayı.

Aksu, M.-Turhan, F. (2012) "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik". *Uluslararası Alanya İşletme Fakültesi Dergisi*. 4 (2), ss. 69-80.

Aktaş (Kaya), G. (2007). "Küreselleşme Sürecinde Türkiye'de Gelir Dağılımı, Yoksulluk ve Soysa Politikaların Evrimi". *Yüksek Lisans Tezi*. Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

Aktel, M.. (2001). "Küreselleşme Süreci ve Etki Alanları". *SDÜ İİBF Dergisi*. 6 (2). ss.193-202.

Aktel, M. (2003), Küreselleşme ve Türk Kamu Yönetimi, Asil Yayın Dağıtım,Ankara.

Aliusta,C.-Bezner, R. (2018). "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci". *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*. 4 (2), ss.35-42.

Andress, J.-Winterfeld, S. (2011). *Cyber Warfare*. ABD:Elsevier.

Arı, T. (2008). *Uluslararası İlişkiler Teorileri*, Ankara: MKM Yayıncılık.

Arman, M.N.(2011). Avrupa Komşuluk Politikasında Sorunlu Alanlar: İnsan Güvenliği ve Komşuluk İlişkisi". *Uluslararası İlişkiler*. 8 (31), ss. 45-68.

Armaoğlu, F. (2010). *20. Yüzyıl Siyasi Tarihi: 1914-1995*. İstanbul: Alkım Yayınevi.

Arnold (1952). "National Security as an Ambitiguous Symbol". *Political Science Wolfers Quarterly*. 67 (4). ss. 481-502.

Ataç, C. (2019). "Ulusal Siber Güvenlik Stratejisi Oluşturma Sürecine Bir Bakış". *Yüksek Lisans Tezi*. Samsun: On Dokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü.

Atalay, A.H. (2012). "Kurumsal Bilgi Güvenliği, Siber Güvenlik". *Mimar ve Mühendis Dergisi*. 68, ss.42-47.

Ataman, M. (2009). "Feminizm: Geleneksel Uluslararası İlişkiler Teorilerine Alternatif Yaklaşımlar Demeti". *Alternatif Politika*. 1 (1), ss. 1-41.

Avrupa Birliği Komisyonu (2013). Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Erişim Tarihi: 20.12.2019).

Avrupa Konseyi (2008). The Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Avrupa Konseyi Direktifi 08/114/EC.

Avrupa Konseyi (2019). Details of Treaty No.185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Erişim Tarihi:18.12.2019).

Aydın, A.-Bakıncak, E. (2016). "Uluslararası Güç Dengesi ve İki Kutupluluk Arasındaki İlişki". *C.Ü. İktisadi ve İdari Bilimler Dergisi*. 17 (1). ss.95-112.

Aydın, H. (2014). "Güvenlikleştirme Kavramı ve 11 Eylül Sonrası Türkiye'nin Ortadoğu'ya Yönelik Dış Politikası". Yüksek Lisans Tezi. İstanbul: Harp Akademileri Stratejik Araştırma Enstitüsü.

Aydın M.-Brauch H. G.-Polat N.-Spring, U. O.-Çelikpala, M. (2012). *Uluslararası İlişkilerde Çatışmadan Güvenliğe Seçme Makaleler*. İstanbul: Bilgi Üniversitesi Yayınları 398.

Baharçiçek, A. (2008). "Hükümet Dışı Örgütler (NGO's) ve Demokratikleşme". *Fırat Üniversitesi Sosyal Bilimler Dergisi.* 18 (2), ss. 297-308.

Balcı, A. (2016). "Yeni Dünya Düzeninde Jeopolitiğin Değişen Konumu". *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. Yıl:5. Sayı:10, ss.107-129.

Baldwin, D.A. (1995). "Security Studies and The End of The Cold War". *World Politics*. Cilt: 48. Sayı: 1, ss.119-125.

Baldwin, D.A. (2004). *Güvenlik Kavramı*. Çiğdem Şahin(Çev.). Uluslararası Güvenlik Sorunları, Kamer Kasım ve Zerrin A. Bakan (Ed.), Ankara: ASAM Yayınları.

Başaran, H. İ. (2010). "Reagan'ın Ortadoğu'da Çevreleme Politikası ve İslami Hareketlerin Bu Politikadaki Rolü". *Yüksek Lisans Tezi*. Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Başeren, S.H (2003*). Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmasının Sırlar*. Ankara: Ankara Üniversitesi Basımevi.

Başeren, S. (2006). *Kavramsal Özellikleri ile Terörizm. Küresel Terörizm ve Uluslararası İşbirliği Sempozyumu*. Ankara: Genelkurmay Basımevi.

Baysal, B.-Lüleci, Ç. (2015). "Kopenhag Okulu ve Güvenlikleştirme Teorisi". *Güvenlik Stratejileri*. 11 (22), ss.61-95.

BBC (2015). "President Obama Creates New Cyber Sanctions Programme". https://www.bbc.com/news/world-us-canada-32151406 (Erişim Tarihi: 20.12.2019)

BBC (2017). "Eski FBI Başkanı Comey: Trump Yönetimi Yalan Söyledi". http://www.bbc.com/turkce/haberlerdunya-40199389. (Erişim Tarihi: 18.11.2019).

Bedir, E.M. (2019). "Ulusal Güvenlik Politikalarında Barışçıl Güvenlik Stratejisi:Atatürk Dönemi Analizi". *Yüksek Lisans Tezi*. Çanakkale: 18 Mart Üniversitesi Sosyal Bilimler Enstitüsü.

Beidleman, S.W. (2009). *Defining And Deterring Cyber War*. ABD Kara Harp Akademisi. http://www.dtic.mil/dtic/tr/fulltext/u2/a500795.pdf (Erişim Tarihi: 18.11.2019)

Bıçakçı, S. (2012). "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu". *Uluslararası İlişkiler Dergisi.* 9 (34), ss.205-226.

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

Bigo, D. (2000). *When two become one: Internal and External Securitisations in Europe*. Kelstrup, Morten; Williams Michael C. International Relations Theory and the Politics of European Integration. London: Routledge.

Bigo, D. (2001). *The Möbius Ribbon of Internal and External Security(ies), Identities, Borders, Orders*. ed. / Mathias Albert; Yosef Lapid; David Jacobson. University of Minnesota Press.

Bigo, D. (2002). "Security and Immigration: Toward a Critique of the Governmentality of Unease". *Alternatives 27*. Special Issue. ss.63-92.

Bigo, D. (2006). "Internal and External Aspects of Security". *European Security*. Cilt 14, Sayı 4, ss. 385-404.

Bilgi Teknolojileri ve İletişim Kurulu (2011). Ulusal Bilgi Güvenliği Tatbikatı Sonuç Raporu http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fBTDNewFolder%2f4_1_1_USGT+2011+Rapor+T%C3%BCrk%C3%A7e.pdf (Erişim Tarihi: 15.10.2019).

Bilgi Teknolojileri ve İletişim Kurulu (2014). "Ulusal Siber Kalkan Tatbikatı". http://www.btk.gov.tr/tr-TR/Sayfalar/SG-Uluslararasi-Siber-Kalkan-Tatbikati-2014 (Erişim Tarihi: 28.10.2019).

Bilgi Teknolojileri ve İletişim Kurumu (2018). "Uluslararası Telekominikasyon Birliği-ITU". https://www.btk.gov.tr/itu (Erişim Tarihi:18.12.2019).

Bilgi Teknolojileri ve İletişim Kurulu (2019). "Siber Kalkanı 2019 Sona Erdi". https://www.btk.gov.tr/haberler/siber-kalkan-2019-sona-erdi (Erişim Tarihi: 25.12.2019).

Bilgi Toplumu İnternet Sitesi (2001). "e-Avrupa Eylem Planı-2003". http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/02/010600eAvrupa+Eylem Plani.pdf (Erişim Tarihi: 19.12.2019).

Bilgi Toplumu Stratejisi Eylem Planı (2006). https://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.htm (Erişim Tarihi: 25.12.2019).

Bilgin, N. (2008). *"Critical Theory", Security Studies An Introduction*. Ed: P.D. Williams. New York: Routledge.

Bilgin, P. (2005a). *11 Eylül Öncesi ve Sonrasında Küreselleşen Güvenliği Anlamak*. Cem Karadeli, der.. Küreselleşme ve Alternatif Küreselleşme. Ankara: Phoenix Yayınevi.

Bilgin, P. (2005b). "Turkey's Changing Security Discourses: The Challende of Globalisation". *European Journal of Political Research*. 44 (1), ss.175-201.

Bilgin, P. (2010). "Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları". *Stratejik Araştırmalar*. 8 (14). ss69-96.

Billo, C.-Chang, W. (2004). Cyber Warfare, An Analysis of the Means and Motivations of Selected Nation States. U.S. Department of Homeland Security.

Birdişli, F. (2014a). "Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü". *Güvenlik Stratejileri*. 10 (20), ss. 229-256.

Birdişli F. (2014b). *Teori ve Pratikte Uluslararası Güvenlik*. Ankara: Seçkin Yayınevi.

Birinci Bilgi Harekâtı Komutanlığı (2018). 1st Information Operations Command (Land). https://www.arcyber.army.mil/Organization/1st-IO-Command/ (Erişim Tarihi: 25.12.2019).

Birleşmiş Milletler Deniz Hukuku Sözleşmesi (1982). Deniz Haydutluğu Tanımı. Madde 101.

Birleşmiş Milletler (2019). History of the United Nations. https://www.un.org/en/sections/history/history-united-nations/ (Erişim Tarihi: 16.12.2019).

Birleşmiş Milletleri İnternet Adresi (2000). Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. https://www.ohchr.org/Documents/ProfessionalInterest/ProtocolonTrafficking.pdf (Erişim Tarihi: 16.12.2019).

Birleşmiş Milletler Silahsızlanma Enstitüsü (2013). The Cyber Index. UNIDIR/2013/3.

Birleşmiş Milletler Silahsızlanma Ofisi (2019). "Small Arms: Armed Violence". http://www.un.org/disarmament/convarms/salw/ (Erişim Tarihi: 20.12.2019).

Birleşmiş Milletler Uyuşturucu ve Suç Dairesi-UNODC (2009). "How to Tackle a Disturbing Consequence of Drug Control". https://www.unodc.org/unodc/en/frontpage/how-to-tackle-a-disturbing-consequence-of-drug-control-.html. (Erişim Tarihi: 20.12.2019).

Birleşmiş Milletler Uyuşturucu ve Suç Dairesi-UNODC (2010a). "Drug Trafficking". http://www.unodc.org/unodc/en/drug-trafficking/index.html (Erişim Tarihi: 20.12.2019).

Birleşmiş Milletler Uyuşturucu ve Suç Dairesi-UNODC (2010b). "Human Trafficing". http://www.unodc.org/unodc/en/drug-trafficking/index.html (Erişim Tarihi: 20.12.2019).

BM Cenevre Ofisi Nezdinde Daimi Temsilciliği (2019). "Uluslararası Telekomünikasyon Birliği". http://cenevreofisi.dt.mfa.gov.tr/Mission/ShowInfoNote/353802 (Erişim Tarihi: 20.12.2019)

BM Genel Kurulu 55/63 Sayılı Kararı (2001). https://undocs.org/en/A/RES/55/63 (Erişim Tarihi: 20.12.2019).

BM Genel Kurulu 56/121 Sayılı Kararı (2002). https://undocs.org/en/A/RES/56/121 (Erişim Tarihi: 20.12.2019).

BM Genel Kurulu 57/239 Sayılı Kararı (2003). https://undocs.org/en/A/RES/57/239 (Erişim Tarihi: 20.12.2019).

BM Genel Kurulu 58/199 Sayılı Kararı (2004). https://undocs.org/en/A/RES/58/199 (Erişim Tarihi: 20.12.2019).

Bolat, T.-Seymen, O. (2005). *Çokuluslu İşletmelerin Kavramsal Açıdan İncelenmesi.* Ankara: Nobel Yayın Dağıtım.

Booth, K. (2007). *Theory of World Security*. New York: Cambridge University Press.

Booth, K. (2012). *Dünya Güvenliği Kuramı*. Çev: Çağdaş Üngör. İstanbul: Küre Yayınları.

Bremmer, I. (2015). "These 5 Facts Explain the Threat of Cyber Warfare". http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/ (Erişim Tarihi: 18.11.2019).

Brill, B. J. (2010). *Law of War Documentary Supplement*. The Judge Advocate General's Legal Center and School. Charlottesville,VA.

Brinck J. K. (1995). "Sources of American Conduct: George Kennan and the Containment Policy". *Yüksek Lisans Tezi*. Washington: The American University Faculty of the School of International Service.

Broad, W. J.-Markoff, J.-Sanger, D.E. (2011). "Israeli Test On Worm Called Crucial In Iran Nuclear Delay". The New York Times. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (Erişim Tarihi: 18.11.2019).

Brunner E.M.-Suter, M. (2008). *Uluslararası Kritik Bilgi ve Altyapıların Korunması El Kitabı 2008-2009*. İsviçre: Güvenlik Çalışmaları Merkezi.

Brüksel Zirve Bildirgesi (2018). "Brussels Summit Declaration". https://www.nato.int/cps/en/natohq/official_texts_156624.htm (Erişişm Tarihi: 22.12.2019).

Brzezinski, Z. (2000). *Büyük Çöküş*. 5. bs. çev. Gül Keskil, Gülsev Paksan, İstanbul: Türkiye İş Bankası Kültür Yayınları.

Bull, H. (2002). *The Anarchical Society: A Study of Order in World Politics*. New York: Columbia University Press.

Burgess R. (2009). "The New Main Battery". Seapower Magazine.

Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era*. New York: Harvester Wheatsheaf.

Buzan, B.-Waver, O.-J.de Wilde (1997). *Security: A New Framework for Analysis Paperback*. London: Lynne Rienner Publishers.

Buzan, B.-Waever, O. (1998). *Liberalism and Security. The Contradictions of The Liberal Leviathan*. Copenhagen: Copenhagen Peace Research Institute Working Papers.

Buzan, B.-Waever, O.-Wilde, J. (1998). *Security: A New Framework for Analysis*. London: Lynne Reinner Publisher.

Bülbül H.B. (2018). "2016 Amerika Birleşik Devletleri Başkanlık Seçimine Rusya'nın Siber Müdahalesi İddialarının Uluslararası Hukuk Açısından Analizi". http://icil.org.tr/2016-amerika-birlesik-devletleri-baskanlik-seciminerusyanin-siber-mudahalesi-iddialarinin-uluslararasi-hukuk-acisindan-analizi/ (Erişim Tarihi: 19.11.2019)

Carnegie Mellon Üniversitesi (2017). "Denial of Service Attacks". CERT Bölümü. https://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_496601.pdf . (Erişim Tarihi: 27.11.2019).

Carr,E. (2001). *The Twenty Years Crisis, 1919-1939*. New York: Perennial.

Carpenter, T.G. (1992). "The New World Disorder". *Foreign Policy*. No: 85, ss.24-39.

Caşin, M. H. (2008). *Uluslararası Terörizm*. Ankara: Nobel Yayın Dağıtım.

Caşin, M.-Özgöker, U.-Çolak, H. (2007). *Küreselleşmenin Avrupa Birliği Ortak Güvenlik ve Savunma Politikasına Etkisi, Avrupa Birliği*. İstanbul: Nokta Kitapevi.

Chicago Zirve Bildirgesi (2012). "Chicago Summit Declaration". https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en%20/ (Erişim Tarihi: 20.12.2019).

Chip Teknoloji Haber Portalı (2009). "TÜBİTAK'tan Ciddi Zararlı Uyarısı". http://www.chip.com.tr/haber/tubitak-tan-ciddi-zararli-uyarisi_10703.html (Erişim Tarihi: 25.12.2019).

Clarke, R.A.-Knake R. K. (2011*). Siber Savaş*. Çev.Murat Enduran. İstanbul: İKÜ Yayınevi.

Cohen, R. (2012). "The White House and Pentagon Deem Cyber-Attacks An Act of War". http://www.forbes.com/sites/reuvencohen/2012/06/05/the-white-house-and-pentagon-deem-cyber-attacks-an-act-of-war/ (Erişim Tarihi: 18.11.2019).

Cohen, S.B. (2009). *Geopolitics: The Geography of International Relations*. London: Rowman&Littlefield.

Collins, A. (2005). *Securitization, Frankenstein's Monster and Malaysian Education*. The Pacific Review. 18 (4), ss. 567-588.

Corera, G. (2015). *Secret History of Chinese Spies*. Paris: Nouveau Monde Editions.

Coşkun, V. (2003). "Güvenliği Özgürlükte Aramak". *Dicle Üniversitesi Hukuk Fakültesi Dergisi*. 8 (8), ss.1-10.

Cox, R. W. (1981). "Social Forces, States and World Orders: Beyond International Relations Theory". *Millennium - Journal of International Studies*. 10(1), ss. 126-155.

Cox, R. W. (2008). *The Point Is not Just to Explain the World but to Change It. The Oxford Handbook Of International Relations*. Ed: S. Snidal. New York:Oxford University Press.

Cowie, J. (2010). "China's 18-Minute Mystery". http://research.dyn.com/2010/11/chinas-18-minute-mystery/ (Erişim Tarihi: 18.11.2019).

Craplet, M. (1997). "The Role of Non-Governmental Organizations". *Addiction*. 92 (3), ss. 103-108.

Çaha, Ö. (1994). "Sivil Toplumun Dünü ve Bugününde Kadın". *Türkiye Günlüğü*. Sayı 26, ss. 52-59.

Çakmak, H.-Altunok, T. (2009). *Suç Terör ve Savaş Üçgeninde Siber Dünya*. Ankara: Barış Platin Kitabevi.

Çalışır, G. (2009). "Küreselleşmenin Ortaya Çıkardığı Olayların Türkiye'deki Televizyon Haberlerine Yansımaları". *Doktora Tezi*. Eskişehir: Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Çaman, M.E. (2006). "Uluslararası İlişkilerde (Neo)Realist Paradigmanın Almanya'daki Gelişimi ve Evrimi. Kindermann ve Münih Okulu". *Uluslararası Hukuk ve Politika*, 2(8), ss.36–52.

Çelik, M. Y. (2012). "Boyutları Ve Farklı Algılarıyla Küreselleşme". *DPUJSS*. 2 (32), ss.57-74.

Çelikel, (Danışoğlu) A. (2004). "Küreselleşmenin Gelir Eşitsizliği ve Yoksulluk Üzerindeki Etkileri". *İstanbul Ticaret Üniversitesi Dergisi*. Sayı:5, ss.35-59.

Çeliktaş, B. (2016). "Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme". *Yüksek Lisans Tezi*. Trabzon: Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü.

Cha, V. D. (2000). "Globalization and the Study of International Security". *Journal of Peace Resarch*. 37 (3), ss. 391-403.

Çiftci, H. (2013). *Her Yönüyle Siber Savaş*. Ankara: TÜBİTAK Popüler Bilim Kitapları.

Çiftci, H. (2017). *Her Yönüyle Siber Savaş*. Ankara: TÜBİTAK Popüler Bilim Kitapları.

Çomak, H.-Sancaktar, C. (2011). *21'inci Yüzyılda Uluslararası Örgütlerin Güvenlik Yaklaşımları ve Balkanlar'ın Güvenliği*. İstanbul: BİLGESAM Yayınları.

Danchev, D. (2011). "China's Blue Army: When Nations Harness Hacktivists for Information Warfare". http://www.zdnet.com/article/chinas-blue-army-when-nations-harness-hacktivists-for-information-warfare/ (Erişim Tarihi: 25.12.2019).

Danışoğlu, A. (2007). "Küreselleşme, Gelir Eşitsizliği ve Yoksulluk Üzerindeki Etkileri". *İstanbul Ticaret Üniversitesi Dergisi*, ss.215-239.

Darıcılı, B. (2014). "Rusta Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi". *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi.* 7 (2), ss.1-16.

Darıcılı, B. (2017a). "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi". *Uluslararası Çalışmalar Dergisi Özel Sayısı*. 1 (1), ss.1-24.

Darıcılı, A. B. (2017b). *Siber Uzay ve Siber Güvenlik Nedir?*. Bursa: Dora Yayınları.

Davutoğlu, A. (2011). *Stratejik Derinlik: Türkiye'nin Uluslararası Konumu (Altmışikinci Baskı)*. İstanbul: Küre Yayınları.

Dedeoğlu, B. (2014). *Uluslararası Güvenlik ve Strateji*. İstanbul: Yenizyüzyıl Yayınları.

Demir, G. (2001). "Küreselleşme Üzerine". *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, No:56(1).

Denk, E. (2011). "Bir Kitle İmha Silahı Olarak Nükleer Silahların Yasaklanmasına Yönelik Çabalar". *Ankara Üniversitesi SBF Dergisi*. 66 (3), ss. 93-136.

Denning, D. (2000). Cyberterrorism. http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf (Erişim Tarihi: 25.12.2019)

Derian, J.D. (1990). "The Simulation Syndrome: From War Games to Game Wars". *Social Text* .24, ss.187-192.

Dicken, P. (2000). *Yeni Jeo-Ekonomi*. Çev., Ahmet Ağca. Ankara: Kadim Yayınları.

Dilan H. ve Kavuncu, S. (2015). 21.Yüzyıl Eşiğinde Yeni Çelişkiler/Yeni Krizler Ortamında Uluslararası Siyasal Sistemin Çok Kutupluluğa Doğru Evrilmesi. https://www.ayk.gov.tr/wp-content/uploads/2015/01/KAVUNCU-Sibel-D%c4%b0LAN-Hasan-21.-Y%c3%9cZYIL-E%c5%9e%c4%b0%c4%9e%c4%b0NDE-YEN%c4%b0-%c3%87EL%c4%b0%c5%9eK%c4%b0LER-YEN%c4%b0-KR%c4%b0ZLER-ORTAMINDA-ULUSLARARASI-S%c4%b0YASAL-S%c4%b0STEM%c4%b0N-%c3%87OK-KUTUPLULU%c4%9eA-DO%c4%9eRU-EVR%c4%b0LMES%c4%b0.pdf (Erişim Tarihi: 16.12.1019).

Doğan, N.(2005) ""NATO'nun Örgütsel Değişimi, 1949-1999: Kuzey Atlantik İttifakından Avrupa-Atlantik Güvenlik Örgütüne". *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*. 60 (3), ss. 69-108.

Doğru, M. (2016). "Siber Harekatın Uluslararası Hukuk Çerçevesinde Analiz". 18. Akademik Bilişim Konferansları. Aydın, ss.1-13.

Doğru, S. (2017). "Uluslararası Deniz Haydutluğu: Uluslararası Toplumun Mücadelesi ve Türkiye'nin Katkıları". *Ankara Üni. Hukuk Fak. Dergisi*. 66 (3), ss. 551-580.

Duran, N. (2018). "Küreselleşme Sürecine Türkiye Üzerinden Bakış". *Yüksek Lisans Tezi*. Kocaeli: Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü.

Dursun, D. (1998). "Küreselleşme/Yerelleşme Paradoksu ve Siyasî Değerlerin Yeniden İnşası, Siyasette ve Yönetimde Etik Sempozyumu". Sakarya Ü. İktisadî ve İdarî Bilimler Fakültesi. Adapazarı Ticaret ve Sanayi Odası, ss. 67-74.

Dünya Sağlık Örgütü (2004). Public Health Response to Biological and Chemical Weapons. https://www.who.int/csr/delibepidemics/biochemguide/en/ (Erişim Tarihi: 16.12.2019).

Efegil, E.-Musaoğlu, N. (2009). "Soğuk Savaş Sonrası Dönemin Uluslararası Sisteminin Yapısına İlişkin Görüşler Üzerine Bir Eleştiri". *Akademik Bakış*. 2 (4), ss.1-24.

Ekinci, İ. (2019). "Küreselleşme, Ülkelerarası Gelir Dağılımı ve Eşitsizliği ve Kof Küreselleşme Endeksi". *Yüksek Lisans Tezi*. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Elçin, A. B. (2012). "Küreselleşmenin Tarihçesi". http://www.meritymm.com/wpcontent/uploads/2013/05/kuresellesme.pdf (Erişim Tarihi: 20.11.2019).

Elman, C. (1996). "Horses for Courses: Why not Neorealist Theories of Foreign Policy". *Security Studies*. Cilt.6. ss.58-61.

Emeklier, B.-Ergül, N. (2010). "Uluslararası İlişkilerdeki Yeri: Jeopolitik Teoriler ve PetroPolitik". *Bilge Strateji*. 2 (3), ss.59-86.

Enein, S. A. (2017). Cybersecurity Challengesin the Middle East. Geneva Papers. ISBN: 978-2-88947-100-3.

ENISA (2011). Analysis of Cyber Security Aspects in the Maritime Sector. ss.1-25.

ENISA (2019a). "About ENISA". https://www.enisa.europa.eu/about-enisa (Erişim Tarihi: 20.12.2019).

ENISA (2019b). "Mission and Objectives". https://www.enisa.europa.eu/about-enisa/mission-and-objectives (Erişim Tarihi: 20.12.2019).

Enloe, C. (1989). *Bananas, Beaches and Bombs: Making Feminist Sense of Internaional Politics*. Berkeley CA: University of California Press.

Erbay, Y. (1997). *Kavram Olarak Küreselleşme, Milli Kültürler ve Küreselleşme*. Ankara: Türk Yurdu Yayınları.

Ercan, M. (2015). "Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri". *Yüksek Lisans Tezi*. İstanbul: Gebze Üniversitesi.

Erçağlar, E. (2017). "Siber Güvenlik Operasyon Merkezi Gereksinimleri". Uzmanlık Tezi. Ankara: Çevre ve Şehircilik Bakanlığı.

Erdoğdu, H. (2004). *Avrupa'nın Geleceğinde Türkiye'nin Önemi ve NATO İttifakı*. İstanbul: IQ Kültür ve Sanat Yayıncılık.

Erdoğan, İ. (2013). "Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı". *Akademik Bakış*. 6 (12), ss.265-292.

Erdoğan, T. (2004). "Küreselleşmenin Ekonomik, Politik ve Kültürel Yansımaları". *Türkiye Sosyal Araştırmalar Dergisi*. 8 (2).

Erdoğan, İ.-Korkmaz, A. (2002). *Öteki Kuram*. Ankara: Erk Yayınevi.

Eren, M. (2017). *Avrupa Birliği'nin Siber Güvenlik Politikası*. İstanbul: Beta Yayınevi.

Eren, E. (2019). Almanya'nın Avrupa Birliği Politikalarının Çevresel Güvenlik Kapsamında İncelenmesi". *Yüksek Lisans Tezi*. Yalova: Yalova Üniversitesi Sosyal Bilimler Enstitüsü.

Eriksson, J.-Giacomello, G. (2006). "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?". *International Political Science Review* 27 (3), ss.221-244.

Ertem, H.S. (2012). "Kimlik ve Güvenlik İlişkisine Konstrüktivist Bir Yaklaşım: Kimliğin Güvenliği ve Güvenliğin Kimliği". *Güvenlik Stratejileri Dergisi*. 8 (16), ss.177-236.

Eser, U. (1995). "Küreselleşme Tehdit Mi Yoksa Fırsat Mı?". *Ekonomik Yaklaşım*. 6 (17) ss.5-20.

Fernando, J.-Heston, A.W. (1997). "NGO's Between States, Market and Civil Society". *Annals of American Political and Social Sciences*, cilt 554, ss. 8-20.

Fındık, İ. (2012). "Kitle İmha Silahları Terörizmi ve Caydırıcılık Stratejisinin Kitle İmha Silahları Terörizmine Uygulanabilirliliği". *Yüksek Lisans Tezi*. Ankara: Kara Harp Okulu Savunma Bilimleri Enstitüsü.

Firoozabi, J.D.-Ashkezari, M.Z. (2016). "Neo-classical Realism in International Relation". *Asian Social Science*. 12 (6). ss.95-99.

Frederik, J.-Arends, M. (2009). "Homerostan Hobbes ve Ötesine: Güvenlik Kavramının Avrupa Geleneğindeki Boyutları". *Uluslararası İlişkiler*, 6 (22), ss.2-33.

Gaddis, J. L. (2005). *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War*. New York: Oxford University Press.

Galler Zirve Bildirgesi (2014). "Wales Summit Declaration". https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Erişim Tarihi: 20.12.2019)

Gedik, D. (2018). "Siber Güvenlik ve Terörizmin Evrilişi: Türkiye Üzerine Etkileri". *Yüksek Lisans Tezi*. Düzce: Düzce Üniversitesi Sosyal Bilimler Enstitüsü.

Geers, K. (2010). "The Challenge of Cyber Attack Deterrence". *Computer Law ve Security Review*. (26), ss. 298-303.

Geiß, R. (2006). "Asymmetric Conflict Structures". International Review of the Red Cross. Vol.88, http://www.icrc.org/eng/assets/files/other/irrc_864_geiss.pdf (Erişim Tarihi: 18.11.2019).

Gençtürk, T. (2012). "*Terör Kavramı ve Uluslararası Terörizme Farklı Yaklaşımlar*". *Başkent* Üniversitesi Stratejik Araştırmalar Merkezi. http://sam.baskent.edu.tr/makaleler/tgencturk/TerorUluslararasi.pdf (Erişim Tarihi:15.12.2019).

Genelkurmay Başkanlığı (2007). "Güvenliğin Yeni Boyutlar ve Uluslararası Örgütler Konulu Uluslararası Sempozyum Açış Konuşması". .http://www.tsk.mil.tr/10_ARSIV/10_1_Basin_Yayin_Faaliyetleri/10_1_7_Konusmalar/2007/konusma_sempozyum31052007.htm (Erişim Tarihi: 13.12.2019).

Gervais, M. (2012). "Cyber Attacks and the Laws of War", *Berkeley Journal of International Law*. 30 (2), ss.525-579.

Göçoğlu, V. (2017). "Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi". *Doktora Tezi*. Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.

Göknel, M. (2008). "Nükleer Enerji, Nükleer Teknoloji ve Güvenlik Cephesi". *Stratejik Analiz Dergisi*. 9 (104).

Gönen, M. A. (2013). "Küreselleşmenin Ekonomik Boyutu Küreselleşmeyi Yöneten Üç Ana Kurum: IMF, Dünya Bankası, Dünya Ticaret Örgütü". *SDÜ Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi*. Sayı: 29, ss.117-134.

Gökpınar, S. (2009). Şebekeler (Ağyapılar) ve Savaş. Sayısal Ortamda Savaş Sempozyumu. Ankara.

Griffiths, M.-O'Callaghan, T.-Roach, S. C. (2013) *Uluslararası İlişkilerde Temel Kavramlar*. Çev. CESRAN, 2.Baskı, Ankara: Nobel Yayınları.

Güleş, E. (2014). "Küreselleşmenin Ulusal Kimlik Üzerine Etkileri". *Yüksek Lisans Tezi*. Ankara:Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.

Gülmez, N.-Tahancı, Bülent (2014). "Soğuk Sava Çekişmelerinden Bir Örnek: U-2 Uçak Krizi". *Çağdaş Türkiye Tarihi Araştırmaları Dergisi*. 14 (28), ss.226-228.

Güneş, E. (2012). "Günümüz Uluslararası Siyasal Sistemin Yapısı ve Güç Dağılımı". *Akdeniz İİBF Dergisi.* 23. ss.78-101.

Güngör, N. (2011). *İletişim Kuramlar ve Yaklaşım*. Ankara: Siyasal Kitabevi.

Güngör, M. (2015). "Ulusal Bilgi Güvenliği:Strateji ve Kurumsal Yapılanma". *Uzmanlık Tezi*. Ankara: Kalkınma Bakanlığı.

Gürcan, M. (2012). *Bir Önceki Savaşa Hazırlanmak: Değişen Küresel Güvenlik Ortamının Geleneksel Savaş Olgusuna Etkisi*. İstanbul: BİLGESAM Yayınları. http://www.bilgesam.org/incele/646/-bir-onceki-savasa-hazirlanmak--degisen-kuresel-guvenlik-ortaminin-geleneksel-savas-olgusuna-etkisi/#.XdPPvdVS_IU (Erişim Tarihi: 18.11.2019)

Güreşçi, R. (2019). "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi". *Savunma Bilimleri Dergisi.* 18 (1). ss.2148-1176.

Gürkaynak, M.-İren, A.A. (2011). "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler". *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*. 6 (2), ss. 263-279.

Gürlesel, C.F.-Demir, M. F. (2002). *Dünyada Çok Taraflı Denge ve Türkiye İçin Yakın Gelecek*. İstanbul: İstanbul Ticaret Odası.

Gürpınar, B. (2016). *Türkiye'de Milli Güvenlik Söylemi ve Dış Politika*. İstanbul: Beta Yayınları.

Haberler İnternet Sitesi (2017). "Ulusal Siber Savunma 2017 Tatbikatı". https://www.haberler.com/ulusal-siber-savunma-2017-tatbikati-10292620-haberi/ (Erişim Tarihi: 25.12.2019).

Habertürk Haber Portalı (2009). Atatürk Havalimanı'nda Virüs Kabusu". https://www.haberturk.com/yasam/haber/125013-ataturk-havalimaninda-virus-kabusu (Erişim Tarihi: 25.12.2019).

Hablemitoğlu, Ş. (2004). *Küreselleşme Düşlerden Gerçekleri*. Ankara: Toplumsal Dönüşüm Yayınları.

Hakimiyet EHaber Sitesi (2014). "Ulusal Siber Kalkan Tatbikatı". http://www.hakimiyet.com/ekonomi/uluslararasi-siber-kalkan-tatbikati-2014-h463544.html (Erişim Tarihi: 08.11.2019).

Halatçı, Ü. (2006). "11 Eylül Terörist Saldırıları ve Afganistan Organizasyonu'nun Bir Değerlendirmesi". *Uluslararası Hukuk ve Politika Dergisi*. 2 (7), ss.80-98.

Haley, C. (2013). "A Theory of Cyber Deterrence. Georgetown Journal of International Affairs". https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley (Erişim Tarihi:20.11.2019)

Harlow G. D.-Maerz G. C. (1991). *Measures Short Of War: The George F. Kennan Lectures At the National War College, 1946-47*. Washington: National Defense University Press.

Haser, Demet (2018). "Uluslararası İlişkilerde Güvenlik Kavramı: Soğuk Savaş Sonrası Dönem Güvenlik". *Yüksek Lisans Tezi.* İstanbul: İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü.

Hatipoğlu, E. (2019). "Enerji Güvenliği". *Güvenlik Yazıları Serisi*. No:44, ss.1-13. https://trguvenlikportali.com/wp-content/uploads/2019/12/Enerji Guvenligi_Emre Hatipoglu_v.1.pdf (Erişi Tarihi: 18.12.2019).

Hawks B. B. (2002). "Agenda-Setting Research". *İstanbul Üniversitesi İletişim Dergisi*, sayı: 13, ss.491-499.

Hayaloğlu, P.-Kalaycı, C.-Artan, Seyfettin. (2015). "Küreselleşme Farklı Gelir Grubundaki Ülkelerde Ekonomik Büyümeyi Nasıl Etkilemektedir?". *Eskişehir Osmangazi Üniversitesi İİBF Dergisi*. 10 (1), ss.119-152.

Hekim, H. (2015). *Oltalama (Phishing) Saldırıları*. Fatih Tombul ve diğerleri (Ed.). Ankara: Global Politika ve Strateji.

Herz, J.(1950). '*Idealist Internationalism and the Security Dilemma'*, World Politics, 2:2. Cambridge University Press, pp. 157-180.

History İnternet Adresi (2019). "President Truman Announces The Truman Doctrine". https://www.history.com/this-day-in-history/truman-doctrine-is-announced. (Erişim Tarihi: 17.12.2019).

Hitchens, T.-Goren, N. (2017). "International Cybersecurity Information Sharing Agreements". https://cissm.umd.edu/sites/default/files/2019-07/Cyber%20information%20sharing%2 0agreement%20report%20-%20102017%20-%20FINAL.pdf (Erişim Tarihi: 25.12.2019).

Hobbes, T. (2008). *Leviathan*. Forgotten Books. London: Ludgate Hill.

Hugh, M. (2000). *The Globalization of Culture?, A Globalizing World? Culture, Economics, Politics.* (Ed. David Held). Kanada:The Open University.

Huysmans, J. (2006). *The Politics of Insecurity Fear, Migration and Asylum in The EU*. Londra: Routledge.

Hwang, J. (2012). "China's Cyber Warfare: The Strategic Value of Cyberspace and the Legacy of People's War". School of Geography, Politics and Sociology University of Newcastle. https://pdfs.semanticscholar.org/3b69/1d2295dfc7161b27d395cda422c6e0730f08.pdf (Erişim Tarihi: 25.12.20019).

Ikenberry, G.J. (2001). *Institutions, Strategic Restraint and The Rebuilding of Order After Major Wars*. New Jersey: Princeton University Press.

Industrial Ethernet Book (2017). "The Stuxnet Worm and Options for Remediation". https://iebmedia.com/index.php?id=7409&parentid=63&themeid=255&hft=61&showdetail=true&bb=1 (Erişim Tarihi: 18.11.2019).

Ingulstad, M. (2014). "The Interdependent Hegemon: the United States and the Quest for Strategic Raw Materials during the Early Cold War". *The International History Review*. ss.1-21.

Işık, M. (2014). *Kitle İletişim Teorilerine Giriş*. Konya: Eğitim Yayınevi.

İduğ, Y.-Çalışkan, F.-Güler, T. (2013). *Caydırıcılık ve Türkiye'nin Siber İmkân ve Kabiliyeti*. 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. Ankara: Bildiriler Kitabı.

İnternet Canlı İstatistikler Portalı (2019). https://www.internetlivestats.com/one-second/#tweets-band (Erişim Tarihi: 21.11.2019).

İskender, S. (2015). "Neorealizm, Neoliberalizm, Konstraktivism ve İngiliz Okulu Modellerinde Uluslararası Sistemsel Değişiklere Bakış". *The Journal of Europe - Middle East Social Science Studies.* (1) 1, ss.14-38.

İşyar, Ö.G. (2008). "Günümüzde Uluslararası Güvenlik Stratejileri: Kavramsal Çerçeve ve Uygulama". *Gazi Akademik Bakış*. 2 (3), ss.1-42.

Jelavich, B. (2009). *Balkan Tarihi: 20.Yüzyıl.* 2.Baskı. Çev.: Zehra Savan ve Hatice Uğur. İstanbul: Küre Yayınları.

Jelinek, P. (2010) "A Code You Can Hack: On CYBERCOM's Logo. Marine Corps Times". https://web.archive.org/web/20100715055816/http://www.marinecorpstimes.com/news/2010/07/ap_military_cyber_command_logo_070810/ (Erişim Tarihi: 25.12.2019)

Jenkins, B.M. (1974). *International Terrorism: A New Kind of Warfare*. Santa Monica: The Rand Corporation.

Jepperson, R.L.-Wendt, A.-Katzenstein, P. J. (1996). *Norms, Identity and Culture in National Security*. New York: Columbia University Press.

Johansen, R.C. (1994). *Building World Security: The Need for Strengthened International Institutions*. New York: Martin's Press.

Jones, W.S. (1991). *The Logic of International Relations*. Seventh Edition. New York: Harper Collins.

Jones, R. W.(1999). *Security, Strategy and Critical Theory*. London:Rienner Publishers.

Kalkan K. Ö. (2012). "Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Okulu Çerçevesinde Tartışılması". *Turan Stratejik Araştırmalar Merkezi Dergisi*, (4)14, s.202-208.

Kara Kuvvetleri Ağ Kurumsal Teknoloji Komutanlığı (2018). "Network Enterprise Technology Command". https://www.arcyber.army.mil/Organization/NETCOM/ (Erişim Tarihi: 25.12.2019).

Kara Kuvvetleri İstihbarat ve Güvenlik Komutanlığı (2018). "780th Military Intelligence Command". https://www.arcyber.army.mil/Organization/780th-MI-Brigade-Cyber/ (Erişim Tarihi: 25.12.2019).

Kara, M. (2013). "Siber Saldırılar-Siber Savaşlar ve Etkileri". *Yüksek Lisans Tezi.* İstanbul: Bilgi Üniversitesi Sosyal bilimler Enstitüsü.

Karabacak, B. (2009). "Kritik Altyapılar ve Sayısal Savaş: Sayısal Teröristlerin Merhametine mi Kaldık?". *MSI Dergisi*. Sayı 49, ss.50-54.

Karabacak, B. (2010). "Ulusal Sanal Ortam Güvenlik Politikası". *4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*. https://islidedoc.org/embed/ulusal-sanal-ortam-guevenlik-politikasi (Erişim Tarihi: 25.12.2019).

Karabacak, B. (2011). "Kritik Altyapılar: Dünya ve Türkiye Özeti*". BİLGEM*. 3 (5), ss. 18-33.

Karabulut, B. (2009). "Küreselleşme Sürecinde Güvenlik Alanında Değişimler: Karadeniz'in Güvenliğini Yeniden Düşünmek". *Karadeniz Araştırmaları*. Cilt: 6. Sayı: 23, ss.1-11.

Karabulut, B. (2015). *Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek*. Ankara: Barış Kitabevi.

Karaca, G. (2007). Küreselleşm ve Büyük Ortadoğu Projesi. *Yüksek Lisans Tezi*. Malatya: İnönü Üniversitesi Sosyal Bilimler Enstitüsü.

Kartal, B. (2018). "Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği". *Güvenlik Stratejileri*. 27, ss. 39-77.

Kartal, Z. (2007). "Kavramsal ve Tarihsel Yönleri İle Küreselleşme". *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, 8 (2). ss.251-264.

Kartepe, S.-Ozan, M.S.-Banazılı, A.M. (2018). "Ulusal Güvenlikte Küresel Bir Tehdit: Biyoterörizm". *ASSAM Uluslararası Hakemli Dergi 13.Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı*. ss.1-13.

Katırcıoğlu E. (2008). *Küreselleşme Çağında Sol Ekonomik Politikalar Yeni Toplum Yeni Siyaset Küreselleşme Çağında Sosyal Demokrat Yaklaşımlar.* İstanbul: Kalkedon Yayınları.

Katzenstein, P., J. (1996). *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press.

Kaya, S. (2008). "Uluslararası İlişkilerde Konstrüktivist Yaklaşımlar". *Ankara Üniversitesi SBF Dergisi.* 63(3).

Keleştemur, A. (2015). *Siber İstihbarat (1. Baskı)*. İstanbul: Yazın Basın Yayınevi.

Kemaloğlu, N. (2010). "Teknolojik Sıçrama; Siber Savaş". http://www.haber7.com/yazarlar/nihal-kemaloglu/427019-teknolojik-sicrama-siber-savas (Erişim Tarihi: 19.12.2019).

Kennan, G.F. (2003). *The Sources of Soviet Conduct*. G.O. Tuathail, S. Dalby, P. Routledge (Eds.). New York: Routledge.

Keskin, F. (2012). *Demokrasinin Yeniden Yapılandırılması Tartışmaları Bağlamında 2011 Milletvekilleri Genel Seçimleri ve Medya*. Ankara: Ankara Üniversitesi Bilimsel Araştırma Altyapı Projesi Kesin Raporu.

Keskin, Ş. (2017). "Realizm ve Liberalizm Işığında Siber Savaş ve Alternatif Bir Kavram Olarak Siber Barış'ın Değerlendirilmesi". *TURAN-SAM*, Sayı 35, ss.287-297.

Keyman, F. (2000). *Küreselleşme, Devlet, Kimlik/Farklılık: Uluslararası İlişkiler Kuramını Yeniden Düşünmek*. İstanbul: Alfa Yayınları.

Keyuan, Z. (2009). "New Developments in the International Law of Piracy". *Chinese Journal of International Law.* 8 (2), ss. 323–345.

Kısacık, K. (2019). "1980 Sonrası Dünya Ekonomisinde Küreselleşme Eğilimleri ve Yoksullaşma". *Yüksek Lisans Tezi*. Bilecik: Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü.

Kıvılcım, F. (2013). "Küreselleşme Olgusu ve Çokuluslu Şirketlerin Küreselleşme Süreci Üzerindeki Rolü". *Ekonomi Bilimler Dergisi.* 5 (2), ss.1-16.

King, R.-Kendall, G. (2004). *State, Democracy and Globalization*. USA, Palgrave Macmillan, Gordonsville VA.

Knutsen, T.L. (2006). *Uluslararası İlişkiler Teorisi Tarihi*. çev. Mehmet Özay. İstanbul: Açılım Kitap.

Kocatepe, A. (2006). *Silahlı Çatışma Hukuku Açısından Cenevre Sözleşmeleri ve Ek Protokolleri El Kitabı.* İstanbul: Harp Akademileri Basımevi.

Koçak, O. (2004). "Elektronik Ticaret ve Çalışma Hayatına Etkisi". *Doktora Tezi*. İstanbul:İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Koçer, G. (2004). "Küreselleşme ve Uluslararası İlişkiler'in Geleceği". *Uluslararası İlişkiler*. 1 (3), ss.101-122.

Kongar, E. (2006). *Tarihimizle Yüzleşmek*. İstanbul: Remzi Kitabevi.

Kolasi, K. (2014) "Eleştirel Teori ve Güvenlik: Kimin İçin Güvenlik?". *Uluslararası İlişkiler Kütüphanesi, ss.*121-154.

Koray, M. (2015). Küreselleşme Süreci ve Ulus-Devlet, Ekonomi, Siyaset Tartışmaları. *Küreselleşme ve Ulus Devlet Bildiriler Kitabı*. İstanbul: Yıldız Teknik Üniversitesi Stratejik Araştırmalar Merkezi.

Korhan, S. (2018). "Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri". *Yüksek Lisans Tezi*. Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Korzak, E. (2017). "UN GGE on Cybersecurity: The End of an Era?". Erişim Tarihi: 03.06.2018. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-justmade-cyberspace-less-safe/ (Erişim Tarihi: 14.12.2019).

Koyuncu, Ç.A. (2012). "Feminist Uluslararası İlişkiler Yaklaşımları Açısından Güvenlik Konusunun Analizi". *Ankara Üniversitesi SBF Dergisi*. 67 (1), ss. 111-139.

Krahmann, E. (2005). *New Threats and New Actors in International Security*. New York: Palgrave Macmillan.

Krasavin, S. (2019). "What is Cyber Terrorism?". http://www.crime-research.org/library/Cyber- terrorism.htm (Erişim Tarihi: 20.11.2019).

Krause, K.-Williams M.C. (1996). "Broadening the Agenda of Security Studies: Politics and Methods". *Mershon International Studies Review*, 40 (2). ss.229-254.

Kuloğlu, A.(2003). "Soğuk Savaş Sonrası Bozulan Dengeler, Irak Krizi ve Bölgesel İstikrar Arayışı, Stratejik Analiz; Azerbaycan'da Devlet Başkanlığı Seçimi". *ASAM*, 4 (44).

Kurtoğlu, R. (2017). *Küresel Para Oyunları ve Psiko-Siber Savaş*. İstanbul: Destek Yayınları

Küçükşahin, A.-Akkan, T. (2007). "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit". *Dergi Pak Akademi*. Sayı:5.

Küresel Risk Raporu (2018). "Dünya Ekonomi Forumu". http://www3.weforum.org/docs/WEF_GRR18_Report.pdf (Erişim Tarihi: 19.12.2019).

Küntay, B.-Elmas, B. (2019) "İdeolojik Çatışmalar ve Ekonomi Savaşları: Yeniz Düzen Arayışı". *Sosyal Araştırmalar ve Davranış Bilimleri Dergisi.* 5 (8), ss. 193-224.

Larkin, E. (2009). "Protecting Against the Rampant Conficker Worm. PC World". https://www.pcworld.com/article/157876/conficker.html (Erişim Tarihi: 20.11.2019)

Lewis, J. A. (2015). "The Role of Cyber Operations in NATO's Collective Defense". *The Talinn Papers No. 8.* NATO Cooperative Cyber Defence Center of Excellence. Litvanya. ss.1-15.

Libicki, M. C. (2009*). Cyberdeterrence and Cyberwar*. Santa Monica. CA:RAND Cooperation.

Lieber, K. A. (2000). "Grasping the Technological Peace: The Offense-Defense Balance and International Security". *International Security*. 25(1), ss. 71-104.

Lilleker, D. G. (2013). *Siyasal İletişim Temel Kavramlar. (ed. Y. Devran, A. Nas, B. Ekşi ve Y. Göksun)*. İstanbul: Kaknüs Yayınları.

Lobell, S. E., Ripsman, Norrin. M. ve Jeffrey W (2009). *Taliaferro, Neoclassical Realism and Foreign Policy*. New York: Cambridge University Press.

Lynn, W.J. (2010.). "Defending a New Domain-The Pentagon's Cyberstrategy". *Foreign* Affairs. 89 (5), ss.97-108.

Macar, O. D.- Aysal, U.Y. "Covıd-19 İle Uluslararası İlişkileri Yeniden Düşünmek: Tarih, Ekonomi Ve Siyaset Ekseninde Bir Değerlendirme". Covid-19 Sosyal Bilimler Özel Sayısı. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi* 19 (37) ss.222-239

Mazanec, B.M. (2015). *Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. Potomac Books.

McAfee Tehdit Raporu (2018). https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterlythreats-jun-2018.pdf (Erişim Tarihi: 20.12.2019).

McConnell, M. (2010). "How to Win the Cyberwar We're Losing". The Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (Erişim Tarihi: 18.11.2019)

Mcdonald, M. (2008a). *"Constructivisim", Security Studies An Introduction*. New York: Routledge.

McDonald, M. (2008b). "Securitization and the Construction of Security". *European Journal of International Relations*. 14 (4), ss. 563-587.

Mearsheimer, J. (2001). *The Tragedy of Great Power Politics*. London: W. W. Nonon & Company.

Medvedev, S. A. (2015). "Offense-Defense Theory Analysis of Russian Cyber Capability". *Masters' Thesis*, California: Naval Postgraduate School.

Memiş, H. (2014). "Küreselleşme ve Yoksulluk İlişkisi". *Akademik Yaklaşımlar Dergisi*. 5 (1), ss. 144-161.

Mesjasz, C. (2004). "Security as an Analytical Concept*". 5th Pan-European Conference on International Relations in The Hague*. Polonya: Krakow Ekonomi Üniversitesi.

Mesjasz, C. (2012). *Ekonomik Güvenlik. Uluslararası ilişkilerde Çatışmadan Güvenliğe.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Metin, İ. (2016). "Dijital Pazarlama Araçlarının KOBİ'lerin İhracatına Etkisi". Journal of Human Sciences.13 (3), ss 4697-4709.

Meyer, P. (2015). "Is cyber peace possible?". https://www.opencanada.org/features/cyber-peace-possible/ (Erişim Tarihi: 14.12.2019).

Microsoft Web Sitesi, http://www.microsoft.com/technet/security/Bulletin/MS10-046.mspx (Erişim Tarihi:12.10. 2015).

Miller Center of Public Affairs (2015). "Harry S. Truman: Life in Brief". University of Virginia. https://millercenter.org/president/truman/life-in-brief (Erişim Tarihi: 17.12.2019).

Milliyet Gazetesi (2014). "Ölümcül Ebola Virüsü Hakkında Bilmeniz Gereken 10 Şey". http://www.milliyet.com.tr/olumcul-ebola-virusu-hakkinda/dunya/detay/1948145/default.htm (Erişim Tarihi: 19.12.2019)

Milliyet Haber Sitesi (2007). "İlk Siber Savaş" http://www.milliyet.com.tr/2007/05/18/dunya/adun.html (Erişim Tarihi: 19.11.2019).

Miş, N. (2011). "Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi". *Akademik İncelemeler Dergisi.* 6 (2), ss.345-381.

Molla, A. (2008). "NATO Savunma Politikaları Çerçevesinde Türk-Amerikan İlişkilerinin Analizi". *Doktora Tezi*. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Moore, D. (2003). "Inside The Slammer Worm". *IEEE Security & Privacy.* 1 (4), ss.33-39

Mulvenon, J. (2009). "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability". http://indianstrategicknowledgeonline.com/web/Ch_8-1.pdf (Erişim Tarihi: 24.12.2019).

Müller, H. (2005). *Security Cooperation. Handbook of International Relations.* London: SAGE Publications.

NATO (2010). "Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation". https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (Erişim Tarihi: 20.12.2019).

NATO (2014). NATO "Industry Cyber Partnership (NICP)". https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx (Erişim Tarihi: 20.12.2019).

NATO (2016). "NATO Cyber Defence Fact Sheet". https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (Erişim Tarihi: 20.12.2019).

NATO El Kitabı (2006). https://www.nato.int/docu/handbook/2006/hb-en-2006.pdf. (Erişim Tarihi: 19.12.2019).

NATO (2008). "Bucharest Summit Declaration". http://www.nato.int/cps/en/natolive/official_texts_8443 (Erişim Tarihi: 13.12.2019).

NATO (2012). "Teröre Karşı Savunma Konsepti. MC 472". https://www.nato.int/cps/en/natohq/official_texts_87905.htm?selectedLocale=en (Erişim Tarihi: 17.12.2019).

NATO (2019). Kısaltmalar ve Tanımlar Sözlüğü-AAP6.

NATO Siber Savunma Mükemmeliyet Merkezi (2019). "About Us". https://ccdcoe.org/about-us/ (Erişim Tarihi: 23.12.2019).

NATO Stratejik Konsept (2010). http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (Erişim Tarihi: 19.12.2019).

Neuneck, G.-Siroli, P. (2013). "Disarmament, Conflict Resolution and New Weapons Technology". 60th Pugwash Conference on Science and World Affairs Working Group 6 Report, İstanbul.

Newman, C. (2001). *Realizm: Küreselleşme ve Bağımsız Devlet.* (Çev. Muammer Türker). *Türkiye Günlüğü*.

New York Times (2016). "Hackers to the U.S. Election". https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html (Erişim Tarihi: 19.11.2019.

Ohr, B.G. (2008). "Effective Methods to Combat Transnational Organized Crime in Criminal Justice Processes". *116th Intenational Traning Course Visiting Experts Papers*. Resource Material Series No:58. ss.40-60. https://www.unafei.or.jp/publications/pdf/RS_No58/No58_08VE_Ohr.pdf (Erişim Tarihi: 20.12.2019).

Olgun, H. (2006). "Küreselleşme Kavramı ve İçeriğine Genel Bir Bakış". *Sosyo-ekonomi Dergisi*. 3 (3), ss.143-152.

Ovalı, A. Ş. (2006). "Ütopya ile Pratik Arasında: Uluslararası İlişkilerde İnsan Güvenliği Kavramsallaştırılması". *Uluslararası İlişkiler*. 3 (10). ss.3-50.

Özbek, Y. (2019). "Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi". *Yüksek Lisans Tezi*. Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü.

Özcan, M. (2010). "Siber Terörizm Ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu". https://docplayer.biz.tr/29878985-Siber-terorizm-ve-ulusal-guvenlige-tehdit-olusturma-boyutu.html. (Erişim Tarihi: 15.12.2019).

Özçoban, C. (2014). "21.Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü". *Yüksek Lisans Tezi*. İstanbul: Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Özel, H.A. (2011). "İktisadi Perspektiften Küreselleşme Kavramı ve Gelişimi". *Sosyal Bilimler Dergisi*. Sayı:2, ss.91-98.

Özer, M. A. (2006). *Avrupa Birliği Yolunda Türk Kamu Yönetimi*. Ankara: Platin Yayınları.

Özerkmen, N. (2004). "Uluslararası Eşitsizliği Derinleştiren Bir Süreç Olarak Ekonomik Küreselleşme". *Ankara Üniversitesi Dil Ve Tarih Coğrafya Fakültesi Dergisi*, 44 (1), ss.135-148.

Özev, M.H. (2017). "Küresel Denklemde Türkiye'nin Enerji Güvenliği". *SETA Yayınları* No:89. https://setav.org/assets/uploads/2017/09/TurkiyeEnerjiGuvenligi.pdf (Erişim Tarihi: 20.12.2019).

Özgür, S. (2006). *Geleceğe Yönelen Tehdit? Kitle İmha Silahları*. 1. Baskı. İstanbul: IQ Kültür Sanat Yayıncılık.

Özpınar, Ö. (2003). "Küreselleşme, İşgücü Piyasaları ve Türkiye". *Doktora Tezi*. Aydın: Adnan Mederes Üniversitesi Sosyal Bilimler Enstitüsü.

Özyurt, C. (2005). *Küreselleşme Sürecinde Kimlik ve Farklılaşma*. İstanbul: Açılım Kitap.

Pamir, N. (2001). "Dünya'da ve Türkiye'de Enerji Güvenliği". *Stratejik Analiz Dergisi*. 1(12).

Paris, R. (2001). "Human Security -Paradigm Shift or Hot Air?". *International Security*. 26 (2), ss.87-102.

Pekcan, E. (2007). "Soğuk Savaş Sonrası Değişen Güvenlik Kavramı Çerçevesinde Terörizm ve NATO". *Yüksek Lisans Tezi.* Trabzon: Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü.

Peker, B. (2010). "Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu". *Yüksek Lisans Tezi*. Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Peterson, S. (1992). *Security and Sovereign States: What is at Stake in Taking Feminism Seriously*. Boulder-Colo: Lynne Rienner.

Peterson, S.-Runyan, A. (1999). *Global Gender Issues*. Oxford: Westview Press.

Perraton, J.-Goldblatt, D.-Held, D.-McGrew, A. (2000). *Küreselleşen Bir Dünyada Ekonomik Aktivite*. Çev., Nedret Demirci, Ankara: Kadim Yayınları.

Philips, K.G. (2013). "Unpacking Cyberwar". *JFQ: Joint Force Quarterly*, vol.70. ss. 70–75.

Radikal E-haber (2011). "ABD Siber Saldırıları 'Savaş Sebebi' Sayacak". http://www.radikal.com.tr/dunya/abd-siber-saldirilari-savas-sebebi-sayacak-1051378/ (Erişim Tarihi: 12.11.2019).

Rearden, S. L. (2012). *Council Of War: A History of the Joint Chiefs of Staff 1942–1991*. Washington: NDU Press.

Resmi Gazete (2006). 26242 sayılı ve 2006/38 numaralı Karar. https://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.htm (Erişim Tarihi: 25.12.2019).

Resmi Gazete (2013a). "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının Kabulü Hakkında Karar". http://www.resmigazete.gov.tr/eskiler/2013/06/20130620.htm (Erişim Tarihi: 24.12.2019).

Resmi Gazete (2013b). "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ". http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (Erişim Tarihi: 22.12.2019).

Richardson, J. (2011). "Stuxnet as Cyberwarfare: Applying the Law of Warto the Virtual Battlefield". *The John Marshall Journal of Information Technology &Privacy Law*, Vol.29, ss.1-28.

Rid, T.-McBurney, P. (2012). "Cyber-Weapons". *The RUSI Journal*. 157 (1), ss.6-13.

Rieker, P (2000). "Security, Integration and Identity Change". NUPI Working Paper. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2394126/WP_nr611_ Rieker.pdf?sequence=3&isAllowed=y (Erişim Tarihi: 01.12.2019)

Ripsman, N. (2016). *Neoclassical Realist Theory of International Politics*. New York: Oxford University Press.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.

Rose, G. (1998). "Neoclassical Realism and Theories of Foreign Policy". *World Politics*. ss.144-172.

Rosenau, J.N. (1990). *Turbulance in World Politics: A Theory of Change and Continuity*. Princeton: Princeton University Press.

Roth, M. (2009). "Bilateral Disputes Between EU Member States and Russia. CEPS Working Document (Centre for European Policy Studies)". https://www.ceps.eu/wp-content/uploads/2009/09/1900.pdf (Erişim Tarihi: 20.11.2019).

Rubinstein, A. Z.(1991). "New World Order or HollowVictory". *Foreign Affairs*. 74 (4), ss.54-56.

Ruys, T. (2010). *Armed Attack and Article 51 of the UN Charter*. London: Cambridge University Press.

Sağıroğlu, Ş.-Alkan, M. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları.

Salamon, L.M.-Anheier, H. K. (1997). "Non-Governmental Organizations". *Society.* 34 (2), ss. 60-65.

Sancak, K. (2013). "Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü". *Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Dergisi.* Sayı:6, ss.123-134.

Sander, O. (2016). *İlkçağlardan 1918'e Siyasi Tarih*. Ankara: İmge Kitabevi.

Sandıklı, A.-Emeklier B. (2011). *Güvenlik Yaklaşımlarında Değişim ve Dönüşüm*. İstanbul: BİLGESAM Yayınları.

Sarahan, Z. A. (2018). "Küreselleşme ve Terörizm: Terörizmin Finansal Kaynakları". *Yüksek Lisans Tezi*. İstanbul: Arel Ünivesitesi Sosyal Bilimler Enstitüsü.

Sarper, B. (2013). "Güvenlik Çalımaları Alanında Kopenhag Okulu'nun Toplumsal Güvenlik Kavramsallatırması Çerçevesinde Bir Etnik Çatışma Örneği Olarak Kosova Sorunu" *Doktora Tezi*. Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Schwartz, M.J. (2013). "Google Aurora Hack Was Chinese Counterespionage Operation". https://www.darkreading.com/attacks-and-breaches/google- aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060 (Erişim Tarihi: 18.11.2019)

Schmitt, M. (2011). "Cyber Operations and the Jus in Bello: Key Issues*". International Law Studies,* vol.87, ss.89-110.

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 1,* Cambridge University Press. New York.

Schaap, A. J. (2009). "Cyber Warfare Operations: Development and Use Under International Law". *Air Force Law Review.* Vol. 64. ss.121-174.

Semercioğlu, H. (2016). "Uluslararası Terörizmde Küresel İşbirliği: Bir Ütopya". *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*. 34 (2), ss. 97-114.

Sempa, F.P. (2002). *Geopolitics: From The Cold War to The 21st Century*. New Jersey: Transaction Publishers.

Sertçelik, A. (2015). "Siber Olaylar Ekseninde Siber Güvenliği Anlamak". *Medeniyet Araştırmaları Dergisi.* 2 (3). ss.25-42.

Sezenler, O. (2009). *Yumuşama Dönemi ve Jeopolitik: Henry Alfred Kissinger*. M.S. Palabıyık (Ed.). Ankara: Orion Kitabevi.

SGR (2012). *Siber Güvenlik Raporu*. Istanbul: Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü.

Siber Filo Komutanlığı (2017a). "United States TENTH Fleet From Anti-submarine Warfare to Cyberspace". https://www.public.navy.mil/fcc-c10f/Pages/ustenthfleethistory.aspx (Erişim Tarihi: 24.12.2019).

Siber Filo Komutanlığı (2017b). "Welcome To FCC/C10F". https://www.public.navy.mil/fcc-c10f/Pages/home.aspx (Erişim tarihi: 25.12.2019).

Singer, D. (2006). "Uluslararası İlişkilerde Analiz Düzeyi Meselesi". *Uluslararası İlişkiler Dergisi*. 3 (11), ss.7-16.

Singer, P.W.-Friedman, Allan (2015). *Siber Güvenlik ve Siber Savaş* (Çev. Ali ATAV). 1.Baskı, Ankara: Buzdağı Yayınevi.

Slaughter, A.M. (2000). *The Real World Order. Globalization and the Challenges of a New Century*. Ed. Patrick Q'meara, Howard D. Mehlinger, Matthew Krain. ABD:Indiana University Press.

Smillie, I. (1997). "NGO's Development Assistance: A Change in the Mind Set". *Third World Quarterly*. 18 (3), ss. 563-577.

Snyder, J. (2004). "One World, Rival Theories". *Foreign Policy*. c. 145, ss. 52-62.

Solis, G.D. (2012). The Law of Armed Conflict: International Humanitarian Law at War. 2nd ed., Cambridge University Press, New York.

Sönmezoğlu, F. (2005). *Uluslararası Politika ve Dış Politika Analizi*. 4. Baskı. İstanbul: Filiz Kitabevi.

Sputnik Haber Sitesi (2017). "Beyaz Saray ABD, 35 Rus Diplomatı 72 Saat İçerisinde Sınır Dışı Edecek". https://tr.sputniknews.com/abd/201612291026553306-abd-rusya-yaptirim-diplomat-sinir-disi (Erişim Tarihi: 19.11.2019).

Stancich, L. (1998). "Discovering Elephants and a Feminist Theory of International Relations". *Global Society*. 12(1), ss.125-140.

Steger, M. B. (2013). *Küreselleşme*. Ankara: Dost Kitabevi Yayınları.

Stewart, S. (1997). "Happy After in the Market Place: Non-Governmental Organizations and Civil Society". *Review of African Political Economy*, 24 (71), ss. 11-34.

Stokes, M.A.-Lin, J.-Hsiao, L.C.R. (2011). The Chinese People's Liberation Armay Signals Intelligence and Cyber Reconnaissance Infrastructure". Project 2049 Institute. https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/ (Erişim tarihi: 25.12.2019).

Solmaz, E. (2014). "OECD Ülkelerinde Ülke İçi Gelir Eşitsizliklerinin Çok Boyutlu Küreselleşme Endeksleri İle İlişkisi". *Süleyman Demirel Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*. 19 (3), ss.91-108.

Şahin, G. (2015). "Soğuk Savaş Sonrası Değişen Güvenlik Anlayışı Bağlamında NATO". *Doktora Tezi*. Edirne: Trakya Üniversitesi Sosyal Bilimler Enstitüsü.

Şahinaslan, Ö. (2013). "Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma". *Doktora Tezi,* Edirne:Trakya Üniversitesi Sosyal Bilimler Enstitüsü.

Şener, U. (2019). "Yeni Güvenlik Anlayışı Çerçevesinde ABD İç Güvenlik Yapılanmasında Kurumsal Dönüşüm ve Türkiye'de Uygulanabilirliği". *Yüksek Lisans Tezi.* Ankara: Milli Savunma Üniversitesi Alparslan Savunma Bilimleri Enstitüsü.

Şenol, M. (2012). "Siber Savaş". Silahlı Kuvvetler Dergisi. Gnkur. ATASE Yayınları. Sayı:413, ss. 14-15.

Şenol, M. (2016). Uluslararası Bilgi Güvenliği Mühendisliği Dergisi. 2 (2), ss:10-17.

Şentürk, H.-Çil, Z.C.-Sağıroğlu, Ş. (2012). "Cyber Secuirty Analysis of Turkey". International Journal of Information Security Science. 1 (4), ss.112-125.

Talin El Kitabı (2013). https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku (Erişim Tarihi: 20.11.2019).

Taner, O. (2004). "Dünya'da ve Türkiye'de Küreselleşme ve Yoksulluk Süreci". *Yüksek Lisans Tezi*. Muğla: Muğla Üniversitesi Sosyal Bilimler Enstitüsü.

Terkan, B. (2007). "Basın ve Siyaset İlişkisinin Gündem Belirleme Modeli Çerçevesinde Bir Analizi". *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. Sayı 17, ss. 561–584.

Terrif, T. (1999). *Security Studies Today*. Cambridge: Polity Press.

The Guardian Haber Sitesi (2010). "Operation Payback Cripples MasterCard Site in Revenge for WikiLeaks Ban". https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks (Erişim Tarihi: 19.11.2019)

Tickner, A.J. (1988). "Hans Morgenthau's Principles of Political Realism: A Feminist Reformulation". *Millennium Journal of International Studies*. 17(3), ss.429-440.

Tickner, A.J. (1997). "You Just Don't Understand: Troubled Engagements Between Feminists and IR Theorists". *International Studies Quarterly*. 41 (4).

Tickner, A.J. (2005). "What Is Your Research Program? Some Feminist Answers to International Relations Methodological Questions". *International Studies Quarterly*. 49 (1).

Tokol, A. (2001). "Çokuluslu Şirketler ve Endüstri İlişkilerine Etkileri". *İş, Güç, Endüstri İlişkileri ve İnsan Kaynakları Dergisi*, 3 (2). http://www.isguc.org/?p=article&id=63&cilt=3&sayi=2&yil=2001 (Erişim Tarihi: 16.12.2019).

Torun, A. (2012). "Uluslararası Güvenlik ve Küreselleşme: Türkiye'nin Ulusal Güvenlik Politikasının Dönüşümünde Küreselleşmenin Rolü". *Doktora Tezi*. Ankara:Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Toure, H. (2019). "ITU Cybersecurity Gateway". http://groups.itu.int/cybersecurity-gateway/HOME.aspx (Erişim Tarihi: 20.12.2019).

Turan, Ş. (2014). "Küreselleşen Dünyada Sürdürülebilir Kalkınmanın Önemi". *Yüksek Lisans Tezi*. Trabzon: Karadeniz Üniversitesi Sosyal Bilimler Enstitüsü.

Turhan, O. (2006). "Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)". *Planlama Uzmanlığı Tezi.* Ankara: Devlet Planlama Teşkilatı.

TÜBİTAK BİLGEM (2011). "Siber Güvenlik Tatbikatı". https://bilgem.tubitak.gov.tr/en/node/198 (Erişim Tarihi: 25.12.2019).

TÜBİTAK MAM (2019). HESKON. http://ee.mam.tubitak.gov.tr/sites/images/ee_mam/heskon_proje_bilgi.pdf (Erişim Tarihi:25.12.2019).

Türkay, Ş. (2013). "Siber Savaş Hukuku ve Uygulanma Sorunsalı". *İÜHFM C. LXXI.* sayı 1, ss. 1177-1228.

Türk Dil Kurumu E-Sözlüğü (2018). "Güvenlik Kavramı Tanımsal Değerlendirmesi". http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK. GTS.5a80ed4c44b7d1.08728 797. (Eriim Tarihi:12.02.2018).

Türk Dil Kurumu (2019). "Terör". https://sozluk.gov.tr/?kelime= (Erişim Tarihi: 14.12.2019).

Topal, A.H. (2010). "Uluslararası Hukukta Deniz Haydutluğu ve Mücadele Yöntemleri". *AÜHFD*. 59 (1). ss.99-130.

Ulaşanoğlu, M. E.-Yılmaz, R.-Tekin, A.M. (2010). "Bilgi Güvenliği: Riskler ve Öneriler". Ankara: Bilgi Teknolojileri ve İletişim Kurumu. http://docplayer.biz.tr/632957-Bilgiguvenligi-riskler-ve-oneriler.html

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016). "Ulusal Siber Güvenlik Stratejisi 2016-2019". https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf (Erişim Tarihi: 20.11.2019)

Ulusal Bilgi Güvenliği Kapısı (2014). "Türkiye'de Siber Güvenliğin Mevzuattaki Yeri". https://www.bilgiguvenligi.gov.tr/mevzuat/turkiye-de-siber-guvenligin-mevzuattaki-yeri-ve-yapilan-calismalar.html (Erişim Tarihi: 25.10.2019). Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Uluslararası Denizcilik Bürosu (2012). Piracy & Armed Robbery Report 2011.

Uluslararası Denizcilik Bürosu (2019). "Piracy & Armed Robbery Report 2019". https://www.icc-ccs.org/index.php/piracy-reporting-centre/live-piracy-report (Erişim Tarihi:20.12.2019).

Uluslararası Denizcilik Örgütü (2009). "Code of Practice For The Investigation of Crimes of Piracy and Armed Robberry Against Ships". http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Guidance/Documents/A.1025.pdf (Erişim Tarihi:20.12.2019).

Uluslararası Göç Organizasyonu Örgütü (2019). "Who is a migrant?". https://www.iom.int/who-is-a-migrant (Erişim tarihi: 19.12.2019).

Uluslararası Telekomünikasyon Birliği (2008). "Overview of Cybersecurity". https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1205 (Erişim Tarihi: 21.11.2019).

Uluslararası Telekomünikasyon Birliği (2018). "Global Cyber Security Index". https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (Erişim Tarihi: 19.11.2019)

Uluslararası Telekomünikasyon Birliği (2007). "ITU Global Cybersecurity Agenda (GCA): A Framework for International Cooperation in Cybersecurity". https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf (Erişim Tarihi: 20.12.2019).

Uluslararası Telekomünikasyon Birliği (2019). "Global Cybersecurity Agenda (GCA)". https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (Erişim Tarihi: 19.12.2019)

Uluç, Güliz. (2002)."Küresel-Yerel Kültürler Üzerinde Yeniden Düşünmek: Melez Kültürler". *Liberal Düşünce*. 7 (27), ss.89-98.

USSTRATCOM (2010). "U.S. Department of Defense, Cyber Command Fact Sheet". http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (Erişim Tarihi: 24.12.2019).

Uzer, U. (2013). "21.Yüzyılda Tek Kutupluluk Tartışmaları". *Bilge Strateji*. 5 (8), ss.69-93.

Ünver, M.-Canbay, C.-Mirzaoğlu, A. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri ve İletişim Kurumu Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

Waltz,N.K. (1979). *Theory of International Politics*. New York: McGraw Hill.

Waltz, N.K. (1993). "The Emerging Structure of Intenational Politics". *International Seccurity*. 18. ss.44-79.

Walt, S.M.(1991). "The Renaissance of Security Studies". *International Studies Quarterly*. 35 (2), ss. 211-239.

Walt, S.M. (2002). "The Enduring Relevance of the Realist Tradition". *Political Science: State of the Discipline.* ss.197-230.

Wamala, F. (2011). "ITU National Cyber Security Strategy Guide. International Telecommunications Union". http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (Erişim Tarihi: 20.12.2019)

Waters, M. (2001). *Globalization: Key Ideas* (2. b.). London: Routledge.

Wedermyer, L.J. (2012). "The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict". https://www.law.msu.edu/king/2011-2012/Wedermyer.pdf. (Erişim Tarihi: 20.12.2019).

Whitney, L. (2010). "U.S. Cyber Command Prepped to Launch". https://www.cnet.com/news/u-s-cyber-command-prepped-to-launch/ (Erişim Tarihi: 25.12.2019).

Wikipedia (2019). https://tr.wikipedia.org/wiki/Siber_sava%C5%9F#cite_ref-hasancifci_1-2 (Erişim Tarihi: 25.12.2019).

Winther, R.-Gran, B. A.-Dahll, G. (2005). *Computer Safety, Reliability, and Security. 24th International Conference SAFECOMP*. Norveç: Fredrikstad.

Wright, Q. (1942). *A Study of War*. London: The University of Chicago Press.

Wohlforth, W.C. (1999). "The Stability of a Unipolar World". *International Security*. 24 (1), ss. 5–41.

Varşova Zirve Bildirgesi (2016). "Wales Summit Declaration". https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Erişim Tarihi: 20.12.2019)

Ventre,C. (2010). "China's Strategy for Information Warfare: A Focus on Energy. Journal of Energy Security". http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361 (Erişim Tarihi: 25.12.2019)

Vogel, K.M. (2013). "Expert Knowledge in Intelligence Assessments: Bird Flu and Bioterrorism". *International Security*. 38 (3), ss.39-71.

Yalçın, E. (2014). "Türkiye'de Siber Güvenliğin Mevzuattaki Yeri ve Yapılan Çalışmalar". TÜBİTAK BİLGEM. http://web.archive.org/web/20160320234637/http://www.bilgiguvenligi.gov.tr/mevzuat/turkiye-de-siber-guvenligin-mevzuattaki-yeri-ve-yapilan-calismalar.html (Erişim Tarihi: 25.10.2019).

Yalçın, İ. (2019). "Soğuk Savaş Sonrası NATO ve Türkiye'de Siber Güvenlik". *Yüksek Lisans Tezi.* Eskişehir: Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Yalçınkaya, H.-Çılbant, Ç.-Yalçınkaya, N. (2012). Küreselleşme ile Yeniden Şekillenen Ulus Devlet Anlayışı. *International Journal of Economic and Administrative Studies.* Sayı 8. ss.1-26.

Yavuz, B. (2009). "Critical Security Studies and World Polirtics". *Uluslararası İlişkiler.* 6 (21).

Yayla, M. (2013). "Hukuki Bir Terim Olarak Siber Savaş". *TBB Dergisi*. 104. ss.177-203. http://portal.ubap.org.tr/App_Themes/Dergi/2013-104-1247.pdf (Erişim Tarihi: 24.11.2019).

Yayla, M. (2014). "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı". *Hacettepe HFD.* 4 (2), ss.181-200.

Yazıcı, A. (2010). "Küresel Tehlike Siber Savaş". *Aselsan Dergisi*. 10 (36).

Yıldız, M. (2014). "Siber Suçlar ve Kurum Güvenliği". *Denizcilik Uzmanlık Tezi*. Ankara: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.

Yılmaz, E. (2011). "Etnik Çatışmalar ve Birleşmiş Milletler Barış Güçleri". *Sosyal Bilimler Dergisi*. Sayı 25, ss. 89-107.

Yılmaz, (Ercan) N.-Ulus, H.İ.-Gönen, S. (2015). "Bilgi Toplumuna Geçiş ve Siber Güvenlik". *Bilişim Teknolojileri Dergisi,* 8 (3), ss. 133-146.

Yüksel, E. (2007). "Kamuoyu Oluşturma ve Gündem Belirleme" Kavramları Nerede Kesişmekte, Nerede Ayrılmaktadır?". *Sosyal Bilimler Dergisi*. sayı:1, ss.571-586.

Zengin, A.K. (2019). "Rusya Federasyonu'nun Ulusal Güvenlik Politikalarına Yön Veren Belgeler ve Etki Eden Güvenlik Yaklaşımları". *Yüksek Lisans Tezi*. Kahramanmaraş: Sütçü İmam Üniversitesi Sosyal Bilimler Enstitüsü.

Zengingönül, O.(2004). *Küreselleşme*. Ankara: Adres Yayınları.

Zoller, R. G. (2010). *Russian Cyberspace Strategy and a Proposed United States Response.* U.S. Army War College.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı ve Soyadı : SONER ÇELİK

Eğitim Durumu

Lisans Öğrenimi : Anadolu Üniversitesi Uluslararası İlişkiler Bölümü
Milli Savunma Üniversitesi Sistem Mühendisliği Bölümü

Yüksek Lisans Öğrenimi :Ufuk Üniversitesi Sosyal Bilimler Enstitüsü
Uluslararası İlişkiler Anabilim Dalı
Hacettepe Üniversitesi Bilişim Enstitüsü
Bilgi Güvenliği Anabilim Dalı