T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİMDALI
ULUSLARARASI İLİŞKİLER BİLİMDALI

GÜVENLİK PARADİGMASININ DEĞİŞİMİ; ABD VE RUSYA REKABETİNİN SİBER ALANDA TEZAHÜRÜ

YÜSKEK LİSANS TEZİ

ONUR YILMAZ

KOCAELİ 2020

T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİMDALI
ULUSLARARASI İLİŞKİLER BİLİMDALI

GÜVENLİK PARADİGMASININ DEĞİŞİMİ; ABD VE RUSYA REKABETİNİN SİBER ALANDA TEZAHÜRÜ

YÜSKEK LİSANS TEZİ

ONUR YILMAZ

DR. ÖĞR. ÜYESİ GÜL CEYLAN TOK

Tezin Kabul Edildiği Enstitü Yönetim Kurulu Karar ve No: 08.07.2020/16

KOCAELİ 2020

İÇİNDEKİLER

İÇİNDEKİLER……..I

ÖZET……..III

ABSTRACT……..IV

SİMGE VE KISALTMALAR…….…V

GİRİŞ……....1

BİRİNCİ BÖLÜM

1. KLASİK GÜVENLİK PARADİGMASININ DEĞİŞİMİ……...5
1.1. Klasik Güvenlik Paradigmasına Getirilen Eleştiriler…….. 9
1.2. Yeni Güvenlik: Yeni Tehditler……..13

İKİNCİ BÖLÜM

2. SİBER GÜVENLİK VE İLGİLİ KAVRAMLAR……..18
2.1. Siber ve Siber Uzay/Alan……...21
2.2. Siber Güvenlik……...23
2.3. Siber Tehditler ve Siber Saldırılar…….25
2.4. Siber İstihbarat……...29
2.5. Siber Suç, Siber Terörizm ve Siber Propaganda……32
2.6. Siber Savaş…….37

ÜÇÜNCÜ BÖLÜM

3. ABD ve RUSYA FEDERASYONU'NUN YENİ REKABET ALANI: SİBER UZAY…….43
3.1. ABD'NİN SİBER GÜVENLİK STRATEJİSİ ve TEMEL METİNLERİ……...……43
3.2. ABD'NİN İLGİLİ SİBER GÜVENLİK KURUM ve KURULUŞLARI……..……..49
3.2.1. ABD Savunma Bakanlığı (The Departmant of Defence)…….49
3.2.2. ABD İç Güvenlik Bakanlığı (Departmant of Homeland Security)……...51
3.2.3. FBI ve CIA…...……53
3.3. RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİSİ ve TEMEL METİNLERİ…….……54
3.4. RUSYA FEDERASYONU'NUN İLGİLİ SİBER GÜVENLİK KURUM ve KURULUŞLARI……59
3.4.1. Federal Güvenlik Servisi (Federal Security Service/FSB)...……60
3.4.2. Federal Koruma Servisi (The Federal Protection Service/FS0)……...61
3.4.3. Rus İstihbarat Servisi (Foreign Intelligence Service/SVR)……..62
3.4.4. Rus Askeri İstihbarat Direktörlüğü (GRU)……...62
3.4.5. Federal İletişim Servisi, Bilgi Teknoloji ve Kitle İletişim (Roskomnadzor)……63
3.4.6. Rusya Federasyonu Dışişleri Bakanlığı……63
3.5.ABD ve RUSYA FEDERASYONU'NUN SİBER STRATEJİ ve ORGANİZASYONLARI'NIN KARŞILAŞTIRILMASI……..64
3.6. ABD ve RUSYA FEDERASYONU'NUN SİBER ALAN İŞBİRLİĞİ VE REKABET DURUMLARI…….66

3.7. SİBER SOĞUK SAVAŞ İDDİALARI……..70
3.8. 2016 ABD BAŞKANLIK SEÇİMLERİNDE SİBER MÜDAHALE İDDİASI……..72

SONUÇ…….80

KAYNAKÇA……87

ÖZET

Dünyanın değişen ve gelişen yapısı beraberinde yeni fırsatların yanında yeni tehditleri de getirmiştir. Klasik güvenlik anlayışı gelişen ve karmaşıklaşan yeni tehditleri anlamakta yeterli olamamıştır. Teknolojinin gelişmesiyle devletler de kritik altyapılarına kadar bu teknoloji ve dijitalleşmeden payını almıştır. Bu anlamda siber alan/uzay; içerisinde birey, grup ve devletleri alan bir geniş yelpazede güvenlik sorunsalının yeni mecralarından birini teşkil etmektedir. Fakat siber uzayın güvenlik parametreleri içerisine alınmasında devletler açısından bir gecikme söz konusu olmuştur. Özellikle 2000'li yıllarda siber uzaydan devletlere yönelen bir takım saldırılar gerçekleşince; bu alanın önemli tehditler ve yıkıcı sonuçlar ortaya çıkarabileceği düşünülmeye başlanmıştır. Siber alanın/uzayın anlaşılmasına yönelik çeşitli kavramsal sorunların olması, bu yeni mecranın anlaşılmasını zorlaştırmıştır. Bu çalışmada siber uzayın ve siber güvenliğin kavramsal altyapısı ele alınmıştır. Kavramların birbirleriyle benzer ve faklı yönleri ortaya konarak; klasik güvenlik terimlerinden farklarına değinilmiştir. Siber uzayda etkinlikleri üst seviyede olan ABD ve Rusya Federasyonu'nun siber alandaki ilişkilerini konu edinen bu çalışma; ilişkilerin işbirliği ve rekabet durumlarını incelemiştir. İki ülkenin siber güvenlik yapılanmaları, strateji belgeleri ve siber politikalarını ortaya koymak suretiyle siber uzayı nasıl algıladıklarına değinilmiştir. 2016 ABD Başkanlık Seçimlerinde Rusya Federasyonu'nun müdahale ettiği iddiası üzerinden iki ülkenin siber alandaki rekabetleri ortaya konmuştur. Rusya Federasyonu'nun ABD seçimlerine etki ettiğine yönelik istihbarat raporları ve soruşturma raporları incelenerek söz konusu müdahale iddiaları ele alınmıştır. Bu çalışma, siber güvenliğin kavramsal altyapısının siber alana özgü terminolojiyle ele alınmasına dikkat etmiştir. Ayrıca siber uzayda rekabet halinde olan ABD ve Rusya Federasyonu'nun siber uzaydaki durumlarına karşılaştırmalı bir yaklaşım getirmesi nedeniyle önemlidir.

Anahtar Kelimeler

Siber Uzay, Siber Güvenlik, ABD, Rusya Federasyonu, 2016 ABD Başkanlık Seçimleri, Siber Müdahaleler

ABSTRACT

The changing and developing structure of the world has brought along new opportunities as well as new threats. Classical security understanding has not been sufficient to understand new threats that are developing and becoming more complex around the world. States have improved their critical infrastructure by taking share from the development of technology and digitalization. In this sense, cyber space; has become one of the new security outlet with a wide range of elements including individuals, groups and states. However, it was relatively late for the states to include cyberspace in the security parameters. The security threat potential of cyberspace was eventually realized in the 2000s when a number of attacks against the states from cyber space took place. The existence of various conceptual problems in understanding cyber space made it difficult to understand this new medium. In this study, the conceptual framework of cyberspace and cyber security is discussed. This study, investigated the cooperation and competition of the relations between the USA and the Russian Federation in cyberspace. By examining the cyber security structures, strategy documents and cyber policies of the USA and the Russian Federarion, this study explored how each state perceive the cyberspace. The claim that the Russian Federation intervened in 2016 US Presidential Elections has been analyzed as an example of the competition of the two countries in this field The intervention claim has been discussed based on the intelligence and investigation reports. This study reveals the significance of using conceptual framework designed for cybersecurity for cybersecurity issues. This study is significant since it brings a comparive analysis of the competition between the USA and RF, in cyber space.

KEY WORDS

Cyber Space, Cyber Security, USA, Russian Federation, 2016 US Presidential Elections, Cyber İnterventions

SİMGE VE KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AGİT	Avrupa Güvenlik ve İşbirliği Teşkilatı
BM	Birleşmiş Milletler
CERT	Computer Emergency Readiness Team
CIA	Central Intelligence Agency
CNSS	Cyber National Security Section
CSS	Cyber Criminal Section
DDOS	Distrubuted Denial of Service
DHS	Department of Homeland Security
DNC	Democratic National Committee
DOD	The Department of Defence
DoS	Denial of Service
DS&T	Directorate of Science & Technology
FSB	Federal Security Service
FSO	Federal Protection Service
FSTEC	Federal Service for Technical and Export Control of Russia
GRU	Glavnoye Razvedyvatel'noye Upravleniye/ Rus Askeri İstihbarat Direktörlüğü
G8	Group of Eight
IRA	Internet Research Agency
ICS-CERT	Industrial Control System Computer Readiness Team
IP	Internet Protocol
IŞİD	Irak Şam İslam Devleti
KGB	Komitet Gosudarstvennoy Bezopasnosti/Devlet Güvenlik Komitesi
NATO	The North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communication Center
NCIJTF	National Cyber Investigative Joint Task Force

NSA	National Security Agency
NSCS	National Cyber Security Strategy
NPDD	National Programme on Dairy Development
RF	Russian Federation
SORM	Sistema Operativno Rozysknih Meropriyatii/ Operasyonel Araştırma Faaliyetleri Sistemi
US	United States

GİRİŞ

Klasik güvenlik paradigması, devlet merkezli ve yalnızca askeri meseleleri dikkate alan yapısıyla Uluslararası İlişkiler disiplininin her geçen gün kompleksleşen ihtiyaçlarına cevap verememiştir. Güvenlik çalışmaları, özellikle 1980 ve 1990'lı yıllardaki gelişmelere paralel bir şekilde hızlanmış; klasik güvenlik paradigmasına çok çeşitli eleştiriler getirilmiştir. Bu eleştiriler liberallerden idealistlere, inşacılardan feministlere, İngiliz Okulundan Frankfurt Okuluna ve daha birçok farklı kesimden yöneltilmiştir. Tüm bu eleştiriler, güvenliğe yeni boyutlar kazandırarak onu sadece askeri meseleler değil çevre, ekonomi, insan, kadın, kimlik, kültür gibi yeni parametreleri de içeren bir konuma taşımıştır. Tüm bu yeni parametreler klasik güvenlik anlayışının gözden geçirilmesini, güvenliği yeni bir yorumlamaya tabi tutulmasını sağlamıştır (Bilgin, 2010: 71-73). Güvenlik paradigmasına son olarak eklemlenen ve güvenliğin yeni parametrelerinden birini oluşturan bir diğer unsur siber alan olmuştur.

Siber alanın önemli bir güvenlik parametresi olarak ele alınmasında; özellikle Estonya'ya yönelik gerçekleştirilen ve sonuçları itibariyle yıkıcı etkiler gösteren siber saldırıların etkisi büyük olmuştur. Fakat siber alanın anlaşılmasında, ele alınmasında ve kavramlarının açıklanmasında bir takım sorunlar ortaya çıkmaktadır. Siber kavramların siber alanın yapısına uygun bir şekilde ele alınmaması bu sorunun temel nedenidir. Bu nedenle siber alanın anlaşılması adına ona ait kavramların doğru açıklanması önemlidir. Siber alanın yakın zamanda önemli bir rekabet alanına döndüğü; gerek siber saldırılar gerek bu alandaki yetkinlik çabalarının sıklaşmasından da anlaşılmaktadır. Siber alanda yetkinlik arayışına giren iki ülke olan ABD ve RF'nin siber yapılanmaları ve birbirleriyle olan ilişkilerinin anlaşılması noktasında derin analizlerin yapılması elzemdir. 2016 ABD Başkanlık Seçimlerinde karşı karşıya gelen iki ülkenin, siber aktivitelerinin anlaşılması için bu alandaki yetkinlik, rekabet ve/veya işbirliği durumlarının gözden geçirilmesi gerekmektedir.

Siber alan ve ona ait kavramların açıklanmasına yönelik çeşitli çalışmalar son yıllarda artış göstermektedir. Bu çalışmalarda çeşitli ülkelere ait siber güvelik stratejilerinin incelendiği görülmektedir. ''Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus Devletin Değişen Stratejisi'' isimli yüksek lisans tezinde Yasemen

Özfındık Kotik; siber alanın uluslararası ilişkilerde ortaya koyduğu yeni duruma işaret ederken; bu yeni durumun ABD ve Rusya'nın siber güvenlik stratejilerinde ne gibi yeniliklere yol açtığına değinmiştir. Ayrıca siber savaş, siber terör, siber istihbarat gibi kavramlara da çalışmasında yer vermiştir. Mehmet Ada; ''NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi'' isimli yüksek lisans tezinde siber kavramlara yer verirken diğer taraftan NATO ülkelerinin siber güvenliğe dair oluşturdukları stratejileri incelemiştir. ''Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik'' adlı çalışmasında Kamil Tarhan siber kavramların, uluslararası ilişkilerdeki yerini ve klasik güvenlik paradigmasının değişimini ele almıştır. ''Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları'' isimli yüksek lisans çalışmasında Su Dilara Alioğlu siber saldırı türlerini ve siber saldırıların sonuçlarının yaratacağı yıkıcı sonuçların üzerinde durmuş, ABD ve Rusya Federasyonu'nu da kapsar bir şekilde ülkelerin siber politikalarını incelemiştir. Duygu Küçükaydın tarafından yürütülen ''Amerika Birleşik Devletleri'nin Ulusal ve Uluslararası Siber Güvenlik Stratejileri: Güvenlikleştirme Hareketi?'' isimli yüksek lisans tezinde ise ABD'nin siber güvenlikteki kurumsal yapılanmasına ilişkin bir analiz yapılmıştır.

Siber güvenlik üzerine yürütülen çalışmalarda nicelik olarak bir artış görülmektedir. Bununla birlikte güvenliğin yeni bir parametresi olarak beliren siber alanın ihtivasının ortaya konması ve niteliğinin geliştirilmesi ve anlaşılması adına yeni çalışmaların gerekliliği de ihtiyaçtır. Siber kavramların, klasik güvenlik terminolojisinden farklı yönlerinin ele alınması, siber alanın kendine özgü yapısıyla özdeş bir şekilde incelenmesi önemlidir. Diğer taraftan siber kavramların birbirleriyle olan ilişkilerinin incelenmesi anlamında belirgin bir eksiklik söz konusudur. Siber alanda ülkelerin sahip oldukları stratejileri ele alan çalışmalar olmakla beraber, bunların strateji ve performanslarının karşılaştırmalı olarak ele alan yeterli veri henüz ortaya konmamıştır. Diğer taraftan ABD ve Rusya Federasyonu özelinde siber alanda cereyan eden ilişkileri derinlemesine ele alan bir çalışma ortaya koymak adına iki ülkenin bu alandaki yapılanmaları, işbirliği ve rekabet alanları yeterince irdelenememiştir. 2016 yılındaki ABD Başkanlık seçimlerine RF'nin müdahalesi iddialarını anlamak adına iki ülkenin siber alana atfettikleri önemi, bu ülkelerin siber alandaki strateji ve hedeflerinin iyi anlaşılması elzemdir. Ayrıca iki

ülkenin kurumsal ve yapısal anlamda siber alandaki durumlarının gözden geçirilmesi gerekmektedir.

Siber alanı ve bu alana yönelik güvenlik tedbirlerinin alınması adına sorunun bütün yönleriyle ele alınması elzemdir. Bütün güvenlik parametrelerini içine alan ve güvenliğin değişen yönlerini ortaya koymak suretiyle bir güvenlik okuması yapmak siber güvenliği anlamakta yardımcı olacaktır. Diğer taraftan yeni rekabet alanı olarak görülen siber alanda, ABD ve Rusya Federasyonu özelinde bir siber mücadeleyi anlamlandırmak, rekabet ve işbirliği alanlarını görmek; siber alanın güvenlikteki hayati önemini kavramanın önemli bir adımı olacaktır. Uluslararası İlişkiler ve güvenlik ilişkisi göz önünde bulundurulduğunda, siber alan ve ilgili kavramlarının ortaya konulduğu kaynaklar eksik kalmakta, kavramlar birbirleriyle bağlantılı olarak ele alınmadığından belirsizlikler ortaya çıkmaktadır. Bu çalışma siber güvenlik kavramlarını siber alanın yaratmış olduğu yeni literatüre uygun bir şekilde ve klasik güvenlik kavramlarıyla farklılık ve benzerliklerini karşılaştırmak suretiyle ortaya koymaktadır. Çalışma ayrıca siber kavramların birbirleriyle olan ilişkilerini tespit etmeye önem göstermektedir. Diğer taraftan ABD ve Rusya'nın siber alandaki rekabet durumlarına yönelik derin ve spesifik çalışmalar bulunmamaktadır. Bu çalışma siber alan ve ona ait kavramların ilintili bir çizgide açıklanması ve siber alanda iki önemli aktör olan ABD ve Rusya'nın siber güvenlik mekanizmaları, kurumsal yapılanmaları, oluşturulan rapor ve strateji belgeleri, politikaları ve hedefleri üzerinden geniş bir inceleme yaparak, bu incelemeler doğrultusunda ortaya çıkan rekabet durumunu ortaya koyan bir yöntem izlemesi yönünden diğerlerinden ayrılmaktadır.

Bu çalışmanın amacı güvenliğin değişen/gelişen/dönüşen yönlerini ortaya koymak suretiyle siber güvenliğin yeni bir parametre olarak açıklanması, siber alana özgü kavramsal altyapının daha iyi anlaşılması ve ABD-Rusya Federasyonu ilişkilerinin bu alandaki yansımalarını ortaya koymaktır. 2016 ABD Başkanlık Seçimleri 'ne Rusya Federasyonu'nun müdahale ettiği iddialarını ayrıntılı bir şekilde ele alan bu çalışma, siber alandaki iki etkin gücün arasındaki rekabet durumunu ortaya koymayı hedeflemektedir. Klasik güvenlik anlayışının değişiminde hangi unsurların rol oynadığı, yeni güvenlik anlayışlarının ne olduğu, güvenliğe eklemlenen yeni parametrelerden biri olan siber alanının ne gibi özellikler gösterdiği

açıklanmaya çalışılan önemli sorular olmuştur. Diğer taraftan bu çalışmanın temel araştırma sorusu ise klasik güvenlik anlayışının değişmesiyle siber alanın yeni ve önemli bir hale geldiği uluslararası mecrada iki büyük güç olan ABD ve Rusya Federasyonu'nun siber uzaydaki ilişkilerinin nasıl geliştiğidir. Söz konusu sorulara cevap aranan bu çalışmada; iki ülkenin siber alandaki rekabet ve işbirliğine yönelik ilişkileri incelenmiştir.

BİRİNCİ BÖLÜM

KLASİK GÜVENLİK PARADİGMASININ DEĞİŞİMİ

1. KLASİK GÜVENLİK PARADİGMASI

Güvenlik olgusu ve meselesi Uluslararası İlişkiler disiplini tarafından sürekli bir şekilde ele alınmış; bu süreklilik çizgisinde değişimler, dönüşümler yaşayan bir seyir izleye gelmiştir. Uluslararası İlişkiler 'de güvenlik meselesine birçok farklı tanımlama ve yaklaşım getirilmişse de, güvenlik okumaları temelde devlet odaklı ve devlet odaklı olmamama durumlarına göre ele alınmaktadır (Duygu, 2015: 8). Devlet odaklı yaklaşımların realist teori tarafından şekillendiği göz önüne alındığında, klasik güvenlik okumalarının realist paradigmadaki yerinin tespit edilmesi elzem olmaktadır. Uluslararası İlişkiler 'in bir disiplin olarak ortaya çıktığı dönem ve kavramlar etrafında ele alındığında; hem disiplinin ontolojisine hem de terminolojisine hâkim olan ekolün realist ekol olduğu fikri yaygın bir şekilde kabul görmektedir. Dolayısıyla uluslararası sistemin temel aktörlerini devlet olarak kabul eden realist paradigma; güvenlik olgusunu devletler için elzem görmekle birlikte, güvenliği de devlet odaklı ve onunla ilgili olarak ele almaktadır.

Klasik realist teorinin doğrudan bir 'güvenlik kuramı' ortaya koymadığını göz önünde bulundurmakla beraber; uluslararası ilişkilerin, uluslararası siyasetin genel yapısının nasıl olması gerektiği üzerindeki realist savlar ve teorilerin; bir 'güvenlik' paradigmasının nasıl olması gerektiği fikrine dolaylı ve etkin bir katkı sağladığı görülmektedir. Böylece bu dolaylı katkı, klasik güvenlik paradigması olarak değerlendirilen güvenlik paradigmasının oluşumuna ön ayak olmuştur. İkinci Dünya Savaşı'nın ardından Uluslararası İlişkiler disiplininin baskın teorisi haline gelen realizm; klasik güvenlik paradigmasının kavram, kuram ve metodolojik altyapısının temel referans noktası haline gelmiştir. Realistler güvenlik kavramını, güvende olmama hali veya sürekli bir biçimde güvensizlik hissiyatının var olması üzerinden tanımlamışlardır (Sandıklı ve Emeklier, 2011: 22).

Realist paradigma bu güvenlik okumasıyla aslında mutlak bir güvende olma durumunun da bir nevi olamayacağını işaret etmektedir. Keza Westphalian düzenin hâkim olduğu 1648 ve sonrası dönemde Hobbes, Machiavelli ve Rousseau gibi realizm fikrinin yaratıcıları kabul edilen düşünürlerin fikirlerini haklı çıkarır şekilde, uluslararası ilişkilerin hâkim aktörleri olarak kabul edilen devletlerin sürekli bir biçimde kendi güvenliklerini sağlama ve çıkarlarını koruma niyetiyle her türlü güç mücadelesinin içerisinde bulundukları görülmüştür (Baylis, 2008: 71-72). E. H. Carr ve H. Morgenthau gibi klasik realist düşünürlerin de katkı verdiği bu anarşist ortamdaki barışın kalıcı olamaması fikri; özellikle dünya savaşlarının meydana gelmesiyle bir nevi kanıtlanmıştır. Özellikle Carr uluslararası alanda mutlak bir barışın sağlanılmasının pek mümkün olmadığını ileri sürmüş, devletlerin bu barış ortamına girebilmesinin uluslararası ya da ulus-üstü kuruluşlara verdikleri taahhütlerle değil ancak güç unsurunun caydırıcılığıyla bir nebze sağlanabileceğini söylemiştir. İki savaş arası dönemin idealizm odaklı politikaları, uluslararası örgüt fikri, savaşın yasaklanmaya çalışılması gibi idealarının başarılı olmaması ve İkinci Dünya Savaşı'nın ortaya çıkması realizmin ön plana çıkmasına sebebiyet vermiştir. Bu durum güvenliğin askeri güç odaklı ve devletlerin birbirilerini tehdit olarak algıladıkları yeni bir dönemi beraberinde getirmiştir (Aydın, 2004: 34-36).

Devletlerin kendi güvenliklerine odaklandığı, diğer devletlerle ilişkilerde yalnızca bu amacı gerçekleştirmeyi hedeflediği ve politikalarını bu frekanslar üzerinden geliştirdiği güç mücadelesi hali; sistemin ana aktörleri kabul edilen devletler tarafından her devletin durumu kendi lehine değiştirebileceği ana kadar devam ettirilmek istenmektedir. Söz konusu güç mücadelesini kendi lehine değiştiren devlet ise hegemon duruma yükselerek diğer bütün devletler için tehdit haline dönüşmektedir. Buna göre devletler böyle bir ortamda ancak hegemon güç oluşturma gayretindeki devleti dengeleyerek bu durumdan kaçınabileceklerdir (Baylis, 2008: 71-72).

Realist paradigmanın işaret ettiği ve güç mücadelesine konu olan, devletlerin temel ve yegâne aktör oldukları uluslararası ortam anarşik bir yapı teşkil etmektedir. Bu da devletlerin, kendi güvenliklerini sağlamada başvurabilecekleri, devletlerden üstün bir otoritenin olmadığını ortaya koymaktadır ki bu durumda devletlerin güvenliklerini ve çıkarlarını muhafaza etmede tek yetkili oldukları sonucunu

doğurmaktadır. Realizme göre bu durumda, güç ilişkileri önemli bir parametre olarak ortaya çıkmaktadır (Sancak, 2013: 125). Devletlerarasındaki bu güç ilişkileri ve dolayısıyla güç çekişmeleri, klasik güvenlik yaklaşımının güvenliği; askeri tehditler ve düşman olgusu üzerinde hareket eder bir zemine oturtmuştur. Güvenliği bu şekilde ele alan yaklaşımın bir sonucu olarak, kendini güvensiz bir durumda hisseden devlet; güç mekanizmalarını geliştirerek, kendini güven altına alırken; bu sefer diğer devletin tehdit okumaları neticesinde kendisini güven altına almak adına karşı hamleler geliştirmesi söz konusu olmaktadır. Bu durumda karşılıklı bir güven bunalımı söz konusu olmakla beraber; bir güvenlik ikilemine taraf devletler karşılıklı olarak sürüklenmektedirler (Demiray ve İşcan, 2008: 152). Klasik realist okumada güvenlik ikilemi kavramı, bütün tarafların neticesinde zarar gördüğü bir durum olarak ele alınmıştır. Bu anlamda daha çok bir güvenlik ikilemi değil bir güvenlik paradoksundan söz edilmektedir. Keza güvenlik ikileminde neticenin olumsuz olması sadece bir ihtimalken güvenlik paradoksunda bu bir kesinlik ifade etmektedir. Çünkü güvenlik ikileminde; bir devletin güvenlik tercihlerinde bir ikilemde olması durumunu söz konusudur ve bu ikilemin sonunda yapılan tercihin olumlu sonuçları da ortaya çıkabilmektedir. Dolayısıyla klasik realist paradigmanın bahsettiği devletlerin güvenliklerini arttırmak adına sürekli bir şekilde silahlanmasının diğer devletleri de bu yöne kanalize etmesi sonucu daha fazla güvensizlik oluşması durumunu güvenlik ikileminden ziyade güvenlik paradoksu olarak düşünmek gerekmektedir (Bilgiç, 2011: 125-130).

Klasik güvenlik ekolünün güvenliği sağlama mekanizması olarak önerdiği başat unsur ise askeri güçtür. Anarşik bir yapıda bulunan uluslararası sistemde, devletler güçleriyle orantılı bir şekilde, ulusal çıkarlarına sahip çıkabilmektedirler. Bu durumda anarşik bir ortamda, devletlerin arasındaki görece hiyerarşiyi sağlayan unsur güç olurken; gücün temel kaynağı ise askeri güç olarak görülmektedir. Bu düşüncenin bir gereği olarak özellikle İkinci Dünya Savaşı'nda ve sonrasında da devletlerin yoğun silahlanma yarışı içerisine girdikleri görülmektedir. Özellikle Soğuk Savaş döneminde her ne kadar sıcak çatışmalara sebebiyet vermediyse de silahlanma yarışının; bir üçüncü dünya savaşına sebebiyet verebilecek duruma geldiği görülmüştür (Uğrasız, 2003: 143-144).

Realizme göre; devletinin çıkarlarını korumak isteyen devlet adamının, kuşku, korku, güvenlik ikilemi, güvensizlik gibi unsurları dikkate alarak hareket etmesi gerekmektedir. Ayrıca güvenlik ikileminin devletleri karşı karşıya getiren bir unsur olduğu dikkate alındığında, düşman olarak görülen devletin güçlenmesinin önlenmesi gerekmektedir. Bunun için güç dengesi mekanizmaları harekete geçirilmelidir. Fakat realist bakış açısına göre sistemde eğer bir hegemon devlet varsa; ona karşı bir güç dengesi oluşturmak da bir hayli zor olacaktır. Tüm bunlar göz önüne alındığında, realizm güvenliğin sağlanması için savaşmayı meşru bir araç olarak ele almaktadır (Çetinkaya, 2012-2013: 247).

Klasik güvenlik yaklaşımına katkı veren bir diğer teori ise neo-realist teoridir. Neo-realist güvenlik yaklaşımı; realist okumaların eleştirildiği bir döneme denk düşmektedir. Neo-realizmde de ulus devletler, uluslararası sistemin temel aktörleri olmakla beraber, diğer devlet dışı aktörlerin de sistemin birer parçası ve etkileyicisi oldukları kabul edilmektedir. Askeri konuların öncelenmesine devam edilmiş, askeri anlamda güç unsurlarının arttırılması gerektiğine yine vurgu yapılmış; bunun yanında ekonomi gibi unsurların da güvenliği sağlama kapasitesi bakımından önemli olduğu kabul edilmiştir (Bakan ve Şahin, 2018: 141-142). Anarşik uluslararası sistemde devletlerin güvenliklerini sağlayamaması halinde beka sorunu yaşayacaklarını ifade eden neo-realist teori; bekayı ise bir devletin en öncelikli amacı olarak görmektedir. Neo-realist paradigmada ekonominin yanında diplomasiyle de çeşitli kazanımlar elde edilebileceği kabul edilmişse de; asıl askeri güç ulusal çıkarların elde edilmesinde önemli ve gerekli görülmüştür (Ağır, 2011; 102).

Klasik güvenlik paradigmasının sac ayaklarını oluşturan klasik realist ve neo-realist paradigma ele alındıktan sonra; klasik güvenlik paradigmasının temel özelliklerini aşağıdaki gibi özetlemek mümkündür:

- Güvenlik, anarşik uluslararası sistemin temel aktörleri olan devletler tarafından sağlanmalıdır.
- Devletlerin uluslararası sistemde rakipleri yine devletler olduğundan; güvenlik tehditleri rakip (düşman) devletlerden kaynaklanmaktadır.
- Uluslararası sistem anarşik bir yapıda olduğu için bir devletin bekasını sağlayabilmesinin tek yolu güçlü olmasından geçmektedir.

- Anarşik uluslararası sistemde hiyerarşi ancak güç yoluyla kurulabilir. Bu durumda devletlerin ulusal çıkarlarını korumalarının tek yolu güçlü olmalarından geçmektedir.
- Bir devletin güçlü olması, askeri anlamda güçlü olmasından geçmektedir. Bu nedenle bir devlet sürekli bir şekilde askeri gücünü arttırmak durumundadır (Arı, 2011: 105-110).

1.1. KLASİK GÜVENLİK PARADİGMASINA GETİRİLEN ELEŞTİRİLER

Güvenlik meselesine daha dar bir açıdan yaklaşan klasik savların, özellikle Soğuk Savaş sonrasında ciddi eleştiriler aldığı görülmüştür. Ulus devletlerin güvenliğini önceleyen klasik yaklaşıma, uluslararası sistemdeki sistemsel ve yapısal değişimlerin ışığında, insani güvenlik, toplumsal güvenlik, çevre güvenliği, gezegenin güvenliği gibi yeni parametreler de eklemlenmeye başlamıştır. Dolayısıyla ulus devlet merkezli geleneksel güvenlik okumalarının tek merkezli olmaktan çıktığı bir döneme girilmiştir. 1970 ve 1980'lerle beraber etkisini göstermeye başlayan eleştirel güvenlik yaklaşımlarının ortaya çıkış sebebi temel olarak klasik güvenlik okumalarının yeni durumu okumakta yetersiz kalması olarak gösterilmiştir. Özellikle ekonomik ve çevresel sorunların artık güvenlik analizlerinde göz ardı edilemeyeceğinin anlaşılması ve ulus-aşırı suç ve terörizm gibi sorunlar yeni durumun geleneksel güvenlik paradigmasıyla anlaşılmasını güçleştirmiştir (Ağır, 2011: 103-104).

İdealizm ve liberalizmin güvenlik anlayışında ise; geleneksel güvenlik yaklaşımının anarşik olarak nitelediği uluslararası ortam; aksine devletlerin bir araya gelerek güvenli bir hale getirebilecekleri bir yapıdadır. Bunun için devletlerin şeffaf ekonomi, barışçıl bir dış politika, ortak güvenlik mekanizmaları kurmaları yeterli olacaktır. Devletlerin sadece kendi çıkarlarını önemseyerek, diğer devletleri düşman görerek güvenlik paradoksuna sürüklenmek yerine; güvenlik tehditlerine karşı birlikte hareket ederek ekonomik ve siyasi iletişimi sürdürmeleri, uluslararası ortamı daha barışçıl ve güvenlikli bir hale getirebilecektir. Bunun için de uluslararası örgüt ve organizasyonlar kurulmalıdır ki dünya barışı kalıcı bir hale getirilebilsin. Ayrıca uluslararası ortamın tek aktörü olarak devletlerin gösterilmesinin eksik bir okuma

yaratacağını ileri sürmektedirler. Buna göre devlet dışı aktörler de analize dâhil edilmelidir ki bunların arasında bireyler, baskı ve çıkar grupları, medya ve bürokrasi sayılabilir. Ayrıca uluslararası ortamda sert-askeri güç unsurları kullanmak yerine yumuşak güç araçları kullanılmalıdır (Bakan ve Şahin, 2018: 142-143).

Klasik güvenlik paradigmasını eleştiren bir diğer yaklaşım ise Uluslararası İlişkiler disiplinindeki özellikle İkinci Dünya Savaşından sonra yer alan İngiliz Okulu Kuramı olmuştur (Demirel, 2017: 47). Her ne kadar İngiliz Okulu da realistler gibi uluslararası sistemin temel aktörlerinin devletler olduğu ve uluslararası sistemin anarşik bir yapı sergilediği fikrini benimsemişlerse de bilhassa anarşinin anlaşılması noktasında bir farklılaşma söz konusu olmuştur. Keza İngiliz Okulu temsilcilerine göre anarşi devletlerin üstünde bir gücün olmaması, güçleri oranında bir hiyerarşinin olması tezlerini savunan realist paradigmanın aksine sadece ortak bir hükümetin olmaması durumunu ifade etmektedir (Devlen ve Özdamar, Bahar 2010: 47-50).

İngiliz Okulu'na göre; uluslararası sistemdeki anarşik yapı devletlerin birbirlerini sürekli bir şekilde tehdit ettikleri, güç ikilemlerine yol açan, çatışmaya elverir bir mahiyet taşımamaktadır. İngiliz Okulu'nun uluslararası toplum fikri de önem kazanmaktadır ki buna göre uluslararası toplumu oluşturan yegâne aktörler devletler değildir. Devletlerin yanında bağımsız siyasi toplumların da olduğu bir yapı sergilemektedir. Bu da özellikle klasik realizmin devlet odaklı yaklaşımına bir eleştiri olarak ortaya çıkmaktadır. Ayrıca uluslararası sistemde istikrarı ve güvenliği sağlamak için güç ilişkilerini değil bürokrasiyi öne çıkarması bakımında İngiliz Okulu'nun geleneksel güvenlik yaklaşımından ayrıldığı görülmektedir. İngiliz Okulu'na göre güvenliğin kurulması ve işletilmesinde uluslararası paktlar ve kurumlar önemli rol oynamaktadır. Ayrıca uluslararası ticaretin geliştirilmesi gerektiği fikri, kültürel ve hümanist etkileşimin yaygınlaştırılması önerileri de uluslararası sistemde çatışma ve güvenlik risklerinin azaltılmasında önemli parametreler olarak ortaya çıkmaktadır (Ağkaya, 2016: 1079-1085).

Feminizmin de klasik güvenlik anlayışına getirdiği eleştiriler önem arz etmektedir. Feministler; klasik güvenlik anlayışının devlet esaslı, militarizmi önceleyen ve bu haliyle yapısal sorunlara gark olan yapısını eleştirmişler; bu anlamda eleştirel güvenliğe katkı sağlamışlardır. Feministlere göre; devletin başat aktör olarak görülmesi doğrudan askeri unsurları ön plana çıkarmakta, bu da

sistemsel bir şekilde savaşı beraberinde getirmektedir. Savaşın hâkim olduğu bu devrede insan unsuru geri planda kalmakta, insan kayıpları ve insan hakları ihlalleri yoğunlaşmaktadır. Bu fikirden yola çıkan feminizm; özellikle savaş aşamasında kadınların dezavantajlı bir duruma geldiklerini ileri sürmektedirler. Çünkü savaş ve onun sürdürücüleri olan militarist yapılanmalar, yapıları itibariyle kadını baştan dışarıda bırakmaktadırlar. Savaşın ortaya çıkardığı şiddetin kadını olumsuz etkilediğini ortaya koyan feminist düşünce, diğer taraftan şiddetin yapısal bir mesele olduğunu da iddia etmektedir. Buna göre; şiddetin yapısal olarak var olması, savaş dışında da kadını hem ekonomik, hem kültürel hem de hukuksal olarak sistemin zayıf noktası haline getirmektedir. Tüm bu saptamalar feminizmi devlet odaklı yaklaşımları reddeden bir hale getirerek, insan odaklı bir yapılanma önermeye itmektedir. Böylece klasik güvenlik anlayışının devlet merkezli yapısına feminizm en başta karşı çıkmakta, onu eleştirmektedir (Tür ve Aydıncı, 2014: 229-230).

Klasik güvenlik yaklaşımını eleştiren ve güvenliğe farklı bir yaklaşım gösteren diğer ekoller; Eleştirel Güvenlik Çalışmaları olarak ele alınmaktadır ve ekseriyetle 1995 ve sonrası dönemi kapsamaktadır. Krause ve Williams'ın derledikleri 1997 tarihli Critical Security Studies: Concept and Cases isimli kitapla ortaya konan ve Soğuk Savaş sonrası dönemde güvenliğe eleştirel yaklaşım gösteren yazarların (Buzan, Waever, Booth, Ayoob, Walker ve Erikkson vs) düşünceleri etrafında güvenlik paradigmasına yeni bir soluk getirildiği görülmüştür. Eleştirel Güvenlik Çalışmaları da temelde devlet odaklı olmayan bir yaklaşım sergilemiştir. Klasik güvenlik paradigmasına aktör, sınırlılıklar ve seviye bazında eleştiriler getirilmektedir. Buna göre, güvenlik aktör bazında devlet odaklı olarak ele alınmamalı uluslararası kurumlar, çıkar grupları, sivil toplum kuruluşları, bireyler, hükümet dışı aktörler de dikkate alınarak bir analiz oluşturulmalıdır. Ayrıca güvenlik dar bir bakış açısının sonucu olarak ulusal sınırlarla ele alınmayıp, küresel, bireysel ve uluslararası güvenlik de analize dâhil edilmelidir. Klasik güvenlik anlayışına bir diğer eleştiri ise güvenliğin askeri tehdit odaklı olarak ele alınmasında görülmektedir. Eleştirel Güvenlik Çalışmaları; çevre, ekonomi, politika ve toplumsal özellikteki tehditlerin de dikkate alınması gerektiğini vurgulamaktadır (Bakan, 2007: 41-42).

Klasik güvenlik anlayışını askeri odaklı olmasına, içeriğinin daraltılmasına karşı çıkan bir diğer okul ise Kopenhag Okulu olmuştur. Kopenhag Okulu'nun en

önemli temsilcilerinden biri olan Barry Buzan özellikle klasikleri, askeri odaklı olmakla eleştirdiği ‘’Halklar, Devletler ve Korku’’ isimli kitabında bu durumu öne çıkarmıştır. Kopenhag Okulu daha çoğulcu ve yapısalcı bir güvenlik anlayışı ortaya koymuştur. Barry Buzan dar kapsamlı güvenlik tanımlamasının yerine; ekonomik, politik, çevresel, sosyal ve askeri unsurların beraber ele alındığı daha geniş bir güvenlik yaklaşımından yana durmuştur. Kopenhag Okulu'na göre askeri anlamda güvenlik kabiliyetleri elbette önemlidir ama diğer unsurlarla desteklenmezse etkili bir güvenlik politikasından söz edilemez. Güvenliği askeri, ekonomi, siyaset, politika ve çevre olmak üzere sektörel bir ayrıma tabi tutulduğu görülmektedir. Kopenhag Okulu'nun temsilcilerinden Ola Waever'e göre sektörler, güvenlikleştirme ve bölgesel güvenlik; Okul 'un üzerinde temellendiği asıl parametreleri teşkil etmektedir (Küçüksolak, 2012: 204-206).

Kopenhag Okulunun bölgesel güvenlik kompleksi yaklaşımının da esasında geleneksel güvenlik teorisine bir eleştiri içerdiğini belirtmek gerekir. Her ne kadar Buzan; güvenliğin sadece bölgesel olarak değil küresel olarak ele alınması gerektiğini daha sonra belirtmişse de önceleri Kopenhag Okulu içerisinde bölgesel güvenlik temelinde coğrafi bir kıstasın göreceli olarak baz alındığı söylenebilir. Buna göre; birbirlerine yakın olan devletlerin, coğrafi olarak aynı bölgede bulunmalarından dolayı; güvenlik yönünden birbirleriyle etkileşimleri ve bağımlılıkları daha fazla olmaktadır (Baysal ve Lüleci, 2015: 73-74). Bu nedenle klasik güvenlik paradigmasının ele aldığı gibi ulusal sınırlarla saptanmış bir müdafaa değil, bölgesel bir bakış açısı ve bu minvalde bir müdafaa öngörmek gerekecektir.

Kopenhag Okulu'nun güvenlikleştirme düşüncesi, hem geleneksel güvenlik anlayışına bir eleştiri getirmekte ve hem de güvenlik paradigmasına özgün bir anlam katarak onu genişletmekte ve derinleştirmektedir. Klasik güvenlik paradigmasında, güvenlik tehditleri askeri ve sınırsal (ulusal) bir anlam ifade ederken, bir konunun güvenlik alanına nasıl girdiği konusunda ise tatmin edici cevaplar verir nitelikte olmamaktadır. Kopenhag Okulu'nun güvenlikleştirme yaklaşımı ise bu soruya eğilmekte ve toplumsal bir meselenin önce nasıl siyasal bir konuya oradan da güvenliği ilgilendirir bir güvenlik tehdidine dönüştüğüne eğilmektedir (Miş, 2011: 348). Buna göre; bir konu hükümet tarafından siyasi bir tercih olarak bir beka sorunu gibi gösterilip, daha sonra dil biliminin (hitabetin) de yardımıyla toplum da

ikna edilerek güvenlik alanına taşınmaktadır (McDonald, 2008: 563-587). Örneğin insanların dini inançları gereği başörtüsü takmaları İslam ülkelerinde yaygın bir durum iken, Türkiye'de başörtüsü takılmasının devlet kurumlarında laiklik ilkesine aykırı olarak değerlendirilmesi; esasında toplumsal bir meselenin nasıl siyasallaşıp sonrasında güvenlik tehdidine dönüştürülmesine iyi bir örnek teşkil etmektedir (Tok, 2009: 113-137). Görüldüğü üzere klasik paradigmada kesinlikle bir güvenlik tehdidi olarak algılanmayacak böylesi bir mesele Kopenhag Okulu'nda bir güvenlik tehdidi olarak dikkate alınmaktadır.

Eleştirel Güvenlik Çalışmalarında, güvenlik üzerine fikir beyan eden ve burada klasik güvenlik temsilcileriyle farklılıklar ortaya koyan bir diğer ekol ise Galler/Aberyswyth ekolüdür. Ortaya çıkış ve gelişim aşamaları Soğuk Savaş sonrası döneme rastlayan bu ekol Ken Booth, Richard Wyn Jones, Andrew Linklater, Keith Krause ve Michael Williams gibi temsilcileriyle Aberyswythh Üniversitesi'nde, eleştirel güvenlik çalışmalarını geliştirmişlerdir. Diğer güvenlik yaklaşımlarından ayrılan yönü ise; güvenliği özgürleşme bağlamında ele almasıdır (Birdişli, 2014: 243-245). Klasik güvenlik yaklaşımı; güvenliğin sağlanmasının temel koşulunun devlet ve düzen olduğu fikrini savunurken; bunun için insanları siyasal, toplumsal, ekonomik, fiziki ve diğer alanlarda çeşitli sınırlamalara tabi tutmayı önermektedir. Galler Okulu ise aksine güvenliğin sağlanabilmesinin önündeki engellerin temelde bu sınırlamalar olduğu savunmaktadır ve çözüm olarak ise insanların bu sınırlamalardan azade edilerek özgürleştirilmesini sunmaktadır. Buna göre; güvenliği sağlamanın yolu güç ve düzenden değil özgürleşme ortamının sağlanmasından geçmektedir (Kolasi, 2014: 138-147).

1.2. YENİ GÜVENLİK: YENİ TEHDİTLER

Klasik güvenlik yaklaşımının tehditleri çok dar bir açıdan yorumlaması ve askeri tehditler dışındaki tehditleri gündemine almaması, en çok eleştirilen yönü olmuştur. Buna paralel olarak ortaya konulan eleştirilerin dikkate alınmasıyla; enerji, çevre, ekonomi, iklim değişiklikleri gibi konular da güvenliğe dâhil edilmiştir (Edwards, 2007: s. 21-24). Diğer taraftan bu çeşitliliğe ek olarak yeni tehditler de ortaya çıkmıştır. Küresel ısınma, göç, nüfus artışı, dini ve etnik çatışmalar, gelir eşitsizliği, küresel terörizm, insan kaçakçılığı bunlardan bazılarıdır (Çıkrıkçı, 2017: 216-224). Sayılan tehditlere karşı savunma mekanizmaları oluşturmak; devletlerin

tek başlarına üstesinden gelemeyecekleri bir duruma evirilmiştir ki bunda küreselleşmenin yaratmış olduğu şeffaf yapılar, sınırların geçişkenliği ve teknolojik imkânların artmasının etkisi büyük olmuştur. Bu paralelde devletlerin nispeten bir güvenlik tehdidi olarak algılamada geç kaldıkları siber alan da yeni güvenlik yaklaşımlarında ele alınması gereken önemli bir parametre olarak belirmiştir (Yılmaz: 2017: 23-27).

Güvenlik tehditlerini sınıflandıran birçok farklı yaklaşım olmasına karşın temelde bunları; siyasi, ekonomik, toplumsal ve çevresel tehditler olarak ele almak mümkündür. Bir devletin iç siyasal yapısının demokratik olmaması, siyaseten istikrarsız bir yapı sunması, insan hakları ihlalleri, ırkçılık, ülke içerisinde cereyan eden şiddet olayları, aşırı milliyetçilik akımları, terör gibi tehditleri siyasi tehditler olarak değerlendirmek mümkündür. Fakirlik ve yoksulluğun tabanda genişlemesi, gelir dağılımında üst gruplarla alt gruplar arasındaki farkın artması, kara para aklama, yasadışı ekonominin yaygınlaşması, pazarlara ulaşma sorunları, az gelişmiş ülkelere karşı yapılan ekonomiyi sabote edici müdahaleler ve bütün bunların tetiklediği toplumsal olaylar ise ekonomik tehditler olarak ele alınmaktadır. Ayrıca küresel ekolojik değişimler, hava ve suyun kirletilmesi, dünya kaynaklarının hızla tüketilmesi, temiz su kaynaklarının azalması ve bu yöndeki insan müdahaleleri ise çevresel tehditler olarak ortaya çıkmaktadır. Son olarak toplumsal tehditlerden de bahsetmek gerekmektedir. Etnik ve dini mezheplere bağlı olarak gelişen çatışmalar, azınlık-çoğunluk çatışmaları, uluslararası uyuşturucu ticareti, kitlesel göç hareketleri, kitle imha silahlarının denetlenemeyecek düzeyde yaygınlaşması ve bulaşıcı hastalıklar gibi tehditler de toplumsal tehditler olarak ortaya çıkmaktadır (Aksu ve Turhan, 2012: 73).

Siyasi tehditlerden içerisinde etkisini en fazla hissettiren ise küresel terörizm olmuştur. Günümüzde güvenliğin en büyük tehdit edicilerinden biri olan küresel terörizm; her geçen gün tırmanmış ve önü alınması zor bir merhaleye erişmiştir. Özellikle 11 Eylül 2001 tarihinde ABD'ye yönelik yapılan terörist ataklar, terörist tehditlerin tek bir bölgeyle sınırlı kalan eylemler olarak kalmadığını, uluslararası sistemi ve düzeni tehdit edebilecek sonuçlar doğurabileceğini göstermiştir (Gloannec, Irondelle ve Cadier, 2013: 7-9). Buradan yola çıkarak ABD özelinde ve diğer devletleri de kapsayan bir netice ortaya çıkmaktadır ki; küresel terörizmle baş

etmenin yolu; ulusal (klasik) güvenlikten değil; topyekûn bir mücadeleden geçmektedir. Aksi takdirde bu tarz terörist tehditlerine karşı her ülke –hatta süper güç ABD bile- güvensiz bir durumla karşı karşıya kalabilmektedir. Küreselleşme süreciyle beraber terörizmin asimetrik bir tehdit olarak ortaya çıktığı görülmektedir. Keza küreselleşmeyle farklı ülkelerde ve bazen de aynı ülkede olmak üzere toplumlar arasında dengesiz bir durum ortaya çıkmıştır. Çünkü ülkeler arasında, küreselleşmenin bir etkisi olarak adil olmayan bir ekonomik dağılım söz konusu olmuştur. Bu ekonomik adaletsizlik de toplumlar arasında gerginlikler oluşturmakta, yoksul ve fakirleri marjinalize ederek, bu grupların farklı siyasi yönelimlere ve hatta terörizme kanalize olmalarına neden olmaktadır. Küresel terörizm de beraberinde göçmen kaçakçılığı, insan ticareti ve kara para aklama gibi yeni tehditleri getirmekte, bunları beslemektedir (Aksu ve Turhan, 2012: 71).

Ekonomik tehditlerin de bir ülkenin güvenliğinde oldukça derin sonuçlara sebebiyet verdiği ortaya konmaktadır. Ekonominin devletleri karşılıklı olarak birbirlerine muhtaç hale getirdiği göz önüne alındığında; bir ülkedeki durumun diğer pek çok ülkeyi ilgilendirir hale geldiği görülmektedir. Küreselleşme fenomeni şüphesiz devletler için birçok fayda sağlamakla beraber, yeni tehditlerin de önünü açmış, tehditlerin çeşitlenmesine sebep olmuştur. Serbest piyasa şartlarının hâkim olduğu yeni düzende, korumacılığın ve sınırların ortadan kalkmasıyla devletlerin ekonomileri yeni aktörlere ve müdahalelere açık bir duruma gelmiştir. Böylece hem sermaye hem mallar ve hem de nispeten işgücünün serbestiyeti sağlanmıştır (Erdoğan, 2013: 272). Bu durum, gelişmemiş ülkelerden gelişmiş ülkelere işçi ve beyin göçünün önünü açarken, kalifiye göç alan ülkeleri, göç veren ülkelere nazaran çok daha güçlü kılmaktadır. Ayrıca piyasanın büyük paydaşları olan ülkeler, diğer ülkeleri ekonomik olarak tehdit edebilmekte, onlara ekonomik ambargolar dayatabilmektedirler. Bu nedenle bir devletin askeri güvenliğini sağlamasının yanında, ekonomik olarak varlığını sürdürebileceği, ekonomik imkânlara ulaşabileceği bir durumda olması da elzemdir.

Güvenlik okumalarının dikkate alması gereken bir diğer unsur ise çevre olarak gösterilmektedir. Keza geleneksel güvenlik paradigması; tehditleri askeri kanatla sınırlı tutmuş, çevresel tehditlerin devletlere sorun çıkaracak sevide görmemiştir. Oysa çevresel tehditler de sonuçları itibariyle siyasi istikrarsızlıklara

neden olabilmekte, ulusal ve uluslararası güvenlik açısından kritik olabilmektedir (Kaypak, 2012, 11). Buna göre; çevresel etmenlerin insan güvenliğine bir tehdit oluşturması durumunda, çevresel bozulmaların devletlerin siyasal süreçlerine etki etmesi durumunda, nükleer denemelerin diğer devletlere yönelik olarak çevresel sorunlar çıkarması ve yahut bu durumlardan birinin çevresel göçe sebep olması durumunda; çevrenin bir güvenlik tehdidi olarak belirdiği görülmektedir. Esasen 1987 tarihli Ortak Geleceğimiz Raporu, BM Dünya Çevre ve Kalkınma Komisyonunca hazırlanarak hükümet ve uluslararası örgütlerin gündemine alınmış olması da çevrenin ne derece mühim bir mesele olduğunu ortaya koymaktadır (Özkan, 2016: 135-137). Çevresel bir güvenlik halinin var olabilmesi için; ekolojik denge korunmalı, çevre ile ilgili devletler arasında işbirliği sağlanmalı, çevre kaynaklı çatışmalar önlenmeli, askeri faaliyetlerin çevreye yaptıkları, yapabilecekleri zararlar saptanarak önlem alınmalı, yoksulluk azaltılarak çevresel göçlere neden olabilecek durumlardan kaçınılmalıdır (Vural, 2018: 32-35). Anlaşıldığı üzere; çevre faktörü ele alınmadan bir güvenlik durumundan bahsetmek mümkün olamamaktadır. Bu nedenle çevresel tehditlerin de göz önüne alınması yeni güvenlik anlayışı için elzem kabul edilmektedir.

Toplumsal tehditler de güvenliğin sağlanmasında göz önüne alınması gereken önemli bir parametreyi teşkil etmektedir. Toplumsal güvenlikte öne çıkan kavram kimlik olmaktadır. Devletler çeşitli sınırlara sahipken, toplumlar bundan azade bir süreklilik gösterebilmekte, aynı anda birçok ayrı devlette aynı toplum ve onun fertleri bulunabilmektedir. Diğer taraftan aynı devlet içerisinde birden çok farklı toplumsal gruplar da bulunabilmektedir. Bu farklı toplumsal gruplar ise kendilerini etnik, kültürel, dini vs. farklı kimliklerle tanımlayabilmektedirler (Waewer, 2008: 155). Tam da bu noktada tehditler de baş göstermektedir ki devlet politikaları veya bu kimliklerin devletlere olan yaklaşımları güvenliği tehdit edecek riskler taşıyabilmektedir. Özellikle Soğuk Savaş döneminde birçok etnik ve dini çatışmanın yaşanmış olması; toplumsal özellik gösteren bu tehditlerin de güvenliğin sağlanmasında dikkate alınmaları gerektiğini ortaya koymuşlardır. Çünkü her ne kadar bir devlet iç egemenlik anlayışı gereği, kendi içindeki toplum için tek söz sahibi (Özman, 1964: 59) konumundaysa da artık bu tez de nispeten geçerliliğini yitirmektedir. Keza bir devletin içerdeki halklara yönelik uygulamalarını referans göstererek müdahalelere girişildiği son yüzyılda sıklıkla görülmüştür.

Toplumsal tehdit olarak algılanabilecek bir diğer unsur ise göçtür. Kendi ülkelerindeki siyasi, sosyal ve diğer sebeplerden ötürü bir ülkeden bir diğer ülkeye yerleşmek amacıyla yer değiştirme (Sayın, Usanmaz ve Aslangiri, 2016: 2) durumu olan göç, göç alan ülke adına çeşitli riskleri ve tehlikeleri de barındırmaktadır. Keza göç edilen ülkenin ekonomisi göçü kaldırabilecek durumda olmayabilmekte ve yahut göç eden insanların sisteme kolayca dâhil edilebilmeleri zaman alabilmektedir. Bir diğer tehlike ise yabancı düşmanlığının çok olduğu ülkelerde; göç karşıtı propagandalar yapılabilmekte, bu durum da hükümetleri zor duruma sokmaktadırlar. Ayrıca göç durumlarında, göç eden insan profili dikkatli bir şekilde incelenemezse kriminal suçluların da ülkeye girişlerinin önü alınamamaktadır. Böylece göç; ekonomik, sosyal, siyasi ve güvenlik bakımından dikkat edilmesi gereken bir parametre olarak ortaya çıkmaktadır.

Bir diğer toplumsal güvenliği tehdit eden unsur; kitle imha silahlarının yayılmasıdır. Soğuk Savaş ve sonrası dönemde büyük güçlerin yanında diğer küçük devletlerin de güvenliklerini sağlamak adına bu tür silahlar satın aldıkları ve yahut onları üretmeye çabaladıkları görülmektedir. Bu durum da şüphesiz insanlar adına tehlikeli bir tırmanışın ve kaçınılmaz bir sonun habercisi olmaktadır. Keza nükleer silahlar ve diğer kimyasal silahlarla insanlar ve onların yaşadıkları tabiat yok edilmekte, geri dönülmesi zor tahribatlara neden olunmaktadır (Doğanalp, 2016: 25-26). Diğer taraftan salgın hastalıklar, uluslararası uyuşturucu ticareti, aşırı nüfus gibi parametreler de yine toplumsal güvenlik bağlamında yeni güvenlik okumalarınca dikkate alınan unsurlar olarak belirmektedir.

Son olarak güvenlik paradigmasının askeri odaklı ve bu nedenle sınırlı çehresi, yeni güvenlik okumaları ve eleştirileriyle, içine yeni konuları ve yaklaşımları da dâhil ederek genişlemiş, güvenlik meselesine yeni boyutlar kazandırılmıştır. Yine de güvenlik ve ele alınış biçimleriyle ilgili tartışmalar devam etmektedir. Genişleyen tehdit skalasında son zamanlarda yeni bir unsur daha öne çıkmaktadır ki bu da siber tehdittir. Dolayısıyla yeni bir meydan okuma olarak ortaya çıkan siber alan; her ne kadar devletler tarafından nispeten geç idrak edilmişse de güvenlik okumalarına dâhil edilmiştir.

İKİNCİ BÖLÜM

SİBER GÜVENLİK VE İLGİLİ KAVRAMLAR

2. SİBER ALANIN GÜVENLİK OKUMALARINA DÂHİL OLMASI

Güvende hissetme ihtiyacı içerisinde olan insan, toplum ve devlet gibi yapılar, tehditlerin ortaya çıkış durumlarına göre çeşitli önlem ve mekanizmalar geliştirmiş, güvende olma durumunu sağlama adına birçok adım atmıştır. Fakat zamanın sürekli olarak yeni meydan okumalar ve değişimleri de beraberinde getiren yapısı, tehditleri daha da çeşitlendirmiş, güvenliği sürekli olarak güncellenmesi ve yeniden ele alınması gereken bir fenomen haline getirmiştir. Kısacası siyaset, toplum, kültür ve teknolojideki değişimleri statik bir güvenlik okumasıyla değerlendirmek; dinamik bir seyir gösteren zamanı ve onun getirdikleri yenilikleri, değişimleri ve dolayısıyla oluşabilecek fırsat ve tehditleri anlamak için yeterli olmamaktadır. Buradan yola çıkarak, 1990'lı yıllardan başlayarak 2000'li yıllarda da hızını arttıran bilgi iletişim teknolojilerindeki gelişim, dünya geneline yayılmış; birçok özel ve kamu hizmetinin elektronik ortamda verilebilir hale gelmesini sağlamıştır. Şüphesiz hayatı kolaylaştıran bu yeni ortam; diğer taraftan da çeşitli tehditleri beraberinde getirmiştir ki bu noktada siber güvenlik meselesinin de artık güvenlik okumalarında dikkat edilmesi gereken bir parametreye evirilmesine şahit olunmuştur (Ünver ve Canbay, 2010: 94).

Bilgi iletişim sistemlerinin 20. yüzyılın sonlarındaki gelişiminde internet en önemli rolü üstlenmiştir. Günümüzde dünya nüfusunun büyük bir çoğunluğu internet kullanmaktadır. Dünya nüfusu 2018 yılı itibariyle 7 milyar 593 milyon iken, 2018 yılı itibariyle internet kullanan insan sayısı 4 milyar 21 milyon olarak belirlenmiştir (Wearesocial Special Report, 2018). İnternetin ortaya çıkışındaki ilk hedef bilgi paylaşmak olmuşsa da yaratılan yeni altyapı sistemleriyle birbirlerine entegre hale getirilen bilişim sistemleri, küreselleşmenin de etkisiyle ekonomiden siyasete,

kültürden güvenliğe kadar birçok alanda etkileşim yaratılmasını sağlamıştır. Bilgi iletişim sistemleri ve internetin bu denli yaygınlaşacağı, insanların sisteme müdahale ederek çeşitli güvenlik ihlalleri ve tehditleri meydana getirebilecekleri öngörülemediğinden; siber alanın güvenlik tarafı önceleri yeterince idrak edilememiş ve geri planda kalmıştır (Yılmaz, Ulus ve Gönen, 2015: 134).

Güvenliğin yeni boyutuyla ele aldığımızda, siber tehlike sadece devlete yönelik değil, birey ve şirketlere yönelik de gerçekleşmektedir. Çünkü kişisel, kurumsal ve kamusal hayat dijitalleşerek online bir seviyeye ulaştırılmıştır. Öyle ki bilgi sistemlerine entegre hale gelmiş olan 21. yy insanı, iletişim kanallarını hemen hemen maliyetsiz, daha hızlı, özgür ve mekandan bağımsız olarak gerçekleştirirken diğer taraftan da sistem üzerinden yapılan-yapılabilecek tehditlere de açık hale gelmektedir. Siber ataklarla, bilgi iletişim kanallarındaki bilgilerin ele geçirilmesi, bu bilgilerle kişinin ekonomik ve sosyal açıdan zarara uğratılması mümkün ve nispeten kolay olmaktadır. Diğer taraftan şirketler ekonomik olarak büyük zararlara uğratılabilmektedir. Özellikle gelişmiş ülkelerde özel sektör, banka hizmetleri, çeşitli devlet hizmetleri, büyük şirketler ve bankalar siber tehditlerin ana hedefi olmaktadırlar. Bu sistemlere yapılan siber saldırılar ile milyon dolarlarca zarara sebep olunabilmektedir. Ayrıca sistem açıklarından faydalanan siber saldırganlar, arkalarında çok da bir iz bırakmadan, az bir riskle bu faaliyetlere girişebilmektedirler (Özgöker ve Yılmaz, 2014: 7-9).

Devletler özelinde de siber saldırılar oldukça yıpratıcı ve geri dönülemez zararlara sebebiyet verebilmektedir. Bir ülkenin kritik altyapılarına yapılacak saldırılar, o ülkede yaşamı oldukça zora sokabilmekte, hükümetlere yönelik siyasi sonuçlara bile yol açabilmektedir. Elektrik üretim ve dağıtım sistemleri, petrol ve gaz sistemleri ile fabrikalar, telekomünikasyon altyapıları, barajlar, e-devlet sistemi, ulusal savunma sistemleri ve yine ulusal finans sistemleri teknoloji ve bilgi sistemleriyle bütünleşmiş bir durumda bulunduklarından, bu gibi kritik altyapılara yapılacak saldırıların sonuçları can ve mal kayıplarına yol açabilecek bir hal alabilmektedir. Bu tarz sızmalarla şüphesiz bir devletin savunma planları, silah yazılımları ve envanterleri kolaylıkla ele geçirilebilmektedir Yine devlet arşivlerinden de çeşitli sızmalar elde edilerek, bunların güvenliği tehdit edebilecek

şekilde kullanılmasının önünde bir engel kalmamaktadır (Öğün ve Kaya, 2013: 162-163).

Siber tehditlerin bir diğer yönü de, bu tehditlerin devletlerin yanında devlet dışı aktörler tarafından da gerçekleştiriliyor olmasıdır. Yani, geleneksel güvenlik yaklaşımının yetersiz olduğu bu noktada da ortaya çıkmaktadır. Çünkü 21.yüzyılda devletler, bilgi teknolojilerini ele geçiren ve burada hâkim olan tek aktör değildir; kişiler, şirketler de bu alanda yeterli bilgi ve donanıma sahip olabilmektedirler (Karagül ve Özkan, 2015: 115-116). Keza siber tehditlerin birçoğu devletten devlete değil, devlet dışı aktörlerden devletlere yönelik olmaktadırlar. Burada amaçlar ise çeşitlenmektedir; hackerler ve hacker grupları ekonomik, siyasi nedenlerle, protesto amaçlı gruplar seslerini duyurmak amacıyla, suç örgütleri haksız ve kolay kazanç elde etme gibi amaçlarla siber alanda faaliyet gösterebilmektedirler (Korhan, 2017: 83-84). Bireyler, şirketler, hacker grupları gibi devlet dışı aktörler, devletlere nazaran siber alanı daha önce keşfetmişlerdir. Devletlerin nispeten bu alana dikkat göstermelerinin gecikmesinin altındaki temel düşünce; burayı güvenlik sorunları çıkarabilecek bir alan olarak görmemelerinden kaynaklanmaktadır. Bu bilgi ışığında, devletlerin alandaki ilk adımlarının siber saldırıların yıpratıcı etkileri görüldükten sonra gerçekleşmesi anlaşılır olmaktadır (Tarhan, 2017: 110).

1982 yılında Sibirya'da meydana gelen devasa patlamanın, doğalgaz boru hatlarına yapılan siber saldırılar neticesinde meydana geldiği daha sonra anlaşılmıştır. Olayın perde arkasında; Sovyetlerin ABD'nin ambargolarını aşmak adına Kanada'da bir şirketin boru hatları sistemlerini ele geçirmesi vardır. Sistemi bütünüyle ele geçirdiğini düşünen Rusya, ABD'nin (CIA) bu girişimi fark ettiğini tespit edememiştir. ''Logic Bomb'' adlı bir nevi saatli bomba özelliği gösteren bir çip kullanan ABD'nin, bunu Rusya'nın ele geçirdiği yazılımlara yerleştirdiği iddia edilmiştir. Neticede ortaya çıkan patlama, bu güne kadar uzaydan görülen en büyük patlama olarak tarihe geçmiştir (Roscini, 2014: 1-5). Bu olaya misilleme olarak kabul edilebilecek bir diğer olay ise Ay Işığı Labirenti olayıdır. Burada da ABD'nin kritik altyapılarına yönelik gerçekleştirilen siber ataklarla, ABD'nin son derece gizli olarak yürüttüğü birçok araştırma-geliştirme projeleri ele geçirilmiştir. Olayın arkasında Rusya'nın olduğu, ABD tarafından gerçekleştirilen teknik takipler neticesinde ortaya çıkmıştır. Söz konusu teknik takip ve siber istihbarat toplama işlemlerini

gerçekleştiren Pentagon ve FBI'ya göre Rusya Federasyonu'nun yönlendirmesiyle gerçekleştirilen bu operasyonda Savunma Bakanlığı, Enerji Bakanlığı, NASA, savunma sanayi ve savunma sanayisiyle çalışan üniversiteler dahi hedef alınmıştır (Schaap, 2009: 139-141). Bunların dışında Kosova Krizi döneminde NATO'ya gerçekleştirilen saldırılar, 2007 yılında Estonya'ya yapılan siber saldırılar, Gürcistan'a gerçekleştirilen siber saldırılar, Wikileaks adı verilen siber saldırılar vs. dikkate alındığında devletlerin bu alanı güven altına alma girişimlerine başvurmaları gerektiğini ortaya koymuştur (Yılmaz, 2017: 33-38).

Sonuç olarak gerek AB ülkeleri, gerek BM ve NATO öncülüğünde siber alanı düzenleyecek, siber tehditlere önlem alacak mekanizmalar ve işbirlikleri oluşturma adımları atılmıştır. Böylece güvenlik okumalarına yeni bir parametre olarak siber alan, devletlerce yeni hâkimiyet kurma alanı olarak ortaya çıkmıştır.

2.1. SİBER VE SİBER UZAY/ALAN

Güvenlik okumalarına dahiliyeti gecikmiş olsa da siber güvenlik ve ona ilintili kavramlar, çağımızda oldukça sık kullanılmakta, internet ve teknolojiyle beraber hayatımızın hemen hemen her alanında karşılaştığımız kavramlar olmaktadırlar. Siber kelimesinin ilk kullanımına Norbert Wiener'in ''Cybernetics: or Control and Communication in the Animal and the Machine'' adlı eserinde rastlanmaktadır (Wiener, 1948: s. 30-180). Bu eserde insanın makinelerle iletişime geçerek alternatif bir ortam yaratabileceği fikri işlenmektedir. Siber kelimesinin Oxford sözlükteki anlamına bakıldığında; bilgisayarlar, bilgi sistemleriyle bağlantılı ve bu iklimin doğal bir parçası anlamında tanımlandığı görülmektedir.

Siber uzay/alan terimi ise ilk defa William Gibson tarafından bir bilimkurgu eser olan Neuromancer adlı romanda 1948 yılında kullanılmıştır. İlk defa bir bilimkurgu romanda kullanılan siber uzay; sonraları akademik anlamda da sıkça referans verilen bir terim haline gelmiştir (Yayla, 2013: 180). Teknolojinin insan hayatının her alanına nüfuz etmesi, siber alana merakı da arttırmış, çeşitli siber uzay tanımlamalarının yapılmasına vesile olmuştur. Bu tanımların birinde siber uzay ABD Savunma Bakanlığı'nca; yüzbinlerce bilgisayarın, sunucunun, yönlendirici ve fiber optik ağların oluşturduğu bir kompozisyon olarak tanımlanmıştır (United States of America Departmant of Defence, 2015).

Fiziksel bir özellik göstermemekle beraber, bilişim sistemleri aracılığıyla insanların birbirleriyle iletişime geçtikleri alan şeklindeki tanımlama diğer siber uzay tanımlamalarına göre daha yaygın bir kabul almaktadır (Önaçan ve Atan, 2016: 14). Fakat burada da itiraz, siber alanın sadece internet alanıyla sınırlandırılması noktasında yoğunlaşmaktadır. Çünkü e-devlet uygulamalarından savunma sanayilerine, ticari alanlardan enerji altyapılarına ve hemen hemen hayatın diğer tüm alanlarında gerçekleşen işlem ve bilgiler siber alanda tezahür etmektedir. Bir diğer yaklaşıma göre; siber alanı optik ağlarla, bilgisayar sistemleriyle, internet altyapılarıyla sınırlandırmak onu konusu yönünden de eksik ele almak anlamına gelmektedir. Çünkü siber alan bir yönüyle de farklı uyruktan insanların, vatandaşların, farklı cinsiyetlerin, dinlerin ve dillerin bir araya geldikleri, etkileşim kurdukları kamusal bir alana tekabül etmektedir ki bu da ona kültürel bir katmanı da ilave etmektedir (Yılmaz, 2017: 87-89). Dolayısıyla siber alana yönelik birçok farklı tanım yapmak ve ona kültürel, siyasi, ekonomik, askeri yaklaşımlar sunmak mümkün olmakla beraber yapılan her tanımlama bazı yönleriyle eksik kalmaktadır. Fakat geliştirilen her yeni tanım da bir öncekinin eksiğini gidermekte ve siber alanın ne olduğunun anlaşılmasında yardımcı birer parametre sunmaktadır. Çalışmanın amacına uygun olarak siber uzay ve yahut siber alan; esasen teknolojinin gelişmesi ve bilgi iletişim teknolojilerindeki paralel ilerlemeyle mekânsal sınırlamaların zayıfladığı, iletişim ve etkileşimin zamansal anlamda çok fazla sürat kazandığı bir durumun oluşturduğu yeni mecra olarak ele alınacaktır.

Siber uzayın fiziksel olarak var olabilmesi için çeşitli bileşenlerin var olması gerekmektedir. Bu tip bir model TCP/IP modelinde dört temel bileşen olarak sunulmaktadır ki buna göre; fiziksel altyapıların mevcut olması, bu altyapıları harekete geçirecek/çalıştıracak programların bulunması, programların işleyeceği, üreteceği bilginin/bilgilerin olması ve bunlar üzerinde harekete geçecek kullanıcıların olması gerekmektedir. Bu dört katmanın bir arada bulunması siber uzayın var olma öncülleri olarak ele alınmaktadır (Tarhan, 2017: 109).

Dördüncü unsur olarak ele alınan kullanıcı boyutu siber alanın anlaşılmasında önemli bir parametreyi oluşturmaktadır. Çünkü siber uzay, fiziksel yönüyle ele alabileceğimiz uzaydan farklı olarak; devletlerin kontrolünde bir yapı arz etmemektedir. Hatta siber uzayda kişilerin ve özel sektörün/şirketlerin öncü

girişimleri söz konusu olmuştur. Devletlerin ilgisi nispeten gecikmiştir. Kişilerin ve özel sektörlerin çeşitli amaçlarla etkin ve etkili şekilde kullandıkları siber alan, devletlerin ise onları yakalamaya çalıştıkları bir vaziyettedir. Kısacası siber alan, devlet merkezli bir yapıda bulunmamakta; bireyler, şirketler, sivil toplum örgütleri gibi birçok aktörün içinde olduğu bir özellik göstermektedir. Diğer taraftan siber alanın/uzayın çok aktörlü bu yapısı; ona anarşik bir yapı kazandırmaktadır (Akyeşilmen, 2016: 45) ki bu durumda siber uzayda güçlü olanların hâkimiyet kurabileceği bir mücadele alanına dönüştürmektedir.

2.2. SİBER GÜVENLİK

Özellikle Soğuk Savaş ve sonrası dönemde; güvenlik tehditlerinin genişlediği, güvenlik algısının da bu yönde değiştiği ve çeşitlendiği bir döneme girilmiştir. Yeni güvenlik anlayışında ekonomik, çevresel, küresel salgınlar, uluslararası terörizm gibi tehditler kendine yer bulmaya başlamış, bu parametreler ışığında güvenlik de çok boyutlu düşünülmeye başlanmıştır. Bu genişlemeye; küreselleşme ve onun hızlandırdığı teknolojik gelişmeler de ilave edildiğinde ortaya yeni bir alan çıkmaktadır ki bu alanı temsil eden kavram siber uzay olmuştur. Çünkü siber uzayda, bilgisayar ve dijital ağ sistemlerinin kullanılagelmesiyle beraber siber saldırı, siber terör gibi tehditlerin güvenlik ihlallerine yol açtığı görülmektedir. Her ne kadar başlangıçta teknik bir mesele olarak ele alınmışsa da; bu tehditlerin siber alan ile hemhal olmuş yapısı sonraki dönemlerde ilginin artarak siber güvenliğe sirayet etmesine sebep olmuştur. Keza siber alanın yapısı itibariyle kontrol edilemeyen özelliği, tehditlerin bu alanda rahatça ve çok yönlü bir şekilde yöneltiliyor olması tıpkı diğer alanlarda olduğu gibi (kara, hava, deniz, uzay) bu alanı da güvenlik yönünden önemli bir yere konumlandırmaktadır (Yangyue, 2015: 17-18).

Siber güvenlik kavramının ilk defa; 1990'lı yıllarda internet ağına bağlı olan bilgisayar sistemlerinde meydana gelen güvenlik sorunlarını ifade etmek için kullanıldığı görülmektedir. Bu tanımlama, daha çok bilgisayar sistemlerindeki verilerin güvenliğini kasteden bir minvalde kullanılmıştır. Buna göre erişilebilirliğin ihlal edilmediği, bilginin gizli bir şekilde muhafaza edilebildiği ve var olan verilerin üzerinde herhangi bir eksilme veya değişime maruz bırakılmadığı durumlarda siber alan güvenli bir hal almakta, siber güvenlik sağlanmış olmaktadır (Aslay, 2017: 25). Günümüzde ise siber güvenlik sadece bilgi güvenliği ile sınırlandırılabilecek bir

parametre değildir. Çünkü hayatımızın her alanı artık siber alana dâhil olmuş, sağlıktan ulaşıma, hükümet hizmetlerinden güvenliğe kadar geniş bir yelpazede siber alanın konusunu oluşturan teknoloji ve ağ sistemleri kullanılmaktadır.

Siber güvenlik meselesi, önceleri devletler tarafından güvenlik tehditlerinin olabileceği, bu tehditlerin de milli güvenliğe halel getirebileceği bir mecra olarak görülmemiştir. Her ne kadar bazı araştırmacılar, siber alan üzerinden yöneltilebilecek tehditlere işaret etmişlerse de siber güvenliğe ilgi ancak 11 Eylül terör eylemeleri ve sonrasında yine Madrid ve Londra gibi metropollerde gerçekleştirilen terör eylemlerinde siber güvenlik açıklarının kullanıldığının fark edilmesinden sonra oluşmuştur. Bu eylemlerde ilk defa, siber alandan gerçekleştirilen bir saldırının da tıpkı konvansiyonel terör eylemlerinde olduğu gibi çok yıkıcı sonuçlara yola açabileceği, masum insanların hayatlarına mal olan durumlar ortaya çıkarabileceği görülmüştür (Dupont, 2013: 67-80).

Siber güvenliğin, ulusal güvenlik için bir tehdit oluşturabileceği fikri özellikle 2007 yılında, Rusya kaynaklı olduğu iddia edilen ve Estonya'ya karşı gerçekleştirilen siber saldırıların neticesinde meydana gelen tahribattan sonra pekişmiştir. Sovyetler döneminden kalan ve Talinn Meydanı'nda bulunan anıtın taşınması üzerine, Estonya ve Rusya arasındaki gerilim artmış, bu gerilim siber alanda da sürdürülmüştür (Darıcılı, 2015: 414). Özellikle her türlü hizmeti, internet üzerinden sağlayabilen/sağlayan Estonya'da, bu saldırılarla adeta hayat durma noktasına gelmiştir. Estonya'ya dünyanın farklı merkezlerinden, iyi koordine edilmiş bir şekilde gerçekleştirilen siber saldırılarda, ülkede en çok kullanılan web siteleri, hükümet hizmetlerinin verildiği altyapı sistemleri, bankacılık sistemleri hedef alınarak tahribat arttırılmıştır. Son derece gelişmiş internet ağına ve bu ağlarla bütünleşik bir organizasyona sahip bir ülke olan Estonya aynı zamanda siber alandan gelen saldırılara da açık ve savunmasız bir hale getirmiştir (Eren, 2017: 36-37).

Günümüzde siber teknolojilerin savunma, sağlık, ulaşım ve sosyal hayatımızın bir bileşeni haline gelmesi; bu alanların tehditlere açık hale gelmesine neden olmuştur. Böylece siber güvenliğin sağlanılması gerektiği fikri ilk zamanlardan bu yana bir gereklilik ortaya koymaktadır (Johnson, 2015: 26-29). Dolayısıyla siber saldırılar ve hatta siber savaşlar, artık devletlerin hem siber güvenlik politika ve altyapısı oluşturmalarını ve hem de entegre savunma sistemleri

oluşturmalarını zorunlu kılmaktadır. Aksi durumda, hem vatandaşlarının yaşamları, hem de ekonomik ve askeri anlamda varlıkları siber alandan gelen tehditlere açık ve savunmasız bir durumda kalmaktadır. Keza hem NATO, BM, AB, AGİT gibi uluslararası kurumlar özelinde ve hem de ülkelerin tek başlarına oluşturdukları politikalar ve savunma sistemleri, siber güvenlik mekanizmaları etkin bir şekilde oluşturulmakta ve kullanılmaktadır (Yılmaz ve Sağıroğlu, 2013: 159).

2.3. SİBER TEHDİTLER VE SİBER SALDIRILAR

Uluslararası İlişkiler disiplininde tehdit olgusu ve ona bağlı kavramlar genellikle klasik güvenlik anlayışının şekillendirdiği ve dolayısıyla eksik kalmış tanımlamalar üzerinden yapılmaktadır. Fakat özellikle bilgi çağı dediğimiz teknolojik yenilik ve bilgi sistemlerinin hayatımıza angaje olduğu 1990'lı yıllardan sonra bu durumun değişmesi gerektiği anlaşılmıştır. Çünkü hayatımızın her alanı bu bilgi sistemleriyle iç içe geçmiş, online bilet alımından online otel rezervasyonlarına, online eğitimden konferanslara, akıllı mobil telefonlardan iş hayatına kadar birçok unsur bilgi sistemlerine konu olmuştur. Diğer taraftan kültür, eğlence, araştırma, savunma, sağlık gibi alanlarda da bilgi sistemlerinin devrim yaratacak etkileri görülmüştür. Tarihte yeni teknolojilerin insan hayatını bu denli etkiledikleri dönemlerde yapısal birçok değişimin de onu takip ettiği bilinmektedir. Fakat bu değişimlerin her zaman olumlu sonuçlar doğurmadığı kimi zaman beraberinde bir takım sorun ve sonuçları, dahası tehditleri getirdiği görülmektedir. Dolayısıyla teknolojideki uzmanlaşma ve bunun sonucunda ona olan bağımlılık ilişkisi de bu tehditleri barındırmaktadır (Cavelty, 2016: 12-14).

Siber uzayda gerçekleştirilen eylemlerin takibinin oldukça zor olması, siber alanı asimetrik bir tehdit alanı olarak ortaya çıkarmaktadır. Diğer taraftan siber alanda ortaya çıkan tehditlerin her geçen gün artması; devletlerin bu asimetrik tehdit alanlarını göz önünde bulundurma durumlarını zaruriyet seviyesine çıkartmıştır. Siber alanda ortaya çıkabilecek tehditler, yıkıcılık ve etki yönünden kitle imha silahlarıyla aynı yıkıcılıkta sonuçlar doğurabilecek seviyelere erişebilmektedir. Diğer taraftan, siber alanın çok taraflı (bireyler, şirketler, terör organizasyonları vs.) bir hâkimiyet alanı olduğu göz önünde bulundurulduğunda; devletlerin tam bir güvenlik

durumu yaratabilmeleri, önlem alma mekanizmalarını tamamen ellerinde bulundurabilmeleri pek mümkün görülmemektedir. Siber alana dahiliyeti tartışmasız olan teknolojinin, insan yaşamının her alanında kullanıldığı göz önüne alındığında; bu teknolojilerin tehditleri beraberinde getirmeleri kaçınılmaz olmaktadır (Seren, 2016: 9).

Siber tehditler virüs, kurtçuk (worm), yemleme (phishing), truva atı (trojan), istem dışı elektronik posta (spam), zombi ve botnetler, klavye izleme yazılımları (key logger), hizmet engelleme saldırıları (Dos, DDos), şebeke trafiğinin dinlenmesi (sniffing ve monitoring), casus yazılımlar (spyware) gibi yöntem ve araçlar üzerinden gerçekleşmektedir. Böylece siber alanda faaliyet gösteren şebekelere ve teknolojilere sızılmakta, yetkisiz bir şekilde şebekelerden bilgi çalınmakta, bilgiler değiştirilebilmekte, çalışamaz hale getirilebilmektedir (Ünver ve Canbay, 2010: 96). Bu tür kötü amaçlı yazılımlar; bireyler, devletler ve şirketler açısından en tehlikeli; diğer taraftan gerçekleştirilmeleri bakımından kolay ve etkilerinin de hızlı bir şekilde görülmelerinden dolayı en fazla kullanılan siber saldırı türleridir. Bu tehditlere sadece ağ üzerinden maruz kalındığı yönündeki yaygın kanaatler gerçeği yansıtmamaktadır. Bu tarz kötü amaçlı yazılımlar; aygıtlara yüklenerek, herhangi bir ağ bağlantısına gereksinim duyulmadan da yapılabilmektedir. Ayrıca bu saldırılar sadece yazılımsal değil donanımsal araçlarla da gerçekleştirilebilmektedir. Klavyelere takılan aparatlarla klavye işlemlerinin kaydedilmesi yahut bankamatikler ve pos cihazları üzerine takılan kayıt çipleri gibi donanımlar da bu tarz saldırılarda kullanılabilmektedir (Yılmaz ve Sağıroğlu, 2013: 162-163).

Siber tehditlerin siber saldırılara dönüşmesi halinde yıkıcı tahribatlara sebebiyet verdikleri görülmektedir. Siber saldırı kavramını, en basit haliyle siber alanda gerçekleştirilen her nevi zarar olarak tanımlamak mümkündür. Söz konusu siber saldırılar, devletler ve yahut devlet dışı organizasyonlar eliyle gerçekleştirilebilmektedir. Diğer taraftan siber alanda iz sürmenin zorluğu nedeniyle, saldıran ve saldırı arasındaki bağıntıyı kesin bir şekilde tespit etmek kolay olmamakta; çoğu defa bu durumda şüpheler ve küçük izler üzerinden hareket edilebilmektedir. Siber saldırılara karşı önlem almanın zorluğu ve siber saldırı gerçekleştirmek için gereken altyapının kolayca ve az bir maliyetle elde

edilebilmesinin yaratmış olduğu durum beraber ele alındığında siber saldırıların neden çok fazla tercih edildiği anlaşılabilmektedir (Doğru, 2013: 5-6).

Siber saldırılar, siber alanda/uzayda, hedef bilgisayar işletim sistemlerinin zarar görmesini arzulayan saldırganlar tarafından gerçekleştirilen eylemlerden meydana gelmektedir. Dolayısıyla, herhangi bir işletim sisteminde hata sonuçlu ve yahut sistemsel aksamaların neden olduğu zararları siber saldırı olarak tanımlamak mümkün değildir. Diğer taraftan siber saldırıların, bütün aşamalarının siber alanda ortaya çıkması söz konusu olmayabilir. Siber saldırı neticesinde ortaya çıkabilecek zarar ekonomik, sosyal, kültürel ya da hükümet fonksiyonlarında, siber saldırının bir sonucu olarak etki edebilmektedir. Diğer taraftan saldırılar iki türlü olarak ortaya çıkmaktadır ki bunlar doğrudan ve dolaylı siber saldırılar olarak sınıflandırabilmektedir. Doğrudan siber saldırılarda amaç; hedeflenen sistemin yok edilmesi, çalışmaz duruma getirilmesi iken dolaylı siber saldırılarda amaç ise hedeflenen sistemin işlevselliğinin önlenmesidir (Kello, 2013: 19).

Siber saldırılar ile klasik saldırılar arasındaki farkı anlayabilmek; siber saldırıların kimliği üzerinde daha iyi bir fikir verecektir. Klasik saldırı anlayışında bir saldırının gerçekleştirilebilmesi için fiziki bir etkinin olması ve bu etkinin de bir mekân üzerinde gerçekleşmesi söz konusu olmaktadır. Fakat siber alan; coğrafya ve fiziki dünyayı aşan bir yapıya sahiptir. Böyle bir durumda siber saldırganlar, bu tür sınırlara ve kısıtlara maruz kalmadan bir başka ülkeye veya o ülkenin vatandaşına saldırı düzenleyebilmektedir. Sonuç olarak bu saldırganlar; saldırının gerçekleştirildiği ülke ile saldırıya uğrayan ülke arasında uluslararası bir seviyeye taşınabilecek sorunlara sebebiyet verebilmektedirler. Siber alanın kimlik öğesini bir nevi silen özelliği, saldırganların gizliliğini sağlamaktadır. Böylece klasik saldırı anlayışının sonunda gerçekleştirilebilecek suç/ceza fenomeni de devre dışında kalmaktadır. Çünkü ortada yine bir suç vardır fakat suç unsurunu gerçekleştiren failin belirsizliği, cezayı da gerçekleştirilebilme durumundan uzaklaştırmaktadır. Örneğin 1941 yılında Japonya'nın ABD'ye yapmış olduğu Pearl Harbor saldırısı klasik bir saldırı özelliği taşımaktaydı. Keza saldırıyı gerçekleştirenler Japon ordusuna mensup, Japon üniforması giyen askerlerdi. Bu durum da saldırının kim tarafından gerçekleştirildiğinin anlaşılmasını kolaylaştırmaktaydı(Brenner, 2010: 3).

Siber alanın bu durumu göz önüne alındığında Mary Kaldor'un eski ve yeni savaş ayırımından da bahsetmek gerekmektedir. Kaldor'a göre; eski tip savaşlarda düzenli ordular savaşırken, yeni tip savaşlarda devlet ordularının yanı sıra devlet dışı silahlı organizasyonlar, paralı askerler, cihadist gruplar gibi çok taraflı katılımcılar savaşmaktadırlar. Ayrıca eski savaşlarda hedef ideolojik veya jeopolitik nedenlerden kaynaklanırken yeni savaşta bu daha çok kimlik temellidir. Fakat eski ve yeni savaşın da tamamıyla birbirinden farklı olmadığı, kimi özellikler yönünden benzerlik gösterdikleri görülmektedir. Bu özelliklerden önemli bir tanesi savaşan tarafların kimliklerinin bir şekilde açık olması yani bilinmesidir[1] (Kaldor, 2013: 1-16).

Diğer taraftan siber uzayda bu eski savaş-yeni savaş ayrımının ötesinde bir durum söz konusu olmaktadır. Siber uzayda cereyan eden ve kimi durumlarda siber savaşlara yol açabilecek denli önemli sonuçlar ortaya çıkaran siber saldırılar ele alındığında bu alanda ne eski tip savaşlarda olduğu gibi düzenli ordular vardır ne de yeni tip savaşlarda olduğu gibi kimlikler açık ve belirgindir. Eski tip saldırıların hangi durumlarda savaş olarak lanse edileceği kolaylıkla saptanabilmekteyken siber saldırılarda böyle bir durum söz konusu değildir. Ayrıca yeni tip savaşlarda olduğu gibi kimlik de çok belirgin değildir. Öncelikle saldırganların kimlikleri sabit ve belirli değildir. Ayrıca saldırganlar devlet dışı aktörler de olabilmektedir. Diğer taraftan saldırılar anonim ağlar üzerinden gerçekleştirildiğinden asıl saldırının nereden ve kim tarafından yapıldığının tespiti ve dolayısıyla saldırının bir savaş ilanın olup olmadığının anlaşılması çok açık ve kesin olmamakla birlikte tartışmalı bir konu olmayı sürdürmektedir (Brenner, 2010: 3).

Siber tehdit ve saldırıların ne derecede tahribat yaratacağı, hangi yollarla ve amaçlarla yapıldığını ortaya koyduktan sonra siber saldırıların ne derecede tercih edilen bir saldırı türü olduğundan da bahsetmek gerekecektir. ABD Siber Komutanlığının verilerine göre Pentago'nun bilgisayar sistemleri saatte 250.000 olmak üzere günde altı milyon defa yetkisiz erişime konu olmaktadır. Şirketlerin nerdeyse %75 'i kötü amaçlı saldırılara maruz kalmakta ve saldırıların neticesinde iş yapamaz duruma düşebilmektedir (NATO, 2010: 9). Özellikle 11 Eylül 2001 tarihinde oldukça yıkıcı neticeler veren terör saldırıların ve yine 2007 yılında Estonya'ya yönelik gerçekleştirilen saldırıların siber kaynaklı saldırılar olduğu

[1] Ayrıntılı bilgi için bakınız: Kaldor, Marry (2012). New and Old Wars. Cambridge: Polity Press.

dikkate alındığında yeni tehdit ve saldırı algısının değişimi daha rahat anlaşılabilmekte ve sonuçlarının yıkıcılığı idrak edilebilmektedir (Kurnaz, 2016: 63). Estonya; hemen hemen her türlü devlet hizmetinin internet üzerinden verilebildiği, internet ağı ve güvenliği açısından da örnek gösterilen ülkelerden biridir. Fakat 2007 yılına girildiğinde Rusya Federasyonu'nun da dâhil olduğu siber saldırılara maruz kalan Estonya üç hafta gibi uzun bir süre boyunca hiçbir hizmeti vatandaşlarına sunamamış, adeta hayat durma noktasına gelmiştir. Çünkü hükümet sistemlerine, bankalara, güvenlik birimlerine, medya şirketlerinin altyapılarına karşı gerçekleştirilen yoğun siber saldırılarda tüm bu sistemleri durdurulmuş, çalışmaları engellenmiştir. Netice itibariyle bu saldırılar diğer devletlerin de siber saldırıların yıkıcı etkilerini dikkate almaları gerektiği fikrine temel oluşturmuştur (Yılmaz, 2016: 36).

2.4. SİBER İSTİHBARAT

Siber tehdit ve saldırıların sayısını, hızını ve etkisini arttırmasıyla paralel bir şekilde devletlerin önlem alma mekanizmalarını geliştirme çabaları da hızlanmıştır. Önlem mekanizmalarını geliştirmek adına en önemli ilk girdi istihbarat verileri olmaktadır. Bu paralelde siber tehdit ve saldırıları ortadan kaldırmak yahut etkisini azaltmak için siber istihbaratın sağlanması gerekmektedir.

İstihbarat kelimesi Türkçe sözlüklülerde bilgi toplama, haber alma gibi anlamlarda kullanılmaktadır (Türk Dil Kurumu Türkçe Sözlük, 1998: 1107). Diğer taraftan istihabarat kelimesine yönelik farklı tanımlamalar ve değerlendirmeler mevcuttur. Eldeki verilerin en iyi şekilde kullanılabilmesi adına bunların analizlerini yapmak ve söz konusu verileri elde etmek suretiyle bunları bir güç unsuruna çevirmek de yine bu tanımlardan biridir (Groš, 2020: 2). İstihbaratın hemen hemen her kaynakta önem atfedilen bir realite olduğu açıktır. Kelimenin özüne yönelik İngilizce, Fransızca, Arapça kaynaklarda genel anlamıyla zekâ, haber alma ve işleme, karşı istihbarat gibi çeşitli manalar mevcuttur. Bilhassa devletlerin bu alanlarda oluşturdukları yapılanmalarla istihbarat anlamında güçlü olmaya çalıştıkları görülmektedir (Avcı, 2004, 5-6). Bütün tanımların ortak paydası olarak istihbarat; veri toplama, analiz etme gibi süreçler sonucunda elde edilen bilgilerin; devletlerin ve kurumların güvenliklerini korumak amacıyla karar alıcıları iletilmesi yahut politika yapıcıların hizmetine sunulması süreçleri olarak tanımlanabilir.

İstihbarat, bu konuda uzman kişilerce elde edilen bilgiler aracılığıyla sağlanmaktadır. Uzmanlık alanları farklı olan kişiler eliyle yürütülen bu süreç aynı zamanda yüksek eğitim gerektiren bir faaliyettir (Çınar, 1997: 131). İstihbarat sağlama işinin farklı alanlarda eğitimli olan kişiler eliyle yürütüldüğü görülmektedir. Bunun nedeni istihbaratın çok yönlü bir disiplin olmasıdır. Siyasi, askeri, ekonomik, sosyal, coğrafya, ulaşım-iletişim, bilimsel-teknik gibi alanlarda istihbarat çalışmaları mevuttur ve bu alanlara son olarak siber istihbaratın da eklemlendiği görülmektedir (Keleştemur, 2017, 44). 21. yüzyılın en büyük nimetlerinden biri olarak görülen internet; beraberinde tehditleri getirmiştir. Dijitalleşmenin devletleri ve bireyleri de içine alır şekilde her aktörü etkilediği düşünüldüğünde; siber uzayda söz konusu her aktörün tehdit ve saldırılara açık halde olduğu bilinmektedir. Bu anlamda bilhassa devletlerin siber uzaydan tezahür edecek tehdit ve saldırıları bertaraf etme yahut bu kanaldan karşı saldırı gerçekleştirmek adına siber istihbarat topladıkları görülmektedir. Ayrıca devletlerin birbirlerine yönelik girişimleri de siber alanda zaman zaman had safhaya çıkabilmektedir. Özellikle siber alanın devletlere mahsus olmayan özerk yapısı ve devletlerin terör gruplarının saldırılarına maruz kalmaları siber istihbarat toplamayı zorunlu kılmıştır (Savaş ve Topaloğlu, 2015: 2-3).

Siber istihbarat, devletler için bu kadar önemli bir konumda iken; siber istihbaratın tam olarak ne olduğunu kavrayabilmek önemlidir. Fakat siber istihbarat; üzerinde henüz yeterli çalışma bulunmayan, tanımına yönelik ortak kanaat sağlanamamış bir kavramdır. Bunun temel nedenlerinden biri siber istihbaratın genç bir disiplin olmasıdır (Niekerk, Ramluckan ve Duvenage, 2016: 558). Diğer taraftan siber istihbarata yönelik çeşitli tanımlamalar bulunmaktadır. Bunlardan birine göre siber istihbarat; siber alandan bilgi toplama ve işleme sürecidir. Böylece siber alanı meydana getiren her türlü elektronik ortam yahut medya üzerinden elde edilen her türlü bilgi, teknik ve araç siber istihbaratın konusu olabilmektedir. Bu tanımlamaya göre siber istihbarat, sadece siber güvenliğe dönük bir kavram olarak ele alınmamaktadır. Çünkü siber alandan elde edilecek herhangi bir bilgi politika, ekonomi, siyasi hedeflere hizmet eder şekilde ele alınmaktadır. Fakat bunun siber istihbaratın temel değil yan işlevlerinden biri olduğu düşünülmektedir. Keza siber istihbaratın siber güvenliği sağlamaya yönelik olarak ele alınması, siber alanın kendine özgü nitelikleri de göz önünde bulundurularak tanımlanması gerekmektedir. Bir diğer tanımlamada siber istihbarat; bağımsız bir disiplin niteliğinde

açıklanmaktadır. Buna göre siber alanla/güvenlikle ilgili her platformdan elde edilen verilerin siber istihbarat için sağlanıyor olması gerekmektedir (Bonfanti, 2018: 110-111). Böylece istihbarat toplama süreçleri olan bilgi toplama, yönlendirme, süreçleme, analiz etme, yayma ve geri bildirim gibi süreçlerin siber alanla ilgili ve ona yönelik olarak gerçekleştirilmesi söz konusu olmaktadır (CyberEdge Group, 2018: 2).

Her türlü bilgi ve stratejik unsurun bilgisayar çağının gerektirdiği şekilde internet üzerinden erişilebilir olması siber istihbaratı önemli ve hayati kılmıştır. Devletlerin siber ortamda, diğer rakip unsurlara ait bilgi ve istihbarat toplayabilmesi hem daha kolay hem de daha az maliyetle gerçekleştirilebilmektedir. Bu durum devletlerin siber alandan bilgi toplama, psikolojik ve taktik harekât ve propaganda gerçekleştirmesini klasik istihbarat tekniklerine nazaran basitleştirmiştir. Diğer taraftan devletlerin kendileri için de bu durum söz konusudur. Yani siber alandan kendi bilgileri de yasal dışı erişime açık hale gelmiş, tehdit ve saldırılar sıklaşmıştır. Böylece devletlerin oluşan yeni duruma adapte olarak siber alanda rakiplerine üstünlük sağlamaları gerekmektedir (Bayraktar, 2014: 129-130). Özellikle siber alanın terör örgütleri tarafından kullanılmasıyla ortaya çıkan yıkıcı sonuçlar, siber istihbarat yönünden güçlü olmanın gerekliliğini ortaya koymaktadır. 11 Eylül 2001 yılında ABD'ye yönelik El-Kaide tarafından yapılan saldırılarda siber alanın kullanıldığı düşünülmektedir. Siber saldırıların özellikle bu tarihten sonra tırmanışa geçtiği görülmektedir. Diğer taraftan siber alanda saldırıların kimler eliyle gerçekleştirildiğinin tespiti ise siber alanın yapısı itibariyle bir hayli zor olmaktadır (Günay, 2018: 87-89).

Siber istihbarat yöntemlerinin, klasik istihbarat yöntemlerinden farklı olduğu görülmektedir. Siber ortamda özellikle sosyal mühendislik, sosyal ağlar, arama motorları ve casus yazılımlar kullanılmaktadır. Sosyal mühendislik, hedef alınan kişi, kurum, toplumsal yahut devlet unsurunun hatalarını istenen hedefe uygun bir şekilde lanse edilerek bilhassa insanların manipüle edilmesi suretiyle harekete geçirilmesidir. Böylece insanların normalde yapmayacakları eylemleri, davranışları, düşünceleri edinmesi neticesinde hedef yıpratılmaktadır. Sosyal ağların sosyal hayatı etkileyen önemli bir unsura dönüştüğü düşünüldüğünde, istihbarat örgütlerinin bu kanalları kullanması kaçınılmaz olmuştur. Twitter, Facebook, YouTube, Wikileaks gibi siber

sosyal ağların sık sık kullanılması bu durumun en açık örneklerini vermektedir. Arama motorları bir diğer siber istihbarat kaynağıdır. Bu ağlar üzerinden bütün arama motorları üzerindeki veriler depolanabilmekte, ayrıca kimlerin ne tür bilgilere erişim sağladığı tespit edilebilmektedir. Bu yolla kurum ve şirketlerin kullandıkları IP'ler (İnternet Protocol) üzerinden önemli bilgilere ulaşılabilmektedir. Casus yazılımlar da en çok kullanılan siber istihbarat araçlarından biridir. Casus yazılımlar ile kişi, şirket ve kurumların bilgileri kopyalanabilmekte, transfer edilebilmektedir. Özellikle geniş bant kullanan bilgisayarların hemen hemen büyük bir oranında bu tarz kötü amaçlı yazılımların bulunduğu düşünülmektedir. Bu yazılımlar aracılığıyla hedef alınan bilgiler kopyalanmakta ve bu işlem yapılırken bu yazılımların gizliliklerini korumayı sürdürmeye çalıştıkları görülmektedir (Oğuz, Ceyhan ve Sağıroğlu, 2015: 2-3).

2.5. SİBER SUÇ, SİBER TERÖRİZM VE SİBER PROPAGANDA

Siber suç kavramı, internet teknolojilerinin gelişmesiyle beraber sıkça anılagelen ve bu teknolojilerin yaratmış oldukları fırsatlardan faydalanılarak meydana getirilen zarar ve suçları nitelendirmek için kullanılmaktadır. Kavram, ortaya çıkış itibariyle tıpkı siber uzay kavramında olduğu gibi bilim kurgusal forumlarda, bilim kurgu metinlerde siber uzayın sanal gerçekliğinde meydana gelen suçlara hitaben kullanılmıştır (Wall, 2008: 46-47). Dar bir bakış açısıyla siber suç; bilgisayar sistemlerindeki verileri ele geçirmek için başvurulan her yol olarak ele alınabilirken; geniş bir bakış açısıyla ise bilişim sistemlerinin dâhil olduğu herhangi bir suç olarak tanımlanabilir. Fakat her iki tanım da eksik kalmaktadır. Çünkü birinci tanımdaki dar bakış; fiziksel dünyada da var olup, fakat bilgisayar sistemleri üzerinde daha etkili bir şekilde meydana gelen bir takım unsurları dışarıda bırakmaktadır. Çocuk pornografisi, dolandırıcılık ve fikri mülkiyet hakları ihlalleri bunlardan sadece bazılarıdır. İkinci tanım ise çok geniş bir banda oturarak, siber suçu belirgin olmayan bir forma itmektedir. Keza günümüzde neredeyse her suç, herhangi bir aşamasında bilgisayar/bilişim sistemleriyle kesişebilmektedir (Seger, 2012: 7).

Siber suç kavramının daha iyi anlaşılabilmesi için; açıklanan suç tipinin yaygın kabul görmesi, suçun tüm unsurlarını barındırması gerekmektedir. Ayrıca

istenen tanımın eski ve yeni suç tiplerini bünyesinde barındırırken, siber uzayın sürekli olarak değişen yapısını da göz ardı etmeyecek bir halde, ileriye dönük beklentileri de kapsaması gerekmektedir. Keza, kanunsuz suç ve ceza olmayacağına dair hukukun genel ilkesi (Eşitli, 2013: 234) göz önünde bulundurularak olası suç tipleri de tanımlanıp, bu anlamda bir boşluk bırakılmamalıdır. Avrupa Konseyi Siber Suçlar Üzerine Budapeşte Mutabakatında siber suçlar; bilgisayar veri ve sistemlerinin bütünlüğüne ve gizliliğine karşı suçlar; yasadışı erişim, yasadışı müdahale, cihazların kötüye (kanun aleyhine) kullanılması da dâhil edilerek ele alınmaktadır. Ayrıca bilgisayarlara yönelik sahtecilik ve sahtekârlık fiilleri de yine siber suç olarak ele alınmıştır. Mutabakatta çocuk pornografisiyle ilgili suçlar, telif hakları ve benzer haklar ile ilişkili suçlar da içerikleri yönüyle siber suç olarak sayılmıştır (Council of Europe/Siber Suç Sözleşmesi, 2012). Siber suç olarak başka kaynakların gösterdiği suç tipleri de söz konusudur; izinsiz siber izleme (takip), siber terörizm, kimlik avı (phishing), bilgisayar zorbalığı, bilgisayar hackleme, internet üzerinden virüs üretmek ve dağıtmak, siteler arası komut dosyalar göndermek bunlardandır (Pande, 2017: 21-25).

Siber suçlarla mücadelede etmekte çeşitli zorluklarla karşılaşılmaktadır. Bu zorluklarda siber uzayın belirsiz yapısının etkisi olmakla beraber; siber uzay ile ilgili kişilerde ve organizasyonlardaki bilgi eksikliğinin de payı vardır. Karşı önlem ve eylem almada faaliyet gösterecek kalitede ve sayıda yetişmiş insan gücünün olmaması; kolluk güçlerinin siber alan ile ilgili yeterli donanımda olmamaları da bu durumu beslemektedir. Ayrıca kritik altyapı sistemlerinin siber suçlarla mücadele edebilecek kalitede olmaması ve bu durumun sürekli olarak gelişen teknolojinin getirdiği tehditlerle meydan okumalara maruz kalması da tehditlerin başarıya ulaşmasına zemin hazırlamaktadır. Siber alan ve teknolojileri ile ilgili yeterli ar-ge çalışmasının olmayışı; hukukçuların ve hukuk sisteminin siber suçlarla ilgili yeterli bilgiye haiz olmayışı gibi etkenler de yine bu zorluklardan bazılarıdır (Pooina, 2014: 119-120).

Siber suç kavramı yeni bir fenomen olduğundan; hangi eylemlerin suç oluşturduğuna yönelik kodifiye bir hukuk sistemi gelişmemiştir. Bu nedenle ceza adaletinin aktörleri konuya henüz tam anlamıyla hâkim olamamışlardır. Siber suçlarda fail ile mağdurun arasındaki mesafe tanımlanamadığı için, nasıl bir ceza

sistemi öngörüleceği tespit edilememektedir. Ayrıca suçu işleyen ile mağdur farklı ülkelerde de olabilmektedir ki bu siber alanın sınır tanımayan özelliğini ortaya koymaktadır. Suçun işlenme şekli ve kullanılan araçların çok çeşitli ve değişken yapısı da suçun tespitini zorlaştırmaktadır. Diğer taraftan siber suçlar az bir gayret ve masraf gerektirirken, suçla mücadele ve adalet mekanizmasını bu yönde harekete geçirmek yoğun emek ve maliyet gerektirmektedir (Önok, 2013: 1232-1236).

Siber alandan gerçekleştirilebilecek daha kapsamlı suçlar söz konusu olmakla beraber terör faaliyetlerinin bunların en yıpratıcı olanlarından biri olduğu düşünülmektedir. Siber alanın, teröristler tarafından eylemlerin gerçekleştirilebildiği bir mecra olarak görülmesiyle beraber bu saldırıların ve pratiklerin sıklaştığı görülmüştür (Virkar, 2016: 1-3). Siber uzayda siber araçlar kullanılarak, çeşitli saiklerle tehlike yaratan ve yaratılan tehlikenin; siber suçlardan farklı olarak terörist faaliyetler niyetiyle ortaya konulduğu durumlar da söz konusu olabilmektedir. Bu noktada sıkça başvurulan terim ise siber terör olmaktadır. Diğer birçok terimde olduğu gibi siber terör kavramı da açık ve üzerinde mutabık olunan bir tanımlamadan yoksun bulunmaktadır. Bunun anlaşılır birçok nedeni olmakla beraber bu belirsizliğin arkasında yatan bir takım sorular vardır. Bir siber atak ne zaman ve hangi koşullarda siber terör kapsamına alınabilir? Siber suç ve siber terör arasındaki fark nereden kaynaklanmaktadır? Bu ve benzeri sorulara cevap vermeyen her tanım, siber terör kavramını açıklamakta da eksik kalmaktadır. (Powers, 2013: 2).

Siber terör kavramının ilk defa 1980'li yıllarda Stratejik ve Uluslararası Çalışmalar Merkezi'nde (CSIS) görevli bir araştırmacı olan Barry Collin tarafından kullanıldığı görülmektedir (Collin, 1977: 15-18). Siber terör kavramı ilk olarak; dijital bilgi sistemleri, ağları ve bunların bileşenlerini kullanmak suretiyle bir terörist kampanya veya eylemi gerçekleştirmek yahut gerçekleştirilmesini kolaylaştırmak olarak tanımlamıştır (Kontselidze, 2015: 26). Fakat bu tanıma eklenmesi gereken parametreler olmakla beraber, tanımın belirginleşmesi açısından da bahsedilen sorulara cevap vermesi gerekmektedir ki bu da siber suç ve siber saldırıyla siber terörizm arasındaki farkı ortaya koyacaktır.

Siber bir saldırının siber terör olarak addedilmesi için söz konusu saldırının yoğun şiddet, ölüm veya ekonomik olarak ağır sonuçlar içermesi gerekmektedir. Diğer taraftan bu sonuçların da politik bir sebeple kasten ve sonuçlarının öngörülerek

gerçekleştirilmesi gerekmektedir. Bu kıstaslar göz önüne alındığında siber terörü siber saldırılardan ayırt etmek daha kolay olmaktadır. Çünkü siber ataklarda propaganda, iletişim kanallarını durdurma, aksatma ve yahut diğer sebeplerle bilgisayar ve ağları kullanırken, siber terörde bu araçlar, sonuca ulaşmayı kolaylaştırmak için kullanılmaktadır (Conway, 2003: 6). Buradan yola çıkarak politik bir amaç içermeyen, fiziksel anlamda çok yıkıcı sonuçlar doğurmayan siber suçları da siber terörden tamamen ayrıştırmak mümkün olmaktadır. Kısacası her siber suç ve siber tehdit siber terör kapsamına alınmamakla beraber, her siber terör eylemi hem bir siber saldırıdan ve hem de bir siber suçtan oluşmaktadır.

Siber terörizmin ne olduğu açıklandıktan sonra bir sonraki aşamada siber teröristin de açıklanması gerekmektedir. Siber teröristin, eli silahlı teröristten farkını ortaya koymak, siber terörizmin arkasındaki sebepleri anlamada kolaylık sağlamaktadır. Siber güvenlik ihlalleri göz önüne alındığında, siber ataklar, suçlar ve terörizmin arkasındaki güçlerin genellikle yabancı menşeli odaklar olduğu görülmektedir. Diğer taraftan bu saldırı ve terörist eylemleri gerçekleştirenlerin genellikle üniversite eğitimlerin tamamlamış, internet-bilgi teknolojileri alanlarında gelişkin ülkelerde çalışmış, kalifiye özelliklere sahip oldukları görülmektedir. Bu eylemleri gerçekleştirenler, mağdur ülke sınırları içerisinde de yaşıyor olma ihtimalleri de söz konusu olabilmektedir. Bu durumda da genellikle bu kişilerin diğer kültür, ideoloji, politika ve hayat tarzlarına sıkıca bağlı oldukları görülmektedir (Baldi, Gelbstein ve Kurbalija, 2003: 34-35).

Diğer teröristler gibi doğrudan kan dökme yoluna gitmeyen siber teröristler, daha ziyade bir metronun bilgisayar sistemlerine sızarak yahut bir uçağın sistemlerine girerek bunları infilak emek, çarpıştırmak, kullanılamaz hale getirmek gibi işlemleri gerçekleştirirler. Fakat bu tarz büyüklükte bir siber terör olayına henüz rastlanmamakla birlikte özellikle ekonomik, politik ve altyapı sistemlerine yönelik saldırıların örnekleri görülmektedir. 2007 yılında Estonya'ya gerçekleştirilen yoğun siber saldırılarda bankacılık sisteminin ağır bir darbe alığı ve bu esnada siber teröristlerin de banka hesaplarına erişim sağladığı düşünülmektedir. 2016 yılında Ukrayna'nın çeşitli bölgelerindeki elektrik sağlayıcılarına yapılan siber saldırılar sonucunda elektrik kesintisi yaşandığı görülmüştür. 2017 yılında ''WannaCry'' isimli virüsle birçok ülkenin devlet kurumları, özellikle hastane sistemleri

hacklenmiştir. Bu virüsle saldırganlar; elde edilen bilgilerin fidye karşılığı geri verilmesi amaçlamışlardır (Yılmaz, 2020: 70-72). Konvansiyonel teröristin gerçekleştirdiği eylemlerde bizzat bulunma durumu, siber terörist için geçerli değildir. Bu tür eylemleri evinde ve daha rahat bir şekilde gerçekleştirebilmektedir. Sonuç itibariyle iki tür terörist de aynı sonuca ulaşmakla beraber farklı yolları takip ederek bu noktaya gelmektedirler. Siber teröristin eylemden etkilenme ihtimali konumu itibariyle mümkün olmayınca, basit ve ucuz teknolojik bilgi ve ekipmanlarla girişilen siber terör eylemi çok daha tehlikeli hale gelmektedir. Çünkü teröristin teknik/fiziki takibi kolay olmamaktadır (Iqbal, 2004: 403).

Siber uzaydan kaynaklanan tehditlerin yapısı itibariyle öngörülememesi, tehdidin kaynağının tespitindeki zorluklar ve en önemlisi; gelişen ve değişen teknolojinin hayatın her alanında kullanılagelmesi; reel dünyayı siber uzaydaki sanal tehlikelere karşı savunmasız bir hale getirirken somut ve yıkıcı sonuçların ortaya çıkmasına da imkân vermektedir. Bilgi sistemlerinin hayatın her alanında yaygın olarak kullanıldığı göz önüne alındığında; telekomünikasyon alt yapıları, elektrik güç merkez sistemleri, petrol ve gaz boru hatları, tüm ulaşım ağları, su dağıtım sistemleri, hastane ve sağlık sistemleri, polis, itfaiye, ambulans gibi acil servis olarak görev yapan kurumların sistemleri ve bunlara ek olarak bütün hükümet ve kurumların sistemleri sanal uzaydan gelecek tehditlere açık olmaktadır (Elliot, 2002: 1-2). Bu duruma siber terör eylemi gerçekleştirmenin ucuz ve yıpratıcı özelliği ilave edildiğinde; siber uzay üzerinden terörizm eylemi gerçekleştirmek siber teröristler için oldukça cazip olmaktadır.

El-Kaide ve Taliban gibi terör organizasyonlarının çeşitli eylemlerde siber ortamı kullandıkları bilinmektedir (Brickey, 2012: 4-8). Özellikle El-Kaide tarafından gerçekleştirilen 11 Eylül 2001 saldırıları, siber terörizmin yıkıcılığını göstermek adına bir nevi milat olmuştur. Çünkü saldırılardan sonra belirtilen uzman görüşlerinde Pentagon'un savunma ağ sistemlerinin yetersiz olduğu ve saldırılarda bunun eksikliğinin hissedildiği vurgulanmıştır. ABD'nin bu saldırılardan sonra güvenlik yapılanmalarını siber güvenlik uzmanlarıyla yürütmesi de bu iddiayı haklı çıkarmıştır (Türk Asya Araştırmalar Dergisi[TASAM], 2004: 1-3). Diğer taraftan son yıllarda Suriye, Irak, Nijerya, Afganistan ve Pakistan gibi ülkelerin terör olaylarına daha fazla maruz kaldıkları görülmektedir. Bu tehditleri yaratan IŞID, Boko Haram,

Taliban gibi örgütler olurken; siber terör bağlamında en etkili örgütler ise IŞID ve Taliban olmuştur (Riglietti, 2016: 14).

Terör örgütlerinin siber alanı kullanırken ana hedeflerinden biri de propaganda yaparak, kamuoyunu korkutmak, kamuoyunun ilgisini yanıltıcı ve çarpıcı bilgilerle çarpıtarak destek bulma yahut şüphe noktaları oluşturmaktır. Tam da bu noktada ele alınması gereken bir diğer siber terimi ise siber propaganda terimidir. Son zamanlarda özellikle IŞID gibi terör örgütlerinin açmış oldukları sosyal medya hesapları üzerinden yaptıkları propagandalar bu duruma örnek verilebilir. IŞID, bu kanallar aracılığıyla hem propaganda yapmakta hem de örgüte eleman devşirebilmektedir (Aytekin, 2016). El-Kaide ve IŞID; Facebook, YouTube ve Twitter ve çeşitli forumları propaganda araçları olarak etkili şekilde kullanmaktadırlar. Ayrıca bu terör örgütlerinin kendi ideolojilerini yaymak ve destek bulmak niyetleriyle bizatihi açmış oldukları internet siteleri de mevcuttur. Terör örgütlerinin genellikle You-Tube'dan propaganda geliştirmek için, Twitter üzerinden ise bomba kullandıkları eylemleri yaymak için faydalandıkları görülmektedir (Choi, Lee ve Cadigan: 2018: 31-32).

İnternetin ve sosyal medyanın özgür ve serbest yapısı, kontrol edilmesinin zorluğu gibi özellikler de terör örgütlerinin bu alanlarda daha rahat aksiyon almalarını sağlamakta, propaganda için onlara hareket alanı sağlamaktadır. Bu yöntemle, hükümetleri zor durumda bırakmak, politik maksatlarını gerçekleştirmek, kamuoyunu yanıltmak ve korkutmak amaçlı birçok girişim yapılmıştır. Ayrıca propaganda sadece terör örgütleri tarafından kullanılan bir metafor değildir, politik amaca hizmet etmek amacıyla bir devlet tarafından da propaganda araçsallaştırılabilmektedir. Özellikle Soğuk Savaş döneminde iki ülke bloklarının birbirlerine karşı bir propaganda savaşına girdikleri de bilinmektedir. Günümüzde de devletler propagandayı, rakip devlet kamuoyunu etkilemek amacıyla gerçekleştirmekte, bu anlamda siber alandan da bu anlamda faydalanmaktadırlar (Vanlıoğlu, 2018: 208).

2.6. SİBER SAVAŞ

Siber alan ve ona ait terimlerin oldukça sık kullanılmasının 21. yüzyıla tekabül etmesi rastlantı olmamıştır. 21. yüzyıl teknolojik gelişmelerin hızlı bir

şekilde birbirini izlediği, internetin yaygınlaştığı, bilginin dijitalleştirildiği, birey, birey grupları ve hatta devletlerin bir nevi yaratmış oldukları bu yeni uzayda her türlü etkileşime rahatça geçebildikleri bir dönem olmuştur. Diğer taraftan gerçek dünyada olduğu gibi sanal dünyada da bu etkileşimler her zaman barışçıl niyetlerle gerçekleşmemiş, gerçekleşmemektedir. Buradan yola çıkarak, siber savaşın ne olduğunu, klasik savaş kavramıyla ne derecede örtüştüğünü, benzerlik, farklılık ve sonuçları itibariyle ortaya koymak önem kazanmaktadır. Söz konusu benzerlik ve farklılıkları anlayabilmek için klasik savaşın ne olduğunu da iyi saptamak gerekmektedir. Bunun için; savaş kavramının geçirmiş olduğu değişimlerin de göz önünde bulundurulması önemli olmaktadır.

Savaşın nitelik ve tanımlama olarak sürekli bir şekilde değişime maruz kalmasının en önemli nedenlerinden biri; teknolojideki değişimlerin de bir süreklilik göstermesidir. Geçmişten günümüze savaşın tanımlanmasında sınırlı-sınırsız, piyade-süvari, ateş gücü-manevra, savunma-saldırı gibi kriterler daha çok eldeki teknolojinin niteliği üzerinden hareketle ortaya çıkmıştır. Bu perspektiften bakıldığında 1648 öncesinde feodal beylerin sahip oldukları paralı askerlerle ve sınırlı bir savaş söz konusuyken, özellikle Sanayi Devrimi sonrasında ortaya konan teknik gelişmeleri izler şekilde savaşın topyekûn ve sınırsız bir aşamaya geçtiği görülmüştür. Bu anlamda Napolyon Savaşları iyi bir örnek teşkil etmektedir. Çünkü Napolyon, belki de Birinci Dünya Savaşı'ndan önce bir nevi yaygın bir savaşın örneğini ortaya koymuştur. Kimilerinin Napolyon Savaşları'nı ilk dünya harbi olarak kabul etmesinin temel nedeni budur. Teknik gelişmelerin ortaya koyduğu yeni durumla savaşı geniş bir coğrafyaya taşıyabilen devletlerin sonraki tecrübeleri de Birinci ve İkinci Dünya Savaşları olmuştur. Bu savaşlarda da muhkem kara ordular, deniz orduları, hava saldırı araçlarının yoğun bir biçimde kullanılması, savaşın niteliğini ve yıpratıcılığını tamamen değiştirmiştir. Soğuk Savaş döneminde ise nükleer silahların elde edilmesinin getirdiği bir yeni durum söz konusu olmuştur. Böylece savaş kavramı, savaş olgusu ve savaşın ortaya konma şekli zaman içerinde ve teknolojik gelişmelerin de etkisiyle farklılıklar göstermektedir. Bu farklılıkları ele alan William S. Lind'e göre; 1860 yılına kadar olanlar savaşlar birinci nesil savaşın örnekleriydi. Bu savaşlarda savaşan ve savaşmayanlar arasında kesin bir ayrım söz konusuydu ve belirsizlik söz konusu değildi. İkinci nesil savaşlar ise Birinci Dünya Savaşına kadar devam eden ve ateş gücünün kullanıldığı savaşlar olmuştur. Lind'e göre; üçüncü

nesil savaşlarda ise hız ve manevra gücü ön plana çıkmış ve İkinci Dünya Savaşı buna örnektir. Lind; günümüz savaşlarını ise ekonomik, siyasi, sosyal ve askeri şebekelerin bütünüyle kullanıldığı ağ tabanlı dördüncü nesil savaşlar olarak niteler. (Yalçınkaya, 2019: 1-7).

Savaşın sınıflandırılmasına yönelik fikirlerin ötesinde kavram olarak savaş, üzerinde mutabakat sağlanmamış bir kavram olmakla birlikte, ortaya atılan savlar itibariyle genel özellikleri yönünden bir fikir vermektedir. Buna göre savaş; düşmanca bir niyet sonucunda devlet ve devlet gruplarının sahip oldukları güç unsurlarını devreye sokarak, tarafların da ortaya çıkan eylemi savaş olarak niteledikleri ve kuvvet kullanımını içeren bir eylemdir (Varlık, 2013: 128). Böylece klasik savaş tanımlarında failler genel olarak devletler olarak düşünülmüştür. Tıpkı savaş kavramında olduğu gibi siber savaş üzerinde de hemfikir olunan bir kavramsallaştırma henüz mümkün olmamıştır. Siber savaşı; savunma mekanizmalarını bertaraf etmek niyetiyle ve yahut ekonomik, siyasi vs. zararlar vermek adına bilgisayar ağları, iletişim sistemleri ve altyapıları üzerinden gerçekleştirilen saldırılar olarak nitelendirmek mümkündür. Bir başka yönüyle siber savaşı; bilgi altyapısını zaafa uğratmak, işlevselliğini engellemek, var olan işlev ve hizmetleri bozmak veya imha etmek niyetiyle düşmanın savunma önlemleri almasını engelleyecek tüm bu süreçleri kapsayan eylemler olarak nitelemek mümkündür (Kaymak, 2017:3).

Görüldüğü üzere, siber savaş da tıpkı savaş kavramında olduğu gibi; zarar verme niyetini içerisinde barındırmaktadır. Yani siber saldırının gerekçesi kasten ve düşmanca bir şekilde, zarar verici sonuçların doğması istemiyle harekete geçirilmiştir. Fakat saldırının başında, klasik savaş kavramında olduğu gibi bir güç kullanımı söz konusu olmamaktadır. Diğer taraftan yukarıda da bahsettiğim gibi savaşın taraflarının değişiminin yanında, savaşın amacı ve araçlarının da değiştiği görülmektedir. Saldırılar, bilişim sistemleri üzerinden harekete geçmektedir ve bir güç unsuru ve yahut şiddet söz konusu değildir. Diğer taraftan savaşta; taraflar devlet veya devlet grupları olarak belirlenmişken, siber savaşta saldırıları gerçekleştiren taraf devlet olmak zorunda değildir. Fakat yaygın görüş, saldıran taraf devlet değilse bile devlet güdümünde bir güç olması gerekmektedir. Ayrıca saldırıları gerçekleştiren devlet olsa dahi, saldırıyı gerçekleştiren veya organize eden devletin,

siber uzayın doğasına uygun bir şekilde kimliğini gizlemesi, düşmanca saldırının kaynağını tespit etmede kesin kanıtlar sunmamaktadır. Sonuçları itibariyle ele alındığında ise, siber savaş neticesinde de tıpkı konvansiyonel savaşta olduğu gibi yıkıcı ve çok yönlü etkiler ortaya çıkabilmektedir. Fakat savaşın neticesinde bir fetih söz konusu olurken/olabilirken siber savaşta; siber uzayın kendine has niteliğinden dolayı bir fetih gerçekleştirilebilmesi söz konusu olmamaktadır (Rogers, 2018: 1).

Siber saldırıların hangi durumlarda siber savaş olarak nitelendirilebileceği üzerinde tartışmalar devam etmektedir. Örneğin Wikileaks belgeleri 2010 yılında kamuoyuna sızdırıldığında, ABD hükümeti bunun hem ABD'nin dış politikasına ve hem de uluslararası topluma yapılmış bir saldırı olarak nitelendirmiştir. Diğer taraftan kimilerince Wikileaks belgelerini yayınlayan Julian Assange'ın bunları bir saldırı niyetiyle değil, dijital bilgi kampanyası niyetiyle sızdırdığını iddia edenler de olmuştur. Fakat diplomatik yazışmaların sızdırıldığı bu olayın bir saldırı niyetiyle yapıldığı daha sonraki gelişmeler ışığında anlaşılmıştır. Wikileaks belgelerinin yayınlandığı sitenin de hacklenmesiyle; Wikileaks destekçilerinin gerçekleştirdiği karşı saldırılar yaygınlaşınca ortaya birçok devletin güvenlik sırlarının ifşa olduğu bir durum ortaya çıkmıştır (Ducheine, Votelink, Stinissen ve Gill, 2012: 102-103).

Siber savaşın diğer siber kavramlarıyla ne derecede örtüştüğünü ve ne derecede ayrıştığını açıklamak gerekmektedir. Keza birçok siber suç, siber saldırı, siber casusluk gibi eylem siber savaş olarak nitelendirilmemektedir. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde siber suçlar; sistemlere yetkisiz erişim, erişilen sistemlere ve sistemlerdeki bilgilere müdahale, bilişim sistemleri aracılığıyla dolandırıcılık ve sahtekârlık olarak belirlenmiştir. Bunun yanında çocuk pornografisi yayma, ırkçılık ve yabancı düşmanlığını körüklemek gibi internet ve bilgi sistemleri üzerinden yapılabilecek eylemler de yine siber suç olarak nitelendirilmiştir. Fakat bunların hiç biri bir devletin milli güvenliğine karşı alenen ve kasten gerçekleştirilmiş suç yahut saldırı yöntemlerinden olmadığından siber savaş olarak nitelendirilmemiştir. Diğer taraftan her siber saldırıyı da siber savaş kapsamına almak mümkün değildir. Örneğin; devlet kademelerinde görev yapan bir grup tarafından dahi yapılsa bu tarz siber saldırılar, karşı taraf bir devlet değilse -yani mağduriyet durumuna düşürülmüş olan bir devlet değilse- yine siber savaş olarak nitelendirilemez. Siber casusluk durumlarında, bir devlete ait olan gizli bilgilerin

ekonomik, siyasi ve yahut başkaca baskı aracı olarak kullanılması amacıyla, siber alanda gerçekleştirilen faaliyetler söz konusudur. Fakat bu faaliyetler de siber savaş olarak nitelendirilmemektedir. Siber casusluk; ancak siber savaşların nedenleri olarak ortaya çıkabilmektedirler. Siber terörizm ise faaliyetleri/eylemleri gerçekleştiren taraflardan birinin devlet olmaması nedeniyle siber savaş olarak nitelendirilmemektedir. Kısacası bir siber saldırının siber savaş olarak kabul edilmesi için; gerçekleştirilen siber saldırının bir devlet veya onun hâkimiyetindeki bir güç tarafından hayata geçirilmesi gerekmektedir. Ayrıca bu devlet yahut onun güdümündeki gücün; bilgisayar veya işletim sistemlerini kullanarak, sonuçları itibariyle genel bir savaşa neden olması gerekmektedir (Yayla, 2014:191-195).

Siber savaşın yeni bir savaş türü ifade edip etmediği üzerinde de birçok tartışma söz konusudur. Siber savaşı, konvansiyonel bir savaş türü olarak gören bakış, siber uzayı anlamada savaş terminolojilerinin kullanılmasını gerektirmektedir. Fakat siber uzayla ilgili henüz bir hukukun oluşmadığı dikkate alındığında, siber savaş ile ilgili de bu eksiklik kendini göstermekte, siber savaş suçları ve yahut siber savaş hukukunun sınırlarını belirlemede hangi kıstasların belirleyici olacağı bilinmemektedir. Keza siber uzayda; siber silahlar aracılığıyla siber saldırılar düzenlemek suretiyle gerçekleştirilen siber savaşların, savaşın yeni bir boyutu olarak algılayan görüşler bu istikamette ön plana çıkmaktadır (De Araujo, 2013:1-2). BM Şartı'nda da güç kullanımına yönelik maddede siber saldırılar neticesinde güç kullanılabileceği yönünde herhangi bir açık bilgi söz konusu değildir. Diğer taraftan siber savaş, konvansiyonel savaşta olduğu gibi güç kullanımı, politik bir amaç ve bu yolda kullanılan araçlar gibi şartların hepsine aynı anda sahip saldırılardan meydana gelmediği için; onu, savaş kavramının ilk anlamıyla değil, kendine özgü yapısıyla ele almak gerekmektedir (Struglinski, 2012: 2).

Siber ortamda ilk çatışmaya, Rus-Çeçen Savaşı esnasında rastlanmaktadır. Rusya, Çeçenistan üzerindeki anayasal hakkını kullanarak, Rusya'nın toprak bütünlüğünü korumak iddiasıyla 1994 yılında Çeçenistan'ın başkenti olan Grozni'ye girmiştir. Çeçenistan direnişinin Rus ordusu karşısında varlık gösteremeyeceği ve kısa süreceği düşünülmüşken; çatışma alanı ilk defa internet ortamına sirayet etmiş, Çeçenlerin etkili bir şekilde kullandıkları internet, medya ve diğer iletişim araçları

üzerindeki propagandayla beraber Rusya zor durumda bırakılmıştır[2] (Askerov, 2015: 8-15). Çatışmalarda öldürülen Rus askerlerinin fotoğraflarının internete yüklenmesi gibi birçok yöntem deneyen Çeçenler, Rus halkını da savaş karşıtı bir duruma itmeyi nispeten başarmışlardır. Ancak Rusya da bu siber hamleyi tespit etmiş, karşı propagandayı yine internet ve bilgi sistemleri üzerinden harekete geçirerek cevap vermeyi başarmıştır. Netice itibariyle ilk defa bir çatışmada siber alanın ne derecede etkili olabildiğinin görülmesi bakımından Rus-Çeçen çatışması iyi bir örnek olmuştur (Bıçakçı, 2012: 208-209).

Bilgi sistemlerinin bütün bileşenlerinin kullanılmasına ise ilk defa NATO'nun 1999 yılındaki Yugoslav müdahalesinde denk gelinmiştir. Daha çok propaganda ve dezenformasyona dayalı bir süreç olsa da sitelere erişimin engellenmesi, DDoS saldırıları ve hatta bir iddiaya göre Sloboden Milosevic'in banka hesaplarının ABD ordusu tarafından hacklenmesi gibi çeşitli siber saldırı yöntemleri de Yugoslavya müdahalesinde kullanılan yöntemler olmuştur. Siber alan ve onun bir elementi olan internetin çatışma boyunca artarak kullanılmış olması, bu müdahalenin kimilerince ilk siber savaş olarak nitelendirilmesini sağlamıştır. 2001 yılında ise Çin ve ABD'li hackerlerin başlattığı ve daha sonra diğer farklı ulustan hackerlerin da müdahil olduğu siber saldırılar bir siber dünya savaşı olarak addedilmiştir. Bu saldırıların arkasındaki neden ise ABD keşif ve gözetleme uçağının Çinli bir jet uçağıyla çarpışması sonucu Çin topraklarına iniş yapmaya zorlanması olmuştur. Örnekleri arttırmak mümkündür. Örneğin 2007 yılında Rusya tarafından gerçekleştirildiği öne sürülen Estonya'ya yönelik siber saldırılar, bir devlet tarafından diğer bir devlete yönelik olarak gerçekleştirilen ilk siber saldırılar olarak kabul edilmiş ve ilk siber savaş olarak addedilmiştir. 2008 yılında yine Rusya'nın Gürcistan'a yönelik olarak bir siber saldırılar furyası[3] gerçekleştirildiği iddia edilmiş ve bu da siber savaş olarak addedilmiştir (Cavelty, 2007: 369-371).

Netice itibariyle, siber alanın güvenlik paradigmasına eklemlenmesiyle beraber ve özellikle teknoloji ve bilgi sistemlerindeki ilerlemeyle siber kavramlar da

[2] Ayrıntılı bilgi için bakınız: Emil, Pain (2001). '' From the First Chechen War Towards the Second.'' Journal of World Affairs, Vol: 8, No. 1, pp. 7-19.

[3]Ayrıntılı bilgi için bakınız: Shakarian, Paulo. '' The 2008 Russian Cyber-Campaign Against Georgia.'' Military Review, January 2011. https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia /10.03.2020.

sıkça karşılaşılan ve dikkat edilmesi gereken kavramlar olmuşlardır. Bu duruma eşlik eder bir vaziyette, siber alandaki çatışma ve saldırıların artması siber savaş kavramını gündeme getirmiş ve onu önemli bir parametreye dönüştürmüştür.

ÜÇÜNCÜ BÖLÜM

3. ABD VE RUSYA'NIN YENİ REKABET ALANI: SİBER UZAY

3.1. ABD'NİN SİBER GÜVENLİK STRATEJİSİ VE TEMEL METİNLERİ

ABD'nin federal devlet yapısının, onun siber güvenlik stratejisinde ortaya çıkan referans belgelerinin de oluşumuna etki ettiği görülmektedir. Siber güvenlik stratejisinin oluşumu bilhassa askeri kanadın güçlendirilmesi yönüne kanalize edilmek istenmişse de, stratejinin oluşumuna katkı veren belgeler arasında askeri doktrinlerin dışında başkanlık direktifleri, eyaletler tarafından ortaya konulan strateji belgeleri, kurumların planlamaları ve çalışmaları da etkili olmuştur (Darıcılı, 2017: 5).

Söz konusu belge, doküman ve raporları bir mantıksal ve tarihsel iz düşümde ele almakta fayda vardır. Bu anlamda 1995 yılında Başkan Bill Clinton tarafından ortaya konan 13010 No'lu Başkanlık direktifi önemli bir yere sahiptir. Bu direktifin içeriğinde ABD'nin kritik altyapılarının devletin devamı için hayati öneme sahip olduğu vurgulanarak; buradan tezahür edecek fiziki veya radyo frekansları-bilgisayar temelli saldırılara (siber saldırılar) karşı uyarmıştır. Ayrıca bu kritik altyapıların ve sağlanan hizmetlerin birçoğunun da özel sektör eliyle hayta geçirildiğinin hatırlatıldığı direktifte, devlet ve özel sektörün bu alanda birlikte çalışarak bir strateji oluşturmaları gerektiği üzerinde görüş bildirilmiştir (Presidency Of USA, Executive Order 13010 Critical Infrastructure Protection). Bu belgenin genel seyri siber tehditlere ve siber güvenliğin saplanmasına yönelik uyarılar ve direktifler ortaya

koyarak, bu alandaki durumun tespitinin yapılmasını istemesi yönünden önemlidir. Böylece ABD'de ilk defa bir resmi belgede siber güvenliğe atıf yapılmıştır.

Bir diğer önemli belge ise yine bir başkanlık direktifi olarak ortaya konan ve 1997 yılında yayınlanan 63 No'lu başkanlık direktifidir. Bu direktifte de ABD'nin her geçen gün siber sistemlere daha bağımlı ve entegre bir yapıya büründüğü tespit edilmiştir. Telekomünikasyon, enerji, banka ve finans, su sistemleri, ulaşım, acil sistemler gibi kurum ve hizmetler kritik altyapılar olarak sıralanmış fakat bunların dışında birçok kritik altyapının olduğu da belirtilmiştir. 63 No'lu karar altyapı sistemlerinin geliştirilmesi ve korunmasına yönelik adımların atılmasında, bu altyapı ve sektörlerin itici gücü olan özel sektöre çağrı yapması bakımından da önemlidir. Bu direktiflerin siber terimlerine atıf yapmaları, bu terimlerin tanımlarına da katkı vermeleri söz konusu olmuştur. Ayrıca direktiflerin yerine getirilmesinde kurum ve görevlilerin atanması ve sorumluluklarının çizilmesi de bir diğer parametredir (Presidential Decision Directive 63 on Critical Infrastructure Protection, 1998).

Amerika Birleşik Devletleri'nin siber stratejisine kaynaklık eden ve tarihsel izdüşümü takip eden bir diğer belge; Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji isimli belgedir. Bu belge Şubat 2003 tarihinde yayınlanmış ve kendinden önceki belge ve direktiflere nazaran daha geniş bir analiz ve hedef skalası sunmuştur. Bu belgede siber uzay; ABD'nin bütün kritik altyapılarını birbirine bağlayan, hizmetlerin iletilmesine aracılık yapan, hemen hemen her alandaki hayati etkisine atfen ülkenin sinir sistemi olarak nitelendirilmiştir. Dokümanda, siber uzayın ülkenin ekonomik ve ulusal güvenliği açısından son derece önemli bir yere sahip olduğu ifade edilmiştir. Keza söz konusu belgenin İç Güvenlik Ulusal Stratejisi'nin ve Fiziki Temel Unsurların ve Kritik Altyapıların Korunmasına Dair Ulusal Stratejinin bir bütünleyicisi ve parçası olarak tanımlanması atfedilen bu önemi doğrular niteliktedir (Harknett ve James, 2011: 456).

Siber uzay; güvenliğin sağlanmasının zor bir mecra olduğu ortaya konulan belgede; siber uzayda hâkimiyeti sağlamak, güvenliği temel kılmak için gerekli ilk adımın toplumun bütün unsurlarıyla bu mücadeleye uyum sağlamalarından geçtiği ifade edilmiştir. Bu belgeye göre bunun yolu; federal devletin, yerel hükümetlerin, devletin, vatandaşların ve özel sektörün de dâhil olduğu bir strateji oluşturmaktan geçmektedir. Söz konusu stratejide özel sektörden bireylere, yerel hükümetten

federal hükümete kadar herkesin yapması gerekenler ifade edilmekte, koordine bir stratejinin gerekleri ortaya konulmaktadır. Siber Güvenlik Ulusal Stratejisi'nin (NSSC) hedefleri; ABD'nin kritik altyapılarına olası terörist atakları engellemek, ülkenin siber saldırılara karşı kırılganlığını azaltmak ve siber saldırılar gerçekleştiğinde oluşabilecek zararları minimize etmek ve onarım sürelerini tespit etmek olarak belirlenmiştir. Metnin devamında da ülkenin kritik altyapı ve olası zayıf yönleri tarif edilmiştir. Siber güvenliğin sağlanmasında devletin, hükümetin, ABD Güvenlik Departmanı'nın görev ve sorumlulukları açık bir şekilde ifade edilmiştir. Siber Uzayın Korunmasına Yönelik Ulusal belgede ABD'nin beş temel önceliğine de değinilmiştir. Federal bilgisayar sistem ve ağlarını korumak, bir müdahale sisteminin kurulması, bir tehditlere karşı kırılganlığı azaltma programı, siber güvenliğe ilişkin ilgi ve duyarlılığı arttırmak amaçlı eğitim programı ve uluslararası işbirliğini sağlamaya yönelik bir sistem kurmak bahsedilen önceliklerden olmuştur (The White House, National Strategy to Secure Cyberspace, 2003).

ABD'nin siber güvenlik belgelerinden bir diğeri; Başkan Obama tarafından göreve geldikten itibaren altı ay gibi kısa bir süre içerisinde, öncelikli bir konu olarak ortaya konan Siber Uzay Politika Revizyonu isimli 2009 yılına ait belgedir. Belge incelendiğinde esasen bir sonraki siber güvenlik stratejisinin ilk emarelerini barındıran, onun habercisi bir nitelik gösterdiği fark edilmektedir. Adeta bir taslak metin olarak addedilebilecek bu metnin temelde bürokratik yapıyı, siber güvenliğin gereklerini yerine getirebilecek bir merhaleye taşımayı hedeflediği görülmektedir. Bürokrasinin doğru yapılanmasının siber güvenliği sağlamada ve yöneltilecek tehditlerle mücadelede önemli bir yere sahip olduğunun dikkate alınmasını gerekliliğini saptayan bu belgeye ayrıca önem atfedilmiştir (Harknett, Callaghan ve Kauffman, 2010: 4-5).

Siber Uzay Politika Revizyonu isimli bu belgenin temel amaçlarından biri de güvenilir ve esnek bir bilgi-iletişim altyapısını sağlamaktı. Bu amaca hizmet eder şekilde, Kongre'den de çeşitli yasalar yapmak suretiyle, Siber Güvenlik yapılarının sağlıklı ve daha basit bir şekilde ele alınmasını sağlayacak şekilde düzenlemeler yapılmıştır. Bu yasaların yürürlüğe girmesiyle beraber kurumlar arasında çeşitli görev transferleri de söz konusu olmuştur. Örneğin; 2009 Siber Güvenlik Yasası'nın öngördüğü en önemli adımlardan biri siber güvenlikle ilgili bir takım

sorumlulukların Savunma Bakanlığından alınarak Beyaz Saray İcra Ofisine devredilmesi olmuştur (Harknett ve Stever, 2009: 1-3).

Temel olarak bu belgenin en önemli özelliği; güçlü, esnek ve işler bir siber güvenlik mekanizmasının kurulmasına referans vermesidir. Bunun sağlanması için belgede gerekli kriterler beş başlık altında toparlanmıştır. İlk başlıkta siber güvenliğin en tepeden yönetilmesi gerektiğine dikkat çekilmiştir. Bunun bir gereği olarak Başkan'a bağlı bir siber güvenlik ofisinin kurulması ve yine Başkan'a bağlı bir takım görevlilerin bu alandan sorumlu hale getirilmesi gerektiği vurgulanmıştır. Ayrıca siber güvenliğe yönelik yasa ve politikaların gözden geçirilmesi gerektiği ifade edilmiştir. Diğer taraftan siber güvenliğe dair federal hükümette, devlette ve diğer kurumlarda bulunan yetkilere ilişkin hesap verilebilirliği sağlamak önemli bir adım olarak ortaya konmuştur. İkinci başlıkta; dijitalleşmiş bir ulusun bu alana dair daha fazla bilinçlendirmesi gerektiği fikri ön plana çıkartılmıştır. Siber güvenlik tehdit ve risklerine yönelik toplumun bilgilendirilmesi gerektiği; bu nedenle bireylerden şirketlere kadar siber güvenliğin öneminin kavranmasının öneminden bahsedilmiştir. Bu süreçte devlet ve federal hükümetin gerekli bilgilendirmeleri yapması elzem addedilmiştir. Üçüncü başlıkta; siber güvenliğin sağlanmasında sorumlulukların federal hükümet, şirketler ve ABD'nin müttefikleriyle paylaşılmasından bahsedilmektedir. Böylece siber uzayda daha geniş ve kapsayıcı bir partnerlik oluşturulabilecektir. Dördüncü başlık; etkili bilgi paylaşma ve olaylara müdahale sisteminin kurulmasının gerekliliğini ortaya koymaktadır. Beşinci başlıkta ise birey, şirket ve özel sektörü yenilik yapma yolunda sürekli bir şekilde teşvik etmenin gerekliliğinden bahsedilmiştir. Buna teknolojik yatırımların yapılmasından akademik araştırmalara kadar birçok alan dâhil edilmiş ve sayılmıştır (The White House, Cyberspace Policy Review, 2009).

Barrack Obama'nın talimatlarıyla hayata geçirilen ve ABD'nin siber uzay hedeflerini ortaya koyan bir diğer belge Mayıs 2011 tarihinde yayınlanan Siber Uzay İçin Uluslararası Strateji: Ağlara Dayalı Bir Dünyada Refah, Güvenlik ve Açıklık isimli strateji belgesidir. Obama, söz konusu stratejinin bir ilk olmadığını ama ilk defa uluslararası partnerlere ve diğer aktörlere ABD'nin siber uzaydaki amaç, vizyon ve hedeflerini açıkça ortaya koyan ve duyuran bir belge olarak bahsetmektedir. Siber uzaydaki tehditleri azaltmak adına uluslararası bir tavırdan bahsederek siber uzayın

güvenli ve açık olması için bütün ülkeleri de bu konuda işbirliğine çağırmaktadır (Fidler, 2011: 1-2).

Mayıs 2011 tarihli bu belgede ABD'nin stratejik yaklaşımından belli başlıklar altında bahsedilmiştir. Buna göre; siber uzayı bir fırsat alanı olarak gören ABD, aynı zamanda buradan doğabilecek olası tehditlerin söz konusu faydalara zarar verebileceğini de öngörmekte, bu nedenle hem ulusal ve hem de uluslararası siber güvenlik politikalarını hayata geçirmeyi hedeflemektedir. ABD, söz konusu ağların (siber alanın etki alanının genişlemesi) ekonomi ve güvenliğe yönelik yeni handikaplar doğduğunu tespit etmektedir. ABD, söz konusu tehditleri temel argümanlar olan özgürlük, bilginin serbestliği ve güvenliği gözeterek elemine etmeyi amaçlamaktadır. Ayrıca açık, güvenilir, yönetilebilir kritik altyapıların inşa edilmesiyle ekonomi ve ticareti teşvik eden bir siber uzay hedeflenmektedir. Bir diğer hedef; bu kriterleri uluslararası alanda diğer devletlerin de paylaştığı bir konuma yerleştirerek, bütün paydaşların hemfikir olduğu diplomasiye dayalı politikalar oluşturmaktır (Eichensehr, 2014).

Belge'de söz konusu öncelikleri dikkate almayarak siber uzayı, tehdit unsuru haline getirmeyi amaçlayan aktörlere karşı ABD'nin karşılık verme hakkının saklı bulunduğu hatırlatılmaktadır. Ayrıca talep edilmesi ve ihtiyaç duyulması halinde gerek uluslararası örgüt ve şirketlere ve gerekse de hükümetlere kritik altyapıların güçlendirilmesine yönelik destek sağlanacağı ifade edilmiştir. Metinde üzerinde mutabık kalınacak uluslararası siber hukuk normlarının oluşturulması gerektiği üzerinde de durulmaktadır. Siber uzayı korumak ve buradan gelebilecek tehlikelerden korunmak için askeri sistemleri ve ağları güçlendirme ihtiyacından bahsedilmektedir (The White House, International Strategy for Cyberspace, 2011; 1-15).

2015 yılının şubat ayında yayınlanan Ulusal Güvenlik Stratejisinde de siber güvenliğe referans verilmiştir. Bu strateji belgesinde ABD'nin siber güvenlik önceliklerine ve gerek Çin gerek Rusya tarafından gelebilecek olası tehditlerden bahsedilmektedir. Özellikle Rusya'nın koşu ülkelerine yapmış olduğu siber saldırılardan endişe duyulduğu ve söz konusu ülkelere ABD'nin her türlü desteği vereceği vurgulanmaktadır (Darıcılı, 2017: 6). Söz konusu belgede ABD'nin bu tehditlere karşı koymak adına her hakkının ve gücünün bulunduğu, özellikle kritik

altyapıların korunması için bu gücünden faydalanacağı belirtilmektedir. Ayrıca kritik altyapıların, internetin ve diğer devletlerin de altyapılarının korunmasına yönelik ABD'nin katkılarının süreceğine işaret edilmektedir (The White House, National Cybersecurity, 2015).

ABD Savunma Bakanlığı Siber Stratejisi isimli belge 2015 yıllında kabul edilen ve Savunma Bakanlığı'na; diğer kurumlarla eşgüdüm halinde ABD anavatanını korumanın yanında yeni bir görev daha tanımlanmıştır. Buna göre ABD Savunma Bakanlığı; siber uzaydan gelebilecek her türlü tehlike ve saldırılara karşı ülkeyi korumakla görevlendirilmiştir. ABD'nin yasalarıyla ve uluslararası yasalarla tutarlı bir şekilde, Savunma Bakanlığı, barış, kriz veya çatışma zamanlarında ABD'nin ulusal çıkarlarına zarar vermek isteyen herhangi bir düşmana karşı saldırıları engellemek ve Birleşik Devletleri savunmakla yükümlü kılınmıştır. Buna göre Savunma Bakanlığının ağlarını, sistemlerini ve bilgilerini savunmak; ülkeyi yıpratıcı siber saldırılara karşı savunmak; operasyonel ve acil durum planlarını desteklemek bakanlığın öncelikli görevleri arasına girmiştir (The Departman of Defense, [DoD], The DoD Cyberstrategy, 2015; 1-5).

ABD Savunma Bakanlığı Siber Stratejisi belgesi 2011 yılında yayınlanan siber strateji belgesine nazaran daha kapsayıcı ve daha şeffaf bir nitelik göstermektedir. Belgede siber saldırılarla baş etmek için istihbarat örgütleri ve özel şirketler arasındaki işbirliğini devam ettirmenin ve geliştirmenin önemi vurgulanmaktadır. Ayrıca siber saldırılara karşı koymak ve caydırıcılık için uluslararası ittifaklar ve ortaklıklar üzerinde yeni bir vurgu yapılmıştır. Bilhassa Ortadoğu, Asya Pasifik ve NATO müttefiklerinin siber güvenliği sağlamak ve bu bölgelerde hâkimiyet adına teşvik etmeye çalışılmaktadır (Zheng, 2015; 1-2).

ABD Savunma Bakanlığı Siber Stratejisi 2018 yılında güncellenmiştir. Bu belgede de yine siber uzayda bir yarışın söz konusu olduğu açıkça ifade edilmektedir. Buna göre ABD'nin rakipleri; ABD'nin siber alandaki yeteneklerini elemine etmek, askeri avantajlarını ve altyapısını aşındırmak için sürekli bir yenilenme ve arayış içindedir. Bu nedenle Bakanlık'ın söz konusu siber tehditleri ortaya çıkarmak, etkisiz hale getirmek ve ABD'nin ağ sistemlerini bu tehditlerden etkilenmeyecek biçimde dizayn etmek gibi görevlerine değinilmektedir. ABD silahlı kuvvetlerinin her alanda olduğu gibi siber alanda da bu tür tehlikelerle baş etme ve savaşabile yeteneğinin

bulunması gerektiğinden bahsedilmektedir. Ayrıca ABD'nin çıkarlarına korumak için müttefik ülkelerle bilgi ve istihbarat temelli karşılıklı çalışmalar yapılmasının gerekliliğine bu belgede de yer verilmektedir (DoD, 2018; 1-7).

Son olarak 2018'de Başkan Trump döneminde yayımlanan Amerika Birleşik Devletleri Ulusal Siber Stratejisi'nden bahsetmek gerekmektedir. Henüz belgenin ilk sayfasında Trump siber güvenliğin ABD için hayati öneminden bahsettikten sonra ülkenin sistemlerinin tam olarak tehdit ve saldırılarla mücadele zorluklar ile karşılaştığından bahsetmektedir. Trump döneminin önemli bir hamlesi, her kurumu ve başkanının kendi inisiyatifleri altındaki kurumun siber güvenliğini sağlamada görevli kılması olmuştur. Ayrıca 13800 No'lu Başkanlık Direktifi: Federal Ağların ve Kritik Altyapıların Güçlendirilmesi belgesinin bu siber stratejiye temel oluşturmuştur. ABD Ulusal Siber Stratejisi'nde de önceki siber stratejilerde olduğu gibi öncelikler ve hedefler belirlenmiştir. Buna göre; ağları, sistemleri, fonksiyonları ve verileri korumak; yurt içindeki yenilikleri daha fazla desteklemek suretiyle ekonomideki dijitalleşmeyi artırarak refahı arttırmak; Birleşik Devletlerin siber kabiliyetlerini arttırarak barışı tehdit eden bir duruma müdahale etme yeteneği kazanmak ve son olarak ABD'nin yurt dışındaki etkinliğini artırarak internetin daha açık ve güvenilir bir hale getirilmesini sağlamak bu hedef ve öncelikler arasına girmiştir (The White House, National Cyber Strategy, 2018).

3.2. ABD'NİN İLGİLİ SİBER GÜVENLİK KURUM VE KURULUŞLARI

ABD siber güvenlikte organizasyon ve kurumsal yapılanma bağlamında karmaşık bir yapı sunmaktadır. Fakat yine de üç temel üzerinden bir siber güvenlik şeması oluşturmak mümkündür. ABD'nin temelde; ABD Savunma Bakanlığı (US DoD), ABD İç Güvenlik Bakanlığı (DHS), ve gizli servisler (FBI/CIA) üzerinden bir siber organizasyonu vardır. Bunların dışında da çeşitli ajanslar ve resmi kurumların siber güvenlik vazife ve inisiyatifleri bulunmaktadır. Diğer taraftan eyaletler de merkezi hükümetin dışında geliştirmiş oldukları siber ağlar eliyle güvenliklerini sağlama yoluna gitmektedirler (Darıcılı, 2017; 7).

3.2.1. ABD Savunma Bakanlığı (The Departmant of Defense)

ABD Savunma Bakanlığı; kendisinin ve kendisine bağlı kuruluşların ağlarını ve yine Savunma Bakanlığının ulusal ve uluslararası bilgi sistemlerini ve kritik öneme sahip altyapılarını, siber uzaydan kaynaklanacak tehdit ve saldırılardan korumakla görevlidir. ABD Savunma Bakanlığı'nın silahlı kuvvetlerde meydana gelen siber suçların araştırılması noktasında da yetki ve sorumlulukları vardır. Ulusal güvenliğin sağlanmasına yönelik olarak, yabancı siber tehditlerin araştırılması ve bilgilerin toplanması da yine Bakanlık'ın görev alanına girmektedir. Siber suçların ve saldırıların önlenmesine yönelik önlemler alma, raporlar hazırlama, diğer kurumlarca hazırlanan raporlara katkı vermek de yine sorumluluklarındandır (NATO Cooperative Cyber Defence Centre of Excellence, 2016: 19).

2015 yılında yayınlanan ABD Savunma Bakanlığı Siber Stratejisi'nde de bakanlığın görevleri açıkça belirlenmiştir. Buna göre kriz, çatışma, savaş ve barış dönemlerinde vatanı; siber uzaydan gelebilecek tehditleri de içeren bir şekilde her türlü tehlikeye karşı savunmak bakanlığın asli görevidir. Bu amaca hizmet eder şekilde; Savunma Bakanlığı'nın dizayn edilmesi ve beklentilere cevap verecek bir organizasyon ve etkinliğe kavuşturulması da görev tanımlamasının içinde yer almıştır. Ayrıca federal hükümet, diğer daire ve ajanslar, eyalet ve yerel yönetimler, müttefik ve partnerler ve özel sektörle koordine bir sistemin geliştirilmesini gözetmek de bu noktada Savunma Bakanlığı'nın önemli sorumluluklarındandır. Bütün bu aşamalarla beraber, ABD Savunma Bakanlığı'nın ulusal stratejinin oluşmasındaki payının da büyük ve önemli olduğu görülmektedir (The Departman of Defense, [DoD], The DoD Cyberstrategy, 2015; 1-32).

Savunma Bakanlığı'nın siber güvenlik ile ilgili en yetkili ve etkin yapılanması US CYBERCOM'dur. CYBERCOM, Savunma Bakanlığı'na bağlı bir şekilde çalışan ve koordinasyondan sorumlu olan USSTRATCOM bünyesinde 2010 yılında kurulmuştur. Amacı ve görevi; ulusal ve uluslararası ortaklarla işbirliği içinde ulusal çıkarları korumak ve ilerletmek için siber planlama ve operasyonları yönlendirmek, senkronize etmek ve koordine etmektir.

- Ordu ABD Siber Komutanlığı (ARCYBER)
- 24. Hava Kuvvetleri - Hava Siber Kuvvetleri (AFCYBER)
- ABD Onuncu Filosu - Filo Siber Komutanlığı (FLTCYBER)
- ABD Deniz Piyadeleri Siber Komutanlığı (MARFORCYBER)

gibi önemli kuvvet ve komutanlıkları bünyesinde barındırması bakımından da siber güvenlikte önemli bir yere sahiptir. Böylece CYBERCOM kara, hava, deniz gibi çok yönlü ve çok taraflı bir şekilde, ABD'yi gelebilecek siber tehditlere karşı korumayı hedeflemektedir (US CYBERCOMMAND, US Cyber Command History, 2019).

ABD Savunma Bakanlığı bünyesindeki Ulusal Güvenlik Ajansı (NSA) da siber güvenlikle ilgili önemli bir kuruluştur. Bu kuruluşun temel hedefi ülkenin siber güvenlik sistemlerini korumak ve savunmaktır. Daha açık olarak; gizli bilgi içeren ve askeri-istihbarat misyonları için kritik öneme sahip ağları korumakla sorumludur. NSA, düşman unsurların da siber faaliyetlerini izleyen bir yapı sergilediği için bu noktada da ilgili kurumlara önemli bilgiler sağlayabilmektedir. NSA siber güvenlik açıklarını, kırılganlıkları ve olası tehditleri kurumlara, özel sektöre ve ilgililere açık bir şekilde duyurmakta, onları bilgilendirmektedir. Savunma Bakanlığı bünyesinde bu kuruluşların altlarında da çeşitli birimler vardır ve her biri kendi alanlarında ve ilgili oldukları kurumlarla beraber uyum içerisinde hareket etmektedirler. Bunlara Birleşik Siber Merkezler denmektedir. Birleşik Siber Merkezlerin de kendi içlerinde Savaş Destek Elemanları isimli yapılanmaları mevcuttur (National Security Agency, Cybersecurity, 2019).

3.2.2. Amerika Birleşik Devletleri İç Güvenlik Bakanlığı (Departmant of Homeland Security/ DHS)

DHS de siber güvenliğin sağlanmasında önemli bir kurum niteliğindedir. İç Güvenlik Bakanlığı, ABD sınırları dâhilinde siber güvenlikten sorumlu birincil kurumdur. Fakat federal bilgi sistemlerinin korunmasında yasal sorumlulukları oldukça sınırlıdır (NATO Cooperative Cyber Defence Centre of Excellence, 2016: 15-16). Bakanlık ayrıca federal hükümeti ve ABD'nin kritik altyapılarını yahut bilgi sistemlerini etkileyebilecek siber uzay olaylarına da odaklanmaktadır. Bu altyapılara herhangi bir tehdit veya saldırı durumunda, kriz yönetimine katkı sunmak, kriz halinde devreye sokulacak olan acil kurtarma planları hakkında diğer kamu kurumlarını ve özel sektörü bilgilendirmek; paydaşların eşgüdümlü bir savunma stratejisi ve planları olması adına onlar arasındaki koordinasyonu sağlamak; ülkenin teknoloji alanındaki gelişmeleri iyi takip edebilmesi adına gerekli araştırma-

geliştirme faaliyetlerini yapmak da önemli görevlerindendir. ABD İç Güvenlik Bakanlığı sayılan görevleri Ulusal Siber Güvenlik Karşılık Sistemi (The National Cyberspace Security Response System) adını verdiği yapılanma eliyle yerine getirmektedir (The White House, The National Strategy to Secure Cyberspace, 2003: 1-60).

ABD İç Güvenlik Bakanlığı'nın operasyonel gücünü temsil eden kuruluşu Ulusal Koruma ve Program Direktörlüğü (NPDD)'dür. Fakat yasal altyapının yetersizliği kurumun da eylem ve hareketlerini kısıtlamaktadır. NPDD kendi içerisinde Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi'ni (National Cybersecurity and Communication Integration Center/ NCCIC) barındırmaktadır ki bu merkez siber güvenlik konusundaki temel aktör olarak lanse edilmektedir. Ülke genelinde ve eyaletlerdeki her türlü siber güvenlik olayını izleme, takip etme ve müdahale etme hakkına sahip bu kurum ayrıca özel sektör ve istihbarat örgütleri arasındaki ilişkide de köprü konumundadır. Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi de bünyesinde Bilgisayar Acil Durum Hazırlık Ekibi (Computer Emergency Readiness Team/ CERT) ve Endüstriyel Kontrol Sistemi Bilgisayar Hazırlık Ekibi (Industrial Control System Computer Readiness Team/ ICS-CERT) gibi iki icracı birim barındırmaktadır. CERT federal kurumlar adına tehditleri tespit ve önleme mekanizmaları geliştirmekle yükümlüdür. Ayrıca özel sektör kuruluşlarına ve uluslararası ortaklara siber alandan kaynaklanabilecek tehditler hakkında bilgilendirmede bulunmaktadır. ICS-CERT ise kritik altyapı şirketleri ve kamu-özel ortaklıklarıyla beraber çalışmakta, izleme ve analitik hizmetler sunarak kritik altyapı hizmetleri sunan şirketlere bilgi ve destek sunmaktadır (Lewis, 2016: 52).

3.2.3. FBI ve CIA

ABD'nin siber güvenlik alanında direk olmasa da siber şemsiyede önemli rolleri olan diğer iki kurum; istihbarat kurumları olan Federal Bureau of Investigation (FBI) ve Central Intelligence Agency (CIA)'dir. FBI'nın hedeflerinden en kritik ve esas olanı; ABD'yi ileri teknoloji ve siber yollar kullanılarak hedef alabilecek terör organizasyonları ve eylemlerine karşı korumaktır. FBI, Adalet Bakanlığı'na siber ortamlarda gerçekleştirilen zorbalık ve kanunsuzlukları, terörist faaliyetleri rapor

eder şekilde; siber suçlara uygulanacak cezai kanun uygulamalarında görüş bildirir mahiyette bir danışma görevi de görmektedir. Söz konusu görevleri yerine getirme dürtüsüyle, FBI; kendi içerisinde bir organizasyonel yapılanma kurmuştur. Bu organizasyon Ulusal Siber Araştırma Birleşik Gücü **(**National Cyber Investigative Joint Task Force/NCIJTF) ile FBI'ya bağlı diğer 56 saha ofisi ve onların altında çalışan diğer araştırmacı kadrolar aracılığıyla sağlanmaktadır. NCIJTF, tüm devlet birimlerinin iç siber tehditler konusunda birbirleriyle entegre, koordine ve bilgi paylaşır vaziyette çalışmasına öncülük ve aracılık etmektedir. NCITJF, istihbarat topluluklarından ve yine kanun uygulayıcı üyelerden oluşmakta ve küresel hedeflere de yönelmektedir. Tüm bu görevleri yerine getirmek amacıyla organizasyon şemasında Siber Suç Bölümü(Cyber Criminal Section/CSS) ve Siber Ulusal Güvenlik Bölümü (Cyber National Security Section/CNSS) gibi örgütlenmelere gitmiştir. ABD Savunma Bakanlığı (DoD) ve ABD İç İşleri Bakanlığı'nın (DHS) aksine savunma faaliyetleri değil, teröristleri ve terörist faaliyette bulunan diğer aktörleri takip ederek imha etmeyi hedefleyen aktif faaliyetler sürdürmektedir (Tırrell, 2012: 60-61).

Netice itibariyle FBI üç türlü siber aktöre karşı tüm savunma ve önlem mekanizmalarını harekete geçirmektedir. Bunlar; finansal hizmet sektörlerini hedef alan ve genellikle profesyonellerden oluşan suç organizasyonları, arkalarında diğer devletlerin olduğu ve fikri mülkiyet dâhil olmak üzere önemli ve stratejik verilere ulaşmaya çalışan siber ajanlar ve ABD ulusal güvenliğine karşı yıkıcı eylemlerde bulunmak üzere siber organizasyon geliştiren ve bunları harekete geçirmeye çalışan siber terörist gruplardır (Tsakanyan, 2017: 343).

ABD üst politika yapıcılarına ulusal güvenlikle ilgili bilgi ve istihbarat sağlayan özerk bir yapı olan CIA (Central Intelligence Agency) bünyesinde Bilim ve Teknoloji Müdürlüğü (DS&T) ve Dijital İnovasyon Müdürlüğü gibi iki önemli kurumu barındırmaktadır. Bunlardan Bilim ve Teknoloji Müdürlüğü; siber tehditlere karşı veri toplama, analiz etme ve bu problemlere yol açan tehditlere karşı koyma görevini üstlenmiştir. Ayrıca bu işlemleri daha hızlı ve güvenilir yapabilme adına gerekli veri toplama, analiz işleme süreçlerini yeni teknolojiyle birleştirme yoluna gidilmektedir. Dijital İnovasyon Müdürlüğü ise en yeni bilişim teknolojileri yardımıyla siber tehditleri bertaraf etmek için gerekli inovasyon geliştirmelerini

sağlamakla yükümlüdür (Cyber Security Intelligence, Cyber Intelligence Agency, 2019). Tüm bu altyapısıyla beraber CIA de tıpkı FBI gibi siber tehditleri analiz ederek bunları etkisiz hale getirmeyi, siber istihbarat sağlamayı ve bunları yaparken de gizli bir yol takip etmeyi görev edinmiştir. CIA birçok farklı ülkede hem istihbarat ve hem de aktif olarak bu görevlerini yerini getirmektedir.

3.3. RUSYA FEDERASYONU'NUN İLGİLİ SİBER GÜVENLİK STRATEJİSİ VE TEMEL METİNLERİ

Rusya Federasyonu'nun siber güvenlik ile ilgili ilk çalışmaları SSCB'ye kadar geri götürülebilir bir geçmişe haizdir. Fakat siber olanın ve siber alanın tartışılmaya başlanmasını takip eden sürece tekabül eden ilk Rusya Federasyonu menşeli belge; 24 Ocak 2000 tarihinde ortaya konmuş olan Rusya Federasyonu Ulusal Güvenlik Konsepti (National Security Concept of Russian Federation) isimli belgedir. Bu belge genel anlamda birey, toplum ve devleti her türlü iç ve dış tehlikelerden korumayı amaçlayan bir hedef ortaya koymaktadır. Rusya Federasyonu'na yönelik tehditlerin ekonomik, politik, teknolojik ve güvenlik gibi çeşitli tasniflerle açıklandığı bu belgede; söz konusu tehditleri bertaraf etmek için uygulanması gereken politikalara da vurgu yapılmaktadır. Bir diğer önemli vurgu ise bu tehditlerle mücadelede enformasyon güvenliğinin öneminedir. Rusya Federasyonu'nun ulusal enformasyon altyapı sistemlerinin korunarak uluslararası bilgi ağına katılımının sağlanması, enformasyon üzerinden gerçekleştirilebilecek her türlü tehdide karşı etkili bir korunma sağlanılması gibi kritik hedefler ve politikaların belirlenmesi gerektiği ortaya konmuştur (The Ministry of Foreign Affairs of the Russian Federation, National Security Concept of The Russian Federation,2000).

Bir diğer önemli belge 9 Eylül 2000 tarihli Rusya Federasyonu Bilgi Güvenliği Doktrini (Information Security Doctrine of Russian Federation)'dir. Bu belge bilgi güvenliği alanında hedefler, politikalar ve prensiplere ilişkin resmi görüşü yansıtan temel bir kılavuz niteliği taşımaktadır. Hükümetin bilgi güvenliğine ilişkin politikasını şekillendirmek, yasal mevzuatı ve prosedürleri geliştirmek, bilimsel-teknik ve organizasyonel altyapının oluşumuna katkı vermek gibi öncelikler üstlenen bu doktrin niteliğindeki belge bu nedenle önemli bir yere sahiptir. Bir diğer önemli

hedefi ise ulusal bilgi güvenliği programlarının oluşturulmasıdır. Bu belgede Rusya Federasyonu'nun dört önemli çıkarının bilgi güvenliği alanında da gözetilmesi gerektiği ortaya konmuş ve bunlara yönelik önlem ve politikalara işaret edilmiştir. Bu çıkarların ilki; Rus vatandaşlarının anayasal haklarının gözetilmesi ve buradan gelebilecek tehditlere karşı korunması, Rus kültürünün, toplumun manevi değerlerinin olumsuz etkilerden uzak tutulmasıdır. İkincisi; Rusya Federasyonu'nun siyasal ve sosyal olaylar karşısındaki resmi duruşunun açık bir şekilde deklare edilerek, devletin güvenirliliğinin ortaya konmasıdır. Üçüncüsü; modern bilgi teknolojilerini teşvik etmek, ulusal bilgi ağını kurarak ülke içindeki paydaşların bu hizmetlerden faydalı bir şekilde yararlanmalarını sağlamaktır. Dördüncüsü ise; bilgi-bilişim kaynaklarını izinsiz erişimlere karşı korumak amacıyla gerekli olan güvenlik önlemlerinin alınmasıdır (Information Security Doctrine of Russian Federation, 2000: 1-5).

12 Mayıs 2009 tarihinde yayınlanan 2020'ye Doğru Rus Ulusal Güvenlik Stratejisi *(Russia's National Security Strategy to 2020)* isimli belgede iç ve dış tehditler tanımlanmakla beraber; bunları bertaraf etme yönünde çeşitli öneriler de bulunmaktadır. Belgenin on yıllık bir hareket planı belirlemesi önemlidir. Bu anlamda söz konusu; belge on yıllık süreçte Rusya Federasyonu'nun güvenlik anlamında dönüşen uluslararası sistemin yapısına uygun politikalar geliştirmesi gerektiği fikrini işlemektedir. Belgenin gerçekçi ve yapıcı bir tavırla ortaya konması da önemli bir özelliğidir. Rusya Federasyonu'nun rakiplerinin olası tehditleri göz önünde bulundurulurken diğer taraftan da uluslararası güvenlik, kalkınma ve ekonomi gibi işbirliği alanlarına da vurgu yapılmıştır. Belge, istikrarı güvence altına alabilecek modern bir orduya geçiş yapmak için silahlı kuvvetlerin organizasyonel yapısının geliştirilmesi, ordunun silahlarının modernleştirilmesi gerektiğini belirtmektedir. Aksi takdirde siber alanda elini güçlendiren ülkelerle baş edilemeyecektir. Fakat hangi ülkelerin siber silahlarını geliştirdiklerine dair açık bir bilgi bulunmamaktadır (Dimitrakopulau ve Liarapoulos, 2010: 1-40).

Rusya Federasyonu Silahlı Kuvvetlerinin Bilgi Alanındaki Aktivitelerine İlişkin Kavramsal Görüşler (The Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space) adlı belge 2011 yılında Rusya Federasyonu Savunma Bakanlığı tarafından yayımlanmıştır. Bu

belgede de göze çarpan ana unsur; bilgisayar ağları üzerinden gerçekleştirilen operasyonları güvenliğin bölünmez bir parçası olarak görmesidir. Dikkat çeken bir diğer unsur; batılı devletlerin kullanmış oldukları siber güvenlik (cyber security) kelimesi yerine bilgi güvenliği (information security) kelimesinin tercih edilmesidir. Söz konusu tercih diğer Rus doktrin ve stratejileri için de geçerlidir (Jaitner ve Mattsson, 2015: 40-41). Bu belgenin aslında bir nevi ABD tarafından 2011'de yayımlanan ABD Savunma Bakanlığı'na ait siber stratejiye bir tepki olarak ortaya çıktığı görülmektedir. Belgede siber alan; silahlı kuvvetlerin operasyon geliştirebilecekleri bir alan olarak tanımlanmaktadır. Bu nedenle Savunma Bakanlığı'nın iletişim ağlarını güçlendirmenin önemine vurgu yapılmaktadır. Ayrıca siber güvenlik stratejisinin uygulanabilirliğinin sağlanması adına kamu-özel sektör birlikteliğinin önemi vurgulanmaktadır. Ayrıca NATO ve ittifakından gelebilecek tehditlere karşı ortak savunma ve önleme sistemlerinin gerekliliği tespit edilmiştir. Son olarak siber alanda etkili olabilmek adına; siber kabiliyetlerin geliştirilmesi gerektiği fikri bu belgeye hâkim olmuştur (Darzcewska, 2016: 17-18).

Siber güvenlikle ilgili önemli belgeler arasında bir diğeri 27 Şubat 2013 tarihinde Military-Industrial Kruer adlı dergide The Value of Science in Prediction isimli Rusya Federasyonu Genel Kurmay Başkanı Valery Gresimov tarafından yazılan makaledir. Söz konusu makale literatüre ise Gresimov Doktrini olarak geçmiştir (Fridman, 2019: 101). Makalede Gresimov; savaşın yakın geçmişte ve bugün algılanış biçimini açıkladıktan sonra yakın gelecekte nasıl bir hal alacağı üzerinde de öngörülerde bulunmaktadır. Gresimov'un konumu itibariyle söz konusu makalede bahsedilen perspektifin, Rusya Federasyonu'nun da savaşa ilişkin görüşlerinin yansıttığı düşünülmüştür (Bartles, 2016: 30). Gresimov'a göre; gelecekteki savaşlar daha ufak çapta cereyan edecektir. Bunun da ötesinde savaşlarda mekânsallık eski önemini yitirecektir. Çünkü ağ bağlantılı komut ve kontrol sistemleri sayesinde yüksek hassasiyetli silahların kullanılmasının önü açılmış, savaşlar da bu minvalde bir değişim geçirmiştir. Gresimov, siber alanı/bilgi alanını düşmanın savaş potansiyelini azaltmak adına önemli bir mecra olarak gördüğünü, bilgi ağları üzerinden devletlerin ve vatandaşlarının algılarının değiştirilebileceğini söylemektedir. Bu nedenle siber alanda/ağlarda üstün kabiliyetlere sahip olmanın önemine makalesinde vurgu yapmaktadır (Gresimov, 2013: 1-10). Her ne kadar Gresimov doktrini olarak adlandırılan belge siber alana ya da Rus terminolojisiyle

bilgi alanına dair bir uyanışa dikkat çekse de kendinden önceki strateji ve belgelerden öteye gitmiş değildir. Diğer taraftan söz konusu belgenin bir doktrin niteliği taşıdığı üzerine tartışmalar oldukça fazladır. Yine de siber alana atfedilen önem bakımından dikkate alınan bir belge niteliği taşımaktadır (Rumer, 2019: 1-4).

Sistematik bir politikalar bütünü özelliği gösteren ve temelde dış politikaya dair temel önceliklerin, amaçların, hedeflerin yer aldığı 2013 tarihli Rusya Federasyonu Dış Politika Konsepti isimli belge (The Ministry of Foreign Affairs of the Russian Federation, 2013: 1) de siber ile ilgili kısımlar barındırması sebebiyle bahsedilmesi gerekeli bir özellik göstermektedir. Keza diğer belgelerde olduğu gibi bilgi alanında meydana gelen yeniliklerin takip edilmesi gerektiği, aksi takdirde bu alandan gelebilecek saldırılara karşı zayıf düşüleceği öngörülmektedir. Ayrıca medya üzerinden Rusya'ya yönelik kara propagandanın engellenmesine yönelik karşı propaganda geliştirilmesi gerektiğine vurgu yapılmaktadır. Enformasyon ve siber alandan gelebilecek tehditlere karşı uyarı niteliği taşıyan belge sonraki dış politika hedeflerine de öncül bir yol açmıştır (Dyner, 2017: 1-2).

2013 yılında yayımlanan 2020'ye doğru bir siber güvenlik vizyonu oluşturmak, bilgi alanındaki hedefleri ve amaçları tayin ederek esasen siber alandan gelebilecek tehditlerle mücadeleyi konu edinen 2020'ye Doğru Rusya Federasyonu'nun Uluslararası Bilgi Güvenliği Alanındaki Temel Prensipleri (Basic Principles for States of the Russian Federation the field of International Information Security to 2020) isimli belge önemlidir. Söz konusu belgede siber alandan tezahür edebilecek tehditler tanımlanarak bunlarla mücadele yolunda atılması gereken adımlar sıralanmıştır. Rusya'nın öz hedeflerinin yanında önceliklerine de yer verilmiştir. Diğer taraftan uluslararası bir ittifak sisteminin kurulması gerektiği fikri bu belgede açık bir şekilde dillendirilmiştir. Belgede Rusya'nın hedefleri arasında yerel, bölgesel ve uluslararası seviyelerde olmak üzere çeşitli bilgi güvenlik sistemlerinin oluşturulmasından bahsedilmiştir. Ayrıca bilgi ve iletişim teknolojileri vasıtasıyla oluşturulan negatif algıların azaltılarak devlete olan güvenin sarsılmasının önüne geçilmesi hedefler arasına konmuştur. Ayrıca bu alanlardan sirayet etmesi muhtemel her türlü terörist faaliyetin önüne geçilmesi için de söz konusu uluslararası bilgi sisteminin gerekli olduğu metne girmiştir. Ayrıca belgede önemli bir diğer atıf ise siber alandan/bilgi alanından devletlerin egemenliğine yönelik tehditlerin bertaraf

edilmesinde yine bu alanda devletlerin eşit bir şekilde temsil edildiği uluslararası bilgi sisteminin öncü bir rol oynaması gerektiği fikri işlenmiştir. Söz konusu sistem oluşturulurken çeşitli yasal düzenlemelerin de gerektiği belgede yer almıştır (Corporation for National and Community Service, Basic Principles for States of the Russian Federation the field of International Information Security to 2020: 1-9).

2015 yılında yayımlanan Rusya Federasyonu Ulusal Güvenlik Konsepti (National Security Concept of the Russian Federation) belgesinde de bilgi güvenliği alanında ilerleme sağlanılması gereği ortaya konmuştur. Bilgi ve teknoloji kanalıyla Rusya Federasyonu'na yönelik faşist, aşırıcı, terörist girişimlerde bulunulduğundan bahsedilmektedir. Söz konusu tehditler sadece terörist girişimler değil yabancı devletlerin istihbarat örgütleri eliyle de harekete geçirilmektedir. Görüldüğü üzere bilgi alanının güvenliğine, ulusal güvenliğin sağlanılmasında hayati bir önem atfedilmiştir. Bilgi alanından/siber alandan gelen tehditlerin bertaraf edilmesi politik sistemin ve toplumun iç barışı için elzem kabul edilmiştir. Belgeye göre; tüm bu tehditleri yok etmenin yolu ise bir sistem geliştirmekten geçmektedir (The Ministry of Foreign Affairs of the Russian Federation, National Security Concept of the Russian Federation, 2015).

Bir önemli belge de 2016 yılında yayımlanan Rusya Federasyonu Bilgi Güvenliği Doktrini (Doctrine of Information Security of the Russian Federation) isimli belgedir. Bu belge de öncekiler gibi Rusya Federasyonu'nun siber alanı tarif ediş şeklini, buradaki ulusal çıkarlarını, ulusal çıkarlarını tehdit eden unsurları ortaya koymaktadır. Söz konusu tehditlerden korunmak için Rusya Federasyonu'nun alması gereken bilgi güvenliği önlemleri, teknolojik gereklilikler, kurumsal yenilenmeler tarif edilerek siber alanın/bilgi alanının önemi ve buradan gelebilecek tehditlerin ciddiyeti ortaya konmuştur. Belgede önemli bir diğer husus ise siber alana yönelik sektörel, kurumsal, akademik çalışmaların yapılması gerektiği fikrine mükerrer bir atıf yapılmasıdır (The Ministry of Foreign Affairs of the Russian Federation, Doctrine of Information Security of the Russian Federation, 2016).

Son olarak 2017 yılında yayımlanan ve Rusya Federasyonu'nun 2017-2030 yılları arasında uygulayacağı stratejiyi ortaya koyan 2017-2030 Rusya Federasyonu'nda Bilgi Toplumunun Gelişimi Stratejisi (Strategy for the Development of the Information Society in the Russian Federation for 2017–2030)

isimli belgeden bahsetmek gerekmektedir. Bu belgede devletin bilgi ve teknoloji alanındaki hedeflerinin, amaçlarının ve ulusal önceliklerinin/çıkarlarının iç ve dış politikaya uyarlanması gerektiği tespit edilmiştir. Bu gereklikler bilgi toplumunun gelişmesi, ulusal dijital ekonominin yerleşmesi, bilgi-iletişim kanallarında bir ilerleme sağlanmasının ön koşulları olarak lanse edilmiştir. Ayrıca siber alandaki bu politikalar hem vatandaşlar ve devlet hem de Rusya devleti ve yerel yetkililer arasında özgür, sürdürülebilir ve güvenli etkileşimin geliştirilmesi için elzem kabul edilmiştir. Diğer taraftan elektronik yeni nesil ağlar, endüstriyel internet ve nesnelerin interneti, ağlarda kimlik doğrulama, biyoteknoloji, robotik gibi alanlar öncelikli olarak bilgi güvenliğinin sağlanılması gereken alanlar olarak gösterilmiştir (President of Russian Federation, Strategy for the Development of the Information Society in the Russian Federation for 2017-2030).

3.4. RUSYA FEDERASYONU'NUN İLGİLİ SİBER GÜVENLİK KURUM VE KURULUŞLARI

Rusya Federasyonu'nun siber güvenlik alanındaki organizasyonunu danışma ve koordinasyon organları; askeri ve istihbarat organları; sivil makamlar olmak üzere üç ana sınıflandırmaya tabi tutmak mümkündür. Danışma ve koordinasyon hizmeti sunan organlar; Güvenlik Konseyi, Bilgi Toplumu Geliştirme Konseyi ve Ulusal Anti-terörist Komite'dir. Güvenlik Konseyi'nin Bilgi Güvenliği Komisyonu adında bir örgütlenmesi mevcuttur. Askeri ve istihbarat organları altında faaliyet gösteren organlar; Federal Koruma Servisi, Federal Güvenlik Servisi, Savunma Bakanlığı ve İç İşleri Bakanlığı'dır. Federal Güvenlik Servisi'nin Lisanslama, Sertifika ve Devlet Sırlarını Koruma Merkezi ile Bilgi Güvenliği Merkezi adında iki alt örgütlenmesi mevcuttur. İç İşleri Bakanlığı ise Division 'K' isimli alt bir yapılanma içermektedir. Sivil Makamlar ise İletişim Bakanlığı ile Dış İşleri Bakanlığı'dır. İletişim Bakanlığı'nın altında ise Federal İletişim Servisi, Bilgi Teknoloji ve Kitle İletişimi adında bir organ bulunmaktadır ki Rusça buna Roskomnadzor denmektedir. Dış İşleri Bakanlığı'nın altında ise Yeni Tehditler ve Zorluklar Departmanı ile Bilgi İletişimin Politik Kullanımı Özel Koordinatörü ve Bilgi Güvenliği Departmanı görev yapmaktadır (Kabanov, 2014: 20-21).

Güvenlik Konseyi ile ona bağlı olarak görev yapan Bilgi Güvenliği Komisyonu'nun temel işlevi siber tehditlerin analiz edilmesi ve olası tehditlerin tespit edilmesidir. Ayrıca bu alanda kanun taslaklarının hazırlanılmasında ve oluşturulacak faaliyetlerin koordinasyonunda görev üstlenmektedir. Bilgi Toplumu Geliştirme Konseyi ve Ulusal Anti-terörist Komitesi; bilgi/enformasyon alanında toplumun ilerlemesine katkı yapmak üzere ortaya konan strateji belgelerini izleme ve gerçekleştirmekle görevlidir. Ulusal Anti-terörist Komite ise bilgi alanından geçekleştirilmesi muhtemel terörist propaganda ve faaliyetlerle mücadeleyi organize etmekle sorumludur.

3.4.1. Federal Güvenlik Servisi (Federal Security Service, FSB)

Rusya Federasyonu'nun sahip olduğu bu siber örgütlenmede temelde bahsedilmesi gereken organlardan ilki askeri-istihbari kanatta yer alan ***Federal Güvenlik Servisi*** (Federal Security Service, FSB)'dir. Esasen söz konusu kurum KGB'nin yerini almıştır. Bu yapılanma direk olarak Başkan'a bağlı olarak görev yapmaktadır. Federal Güvenlik Servisi, siber alandan sirayet edebilecek her türlü tehditle mücadelede devletin kontrolünü sağlamakla ve terörist atakları engellemekle sorumludur (Gady ve Austin, 2010: 5). Rusça kısaltmasıyla FSB; federal düzeyde enformasyon güvenliği alanındaki birincil otorite olarak lanse edilmektedir. Fakat FSB, sadece siber/bilgi alanında değil genel anlamda devletin güvenliğiyle sorumludur. Bu nedenle güvenliğin her yönüyle ilgili sorumluluk ve yetkileri vardır. Siber alandaki yetkilerine bakıldığında da bu yetkilerin geniş bir yelpazeye uzandığı görülmektedir. Telefon kayıtlarının ve telefon hatlarının kontrol edilebilmesi, elektronik postalara ulaşım, internet ağları üzerinde gözetim gibi birçok yetkiler bunlardan bazılarıdır. FSB istihbarat alanındaki en yetkin kurum olduğundan, internet trafiğiyle ilgili her türlü gözetleme ve istihbarat toplama hakkına da sahiptir. Diğer taraftan ülkede faaliyet gösteren telekom şirketlerinin de FSB'ye bilgi aktardığı bilinmektedir. Diğer federal ajanslar tarafından kullanılan bilgi ve iletişim sistemleri için sertifika ve lisans verme yetkisi de yine Federal Güvenlik Servisi'ne aittir. Siber tehditlerle mücadelede savunma, manipülasyon ve saldırı yetkileri de yine bu kurumun yetkisindedir. Devlete ve hükümete yönelik propagandaya yönelik karşı propaganda oluşturmak ve yürütmek görevi de vardır (Heickerö, 2010: 29-30).

FSB söz konusu yetkilerini kullanırken çeşitli kurum ve ajanslardan da destek almaktadır. Özellikle siber istihbarat toplamada Operasyonel Araştırma Aktiviteleri Sistemi (SORM) isimli sistem etkin bir işlevi yerine getirmektedir. 1990'lı yıllardan itibaren kullanılmaya başlanan SORM sistemi üçayaklı olarak hayata geçirilmiştir. SORM-1; mobil ve sabit telefonlar üzerinden gerçekleşen haberleşme trafiğini kontrol etmektedir. SORM-2 aynı görevi internet ağları üzerinden gerçekleştirirken; SORM-3 ise medya üzerinden bilgi ve istihbarat toplarken bunlara sosyal medya da dâhildir (Lewis, 2014). FSB'nin hizmetlerinden yararlandığı bir diğer kurum da Federal Rusya Teknik ve İhracat Kontrol Servisi (Federal Service for Technical and Export Control of Russia, FSTEC)'dir. Bu kurum, güvenlik alanında hükümet politikasını uygulama, departmanlar arası koordinasyonu sağlama ve devlet güvenliğin sağlanmasına yönelik özel kontrol sistemleri geliştirmekle yükümlüdür. Bu tanımlamaya yönelik FSB ile bağlantılı görevleri siber alana yönelik olarak gerçekleştirilmektedir (The Goverment of the Russian Federation). FSB'nin bir diğer yardımcı kurumu olan Lisanslama, Sertifika ve Devlet Sırlarını Koruma Merkezi ise bilgi/siber alanda standartların geliştirilmesi, yeni standartların oluşturulması ve bu alanda lisans verme gibi işleri yürütmektedir. FSB'nin ikinci alt kuruluşu olan Bilgi Güvenliği Merkezi elektronik ticaret ve kişisel bilgi alanına internet ve elektronik yollardan yöneltilen suçları araştırmakla görevlidir. Ayrıca siber aladan tezahür eden tehditlerle mücadele de bu kurumun diğer bir görevidir (Kabanov, 2014: 20).

3.4.2. Federal Koruma Servisi (The Federal Protection Service, FSO)

Askeri-istihbari kanatta yer alan ikinci önemli kurum; Federal Koruma Servisi (The Federal Protection Service, FSO)'dur. FSO, istihbarat kısmında önemli bir rol oynamaktadır. Başkana gözetim alanlarından sağlanan üst düzey istihbarat bilgilerinin aktarılması görevlerindendir. Ayrıca kara kutu olarak lanse edilen ve Rusya Federasyonu'na ait nükleer karşılık sistemi de yine FSO'nun sorumluluğunda bulunmaktadır. FSO'nun altında görev yapan Özel İletişim ve Bilgi Servisi de devlet ajanslarının kullandıkları özel enformasyon sistemlerine harici sızmaları engellemekle görevlidir. FSO internet üzerinden istihbarat sağlarken, telefon ve uydu sinyalleri üzerinden de bu görevini ayrıca sürdürmektedir (Heickerö, 2010: 28). KGB'nin görevlerinden bazılarını üstlenmiş olan FSO, sahip olduğu on binlerce üyesiyle beraber kendi görev alanında oldukça geniş yetkilere sahiptir. Bunlar

arasında araştırma ve istihbarat operasyonları geliştirmek, kimlik bilgilerini sorgulamak, tutuklama yapmak, diğer devlet organlarına ilgili alanda emir ve direktifler vermek, sahibinin iznine başvurmaksızın tesislere girmek, devlete ait yerlere girişi yasaklamak gibi yetkiler bulunmaktadır (Pike, 1997). Rusya İçişleri Bakanlığı'nın siber alandaki en etkin yapılanması ve bu alandaki aktör konumundaki kurumu Division ''K'' adlı yapılanmadır. Bakanlık bünyesinde görev yapan Division ''K'' daha çok siber suçlar üzerine yoğunlaşmaktadır. Başlıca görevi de bilgisayar ve enformasyon kanalları üzerinden gerçekleşmiş, gerçekleşen ve gerçekleşebilecek olan suçlarla mücadele etmektir (Connell ve Vogler, 2017: 7).

3.4.3. Rus İstihbarat Servisi (Foreign Intelligence Service, SVR)

Rus İstihbarat Servisi (Foreign Intelligence Service, SVR), siber istihbarat alanında bahsedilmesi gereken kurumlardan biri olarak ortaya çıkmaktadır. Bu kurum da tıpkı FSB gibi direk olarak Rusya Federasyonu Başkanı'na bağlı olarak görevlerini yerine getirmektedir. SVR, esasında KGB dağıldıktan sonra onun dış istihbaratla ilgili sorumluluklarını üstlenmiş bir yapı olarak ortaya çıkmıştır (Kari, 2019: 64). SVR, hükümet ve federal meclise de bilgi aktarmakla yükümlüdür. Ayrıca istihbarat kuruma; faaliyetlerini yürütürken, kendisine yasalarca tanımlanan yetkileri aşmamak kaydıyla telekomünikasyon, bilgi sistemleri, iletişim sistemleri üzerinde sızıntılar ve bilgi hırsızlığını engellemek adına sistem/sistemler kurma yetkisi de verilmiştir (Russian Federation Foreign Intelligence Service, Powers). Bunun dışında SVR'nin Operasyonel girişimlerde önceden söz konusu hedefe yönelik birçok alanda istihbari faaliyetler yürüttüğü bilinmektedir.

3.4.4. Rus Askeri İstihbarat Direktörlüğü (GRU)

Rus Askeri İstihbarat Direktörlüğü (GRU) 1992'de Sovyetler Birliği'nin yıkılmaya başlamasıyla birlikte günümüze kadar gelen süreçte yapısal birçok değişim geçirmesine rağmen, istihbarat yönünden güçlü ve etkili bir kurum olma durumunu korumayı başarmıştır. Hatta Rus ordusunun bütçesinin küçüldüğü yıllarda dahi bu kurumun bütçesine dokunulmamıştır (Pike, 1997). GRU da tıpkı SVR gibi oldukça geniş yelpazede istihbarat faaliyetleri yönetmektedir. Bu alanlardan biri de siber alandır. GRU siber alanda SVR'nin sahip olduğu tüm yetkilere sahiptir. İkisinin arasındaki fark; SVR politik istihbarat toplarken GRU askeri istihbarat

toplamaktadır. GRU altında görev yapan direktörlükler vasıtasıyla dünyanın birçok yerinde askeri istihbarat toplamaktadır. Bunun yanısıra siber savaş yürütme görevi de yine bu kuruma aittir. GRU'nun birçok operasyonda müdahil olduğu iddia edilmektedir (Turovsky, 2018). Bu operasyonlar arasında NotPetya isimli kötü amaçlı yazılımın kullanılarak Ukrayna seçim sistemine saldırılması ve 2016 yılında ABD Başkanlık Seçimlerine müdahale girişimlerini saymak mümkündür. Sandworm ve Fancy Bear gibi hacker gruplarının GRU bünyesinde hareket ettikleri yahut buradan çıkan hackerlar tarafından oluşturulduğu düşünülmektedir (Greenberg, 2019).

3.4.5. Federal İletişim Servisi, Bilgi Teknoloji ve Kitle İletişim (Roskomnadzor)

Danışma, askeri ve istihbari kanadın yanında Rusya Federasyonu'nun bilgi/siber alanda diğer bir takım kurum ve kuruluşlardan da destek aldığı görülmektedir. Bunları sivil makamlar olarak ele almak mümkündür. Bunlardan İletişim Bakanlığı'nın altında görev yapan Federal İletişim Servisi, Bilgi Teknoloji ve Kitle İletişim'inin önemli görevleri bulunmaktadır. Bu kurum Rusça kısaca Roskomnadzor olarak adlandırılmaktadır (Richter ve Richter, 2015: 6). Roskomnadzor; Hükümetin siber alandaki politikalarını geliştirmek, politika önerileri getirmek, bu alanda standartlar oluşturmak gibi görevleri iletişim, medya gibi alanlara yönelik olarak gerçekleştirmektedir. İletişim ekipmanlarının doğru, kesintisiz bir biçimde sürdürülmesi ve bu alandaki devlet kontrol noktalarının belirlenmesinde Roskomnadzor rol oynamaktadır. Buradaki esas rolü ise tüm bu sürecin hangi standartlarda yürütüleceğinin tespiti noktasında gerçekleşmektedir (Afanesyeva, Bogatyrev ve Wilke, 2019: 5). Roskomnadzor'un medya ve internet üzerinde olduğu gibi telekomünikasyon alanında da ilgili yasanın izin verdiği ölçüde düzenleme, yenileme ve kısıtlama gibi çeşitli yetkileri söz konusudur. Roskomnadzor'un yetkileri kişisel verilerin korunması anlamında da oldukça fazladır. Burada yasanın öngördüğü gerekleri sağlamak, suç işlenilmesi durumunda müdahale etmek, çocukların korunmasını sağlamak gibi amaçlar söz konusu olmaktadır (The Government of the Russian Federation Regulation, No: 228 of March 16).

3.4.6. Rusya Federasyonu Dışişleri Bakanlığı

Sivil makamlar sınıflandırmasında bahsedilmesi gereken diğer kurum RF Dışişleri Bakanlığı'dır. Bakanlık; bünyesinde faaliyet gösteren Yeni Tehditler ve Zorluklar Departmanı ile Bilgi İletişimin Politik Kullanımı Özel Koordinatörü ve Bilgi Güvenliği Departmanı ile bilgi alanındaki görevlerini yerine getirmektedir. Yeni Tehditler ve Zorluklar Departmanı; siber alandaki terörist faaliyetler ve bunların finans yapılanmaları, uyuşturucu, kara para aklama gibi çeşitli tehditlerle mücadele etmektedir (UN Organization, Deputy Director of New Threats and Challenges Department's Statement, 2016). Bilgi İletişimin Politik Kullanımı Özel Koordinatörü ve Bilgi Güvenliği Departmanı da yine benzer ve paralel hedeflere ulaşmayı amaçlamaktadırlar. Tüm bu yapılanmasıyla Rusya Federasyonu Dışişleri Bakanlığı'nın yapmaya çalıştığı temel vazife; siber alandaki ulusal çıkarları belirlemek, korumak ve geliştirmektir.

3.5. ABD VE RUSYA FEDERASYONU'NUN SİBER STRATEJİ VE ORGANİZASYONLARININ KARŞILAŞTIRILMASI

Amerika Birleşik Devleti ve Rusya Federasyonu'nun siber stratejilerini, bu stratejileri oluşturan belgeleri, hayata geçiren kurumsal yapılanmalarını ortaya koyduğumuzda bir takım benzerlikler ve farklılıkların olduğu görülmektedir. Şüphesiz bu farklılıklar ve benzerliklerin kendi içeisinde bir nedenselliği mevcuttur. Bu nedenler iki ülkenin coğrafyası, kültürü, yönetim biçimleri arasındaki farklılıklar olabileceği gibi tehdit algısı, siyasi/askeri öncelikler veyahut dış politika tercihlerinden kaynaklanabilmektedir.

Rusya Federasyonu ve ABD siber alanın önemine özellikle vurgu yapan iki ülke olarak dikkat çekmektedirler. Bu durum kendisini henüz 1998 yılında iki ülkenin başkanları olan Bill Clinton ve Boris Yeltsin'in enformasyon devriminin ortaya çıkardığı yeni tehditleri azaltmaya yönelik ortak deklarasyonunda göstermiştir. İki ülkenin stratejelerinde görülen bir diğer benzerlik de yine rekabet ve tehdit hanesinde ilk sırada birbirlerini görmeleri olmuştur. Diğer taraftan siber güvenliğin tanımlamasına yönelik olarak bir farklılaşma olduğu da görülmektedir. Çünkü ABD siber alanı ve siber güvenliği birincil önemde ve sıkça internet

dünyasıyla ilintili bir çerçevede ele alırken Rusya Federasyonu; siber alanı ve siber güvenliği enformasyon güvenliğinin bir parçası olarak ele almaktadır. Rusya Federasyonu'nun buradaki yaklaşımı siber güvenliği ayrı bir mecra değil, ulusal güvenliğin bir parçası olarak gördüğünü göstermektedir. Rusya ve ABD siber alanın açık ve kontrol edilebilir bir yer olması konusunda da aynı fikirde değildir. ABD, siber alanda bilgi akışının açık bir şekilde gerçekleştirilmesi gerektiği fikrine daha yatkınken Rusya Federasyonu bu fikre nispeten olumsuz bakmaktadır (Van Epps, 2013: 35-38).

ABD ve Rusya'nın siber uzayı/alanı ve siber güvenliğe ilişkin kullandıkları terminoloji yönünden de bir fark söz konusu olmaktadır. RF'ye göre siber güvenlik ve siber alan kelimeleri dar bir tanımlamaya tekabül etmektedir. Daha ziyade teknolojik bir anlam ifade eden bu terimin yerine Rusya; bilgi/enformasyon alanı ve bilgi/enformasyon güvenliği kelimelerini tercih etmektedir. Çünkü bu kelimeler sadece teknolojik bir öz taşımamakta; anlama filozofik ve politik bir zenginlik de katarak daha geniş bir yelpaze sunmaktadır (Gady ve Austin, 2010: 5).

Siber güvenlik alanında çalışmalar yapan, siber uzayın önemine atıf yapan lider ülke ABD olmuştur. ABD, siber uzayın yaratabileceği tehlikeleri ve bunlara önlem alınması gerektiği düşüncesini yayımladığı belgelerde açık bir şekilde ifade etmiştir (Tsakanyan, 2017: 342). ABD'nin siber güvenlik konseptinin parçalarını oluşturan bu belgeler; başkanlık direktifleri, bilgi güvenliği doktrinleri, kurumlara ait strateji dokümanlarından oluşmaktadır. Diğer taraftan Rusya Federasyonu da siber alanda faaliyetlere erken başlamış, etkin sonuçlar almayı başarabilmiş ve en etkili siber kabiliyetler geliştirmiş ülkelerden biri konumundadır. RF'nin siber güvenlik konseptini ise bilgi güvenliğine dair doktrinler, savunma bakanlığına ait bilgi/siber güvenliğine dair strateji belgelerinden oluşmaktadır (Thomas, 2001: 341-358). İki ülkenin de siber güvenlik konseptlerini oluşturan belgeler oldukça fazladır. Bunun temel nedeni iki ülkenin de kurum ve ihtiyaç bazlı çalışmalar yapmış olmalarından kaynaklanmıştır. Daha sonra bu belgelerin daha geniş bir yelpazeye (doktrin) hizmet ettikleri görülmektedir.

ABD ve Rusya'nın siber güvenlik konseptlerinde siber alanın çok merkezli olduğunun verili kabul edildiği görülmektedir. Çünkü her iki konseptte de siber alanın çeşitli grupların (devletler, terör örgütleri, hackerlar vs) müdahil olduğu,

çeşitli amaçlarla tehlike yaratabilecek faaliyetlere giriştikleri/girişebilecekleri bir yer olarak lanse edilmiştir. ABD siber alandan tezahür edecek tehditlerle mücadele oldukça titiz davranmakta ve özellikle ülkenin kritik altyapılarının korunması gerektiğini göz önünde bulundurulmaktadır. Ayrıca siber propagandaya karşı koymak da ülkenin temel hedefleri arasındadır (Harknett ve James, 2011: 456). Diğer taraftan Rusya Federasyonu; siber tehditlerin sadece kritik altyapılara yönelik olarak değil bilhassa toplum yapısına ve kültürel kimliğe yönelik de gerçekleştirilmesi ihtimali üzerinde durmaktadır. Ayrıca söz konusu tehditlerin Batı/NATO/ABD hattından gelebileceğine yönelik inanç oldukça yaygındır. Söz konusu düşüncenin bir sonucu olarak, ülkenin siber güvenlik konseptinde bu fikir sürekli olarak işlenmektedir (Soldatov ve Irina Borogan, 2018: 16).

İki ülkenin kurumsal yapılanmaları bir karşılaştırma yaparken dikkat edilmesi gereken bir parametredir. Yukarıda da incelendiği gibi Rusya Federasyonu'nun da Amerika Birleşik Devletleri'nin de siber yapılanmaları kendi ülkelerinin siyasal düzeninin gerektirdiği yönde şekil almaktadır. İki ülke de savunma, içişleri, dışişleri ve teknolojik altyapıyı ve gerekse de ekonomik altyapıyı güven altına almak adına bu alanlarda sıkı bir örgütlenmeye gitmişlerdir. Gerek bakanlıklar, bakanlıklara bağlı kurumlar gerekse de direk başkana bağlı olarak görev yapan kurumların amaçları ülkelerini siber alandan gelebilecek her türlü tehdide karşı korumak olmuştur. Bu anlamda hem ABD hem Rusya Federasyonu önemli yol katetmişlerdir. İki ülkenin siber organizasyonlarına verdikleri önemin şiddeti aynı olsa da oluşturdukları organizasyonların işleyişine yönelik şeffaf bilgilere ulaşmada bir farklılık söz konusudur. Keza ABD'nin organizasyonel yapısında görev tanımlaması ve sorumluluklar daha açıklayıcı bir şekilde ortaya konmuşken; aynı durum RF için geçerli olmamaktadır. Bunun Rusya Federasyonu ile ABD'nin yönetim biçimleri ve siyasal zemininin farklılığının bir sonucu olduğu düşünülebilir.

3.6. ABD VE RUSYA FEDERASYONU'NUN SİBER ALAN İŞBİRLİĞİ VE REKABET DURUMLARI

Gerek ABD gerekse Rusya Federasyonu'nun siber güvenlik okumalarının güvensizlik üzerine bina edildiği görülmektedir. Özellikle siber alandan kaynaklanabilecek tehditlerin ciddiyetinin anlaşıldığı ilk zamanlarda bu durum bir

güvensizlik kaynağı olarak addedilmiştir. Söz konusu düşüncenin arkasında yatan ana etken ise iki ülke için de aynı sebepten kaynaklanmıştır ki bu; hazır olmama halidir. Söz konusu durum hem ABD hem de Rusya Federasyonu tarafından defaatle dillendirilmiş; tehlikenin ne boyutlara varabileceği başkanlar düzeyinde de vurgulanmıştır. 2008 yılında Washington D.C'de toplanan Stratejik ve Uluslararası Çalışmalar Merkezi'nin siber alanı gizli bir savaş olarak lanse edip ABD'nin bu alandaki hazırsızlığını dikkat çekmesi bu fikri desteklemektedir. Diğer taraftan Rusya Federasyonu Başkanı V. Putin'in imza ettiği 2000 yılındaki Bilgi Güvenliği Doktrini de aynı tehlikeden ve hazırsızlık durumundan bahsetmiştir. Özellikle ülkenin siber alandan sirayet edecek tehlikelerle mücadele etmek için yerli teknoloji ve yazılımların geliştirilmesi gerektiği, aksi takdirde ülkenin saldırılara açık bir halde olacağına dikkat çekilmiştir (Gady ve Austin, 2010: 1).

İki ülkenin de siber alanın önemini idrak etmesinden sonraki süreçler de benzer özellikler göstermiştir. Özellikle bu alanda farkındalık yaratmak ve sonrasında güçlenmek adına çeşitli girişimler iki ülke için de birbirini izlemiştir. Söz konusu çalışmalarda vurgu yapılan ana unsurlar siber tehditler ve bu tehditlerin kaynağı noktasındadır. Özellikle oluşturulan siber stratejiler, bu alanda yürütülen çalışmalarda iki ülkenin birbirini rakip ve tehdit olarak algıladığı açık bir şekilde anlaşılabilmektedir. ABD ve Rusya; kendi ülkelerinde ya da üçüncü ülkelerde, istihbarat toplamak yahut zarar vermek için sistemlere sızma gibi çeşitli siber girişimleri hayata geçirdikleri yönünde birbirlerini sık sık suçlamaktadırlar (Ajir, Haas ve Vailliant, 2018: 6-12).

ABD ve RF'nin birbirlerini rakip ve tehdit olarak görmesi, tarihin olağan akışı içerisinde ele alındığında anlaşılması zor bir durum olmamaktadır. Rusya Federasyonu ve Amerika Birleşik Devletleri arasındaki siber ilişkilerin rekabet ve güvensizlik üzerinden algılanmasının son örneği 2016 yılındaki ABD Başkanlık Seçimleri olmuştur. Rusya'nın siber kanalları kullanarak seçimi sabote ettiği iddiası iki ülke arasındaki ilişkileri oldukça germiş, siber alanın önemini ise bir kez daha ortaya koymuştur (Harding, 2016). Diğer taraftan Rusya Federasyon'un siber alanda partner olarak gördüğü ülkeler ekseriyetle Asya kıtasında yer almakla beraber, diğer ülkelerle de işbirliği sağlamanın önemli olduğu düşünülmektedir. ABD'yi de bu bağlamda ele almak mümkündür. Her ne kadar siber alandaki esas rakip olarak

görülse de; bir takım prensiplerde işbirliği alanlarının arandığı göz önünde bulundurulmalıdır. Rusya; ABD ve NATO'yu, kendi stratejik varlığına muhalif yönde hareket etmekle itham etse de, uluslararası ilişkilerin gerektirdiği şartlarda uzlaşma alanlarının da arandığı görülmektedir (Raik, Aaltola, Kallio ve Pynnöniemi, 2018: 44-47).

ABD ve RF'nin siber uzay münasebetleri rekabetten ibaret değildir. İki ülkenin siber alan/bilgi alanında işbirliğine gittikleri dönemler/koşullar da olmuştur. İki ülkenin birbirleriyle rekabet halinde olmaları, iki tarafın da bir takım müşterekleri paylaşmasını engellememektedir. Özellikle herhangi bir düzenleyici uluslararası kuralın olmadığı siber uzayda, tehditlerden korunmak, terörist saldırıları bertaraf etmek, birey, şirket ve devleti korumak daha zor bir hal almaktadır. Tam da bu noktada anarşik siber uzaydan kaynaklanabilecek tehditleri minimize etmek adına zaman zaman iki ülkenin işbirliği yaptıkları görülmektedir. Bunlardan ilki 1998 yılında yapılan ''21. Yüzyılın Eşiğinde Genel Güvenlik Sorunları'' (Common Security Challenges at the Threshold of the Twenty-First Century) isimli başkanlar düzeyindeki ortak görüş bildiren belgedir. Bu belgede iki taraf da yeni bir güvenlik alanı olarak ortaya çıkan siber ortamdan iki ülkenin de olumsuz etkilenmesinin önlenmesi adına riskleri azaltmak gerektiği konusunda hemfikir beyanda bulunmuşlardır. Ayrıca iki teknoloji/bilişim hattından kaynaklanabilecek tehlikeleri bertaraf etmek adına iletişim kanallarını açık tutmayı kararlaştırmışlardır (Administration of William J. Clinton, 1998, Joint Statment on Common Security Challenges at the Threshold of the Twenty-First Century).

1998 yılındaki bu ortak deklarasyon sonrasında bir fırsat daha ortaya çıkarmıştır. Avrupa Konseyi Siber Suçlar Sözleşmesi(Council of Europe's Convention on Cybercrime) isimli belge siber suçlarla mücadelede ilk uluslararası sözleşme niteliğine haiz durumdayken ABD'nin bu sözleşmeye taraf olmasına karşın Rusya Federasyonu sözleşmeye imza atmamıştır. 2001 yılında yürürlüğe sokulan bu belge internet ve teknolojik cihazlar yoluyla işlenecek siber suçlarla mücadelede kategorik sınıflandırmalarla bir suç ve ceza sistemi öngörür şekilde oluşturulmuştur. Diğer taraftan bu belge Rusya'nın dışında İngiltere tarafından da imza edilmemiştir (Gady ve Austin, 2010: 1-2).

Rusya'nın başkanlığında gerçekleştirilen 2006 yılı G8 Zirvesi siber alanda diplomatik açıdan önemli adımların atıldığı bir diğer süreç olmuştur. Zirveye katılan ülkeler siber uzayda internetin kötüye kullanılmasıyla insanların radikalleştirilmesi, gizli ve hassas bilgilerin internet üzerinden terörist hackerlar/organizasyonlar tarafından elde edilmesi, internet ve uydu bazlı kritik altyapı iletişim kanallarına zarar verilmesi gibi tehditleri bertaraf edilmesi gerektiği fikrini paylaşmışlardır. RF Bilgi Teknolojileri Ajansı, siber uzayda güvenli bir alan yaratılması fikrini sunarak, siber terör gruplarına karşı eşgüdümlü bir korunma sistemi önermiştir. Bu önerilere ABD menşeli şirketler de katılmışlar fakat somut olarak pek bir yol katedilmemiştir (G8 Intiative for Public-Private Partnership to Counter Terrorism, 2006: 6-10).

2009 yılında BM Silahsızlanma ve Uluslararası Güvenlik Komitesi toplantısında ABD ve RF, siber güvenlik alanında ilişkileri geliştirmek ve siber uzaydaki askeri operasyonlar için normlar geliştirmek için mutabakata varmışlardır. Bu ilişkilerin kimi zaman Birleşmiş Milletler eliyle de devam ettiği görülmüştür. 2009 yılındaki ABD-Rusya mutabakatında sonra BM Genel Kurulu bilgi güvenliğinin sağlanması, telekomünikasyon ve diğer önemli altyapıların korunması adına ortak önlemler duyurmuştur. 2011 yılında ABD Siber Güvenlik Koordinatörü Howard Schmidt ile Rusya Ulusal Güvenlik Konseyi Sekreter Yardımcısı Nikolay Klimashin, siber uzayda ulusal güvenliğe yönelik ortak anlayışı geliştirmeyi amaçladıklarını resmi olarak açıklamışlar ve bu açıklama önemli bir adım olarak görülmüştür (Van Epps, 2013: 38-40).

2013 yılında ABD Başkanı Barrack Obama ile RF Başkanı Vladimir Putin'in görüşmeleri sonucunda Güven İnşasında Yeni İşbirliği Alanı olarak açıklanan ortak mutabakatta amaç yine siber güvenliğin sağlanılmasına yöneliktir. Mutabakatta iki ülkenin de yeni teknoloji ve iletişim ağından kaynaklanacak her türlü askeri, politik ve yahut terörist tehdide karşı dayanışma ve işbirliği geliştirmeyi hedeflediklerinden bahsedilmektedir. Siber alana yönelik olarak gerçekleştirilecek bu ortak anlayışın hem iki ülkenin hem de uluslararası güvenliğin sağlanılmasında önemli bir adım olduğu belirtilmiştir. Ayrıca kritik altyapıların korunmasını sağlamak adına iki ülke acil bilgisayar karşılık sistemlerinin bilgi alışverişinin hızlıca ve koordineli bir şekilde sağlanılması hedeflenmiştir. Nükleer Risk Azaltma Merkezlerinin eşgüdümlü çalışmalarıyla iki ülke arasında oluşabilecek yanlış anlama ve olası çatışmaların

engellenmesi öngörülmüştür. Son olarak bilgi iletişim teknolojileri kanalıyla oluşabilecek olası tehditlerle etkin bir mücadelenin ortaya konulması adına Beyaz Saray ve Kremlin arasında direkt iletişim ağlarının oluşturulması kararlaştırılmıştır. Ayrıca ABD-RF İkili Başkanlık Komisyonu kurulması ve bu komisyon aracılığıyla iletişim ve etkileşimin kolaylaştırılması planlanmış ve birkaç ay sonra da hayata geçirilmiştir (The White House, Joint Statement on New Field of Cooperation in Confidence Building,2013). Sonraki yıllarda iki ülke arasında direkt olarak siber alana yönelik herhangi işbirliğine yönelik adım atılmamışsa da Birleşmiş Milletlerin çalışmalarında iki ülkenin ortak metinlerin altına imza attıkları gözlemlenmiştir. Fakat özellikle Edward Snowden olayıyla birlikte ikili ilişkilerin olumsuz yöne hızlı bir şekilde kaydığı görülmektedir. İki ülke birbirini muhtelif siber vakalar üzerinden suçlamaya devam etmiş, 2016 yılında gerçekleştirilen ABD Başkanlık Seçimleri 'ne Rusya Federasyonu'nun müdahil olduğu yönündeki iddialarla da iyice çıkmaza girmiştir (Sharikov, 2013: 1-7).

3.7. SİBER SOĞUK SAVAŞ İDDİALARI

1945-1947 yılları arasında İkinci Dünya Savaşı'ndan güçlü bir şekilde çıkan, kapitalizm ve Marksizm gibi karşıt iki ideolojiyi benimsemiş ABD ve Sovyetler Birliği'nin bu ideolojileri ekonomik ve politik yönden dünyanın geri kalanına empoze etmeye çalıştıkları dönem tarihe Soğuk Savaş olarak geçmiştir. İki ülkenin birbirlerini temel tehdit olarak algıladıkları bu dönemde, birinin varlığı diğerinin yaşam alanının daralması anlamında ele alınmıştır. Böylece iki ülke, diğer devletleri de kendi taraflarına çekerek dünyayı adeta iki kutuba bölmüş; gerilim ve tansiyonun yüksek olduğu bir evreye girilmiştir (Lightbody, 1999: 4). Soğuk Savaş döneminde kutup liderleri olan ABD ve SSCB arasında herhangi bir sıcak çatışma yaşanmazken, diğer bölgelerde başka devletler üzerinden fakat geri planda yine kutup liderlerinin olduğu bir takım çatışmalara şahit olunmuştur. Bu dönem daha çok etki alanlarının oluşturulduğu, güvenlik açmazlarının yoğunlaştığı bir dönem olmuştur. Buna benzer şekilde siber uzayda da yeni bir soğuk savaş durumunun olduğu iddiaları ortaya atılmaktadır. Siber uzayda devletlerin birbirlerini tehdit olarak gördükleri, bu alanda

güç arayışlarına girdikleri düşünüldüğünde Siber Soğuk Savaş iddialarının dikkate alınması gereken yönleri oldukça fazladır (Tarhan, 2020: 193-194).

Siber alanda görülen devletlerin birbirleriyle olan ilişkilerindeki saldırgan eğilimler kimi zaman siber savaş merhalesine evirilebilecek izlenimi verse de günümüzde bunun bir siber soğuk savaşa dönüşeceğine yönelik yeterli kanıta ulaşılamamıştır. Yine de ABD ve Rusya Federasyonu'nun soğuk savaş ilişkileri ve siber alan ilişkileri karşılaştırmalı olarak ele alındığında bir takım benzerlik ve farklılıklara ulaşılabilmektedir. Bu benzerliklerden biri Soğuk Savaş öncesi dönem ile siber alandaki günümüzde gerçekleşen güçlenme arayışları, siber teknolojideki yarışta öne geçme çabalarıdır. Soğuk Savaş döneminde devletlerin silahlanma, nükleer gücü elde edebilme, istihabarat birimlerinde etkin olma gibi alanlarda bir yarışa girdikleri gözlemlenmekteydi. Bugün de devletlerin benzer hedeflerini siber alanda lider olma arzusu içerisinde gerçekleştirdikleri görülmektedir. Diğer taraftan bu noktada bir farklılık da ortaya çıkmaktadır. Çünkü Soğuk Savaş döneminde kutup lideri olan devletler arasında bir sıcak çatışma yaşanmamış; böyle bir şeyin yaşanması savaş sebebi olarak görülmüştür. Buradan yola çıkarak Soğuk Savaş döneminde devletlerin adı konulmamış bir takım kurallara uydukları görülmektedir. Ayrıca devletlerin eylemlerinden sorumlu oldukları düşünüldüğünde eylemi gerçekleştirenin sonuçlarına katlanması gerektiği bir düzen söz konusudur. Fakat siber alanda; devletlerin henüz herkesin sorumlu olduğu bir kurallara ulaşılamamıştır. Diğer taraftan siber alanın merkezi olmayan yapısı, saldırıların izinin sürülmesindeki zorluklar gibi bir takım özgün yapısı Soğuk Savaş dönemiyle benzerlikler göstermemektedir. Kısaca bir devletin gerçekleştirmiş olduğu saldırıların tespiti kolay olmamakta, bu da durumun savaş sebebi olarak addedilmesini zorlaştırmaktadır (Singer, 2017).

Soğuk Savaş döneminde iki kutup liderinin doğrudan karşı karşıya gelmediği, diğer kutup ülkelerinin topraklarında dolaylı olarak çatışmaların birer parçaları oldukları görülmüştür. Siber alanda gerçekleşen saldırılarda da bu durumun zaman zaman ortaya çıktığı görülmektedir. Örneğin Rusya'nın 2007 yılında Estonya'ya yönelik gerçekleştirmiş olduğu siber saldırılar sırasında hem NATO'nun hem de ABD'nin Estonya'ya yardım ettikleri görülmüştür. Hatta bu sırada hayata gerçekleştirilen bir takım kurumsal yapılanmalarla siber alanının ve güvenliğin

sağlanılmasına yönelik NATO ülkelerine eğitimlerin verilmesi, araştırmaların yapılması gibi çeşitli girişimlerde de bulunulmuştur. Diğer taraftan siber uzayda etkinliğini arttırmaya yönelik girişimler İran, Çin, Kuzey Kore gibi devletler tarafından da hedeflenmekte; bu ülkelerde de çeşitli girişimler bulunmaktadır. Ayrıca AB de siber alana yönelik mevzuatlar geliştirmekte, bu alanda güvenliği sağlayabilecek yetkinliği elde etmeye çalışmaktadır (Darıcılı, 2018: 319-320). Bu durum tıpkı Soğuk Savaş'ta olduğu gibi doğu ve batı blokları arasında yeni bir cepheleşmenin olabileceğine işaret etmektedir. Diğer taraftan ABD ve Rusya Federasyonu'nun siber alanla ilgili metinlerinde de sürekli bir şekilde birbirlerini tehdit olarak ele aldıkları gözlenmektedir.

Siber alanda bir Soğuk Savaş ihtimali bilhassa batılı kaynaklar tarafından iddia edilmektedir. Bu noktada gerek Çin'in gerek Rusya Federasyonu'nun siber alandaki etkinliklerini arttırmaları, RF'nin siber saldırı deneyimlerini birçok ülkede hayata geçirmesi dikkat çekici bulunmakla beraber ABD'nin ise bu derecede hazır olmadığı iddia edilmektedir. Böyle bir senaryo Çin tarafından reddedilmekle birlikte zaman zaman ABD ile ilişkilerde gündeme gelen bir konu olmaya devam etmektedir. Batı'da olası bir genel çatışmanın eğer siber uzayda cereyan edecek olduğu varsayılırsa; ABD'nin bu alanda yeterince direnç gösterebileceğinden endişe duyulmaktadır. ABD'nin bu alanda bir gelecek perspektifi ortaya koyarak güçlenmeye çalışması gerektiği fikri Batı'da birçok otorite tarafından paylaşılmaktadır. Özellikle nükleer tesislerin yahut balistik füzelerin siber alandan müdahale edilir bir hale getirildiği takdirde hem ABD hem de müttefikleri için oldukça yıkıcı sonuçlar doğurabileceği düşünülmektedir. Bu anlamda özellikle üçüncü bir dünya savaşının meydana gelebileceği öngörülmektedir. Bu senaryo ise tıpkı Soğuk Savaş'ta olduğu gibi üçüncü bir dünya savaşı korkusunun devam ettiğini göstermektedir (Richards, 2014: 43-54).

Siber alanda yeni bir soğuk savaşın olabileceğine yönelik iddiaların bir diğer nedeni; siber alanda etkin ve güçlü ülkelerin, siber alana yönelik görüş farklılıklarının bulunması ve bu farklılıklara yönelik müzakere masalarının henüz istenen seviyede kurulamamış olmasıdır. Özellikle ABD ve RF siber alana yönelik bir uluslararası mutabakatın hangi ilkeler üzerinde kurulması gerektiği üzerinde birbirlerine zıt durmaktadırlar. Siber Soğuk Savaş iddialarının zirve yaptığı nokta;

2016 yılında Rusya tarafından gerçekleştirildiği savunulan ABD Başkanlık Seçimleri ’ne müdahale iddiaları olmuştur.

3.8. 2016 ABD BAŞKANLIK SEÇİMLERİNDE SİBER MÜDAHALE İDDİASI

9 Aralık 2016 tarihinde ABD Başkanlık seçimleriyle ilgili bir değerlendirme yazısıyla okurlarının karşısına çıkan Washington Post, çok önemli bir iddiayı gündeme getirmiştir. ABD istihbarat örgütlerine dayandırılarak yazılan bu değerlendirme makalesine göre Rusya Federasyonu ABD Başkanlık Seçimlerine müdahalede bulunmuştur (Baezner ve Robin, 2017: 8). Makaledeki değerlendirmeye göre Rusya Federasyonu; seçimlerde Donald Trump’ın kazanması için çaba sarf etmiş ve başarılı olmuştur (Alexander, 2016). Rusya Federasyonu’nun ABD Başkanlık seçimlerine politik anlamda Hillary Clinton’ın başkanlığını engellemek ve Donald Trump’ın onun yerine seçilmesini sağlamak, ABD seçim sistemine ve sonucuna güveni azaltmak gibi saiklerle müdahale ettiği düşünülmektedir (Fisher, 2019: 9-10). Rusya Federasyonu’niun siber manipülasyon ve siber ataklarla, etkilemeye çalıştığı seçimlere yönelik hamlelerin bir diğer nedeninin; ideolojik olarak kendi anlayışına yakın yahut en azından karşıt olmayacak liderlerin başa geçmesi arzusu olarak düşünülmektedir (Gude, 2017: 1-5). ABD seçimleri dikkate alındığında daha sağcı politikalar yürüten Trump’ın desteklendiği iddiası bu görüşün dikkate alınması gerektiğini göstermektedir.

Devletlerin çeşitli amaçlarla diğer devletlerin seçim sistemlerini etkilemeye çalıştıkları uzun zamandır bilinmekle beraber RF açısından bu iddialar oldukça fazladır. Özellikle Batı demokrasilerine ve onların demokratik seçimlerine karşı birçok manipülasyonun RF tarafından gerçekleştirildiği görülmektedir. Siber alandaki etkinliğini kullanarak Estonya, Gürcistan, Ukrayna (Pernik, 2018: 53-64) Litvanya Kırgızistan, Kazakistan, , Fransa, Almanya, Hollanda, Finlandiya, İngiltere gibi çeşitli ülkelerde seçimleri manipüle etmeyi deneyimleyen Rusya Federasyonu’nun 2016 yılında gerçekleştirdiği ABD Başkanlık seçimlerine yönelik müdahale iddiası ise bu süreçte yeni ve kritik bir durumu ortaya çıkarmıştır. Rusya Federasyonu’nun gerek ABD’ye gerek diğer AB ülkelerine yönelik olarak girişmiş olduğu bu siber saldırılar; ne ABD’nin ne de AB ülkelerinin siber saldırılara karşı

dayanıklı birer seçim sistemine/siber koruma mekanizmasına sahip olmadıklarını gözler önüne sermiştir (Brattberg ve Maurer, 2018: 1-5).

ABD Başkanlık seçimlerine Rusya Federasyonu Başkanı Vladimir Putin'in bizzat emriyle ve Donald Trump lehine müdahale edildiğini iddia eden ABD istihabarat örgütlerine göre; büyük çapta ve yüksek etki uyandırıcı bir stratejiyle hareket edilmiştir. Buna göre Rus Askeri İstihbarat Direktörlüğü (GRU) tarafından yürütülen organizasyonla hem Demokratik Ulusal Komite server'leri hem de Hillary Clinton'un kampanya direktörü John Podesta'nın e-mail hesabı hacklenmiştir (Ünver, 2019: 4). Demokratik Ulusal Komite (DNC) de söz konusu sızma/hackleme işleminin Rusya bağlantılı hacker grupları olan ''Cozy Bear'' ve ''Fancy Bear'' tarafından gerçekleştirilmiştir (CNN, Aralık 2019).

Hacklenen maillerin internette yayınlanmasıyla Clinton karşıtı bir hava oluşturulmak istenmiştir. Özellikle Twitter, You-Tube, İnstagram ve Facebook gibi sosyal medya araçları da bu propagandanın yürütülmesinde en çok kullanılan kanallar olmuştur. Diğer taraftan Trump'ın kampanyasına destek amaçlı çeşitli toplantıların da yapıldığı iddia edilmektedir. Bu propagandayı gerçekleştiren grupların resmi olmasa da GRU'nun kontrolünde ve Putin'in bilgisi dâhilinde hareket ettikleri ileri sürülmektedir. Rusya'nın müdahalesinin direkt olarak geçerli oyların sistemsel olarak değiştirilmesi üzerine kurulmamış, daha çok oy kullanacak seçmenlerin kararlarını etkilemek için siber propaganda geliştirilmesine dayandırıldığı görülmektedir (Abrams, 2019: 1-4).

H. Clinton'un seçim kampanyasını manipüle etmek amacıyla kullanılan bir diğer kanal Julian Assange tarafından kurulan Wikileaks adındaki internet sitesidir. Daha önce de ABD istihbarat örgütlerine ait yaklaşık 5 milyon gizli belge ile görüntüleri yayarak adından söz ettiren Assange; 2016 Başkanlık Seçimlerinde ise Clinton'ın hesabından hacklenen 2012-2014 yılları arasındaki bir takım e-postaları ve gizli görüşmeleri yayımlamıştır. Bu sırada Londra'nın Kolombiya büyükelçiliğine sığınmış durumda bulunan Assange, elçilikte internetin kesildiğini duyurmuştur. Kolombiya hükümeti ise bu kararın Wikileaks 'in ABD seçimlerini etkileyebileceği yönündeki kanaatinden dolayı alındığını doğrularken, kararın herhangi bir şekilde ABD baskısının bir sonucu olmadığı belirtilmiştir (BBC News, Nisan 2019).

Hacklenen hesapta, Demokrat Parti'den adaylık için yarışan bir diğer isim olan Bernie Sanders'in kampanyasını manipüle ederek H. Clinton'un adaylığını kesinleştirmeye yönelik mailleşmelere rastlanmıştır. Bunun dışında Clinton'un devlet uzantılı mail hesabının yerine özel bir mail hesabı kullanması da tepki çekmiştir. Özellikle güvenilmez olduğu, amacına ulaşmak adına her şeyi deneyebilecek bir yapıya sahip olduğu yönünde birçok eleştiri yapılmış, kamuoyu yoklamalarında kendisine verilen desteğin zedelendiği ve Trump ile arasındaki farkın kapandığı gözlemlenmiştir (Alsan, 2016).

RF'nin kendi lehine seçimleri manipüle ettiği iddiasıyla ilgili olarak Trump, söz konusu iddiaların hiçbirinin gerçeği yansıtmadığını, Rusya'nın ABD seçimlerine yönelik herhangi bir müdahalede bulunmadığını iddia etmiştir. Buna rağmen FBI, ABD Senato Seçim İstihabarat Komitesi, ABD Temsilciler Meclisi İstihbarat Daimi Seçilmiş Komitesi, Temsilciler Meclisi Gözetim ve Reform Komitesi, Amerika Birleşik Devletleri Senatosu Yargı Komitesi ve Amerika Birleşik Devletleri Özel Danışmanlık Ofisi gibi federal ve kongresel düzeylerde araştırma/soruşturma işlemleri gerçekleştirilmiş ve raporlar oluşturulmuştur (CNN, Aralık 2019).

FBI, 2016 yılının henüz temmuz ayında yapmış olduğu istihbarat soruşturmalarıyla seçim sürecine dönük ilk değerlendirmeyi yapan kurum olmuştur. Buna göre FBI; seçimlere Rusya'nın müdahalesinin olduğuna dair açık kanısının oluştuğunu defaatle süreç içerisinde ve sonrasında yapmış olduğu açıklamalarla desteklemiştir.

FBI'nın dışında seçimlere olası müdahaleleri araştıran bir diğer kurum ise yine ABD istihbarat topluluğunu denetlemekle görevli ve senato üyelerinden oluşan ABD Senato Seçim İstihbarat Komitesi'dir. Son ABD seçimlerinde Rusya etkisinin incelenmesi ve söz konusu siber ilişkiyi incelemeyi hedefleyen Komite sınıflandırılmamış bir rapor ortaya koymuştur. Rapor FBI, CIA ve NSA ortak fikirlerini/çalışmalarını beyan eder bir şekilde oluşturulmuştur. Rapora göre Rusya Federasyonu, H. Clinton'un kampanyasını devre dışı bırakmak suretiyle Donald Trump lehine olacak şekilde bir etki kampanyasına girişmiştir. Söz konusu etki kampanyasına özellikle Hillary Clinton'un başkanlığının yüksek ihtimalle gerçekleşeceği fikri oluşunca harekete geçirilmiştir. Etki kampanyasının bir parçası olarak Rus hükümet ajansları, üçüncü taraf aracılar, troll olarak adlandırılan sosyal

medya hesapları ve Rusya hükümeti fonlu medya aracılığıyla kurgulanmış bir algı sistemi kurulmuştur. Rapora göre Rus istihabarat servisleri 2016 Başkanlık Seçimlerinde iki büyük partiye de siber operasyonlar gerçekleştirmiştir. Ayrıca GRU'nun DC.Leaks.com adresini kullanarak ABD'den devşirdikleri dataları sosyal medyaya yaymışlardır. Wikileaks 'ten alınan maillerin bu site ve Guccifer 2.0 adlı kullanıcı aracılığıyla sızdırıldığı bilgisine erişilmiştir. Rapor, Rus kaynaklı hackleme operasyonunda ABD'nin birkaç eyalet bazlı yerel seçim kurullarına da sızıldığını ortaya koymuştur. Fakat söz konusu sızmada oyların değiştirilmesine yönelik herhangi bir işlemin yapılmadığı belirtilmiştir (Director of National Intelligence, Declassified Report).

ABD Temsilciler Meclisi İstihbarat Daimi Seçilmiş Komitesi de Rusya'nın müdahil olduğu iddia edilen 2016 ABD Başkanlık seçimlerine dair oldukça geniş kapsamlı bir rapor ortaya koymuştur. Ocak 2017 başlatılan ve bir seneyi aşkın süre devam eden soruşturma 2018 yılında tamamlanmıştır. 22 Mart 2018 tarihinde yayımlanan raporda Rusya'nın ABD'ye karşı giriştiği siber saldırı, bu saldırılarda kişilerin Rusya 'yayla bağlantılarının etkisi, ABD istihbarat örgütlerinden sızdırılmış bilgilerin neler olabileceği, ABD'nin bu saldırıya nasıl reaksiyon gösterdiği, Clinton'un kampanyasına Rusya'nın etkisi ve bundan sonraki saldırıların önüne geçilebilmesi adına çeşitli öneriler yer almaktadır. Rapora göre; Rusya'nın yürüttüğü seçimlere yönelik etki politikası çok yönlü ve çok taraflıydı. Gizli platformların kullanıldığı, sosyal medya, üçüncü taraf aracılar ve medya bu süreçte en fazla yararlanılan kaynaklar olarak görülmüştür. Tüm bu taraflar üzerinden etkili bir ağ kurularak seçimler üzerinde manipülasyon yaratılmış ve ABD toplumunun seçimlere ve yöneticilerine olan güveni sarsılmak istenmiştir. Bunu yapmak adına sosyal medya üzerinden sürekli ve planlı bir şekilde sahte tweetlerin atıldığı tespit edilmiştir. Raporda RF'nin bu amacına kesin bir şekilde ulaştığı belirtilmiştir. Diğer taraftan ABD hükümetinin seçim süresince Rusya'nın bu politikasına karşı yavaş ve tutarsız bir tutum sergilediği, aynı kötü performansın FBI tarafından da ortaya konduğu açıklanmıştır. FBI'nın tutarsız ve yavaş performansı, istihbarat verdiği kurumlar açısından tehditleri tanıma ve önleme noktasında dezavantaj yaratmıştır. Seçim sürecine bazı eyaletlerin DHS'yle işbirliği yapmakta gönülsüz davrandığı görülmüştür. Ayrıca her ne kadar oyların sayılmasında veya korunmasında bir müdahale söz konusu olmadıysa da sistemlerin bir etkiye kolayca maruz

kalabileceği, kırılgan ve dayanıksız bir yapıda olduğu rapora girmiştir. Trump'ın kampanyasının Rusya tarafından desteklendiği, koordine edildiği yahut üzerinde komplo kurulduğuna dair; raporda kesin bir kanıta ulaşılmadığı fakat kesin olmayan yargılara ulaşılabildiği ifade edilmiştir. Trump Tower'da, Clinton'un kampanyası aleyhine bilgisi olduğu iddia dilen bir Rus avukat ile Trump kampanyasını yürüten kişilerin buluşması buna örnek verilmiştir (House Permanent Select Committee on Intelligence, Report on Russian Active Measures, 2018: 1-10).

ABD Temsilciler Meclisi'nin ana soruşturma komitesi olan Gözetim ve Reform Komitesi ile Senato'ya bağlı Senato Yargı Komitesi ise seçimlere yönelik müdahale konusunda özellikle bireysel müdahalelerin olup olmadığı üzerinde çeşitli soruşturmalar gerçekleştirmişlerdir. Gözetim ve Reform Komitesi'nin 2017 yılında eski Ulusal Güvenlik Başdanışmanı Mike Flynn'ı, daha sonra ise Trump'ın kovmasıyla beraber FBI direktörü James Comey'i sorgulaması bunlardandır. Diğer taraftan Senato Yargı Komitesi de hem James Comey'i hem de Donald Trump Jr.'ı seçimler ve bağlantılı konular hakkında sorgulamışlardır (CNN, Aralık 2019).

ABD Seçimlerine Rusya'nın müdahil olduğuna yönelik bir diğer soruşturma ABD Başsavcı vekili Rod Rosenstein tarafından 2017 yılında görevlendirilen özel danışman, eski FBI Direktörü Robert Mueller eliyle gerçekleştirilmiştir (BBC News, Temmuz 2019). Oldukça ayrıntılı bir şekilde ele alınan 448 sayfalık rapor yaklaşık olarak iki yıllık bir süreye yayılmıştır. Temelde 2016 ABD Başkanlık seçimlerinde Rus müdahalesi olup olmadığını araştıran Mueller, aynı zamanda bir müdahale var ise söz konusu müdahalenin taraflarını belirleme niyeti de taşımıştır. Bu nedenle gerek Trump, Trump'ın seçim kampanyası ve kampanyayı yürütenler gerekse Beyaz Saray görevlileri soruşturmanın birer parçası olagelmiştir. Meuller'in raporunda en merak edilen sonuç ise Trump'ın kampanyası ile RF'nin herhangi bir şekilde ilişkilendirilip ilişkilendirilmediği olmuştur (The New York Times, Mart 2019).

Mueller Raporu'na göre Rusya Federasyonu, Trump'ın kampanyasını lehine olmak üzere ve aynı zamanda Hillary Clinton'un kampanyasının ise aleyhine İnternet Araştırma Ajansı (IRA/Internet Research Agency) eliyle bir takım girişimlerde bulunmuştur. Raporda sosyal medya üzerinden tweetlerle, çeşitli paylaşımlar ve sahte hesaplarla Clinton aleyhine imaj yaratan, Ajans tarafından görevlendirilen troll hesap sahiplerinin New York, Florida ve Pensilvanya kampanyalarında Trump lehine

çalıştıkları ifade edilmiştir. Ayrıca IRA'nın gerçek kişilerle etkileşime girerek bunları da sosyal medya üzerinden etkilemeye çalıştıkları belirlenmiştir. Diğer taraftan rapora göre IRA; Trump kampanyasını yürüten yetkilerle çeşitli politik hedefleri belirleme, yol haritası çizme gibi saiklerle bir araya gelme girişimlerinde bulunmuşsa da herhangi bir yetkiliyle bu konuda işbirliği yaptıklarına dair bir kanıta ulaşılamamıştır. Raporda GRU'nun Clinton'un kampanyası için çalışanların, gönüllü yardım edenlerin hatta kampanya direktörü John Podesta'nın maillerinin hacklenmesinde dahiliyeti olmuştur. Ayrıca H. Clinton'un maillerinin hacklenmesi ve DCLeaks ve Wikileaks gibi mecralarda dağıtılmasından yine GRU sorumlu tutulmuştur. Raporda Trump'ın kampanyasına da yer verilmiştir; Trump kampanyasının Wikileaks aracılığıyla sızdırılan bilgilere ilgi göstermesi, Trump Tower'da bir Rus yetkiliyle görüşüldüğü iddiası, Trump Jr. 'ın Wikileaks ile mailleşmeleri bunlardan sadece bazılarıdır. Raporda ayrıca Rusya Federasyonu ile Trump kampanyasının herhangi bir şekilde direkt olarak bağlantılı hareket edildiğine dair herhangi bir kesin kanıta ulaşılmadığına kanaat getirmiştir. Ayrıca Trump'ın gerek seçim sürecinde gerekse seçim sonrasında hem kendi kampanya yürütücüleriyle olan diyalogları hem de kamuoyu ve rakipleriyle girdiği tartışmaları tek tek incelenmiştir. Diğer taraftan kampanya yürütücülerinin de bilgisine başvurularak oluşturulan rapor ortaya şöyle bir netice koymuştur; Başkan Trump'ın bilerek ve isteyerek Rusya Federasyonu tarafından ortaya konan seçimlere müdahale girişimlerinde, Rusya Federasyonu ile birlikte hareket ettiğine kesin kanaat ve kanıt oluşmamıştır. Bununla birlikte rapor, onu tamamen temize de çıkarmamaktadır (Report on Investigation Into Russian Interference in the 2016 Presidential Election, 2019: 1-448).

Trump seçimlere RF'nin müdahalesini henüz baştan reddetmiş, kendisinin adaleti engellediğine dair iddiaları da bir operasyon olarak lanse etmiştir. Mueller Raporu'nun sonucunu da kendisinin haklılığının bir teyidi olarak değerlendirmiştir. Fakat Trump karşıtları Mueller Raporu'nda; özellikle Başkan'ın adaletin engellemediğine dair kesin bir hüküm bulunmaması üzerinden eleştirilere devam etmişlerdir (BBC News, Nisan 2019). 2016 ABD Başkanlık Seçimleri ve sonrasındaki süreç ABD ve RF ilişkilerini de olumsuz yönde etkilemiştir. Özellikle henüz seçim aşamasındayken Obama; GRU'nun seçimlere müdahale girişiminde bulunduğu iddiaları üzerine RF Başkanı Putin'i bu konuda uyarmış, hacklemelerin

durdurulmasını istemiştir (New York Times, Kasım 2016). Sonrasında ise misilleme olarak 35 Rus diplomat süresiz olarak ABD'den sınır dışı edilerek ülke dışına çıkarılmıştır. Diplomatların sınır dışı edilmelerinin sebebi GRU ve FSB'nin ABD seçimlerine yönelik manipülasyon girişimleri olarak gösterilmiştir. Diğer taraftan RF, 35 diplomatının sınır dışı edilmesinin ve RF'nin ABD seçimlerine müdahale ettiğine dair iddiaları hiçbir zaman kabul etmemiştir. Fakat Rusya beklenenin aksine ABD'nin diplomatları sınır dışı etmesine rağmen herhangi bir karşı hamlede bulunmamıştır (The Guardian, Aralık 2016). Putin de ABD Başkanlık seçimlerine yönelik devlet bazında herhangi bir müdahalenin söz konusu olmadığını baştan itibaren savunagelmiştir. Fakat özellikle bir müdahale söz konusu ise bunun Rus vatansever hackerler tarafından inisiyatif alınarak yapılmış olabileceğine dair açıklamaları da süreci iyice germiştir (Independent, Haziran 2017).

RF'nin ABD 2016 Başkanlık seçimlerine müdahale ettiğine dair tartışmalar devam etmekle beraber, söz konusu müdahale iki ülke ilişkilerini zaman zaman germeye devam etmektedir. Ayrıca söz konusu müdahale iddialarının da siber alandan vuku bulması iki ülkenin rekabet durumlarının yeni bir mecraya taşındığını göstermektedir. Bu anlamda iki ülke de oluşturdukları kurumsal yapılanmalar, önlem ve saldırı mekanizmaları ile bu rekabetteki üstünlük arayışlarını sürdürmektedirler.

SONUÇ

Güvenlik, geçmişten günümüze uluslararası ilişkilerin ve onun temel aktörü olan devletlerin birincil önemdeki meselelerinden biri olmuştur. Uluslararası arenadaki temel hedefi hayatta kalmak olan devletlerin bu hedefi gerçekleştirme adına hem savunma mekanizmalarını güçlendirme hem de saldırı yeteneklerini arttırma yolunu seçtikleri görülmektedir. Devletlerin güvenlik okumaları dâhilinde, güvenlik tehdidi olarak algıladıkları unsurlar üzerinden savunma ve saldırı mekanizmaları oluşturdukları bilinmektedir. Bu durumda klasik güvenlik paradigması, güvenliği askeri unsurlarla sınırlandıran yapısı itibariyle devletlere ve onlara yöneltilen tehditlere karşı eksik bir anlayış sunmaktadır.

Devletlerin güvende olma durumlarını sağlamaları açısından güvenlik tehditlerini doğru ve eksiksiz bir şekilde ele almaları gerekmektedir. Bu doğrultuda klasik güvenlik anlayışına getirilen eleştiriler dikkate alınarak yeni tehditlerin mahiyetini, seviyesini ve ortaya çıkarabilecekleri yıkıcı sonuçları da göz önünde bulundurmak önem kazanmaktadır. Güvenliğin her yönüyle ele alınması gereken bir mefhum olduğu; tarihsel süreç içerisinde aksi yapıldığı takdirde ortaya çıkan yıkıcı etkileriyle birçok defa görülmüştür ve görülmeye devam etmektedir. Bu anlamda güvenliğin yeni bir parametresi olan siber güvenlik; son yıllarda ön plana çıkmakta, dikkate alınması gereken bir unsur olarak belirmektedir.

Siber alanın güvenlik okumalarına dâhil edilmesinde devletlerin geciktiği görülmüştür. Bunun altında yatan ana sebebin; gelişen teknolojinin, dijitalleşen dünyanın ve devletlerin bu alandan gelecek tehditlerden ne derecede etkilenebileceklerinin yeterince idrak edilememesi olmuştur. Fakat Estonya'ya yönelik olarak 2008 yılında gerçekleştirilen siber saldırılar bu kanıyı temelinden sarsarak; devletlerin siber alanda önlem almalarına, politika ve strateji geliştirmelerine, saldırı ve savunma mekanizmaları oluşturmalarına sebebiyet vermiştir. Siber alanın rekabet ve işbirliğine açık bir alan olarak görülmesi de bu sürecin kaçınılmaz bir aşamasını oluşturmuştur.

Siber alanın kendisine has bir yapı sergilediğini ortaya koyan bu çalışmada; siber güvenlik ve ona ait kavramlara yönelik ilintili, ilişkili ve farklılıkları dikkate alan bir inceleme yapılmıştır. Siber güvenlik kavramlarının klasik güvenlik veyahut kodifiye bir hal alan hukuk terimleri üzerinden anlamlandırılması, alana yönelik eksik ve yanlış analizler doğurmaktadır. Bu nedenle siber kavramların klasik güvenlik kavramlarından ne derecede farklılık ve benzerlikler gösterdiğine dikkat çekilmiştir.

Siber güvenliğin özellikle 2000'li yıllar sonrasında devletlerin dikkatini çekmeye başlamasıyla bu alana yönelik çalışmalar hız kazanmıştır. Fakat siber tehditlerin ve saldırıların özellikle teknoloji alanında yetkin ülkeleri dahi zor durumda bırakacak bir hale bürünmesi bu çalışmaların ciddiyetinin had safhada seyir etmesini sağlamıştır. Özellikle teknoloji alanında ileri seviyelere ulaşan ülkelerin, siber alanı bir hâkimiyet/rekabet ortamı olarak gördükleri bilinmektedir. Uluslararası ilişkilerin güç odaklı yapısının siber alana yansıması da bu anlamda anlaşılır görülmektedir. Fakat siber alan sadece devletlerin hâkimiyetindeki bir alan olmaktan oldukça uzaktır. Bu nedenle devletler siber alanda hem bireylerle, terör gruplarıyla ve hem de birbirleriyle rakip olma durumundadırlar. Siber alanda ilişkiler; gerek devletler gerekse devlet dışı aktörler arasında cereyan ederken bu ilişkiler çok yönlü bir mahiyette seyir etmektedir. Bu çalışmada; ilişkilerin sadece rekabet temalı gelişmediğini, işbirliği alanlarının da varlığına dikkat çekilmiştir.

ABD ve RF'nin siber alandaki ilişkileri üzerine eğilen bu çalışma iki ülkenin siber alandaki yapılanmalarını analiz ederek var olan durumu ortaya koymayı hedeflemiştir. ABD ve Rusya Federasyonu'nun siber alandaki ilişkilerini anlamak için; iki ülkenin siber alandaki strateji, hedef ve kurumsal yapılanmaları detaylandırılmıştır. ABD'nin siber güvenlik strateji belgeleri temelde kritik altyapıların korunması fikri üzerinden savunulmuştur. Diğer taraftan Rusya Federasyonu için de durum pek farklı değildir. Rusya Federasyonu, siber alandan ülkeye yönelik bir takım girişimlerin olduğunu ve bu girişimlerin ekseriyetle Batı merkezli olduğunu savunmaktadır. Bu nedenle siber alanda iki ülkenin de güç elde etme arayışı ve çabasında olduğu görülmektedir. Siber alanda da rekabet ettikleri anlaşılan bu iki ülkenin, siber alana yönelik tanım, tasnif ve kurumsal farklılıkları bulunmasına rağmen siber alana atfettikleri önem ileri düzeyde seyretmektedir. Diğer

taraftan iki ülkenin siber alandaki ilişkilerinin sadece rekabet yönünde gelişmediği görülmüştür. Siber alanın tanımlanması, düzenlenmesine yönelik bir takım işbirliği girişimleri de bulunmakla beraber bu işbirliği arayışlarının özellikle 2016 ABD Başkanlık Seçimleri sonrasında kesintiye uğradığı görülmektedir.

Bu çalışmanın ABD ve Rusya Federasyonu'nun siber alandaki rekabetlerini incelediği göz önüne alındığında bunun en önemli parametresini 2016 ABD Başkanlık Seçimleri 'ne Rusya Federasyonu'nun müdahale ettiğine ilişkin iddialar oluşturmaktadır. Gerek seçimlere ilişkin müdahale iddialarının ve neticesindeki tartışmaların henüz devam ediyor olması gerekse iki ülke arasındaki işbirliği olasılıklarının bir nevi önünü kapatması nedeniyle bu müdahale iddiası; ilişkilerde önemli bir yer tutmaktadır. ABD istihbarat örgütlerinin iddiaları ve sonrasında ortaya koydukları istihbarat raporları, diğer taraftan komisyonlar ve özel yetkili kişilerce gerçekleştirilen soruşturma raporları incelendiğinde Rusya'nın ABD seçimlerine etkide bulunduğu görülmektedir. Raporlar ve bir takım Rus yetkililerin açıklamaları dikkate alındığında ABD seçimlerine yönelik gerçekleştirilen siber faaliyetlerin Rusya bağlantılı olduğu kısmen teyit edilebilmektedir. Fakat bu saldırıların direkt olarak seçim sistemine veya kullanılan oylara yönelik olmadığı görülmektedir. Yine Trump'ın seçim kampanyası ön plana çıkarılırken Clinton'un seçim kampanyasının başarısız olması yönünde girişimlerde bulunulduğu tespit edilebilmektedir.

ABD Seçimlerine yönelik RF'nin siber faaliyetlerinin etkili olması iki ülkenin rekabetinde ABD aleyhinde bir algı yaratmıştır. Ayrıca Rusya Federasyonu'nun ilgili siber güvenlik kurumlarının süreci daha iyi yönettiği görülmüştür. Rusya Federasyonu, ABD ve Batı demokrasilerinin seçim süreçlerine yönelik manipülasyonlar gerçekleştirerek, bu sistemlere olan güveni sarsma niyetini gerçekleştirmiştir. Diğer taraftan ABD'nin siber yapılanmasının önemli birer parçalarını oluşturan istihbarat örgütleri ve bakanlık seviyesindeki kurumlarının iyi bir sınav veremedikleri görülmüştür. ABD seçimlerine yönelik bu durum siber alandan az maliyetle yıkıcı etkiler gösterebilecek saldırıların, siber kapasiteleri yönünden güçlü ülkeler açısından bile ortaya çıkabileceğini göstermesi itibariyle önemli bir kilometre taşı olmuştur. İki ülkenin siber alandaki rekabet durumlarının devam edeceği, işbirliği alanlarının ve girişimlerinin ise daralacağı anlaşılmaktadır. Netice itibariyle iki güçlü ülke olan ABD ve Rusya Federasyonu, her alanda olduğu

gibi siber alanda da rekabet üzerine yoğunlaşmaya devam edeceklerdir. Rekabette belirleyici olan ise siber alandaki güç durumunu kimin kendi lehine geliştireceğine bağlı olacaktır. Yakın zamanda ABD ve Rusya Federasyonu'nun başta ilişkilerindeki bu gerilmelerin diğer ülkeler nezdinde ne türlü sonuç ve etkiler doğuracağı henüz bilinmemekle beraber yeni bir Soğuk Savaş ihtimalinin siber alanda ortaya çıkması ihtimalinin göz ardı edilmemesi gerekmektedir. Bu anlamda iki ülke ve onların müttefik ilişkilerinin gelecekte yeni bir soğuk savaşa evirilmesi siber alanda yeni bir durumu ortaya çıkaracaktır. Kısacası ABD ve Rusya Federasyonu'nun siber alandaki rekabet ve ilişkilerinin dünya barışı ile direkt ilintili olduğu sonucuna varılabilir. Bu aşamada iki ülkenin işbirliği ve rekabet durumları gelecekte dünya politikasına yön verir bir mahiyet taşımaktadır.

ABD ve Rusya Federasyonu özelindeki rekabeti ele alan bu çalışma; siber alanın devletler açısından yeni bir cephe olacağını ortaya koymaktadır. Devletlerin siber alana yönelik strateji belirlemeleri, bu stratejileri uygulayacak kurumsal ve yasal düzenlemeleri hayata geçirmeleri gerekmektedir. Aksi takdirde, günümüz teknolojisi ve bu teknolojiye bağlı hale gelen devlet sistemleri de dikkate alındığında topyekûn savaşlardan daha yıkıcı sonuçlarla karşılaşma ihtimali büyümektedir. Diğer taraftan dünya barışının sağlanabilmesi, yeni bir topyekûn savaştan kaçınılması adına siber alanda/uzayda uluslararası mutabakat metinlerinin oluşturulması elzemdir. Bu nedenle ABD ve RF başta olmak üzere siber alanda yetkin diğer ülkelerin de katılımıyla müzakere masalarının kurulması ve siber alanın yeni bir gerilim ve çatışma alanı olmasının önüne geçilmesi gerekmektedir.

Siber alanın manipülasyona açık ve bu alanda manipülasyon tekniklerinin gelişkin olması bir takım yeni sorunların ortaya çıkması ihtimalini doğurmuştur. Özellikle 2016 ABD Başkanlık Seçimlerin 'de de görüldüğü gibi siber alan kullanılarak popülist söylemlerin yayıldığı bir mecra yaratılabilmektedir. Doğru olmayan kaynaklar yoluyla bir takım iddiaların ortaya atılması sonucu yaratılan algı ile toplum keskin kamplara ayırılmakta, bu durum üzerine bir takım politikalar kurulmaktadır. 2016 ABD seçimleri özelinde bu durum yaşanmıştır. Gerçek ötesi bir durum yaratılarak Clinton'un kampanyasının manipüle edilerek toplumun gözünde güvenilmez bir imaj yaratılması politikasını yaratan Trump, başkan olduktan sonra ise benzer bir politikayla kendisi karşı karşıya kalmıştır. Çünkü Rusya

Federasyonu'nun Trump ile işbirliği yaptığı iddiaları karşısında toplumun bir diğer kesimi Trump aleyhinde düşüncelere sahip olmuşlardır. Diğer taraftan Rusya Federasyonu'nun seçimlere direkt olarak, oy değiştirme yahut oy sayımına müdahale gibi siber faaliyetlerinin olmadığı uzmanlar tarafından belirtilmişse de ABD vatandaşlarında yaygın bir şekilde Rusya'nın seçimlere doğrudan müdahalede bulunduğu düşüncesi oluşmuştur.

2016 ABD seçimlerinde siber alan kullanılarak çeşitli propaganda yollarının denendiğinden çalışmada bahsedilmiştir. Aynı olaylar 2016 yılındaki Brexit olaylarında da meydana gelmiştir ki bu iki olay yeni bir durumun ortaya çıktığını göstermektedir. Hem Brexit oylamasında hem de ABD seçimlerinde seçmenlerin kararlarının değiştirilmesine yönelik yapılan hamlelerin arkasında yatan gerçeklerin sorgulanır olması yeni bir gerçekliğin kurulduğu ya da gerçekliğin ötesine geçildiği yönünde tartışmaları da beraberinde getirmektedir. Bu gerçek ötesi politikalarla politikacıların kendi lehlerine gerçeği farklı göstererek bir takım girişimlerde bulundukları, kitlelerin de bu gerçek ötesini gerçeğe tercih ettiklerine şahit olunmaktadır. ABD seçimlerinde Trump'ın kampanyasının göçmen karşıtlığı üzerine kurmasında asıl hedef bu gerçek ötesi durum üzerinden oylarını arttırmak olmuştur. Bu amaca hizmet eder şekilde Trump, Meksika gibi ülkelerin, sorunlu vatandaşlarını ABD'ye göçe teşvik etmek suretiyle ülkelerini zayıf düşürmek için hamleler yaptığını ileri sürmüştür. Neticesinde bu söylem birçok eleştiriyi de beraberinde getirmişse de insanlar Trump'ın görüşlerine önemli derecede destek vermişler ve onu başkan seçmişlerdir. Brexit oylamasında da benzer bir söylem Avrupa Birliği'nden ayrılma yönünde oy kazanmak adına Boris Johnson gibi liderler tarafından gerçekleştirilmiştir. Brexit oylamasında ayrılma yönünde bir kamuoyu oluşturma adına; Birleşik Krallık'ın her yıl milyonlarca Euro'yu AB'ye fon olarak aktardığı, bu fonlarla İngiltere'nin daha iyi şartlara kavuşturulabileceği iddia edilmiştir. Uzmanlar bunun gerçeği yansıtmadığını, İngiltere'nin AB'den ayrılması durumunda ciddi kayıplar yaşayacağını çeşitli platformlarda belirtmişlerse de insanlar onlara inanmak istememişlerdir. Bunun altında; parti programlarının insanların gerçek sorunlarını yansıtmaması, ekonomik anlamda dezavantaj yaşayan kesimlerin tepkilerini gerçeğin ötesine çekmenin kolay olması, nostaljik değerler üzerinden muhafazakâr, milliyetçi çevrelerin istismar edilerek taraftar kazanmanın siyasilerce pragmatik bir yol olarak görülmesi gibi sebepler yatmaktadır. 'Gerçek ötesi' durumun gerçeğin önüne geçtiği

bu durumlarda birçok devletin demokrasinin de yeni sürece girdiği, ekseriyetle anti-demokratik uygulamaların normalleştiği görülmektedir (Rose, 2017: 555-558).

Toplumun elit kesimleriyle dezavantajlı kesimlerinin sık sık karşı karşıya geldiği, ekonomik anlamda iyi durumda olanlar ile kötü durumda olanların cepheleştiği toplumlarda özellikle popülist söylemlerle yaratılan ortamın bu anti-demokratik eğilimlerin önünü açabildiği görülmektedir. Yine terör olaylarının fazla olduğu yahut göç olaylarının görüldüğü toplumlarda da bu anlamda cepheleştirmelerin yaratılması daha kolay olabilmektedir. Bu ortamın varlığı gerçek-ötesi(post-truth) söylemleri kullanan liderleri siyaset sahnesinde ön plana çıkarabilmektedir. Bu söylemlerin en kolay yayılma ortamı ise yine siber alandır. Çünkü siber alanda haberlerin, düşüncelerin, gönderilerin kolayca yayılabiliyor olması bu mecraları operasyonel olarak cazip kılmaktadır. Çeşitli sahte hesaplarla yalan haberlerin yayılması ve bu haberlerin etkili ve hızlı sonuçlar meydana getirebilmesi siber alanın tercih edilmesinin en önemli nedenlerinden birkaçıdır.

Diğer taraftan bu haberlerin kolayca yalanlanabilir, gerçeğin ortaya çıkarılabilir olduğu gözden kaçırılmamalıdır. Fakat bu durum dahi uzman kişilerin yahut yetkililerin bilgilendirmeleri boşa çıkarılabilmekte, popülist ve gerçek-ötesi bilgilerin tercih edildiği sık sık görülmektedir. Kendilerine adaletsizliğin karşısında, toplumun tarafında gösteren popülist liderlerin bu kanallar yoluyla başarılı siyasi çıkışlar yaptığına şahit olunmaktadır. Söz konusu durum ise liberal demokratik yönetimlerin yerine daha kapalı ve anti-demokratik yönetimlerin muhkem olmasının önünü açmaktadır (Turkan-İpek, 2018: 65-79). Son yıllarda gerçeğin yerine gerçek-ötesi bilgilerin tercih edildiği uzmanlarca paylaşılan bir kaygı olmuştur. Özellikle Twitter gibi sosyal paylaşım mecralarında bu tarz bilgilerle oluşturulan yalan haberlerin yansımalarının gündem belirleyici özellikleri bu durumu kanıtlar niteliktedir. Sahte kullanıcılar, troll hesaplar ve popülist liderlerin yoğun şekilde kullandıkları sosyal medya ve diğer siber teknolojiler yoluyla oluşturulan gündemler, toplumları her geçen gün ayrıştırmakta, demokratik olmayan politikalar doğurmaktadır (Sismondo, 2017: 3-6).

Sonuç olarak siber alan; barındırdığı riskler ve fırsatlarla gelecekte de ulusal ve uluslararası güvenliğin önemli bir parametresi olacaktır. Uluslararası politikanın tüm aktörlerinin etkileşim içerisinde bulundukları bu alan siber kapasite ve

kabiliyetlerini arttıran aktörler için güvenli bir alan; bu alanda güç unsurlarını lehine çeviremeyen aktörler için ise güvenlik sorunları yaratmaya devam edecektir.

KAYNAKÇA

1. Kitaplar

Akyeşilmen, Nezir (2018). Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik. Ankara: Orion.

Arı, Tayyar (2011). Uluslararası İlişkiler ve Dış Politika. Bursa: MKM Yayıncılık.

Avcı, Gültekin (2004). İstihbarat Teknikleri: Aktörleri, Örgütleri ve Açmazları. İstanbul: Timaş Yayınları.

Cavelty, Myriam Dunn (2007). ‘’Cyber Security.’’ Şu kitapta: Ed. Allan Collins. Contemporary Security Studies. Oxford: Oxford Universty Press.

Cavelty, Myriam Dunn (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London and New York: Routledge.

CyberEdge Group (2018). The Threat Intelligence Handbook. Annapolis: CyberEdge Press.

Çınar, Bekir (1997). Devlet Güvenliği, İstihabarat ve Terör. Ankara: Sam Yayınları.

Darıcılı, Ali Burak (2018). ‘’Askerileştirilen ve Silahlandırılan Siber Uzay.’’ Şu kitapta: Ed. Ali Acaravcı. Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri. Ankara: Nobel Akademik Yayıncılık.

Ducheine, Paul, Joop Voetelink, Jan Stinissen ve Terry Gill (2012). ‘’Towards A Legal Framework for Military Operations.’’ Şu Kitapta: Ed. Paul Ducheine, Frans Osinga, Joseph Soeters. Cyber Warfare: Critical Perspectives. The Hague: Asser Press, pp. 102-103.

Dupont, Benoit (2013). ‘’The Proliferation of Cyber Security Strategies and Their Implications for Privacy.’’ Şu Kitapta: Ed. Karim Benyekhlef and Esther Mitjans. Circulation Internationale de l’information et Sécurité. Montreal: Les Éditions Thémis.

Greenberg, Andy (2019). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers. New York: Doubleday.

Johnson, Thomas A. (2015). ‘’Historical Reference Points in the Computer Industry and Emerging Challengs in Cybersecurity.’’ Şu Kitapta: Ed. Thomas A. Johnson. Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. New York: CRC Press.

Lightbody, Bradley (1999). ‘’Cold War.’’ Şu Kitapta: Ed. Stephan J.Lee ve Sean Lang. The Cold War. New York: Routledge.

Richards, Julian (2014). Siber Savaş: Küresel Güvenlik Tehdidinin Anatomisi. Basingstoke: Palgrave Macmillan.

Roscini, Marco (2014). Cyber Operation and the Use of Force in International Law. Oxford: Oxford Universty Press.

Sandıklı, Atilla, Emeklier Bilgehan (2011). ‘’ 21. Yüzyılda Yeni Güvenlik Anlayışları ve Yaklaşımları’’. (Ed.) Hasret Çomak, Caner Sancaktar. 21’inci Yüzyılda Uluslararası Örgütlerin Güvenlik Yaklaşımları ve Balkanlar’ın Güvenliği. Kocaeli: 22.

Tarhan, Kamil (2020). ‘’Klasik Soğuk Savaş’tan Küresel Siber Soğuk Savaş’a Siber Uzay Kavramının Analizi.’’ Şu Kitapta: Ed. Ali Burak Darıcılı. Güvenlik, Teknoloji ve Yeni Tehditler. Ankara: Nobel Yayıncılık.

Tür, Özlem, Çiğdem Aydın Koyuncu (2014). ‘’Uluslararası İlişkilerde Toplumsal Cinsiyet.’’ Şu kitapta: Ed. Evren Balta. Küresel Siyasete Giriş: Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler. İstanbul: İletişim Yayınları.

Virkar, Shefali (2016). ‘’The Mirror Has two Faces: Terrorist Use of the Internet and the Challenges of Governing Cyberspace.’’ Şu Kitapta: Ed. Eugenie de Silva. National Security and Counterintelligence in the Era of Cyber Espionage. USA: IGI Global.

2. Makaleler, Bildiriler, Diğer Basılı Yayınlar

Ağır, Bülent Sarper (2011). ‘’Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı.’’ Güvenlik Stratejileri Dergisi, Sayı 22, Sayfa 102.

Ağkaya, Onur (2016). ‘’İngiliz Okulu ve Uluslararası Toplum Düşüncesi.’’ Ankara Üniversitesi SBF Dergisi, Cilt 71, No 4, Sayfa 1079-1085.

Aksu, Muharrem, Faruk Turhan (2012). ‘’Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik’’. Uluslararası Alanya İşletme Fakültesi Dergisi, Cilt 4, Sayı 2, Sayfa 71.

Akyeşilmen, Nezir (2016). ‘’ Siber Güvenlik ve İnsan Hakları: Yeni Bir Paradigma İhtiyacı Mı?.’’ Siber Politikalar Dergisi, Cilt 1, Sayı 1, Sayfa 45.

Askerov, Ali (2015). ‘’ The Chechen Wars, Media, and Democracy in Russia.’’ Innovative Issues and Approaches in Social Sciences, Cilt 8, Sayı 2, Sayfa 8-15.

Aslay, Filiz (2017). ‘’ Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi.’’ International Journal of Multidisciplinary Studies and Innovative Technologies, Volume 1, Issue 1, Pages 25.

Aydın, Mustafa (2004) “Uluslararası İlişkilerin “Gerçekçi” Teorisi: Kökeni, Kapsamı, Kritiği”, Uluslararası İlişkiler, Cilt 1, Sayı 1, s. 34-36.

Baezner, Marie, Robin Patrice (2017). Hotspot Analysis: Cyber Conflict Between United States of America and Russia. Center for Security Studies(CSS), ETH Zürich.

Bakan, Selahaddin, Sonay Şahin (2018). ‘’Uluslararası güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler’’. The Journal Of International Lingual,Social and Educational Science, Volume 4, Number 2, Page 141-142.

Bakan, Zerrin Ayşe (2007). ‘’Soğuk Savaş Sonrasında Yeni Güvenlik Teorileri ve Türkiye’nin Güvenlik Algılamaları.’’ 21. Yüzyıl Dergisi, Ekim-Kasım-Aralık 2007, Sayfa 41-42.

Bartles, K. Charles (2016). ‘’Getting Gerasimov Right.’’ Military Rewiev, Cilt 96, Sayı 1, Sayfa 30.

Baylis, John (Yaz 2008). “Uluslararası İlişkilerde Güvenlik Kavramı.” Uluslararası İlişkiler Dergisi, Cilt 5, Sayı 18, s. 69-85.

Baysal, Başar, Çağla Lüleci (2015). ‘’Kopenhag Okulu ve Güvenlikleştirme Teorisi’’. Güvenlik Stratejileri Dergisi, Yıl 11, Sayı 22, Sayfa 73-74.

Bayraktar, Gökhan (2014). ‘’Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat.’’ Güvenlik Stratejileri Dergisi, Yıl 10, Sayı 20, Sayfa 129-130.

Bıçakçı, Salih (2012). ‘’Yeni Savaş ve Siber Güvenlik Arasında NATO’nun Yeniden Doğuşu.’’ Uluslararası İlişkiler, Cilt 9, Sayı 34, Sayfa 208-209.

Bilgiç, Ali (2011). ““Güvenlik İkilemi”ni Yeniden Düşünmek Güvenlik Çalışmalarında Yeni Bir Perspektif”, Uluslararası İlişkiler, Cilt 8, Sayı 29 (Bahar 2011), s. 125-130.

Bilgin, Pınar (2010). ‘’Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları.’’ Stratejik Araştırmalar, Cilt 8, Sayı 14, Sayfa 71-73.

Birdişli, Fikret (2014). ‘’Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü.’’ Güvenlik Stratejileri Dergisi, Cilt 10, Sayı 20, Sayfa 243-245.

Bonfanti, Matteo E. (2018). ‘’Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice.’’ Cyber, Intelligence and Security, Cilt 2, Sayı 1, Sayfa 110-111).

Brattberg, Erik, Tim Maurer (2018). ‘’Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks.’’ Carnegie Endowment for International Peace, Sayfa 1-5.

Brickey, Jonalan (2012). ‘’Defining Cyberterrorsim: Capturing A Broad Range of Activities in Cyber Space.’’ CTC Sentinel, Volume 5, Issue 8, Page 4-8.

Butler, Robert J. (2016). ‘’ Technology, Threats and Trust in an Interconnected World.’’ Rajaratnam School Of International Studies, Edited Volume, Pages 68.

Cappello M. (ed.), Regulation of Online Content in the Russian Federation, IRIS Extra, European Audiovisual Observatory, Strasbourg, 2015.

Collin, Barry (1997). ‘’Future of Cyberterrorism: The Pyshical Virtual Worlds Converge.’’ Crime and Justice İnternatoinal, Volume 13, Issue 2, pp 15-18.

Connell, Michael, Sarah Vogler (2017). ‘’Russia’s Approach to Cyber Warfare.’’ CNA’s Analysis&Solutions, Federal Government Contract No. N00014-16-D-5003.

Conway, Maura (2003). ‘’Cyberterrorism: The Story So Far.’’ Journal of Information Warfare, Vol 2, No 2, pp 39.

Çetinkaya, Şeref (Aralık-Ocak-Şubat 2012-2013). ‘’Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları’’, 21. Yüzyılda Sosyal Bilimler Dergisi, Sayı 2, Sayfa 247.

Çıkrıkçı, Tolga (2017). ‘’Uluslararası İlişkilerde Güvenliğin Referans Nesnesi Sorunsalı: Klasikten Yeniye Kavramsal Bir Analiz.’’ Giresun Üniversitesi İktisadi ve İdari Bilimler Dergisi, Cilt 3, Sayı 6, Sayfa 216-224.

Darıcılı, Burak (2015). ‘’NATO’nun Siber Güvenlik Stratejisinin Analizi’’. Ed. Tayyar Arı ve Barış Özdal / VII. Uludağ Uluslararası İlişkiler Konferansı. Bursa: Dora Basım-Yayın: 414.

Darıcılı, Ali Burak (2017). ‘’ Demokrat Parti Hack Skandalı ABD ve RF’nin Siber Güvenlik Stratejilerinin Analizi.’’ Uluslararası Çalışmalar Dergisi, Özel Sayı, Sayfa 5.

Darıcılı, Ali Burak (2017). ‘’ Demokrat Parti Hack Skandalı ABD ve RF’nin Siber Güvenlik Stratejilerinin Analizi.’’ Uluslararası Çalışmalar Dergisi, Özel Sayı, Sayfa 7.

Darzcewska, Jolanta (2016). ‘’Russia’s Armed Forces In The Information War Front: Strategic Documents.’’ Centre For Eastern Studies OSW, Sayı 57, Sayfa 17-18.

De Araujo, Marcelo (2013). ‘’Cyber War, Political Realism, and World State’’ [Bildiri]. 6th International Symposium on Justice, At The Pontifical Catholic University, Porto Alegre, Brazil.

Demiray, Muhittin, İsmail Hakkı İşcan (Ağustos 2008). ‘’Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı’’. Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, Sayı 21, Sayfa 152.

Demirel, Murat (2017). ‘’Hedley Bull Perspektifinden ‘Uluslararası Toplum’ Kavramlaştırması ve Kurumları’’. Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Dergisi, Sayı 2017 Kış, Sayfa 47.

Devlen, Balkan, Özgür Özdamar (Bahar 2010). ‘’Uluslararası Sistemde İngiliz Okulu Kuramı: Kökenleri, Kavramları ve Tartışmaları’’. Uluslararası İlişkiler, Cilt 7, Sayı 25, Sayfa 47-53.

Dimitrakopulau, Sophia, Liarapoulos Andrew (Winter 2010). ‘’ Russia’s National Security Strategy to 2020: A Great Power In The Making?.’’ Caucasian Review of International Affairs, Cilt 4, Sayı 1, Sayfa (1-40).

Doğanalp, Tuğba (2016). ‘’Uluslararası Hukukta Kitle İmha Silahları ve Silahsızlanmaya Yönelik Girişimler.’’ Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi, Cilt 3, Sayı 4, Sayfa 25-26.

Dyner, Anna (2017). ‘’ The Russian Federation’s New Foreign Policy Concept and Threatening a Pivot towards Asia: A New Foreign Policy Concept of the Russian Federation.’’ Polish Institute of International Affairs, Sayfa 1-2.

Erdoğan, İbrahim (2013). ‘’Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı.’’ Akademik Bakış Dergisi, Cilt 6, Sayı 12, Sayfa 272.

Eren, Mehmet (2017). ‘’ Avrupa Birliği’nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve Ve Strateji Belgesi Öncesi AB’nin Eylemleri.’’ Siber Politikalar Dergisi, Cilt 2, Sayı 3, Sayfa 36-37.

Eşitli, Ezgi Aygün (2013). ‘’Suçların ve Cezaların Kanuniliği İlkesi.’’ Türkiye Barolar Birliği Dergisi, Sayı 104, Sayfa 234.

Fidler, David P. (2011). ‘’ International Law and the Future of Cyberspace: The Obama Administration’s International Strategy for Cyberspace’’. Insights, Volume 15, Issue 15, Pages 1-2.

Fridman, Ofer (2019). On ‘Gerasimov Doctrine’: Why the West Fails to Beat Russia to the Punch. Cilt 8, Sayı 2, Sayfa 101-112.

Günay, Vahit (2018). ‘’Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Örgütler.’’ Güvenlik Stratejileri Dergisi, Yıl 14, Sayı 27, Sayfa 87-89.

Gresimov, Valery (2013). ‘’The Value of Science In Prediction.’’ Military-Industrial Kurier, Şubat 27, sayfa 1-11.

Harknett, Richard J., James A. Stever (2009). ‘’The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen.’’ Journal of Homeland Security and Emergency Management, Volume 6, Issue 1, Pages 1-3.

Harknett, Richard J., John P. Callaghan, Rudi Kauffman (2010). ‘’Leaving Deterrence Behind: War-Fighting and National Cybersecurity.’’ Journal of Homeland Security and Emergency Management, Volume 7, Issue 1, Pages 4-5.

Harknett, Richard J., James A. Stever (2011). ‘’The New Policy World of Cybersecurity’’. Public Administration Review, Vol. 71, Issue 3, Pages 456.

Heickerö, Roland (2010). Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. Stocholm: Sweedish Defence Research Agency (FOI). A12001.

Iqbal, Mohammad (2004). ‘’ Defining Cyberterrorism.’’ The John Marshall Journal of Information Technology & Privacy Law, Volume 22, Issue 2, Pages 403.

Jaitner, Margarita, Mattsson A.Peter (2015). ‘’Russian Information Warfare of 2014.’’ 2015 7th International Conference on Cyber Conflict, NATO CCD COE Publications, Talinn.

K. Choi, C.S. Lee, & R. Cardigan. (2018). ‘’ Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS’’. International Journal of Cybersecurity Intelligence and Cybercrime, Volume 1, Issue 1, Pages 31-32.

Keleştemur, Atalay (2017). ‘’Dünyayı Yöneten Güç: Siber İstihbarat’’. Siber Güvenlik, Sayı 1, Sayfa 44.

Kabanov, Yury (2014). ‘’ Information (Cyber-) Security Discourses and Policies in the European Union and Russia: A Comparative Analysis.’’ Centre for German and European Studies (CGES), No:1, Sayfa 20-21.

Kaldor, Mary (2013). ‘’ In Defence of New Wars.’’ Stability, Cilt 2, Sayı 1, Sayfa 1-16.

Karagül, Soner, Muhammet Fatih Özkan (2015). ‘’Bilgi Teknolojileri ve Uluslararası İlişkilerde Fırsat-Tehdit Paradoksu’’. Bilgi Ekonomisi ve Yönetimi Dergisi, Cilt 10, Sayı 1, Sayfa 115-116.

Kari, Martti J. Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats Jyväskylä: University of Jyväskylä, 2019.

Kaypak, Şafak (2012). ‘’Güvenlikte Yeni Bir Boyut: Çevresel Güvenlik.’’ Ekonomik ve Sosyal Araştırmalar Dergisi, Cilt 8, Sayı 8, Sayfa 11.

Kello, Lucas (2013). ‘’The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.’’ International Security, Vol: 38, No: 2, Page 19.

Kontselidze, Achiko (2015). ‘’Cyberterrorism- When Technology Became A Weapon.’’ European Scientific Journal, Volume Special, pp 26.

Korhan, Sevda (Güz 2017). ‘’Siber Uzayda Aktör-Güç İlişkisi.’’ Siber Politikalar Dergisi, Cilt 2, Sayı 4, Sayfa 83-84.

Kurnaz, İbrahim (2016). ‘’Siber Güvenlik ve İlintili Kavramsal Çerçeve.’’ Siber Politikalar Dergisi, Cilt 1, Sayı 1, Sayfa 63.

Küçüksolak, Övgü Kalkan (2012). ‘’Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Okulu Çerçevesinde Tartışılması.’’ Turan Stratejik Araştırmalar Merkezi Dergisi, Cilt 4, Sayı 14, Sayfa 204-206.

Lewis, James Andrew (2016). ‘’ Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States.’’ Institutional Capacity of the State Division, Discussion Paper, No: IDB-DP-457.

McDonald, Matt (2008). ‘’Securitization and the Construction of Security.’’ European Journal of International Relations, Volume 14, Issue 4, pp. 563-587.

Miş, Nebi (2011). ‘’Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi.’’ Akademik İncelemeler Dergisi, Cilt 6, Sayı 2, Sayfa 348.

Mueller, Robert S. (2019). Report on Investigation Into Russian Interference in the 2016 Presidential Election. Washington DC: Department of Justice. 28 C.F.R. § 600,8(c).

Niekerk, Van Brett, Trishana Ramluckan, Petrus Duvenage (2019). ‘’An Analysis of Selected Cyber Intelligence Texts’’. 18th European Conference on Cyber Warfare and Security, Coimbra.

Önaçan, Mehmet Bilge Kağan, Hasan Atan (2016). ‘’Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği’’. Trakya University Journal of Engineering Sciences, Vol 17, No: 1, pp 14.

Önok, Murat (2013). “Avrupa Konseyi Siber Suç sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği.” Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 19, Sayı 2, Sayfa 1232-1236.

Özkan, Arda (2016). ‘’Güvenlik Paradigmasında Sınıraşan Bir Çevre Sorunsalı: Nükleer Zarar.’’ Alternatif Politika Dergisi, Cilt 8, Sayı 1, Sayfa 135-137.

Özman, M. Aydoğan (1964). ‘’Devletlerin Egemenliği ve Milletlerarası Teşekküller.’’ Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 21, Sayı 1, Sayfa 59.

Pernik, Permit (2018). ‘’The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine.’’ European Union Institute for Security Studies Chaillot Papers, No: 148, Sayfa 53-64.

Pooina, Ajeet Singh (2014). ‘’Cyber Crime: Challenges and its Classification.’’ International Journal of Emerging Trends of Technolgy in Computer Science, Volume 3, Issue 6, pp 119-120.

Raik, Kristi, Mika Aaltola, Jyrki Kallia ve Katri Pynnöniemi (2018). The Security Strategies of the US, China, Russia and the EU. Finnish Institue of International Affaris. 56.

Riglietti, Gianluca (2016). ‘’ Defining The Threat: What Cyber Terrorism Means Today and What it Could Mean Tomorrow.’’ The Business and Management Review, Volume 8, Number 3, Page 14.

Rose, Jonathan (2017). ‘’ Brexit, Trump, and Post-Truth Politics.’’ Public Integrity, Cilt 19, Sayı 6, Sayfa 555-558.

Rumer, Eugene (2019). ‘’ The Primakov (Not Gerasimov) Doctrine in Action.’’ CARNEGIE Endowment For International Peace, Sayı Haziran 2019, Sayfa 1-4.

Sancak, Kadir (2013). ‘’Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü.’’ Karadeniz Teknik Üniversitesi Sosyal Bilimler Dergisi, Sayı 6, Sayfa 125.

Sayın, Yusuf, Ahmet Usanmaz, Fırat Aslangiri (2016). ‘’Uluslararası Göç Olgusu ve Yol Açtığı Etkiler: Suriye Göçü Örneği.’’ KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi, Cilt 18, Sayı 31, Sayfa 2.

Savaş, Serkan, Nurettin Topaloğlu (2015). ‘’Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri’’. VIII. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. Ankara.

Seren, Merve (Aralık 2016). ‘’ Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık.’’ Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı, Sayı 183, Sayfa 9.

Schaap, Arie J. (2009). "Cyber Warfare Operations: Development and Use Under International Law." Air Force Law Review, Cilt 64, Sayfa 139-141.

Sismondo, Sergio (2017). ‘’Post-Truth?.’’ Social Studies of Science, Cilt 47, Sayı 1, Sayfa 3-6.

Soldatov Andrei, Irina Borogan (2018). Hacks, Leaks and Disruptions: Russian Cyber Strategies, European Union Institute for Security Studies Chaillot Papers, No: 148, Sayfa 16.

Tarhan, Kamil (2017). ‘’Siber Uzayda Realist Teorinin Değerlendirilmesi.’’ Siber Politikalar Dergisi, Cilt 2, Sayı 3, Sayfa 101.

Tarhan, Kamil (2017). ‘’Siber Uzayda Realist Teorinin Değerlendirilmesi.’’ Siber Politikalar Dergisi, Cilt 2, Sayı 3, Sayfa 109.

Thomas, Timothy L. (2001). ‘’Information Security Thinking: A Comparison of U.S, Russian and Chinese Concepts.’’ The Science and Culture Series — Nuclear Strategy and Peace Technology, AIDS and Infectious Diseases, Sayfa 341-358.

Tırrell, William K. (2012). United States Cyber Security Strategy, Policy and Organization: Poorly Postured To Cope With A Post 9/11 Security Environment? Master These, The George Washington Universty, Military Art and Science, Kansas.

Tok, Gül Ceylan (2009). ‘’The Securitization of the Headscarf Issue in Turkey: ‘The Good and Bad Daughters’ of the Republic.’’ Annual Review of International Studies, Cilt 8, Sayfa 113-137.

Tsakanyan, V.T. (2017). ‘’The Role of Cyber Security in World Politics.’’ Vestnik Rudn. International Relations, Cilt 17, Sayı 2, Sayfa 342-343.

Türk Dil Kurumu (1998). Türkçe Sözlük, Cilt:1, Türk Tarih Kurumu Basımevi, Ankara, 1998, s. 1107.

Türkan-İpek, Işıl Zeynep (2018). ‘’Risk Toplumunda Seçimler.’’ Sosyoekonomi, Cilt 26, Sayı 36, Sayfa 65-79.

Uğrasız, Bülent (2003). ‘’Uluslararası İlişkilerde İki Farklı Yaklaşım: İdealizm ve Realizm.’’ Dokuz Eylül Üniversitesi Sosyal Bilimler Dergisi, Cilt 5, Sayı 2, Sayfa 143-144.

Ünver, Mustafa, Cafer Canbay (2010). ‘’Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik’’. Elektrik Mühendisliği Dergisi, Sayı 458, Sayfa 94.

Ünver, Akın (2019). ‘’Russian Digital Media and Information Ecosystem in Turkey.’’ Center for Economics and Foreign Policy Studies [EDAM], Cyber Governance and Digital Democracy 2019/1, Sayfa 4.

Van Epps, Geoff (2013). ‘’US and NATO Engagement With Russia in the Cyber Domain.’’ Connections, Cilt 12, Sayı 4, Sayfa (35-38).

Vanlıoğlu, Muhammet (2018). ‘’Siber Propaganda ve Dezenformasyon: Kitle Kaynaklı Troll Birimleri.’’ Uluslararası Kriz ve Siyaset Araştırmaları Dergisi, Cilt 2, Sayı 1, Sayfa 208.

Varlık, Ali Bilgin (2013). ‘’Savaşı Tanımlamak: Terminolojik Bir Yaklaşım.’’ Avrasya Terim Dergisi, Cilt 1, Sayı 2, Sayfa 128.

Vural, Çağla (2018). ‘’Çevresel Güvenliğin Gelişimi.’’ Ankara Üniversitesi Çevre Bilimleri Dergisi, Cilt 6, Sayı 1, Sayfa 32-35.

Yalçınkaya, Haldun (2019). "Savaşın Değişimi ve Kuramsal Tartışmalar", Güvenlik Yazıları Serisi, No.46, Sayfa 1-7.

Yayla, Mehmet (2013). ''Hukuki Bir Terim Olarak Siber Savaş.'' Türkiye Barolar Birliği Dergisi, Sayı 104, Sayfa 180.

Yayla, Mehmet (2014). ''Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı.'' Hacettepe Hukuk Fakültesi Dergisi, Cilt 4, Sayı 2, Sayfa 191-195.

Yılmaz, Birkan Anıl (2020). ''Siber Terörizm ve Değişen İstihbarat Anlayışı.'' Anadolu Strateji Dergisi, Cilt 2, Sayı 1, Sayfa 70-72.

Yılmaz, Ceren (2017). ''Siber Güvenlik ve İnsan Hakları.'' Siber Politikalar Dergisi, Cilt 2, Sayı 3, Sayfa 87-89.

Yılmaz, Ercan Nurcan, Halil İbrahim Ulus, Serkan Gönen (2015). ''Bilgi Toplumuna Geçiş ve Siber Güvenlik''. Bilişim Teknolojileri Dergisi, Cilt 8, Sayı 3, Sayfa 134.

Yılmaz, Onur (2017). ''Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik.'' Cyber Politik Journal, Volume 2, Number 4, pp. 23-27.

Yılmaz, Seda, Şeref Sağıroğlu (2013). '' Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri''. [Bildiri]. 6. International Information Security & Cryptology Conference, Ankara.

Waewer, Ola (Yaz 2008). ''Toplumsal Güvenliğin Değişen Gündemi.'' Uluslararası İlişkiler Dergisi, Cilt 5, Sayı 18, Sayfa 155.

Wall, D.S. (2008). ''Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime', International Review of Law, Computers and Technology.'' Cilt 22, Sayı1-2, Sayfa 45–63.

3. Elektronik Kaynaklar

Abrams, Abigail (18.04.2019). ''Here's What We Know So Far About Russia's 2016 Meddling.'' Time. https://time.com/5565991/russia-influence-2016-election/ /03.03.2020.

Administration of William J. Clinton (1998). Joint Statment on Common Security Challenges at the Threshold of the Twenty-First Century. https://www.govinfo.gov/content/pkg/WCPD-1998-09-07/pdf/WCPD-1998-09-07-Pg1696.pdf /07.02.2020.

Afanesyeva, Anna, Sergey Bogatyrev ve Natalia Wilke (2019). ‘’Information Technologies in Russia.’’ https://www.beiten-burkhardt.com/sites/default/files/downloads/Information%20Technologies%20in%20Russia.pdf /27.01.2020.

Ajir, Media, Shelby Haas ve Bethany Vailliant (2018). ‘’Russia Information Warfare & Implication for Deterrence Policy.’’ Sayfa 6-12. https://stratcomds.com/wp-content/uploads/2018/04/UNO-Team-Paper-Russian-Information-Warfare.pdf /04.02.2020.

Alexander, David (10.12.2016). ‘’ CIA Says Russia Intervened to Help Trump Win White House: Washington Post’’. Reuters. https://www.reuters.com/article/us-usa-election-cyber-russia/cia-says-russia-intervened-to-help-trump-win-white-house-washington-post-idUSKBN13Z02Q /20.02.2020.

Alsan, Altuğ (2016). ‘’Wikileaks Belgeleri: Trump-Rusya İlişkisi.’’ https://diplomatikgozlem.com/_haber/wikileaks-belgeleri-trump-rusya-iliskisi /07.03.2020.

Baldi, Stefano, Eduardo Gelbstein, Jovan Kurbalija (2013). ‘’Hacktivisim, Cyber-Terrorism and Cyberwar: The Activities of The Uncivil Society In Cyberspace’’. The Information Society Library. https://baldi.diplomacy.edu/italy/isl/Hacktivism.pdf

BBC News (18.04.2020). ‘’Mueller Raporu: ABD Adalet Bakanı Barr: Rusya’yla İşbirliğine ve Trump’ın Adaletin Tesisini Engellediğine Dair Kanıt Yok.’’ https://www.bbc.com/turkce/haberler-dunya-47976296 /14.03.2020.

BBC News (24.07.2019). ‘’Special Counsel: What is it and what did Robert Mueller Investigate?.’’ https://www.bbc.com/news/world-us-canada-39961732 /15.03.2020.

BBC News (11.04.2019). ‘’Julian Assange kimdir? Cesur Bir Aktivist mi, İnsanların Hayatını Tehlikeye Atan Bir İlgi Bağımlısı mı?.’’ https://www.bbc.com/turkce/haberler-dunya-39975457 /03.03.2020.

Brenner, W. Sussan (2010). ‘’Threat Morphing In Cyberspace.’’ https://www.e-ir.info/2010/03/08/threat-morphing-in-cyberspace-by-susan-w-brenner/ /08.02.2019.

Corporation for National and Community Service, Basic Principles for States of the Russian Federation the field of International Information Security to 2020 (2013). https://www.cncs.gov.pt/content/files/ru_state-policy_information_security.pdf /30.12.2019.

CNN (14.12.2019). ‘’2016 Presidential Election Investigation Fast Facts.’’ https://edition.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html /07.03.2020.

Council of Europe/Siber Suç Sözleşmesi (2012). ‘’Global Project on Cybercrime (2012): Article 15 – Conditions and Safeguards under the Budapest Convention on Cybercrime.https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa421 /03.03.2019.

Cyber Security Intelligence, Central Intelligence Agency (2020). https://www.cybersecurityintelligence.com/central-intelligence-agency-cia-397.html /20.05.2019.

Director of National Intelligence, Declassified Report (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 /10.03.2020.

Duygu, Nil (2015). Tuic Akademi. http://www.tuicakademi.org/uluslararasi-sistem-acisindan-guvenlik-ve-guvenlik-algisinda-yasanan-degismeler/ / 5.11.2018.

Doğru, Ahmet (2013). ‘’Uluslararası Hukukta Kuvvet Kullanma Hukuku, Siber Saldırılar ve Stuxnet Saldırısının Analizi.’’ Academa.edu. https://www.academia.edu/13197332/ULUSLARARASI_HUKUKTA_KUVVET_KULLANMA_HUKUKU_S%C4%B0BER_SALDIRILAR_VE_STUXNET_SALDIRISININ_ANAL%C4%B0Z%C4%B0 /07.02.2019.

Edwards, Charlie (2007). https://www.comw.org/qdr/fulltext/0711edwards.pdf /01.01.2019.

Eichensehr, Kristen (2014). ‘’The US Needs a New International Strategy for Cyberspace’’ Just Security. https://www.justsecurity.org/17729/time-u-s-international-strategy-cyberspace/ 22.03.2019.

Elliot, Colonel Joyce E (2002). ‘’Cyberterrorism: A Threat to National Security.’’ Strategy Research Project, file:///C:/Users/bilal/Downloads/441482.pdf 08.03.2019.

EWI’s Discussion Paper (2006). G8 Intiative for Public-Private Partnership to Counter Terrorism. https://www.files.ethz.ch/isn/90482/2006-11-28_G8-Initiative-for-PPPs.pdf /07.02.2020.

Fisher, Kate (2019). ‘’Russian Interference in the 2016 United States Presidential Election.’’https://repositories.lib.utexas.edu/bitstream/handle/2152/75445/Fisher_Thesis_Russian%20Interference%20in%20the%202016%20United%20States%20Presidential%20Election_2019.pdf?sequence=1 /30.02.2020.

Gady, Franz-Stefan ve Austin, Greg ‘’Russia, The United States. And Cyber Diplomacy: Opening The Doors’’. EastWest Institute (2010). https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf /15.01.2020.

Groš, Stjepan (2020). ‘’Research Directions in Cyber Threat Intelligence’’. https://arxiv.org/pdf/2001.06616.pdf /20.01.2020.

Gude, Pen (2017). ‘’Russia’s 5th Column’’. Center for American Progress. https://www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-column/ 02.03.2020.

Harding, Luke (16.11.2016). ‘’What We Know About Russia’s Interference in the US Election’’. The Guardian, https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election /07.02.2020.

House Permanent Select Committee on Intelligence (2018). ‘’Report on Russian Active Measures’’ https://docs.house.gov/meetings/IG/IG00/20180322/108023/HRPT-115-1_1-p1-U3.pdf /12.03.2020.

Independent (01.06.2017). ‘’ Vladimir Putin hints 'patriotic' private Russian hackers could have meddled in 2016 US Election.’’ https://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-russian-hackers-patriotic-private-us-election-2016-donald-trump-win-dnc-hillary-a7767436.html /17.03.2020.

Kaymak, Oktay (2017). ‘’Siber Harekâtlar ve Uluslararası Hukukta Meşru Müdafaa Hakkı.’’ https://www.ilimvemedeniyet.com/siber-harekatlar-ve-uluslararasi-hukukta-mesru-mudafaa-hakki.html /15.02.2019.

Kolasi, Klavis (2014). http://www.academia.edu/9587264/Ele%C5%9Ftirel_Teori_ve_G%C3%BCvenlik_Kimin_i%C3%A7in_G%C3%BCvenlik / (27.12.2018).

Lewis, James Andrew (2014). Center for Strategic & International Studies. https://www.csis.org/analysis/reference-note-russian-communications-surveillance /17.01.2020.

Le Gloannec, Anne-Marie, Bastian Irondelle, David Cadier (2013). https://spire.sciencespo.fr/hdl:/2441/2tb654p5g79rg9aejj1ah6job0/resources/tw-wp-13.pdf / 01.01.2019.

National Security Agency, Cybersecurity (2019). https://www.nsa.gov/What-We-Do/Cybersecurity/ 15.04.2019.

NATO, https://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_new-security-challenges-tu.pdf /10.02.2019.

NATO Cooperative Cyber Defence Centre of Excellence (2016). ‘’National Cyber Security Organization: United States.’’ https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf 12.04.2019.

New York Times (16.12.2016). ‘’Obama Says He Told Putin: ‘Cut it Out’ on Hacking.’’ https://www.nytimes.com/2016/12/16/us/politics/obama-putin-hacking-news-conference.html /14.03.2020.

Oğuz, Samet, Eyüp Burak Ceyhan, Şeref Sağıroğlu (2015). ‘’Teknolojinin Casuslukta Kullanılması ve Karşı Önlemler.’’

https://www.researchgate.net/publication/303999660_Teknolojinin_Casuslukta_Kullanilmasi_ve_Karsi_Onlemler / 12.04.2020.

Özgöker, Uğur, Serdar Yılmaz (2014). ‘’New Security Threads within The Context of Globalization: Cybercrimes’’. http://www.academia.edu/37805421/New_Security_Threads_within_the_context_of_Globalization_Cybercrimes1_U%C4%9Fur_%C3%96ZG%C3%96KER2_Serdar_YILMAZ3 / 02.01.2019.

Pande, Jeetendra (2017). ‘’Introduction to Cyber Security.’’ Uttarakhand Open University, Creative Commons Attribution-ShareAlike 4.0 International License. http://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf /05.03.2019.

Pike, John (1997). Military Intelligence Service (GRU) https://fas.org/irp/world/russia/gru/ops.htm /24.01.2020.

Powers, Sam (2013). ‘’The Threat of Cyberterrorizm to Critical Infrastructure.’’ E-International Relations Students, Sayfa 2. https://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/ 07.03.2019.

President of Russian Federation, Strategy for the Development of the Information Society in the Russian Federation for 2017-2030 (2017). http://publication.pravo.gov.ru/Document/View/0001201705100002 7.01.2020.

Russian Federation Foreign Intelligence Service, Powers. http://svr.gov.ru/svr_today/polnom.htm /23.01.2020.

Rogers, Megan (2018). ‘’Rethinking Warfare Concepts in the Study of Cyber War and Security.’’ https://www.e-ir.info/2018/12/01/rethinking-warfare-concepts-in-the-study-of-cyberwar-and-security/ /20.02.2019.

Seger, Alexander (March 2012). Global Project on Cybercrime: Cybercrime Strategies. https://rm.coe.int/16802fa3e1 /03.03.2019.

Sharikov, Pavel (01.11.2013). ‘’U.S-Russia Relations in the Sphere of Information Security’’. CARNEGIE. https://carnegieendowment.org/2013/11/01/u.s.-russia-relations-in-sphere-of-information-security-pub-63163 /12.02.2020.

Singer, Peter W. (2017). ‘’Is the Cyber Era New Cold War?’’ Röportaj. https://www.zocalopublicsquare.org/2017/03/29/cyber-era-new-cold-war/ideas/nexus/ / 16.02.2020.

Struglinski, Damian (2012). ‘’ How Serious is the Threat of Cyber Warfare.’’ https://www.e-ir.info/2012/05/22/how-serious-is-the-threat-of-cyber-warfare/ /30.02.2019.

The Departman of Defense, DoD Cyber Strategy (2015). https://archive.defense.gov/home/features/2015/0415_cyberstrategy/final_2015_dod_cyber_strategy_for_web.pdf /01.04.2019.

The Departman of Defense, Cyber Strategy (2018). https://media.defense.gov/2018/Sep/18/2002041658/1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF /05.04.2019.

The Goverment of The Russian Federation, Federal Service for Technical and Export Control. http://government.ru/en/department/96/ /17.01.2020.

The Government of the Russian Federation Regulation, Statue of Roskomnadzor. No. 228 of March 16, 2009. http://eng.rkn.gov.ru/about/ 27.01.2020.

The Guardian (30.12.2016). ‘’Obama Expels 35 Russian Diplomats in Retalation for US Election Hacking.’’ https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack /15.03.2020.

The Ministry of Foreign Affairs of the Russian Federation (2013). https://www.mid.ru/en/foreign_policy/official_documents / 12.12.2019.

The Ministry of Foreign Affairs of the Russian Federation, Doctrine of Information Security of the Russian Federation, (2016). https://toinformistoinfluence.com/2016/12/19/information-security-doctrine-of-the-russian-federation-6-december-2016/ 30.12.2019.

The Ministry of Foreign Affairs of the Russian Federation, Information Security Doctrine of Russian Federation (2000). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf 20.08.2019.

The Ministry of Foreign Affairs of the Russian Federation, National Security Concept of The Russian Federation (2000). https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768 /07.06.2019.

The Ministry of Foreign Affairs of the Russian Federation, National Security Concept of the Russian Federation (2015). http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf /6.01.2020.

The New York Times (22.03.2019). ‘’The Meaning of the Mueller Report.’’ https://www.nytimes.com/2019/03/22/opinion/mueller-report release.html?auth=login-google /12.03.2020.

The White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (2009). https://fas.org/irp/news/2009/05/cyber-fs.html / 21.03.2019.

The White House, International Strategy for Cybersecurity: Prosperity, Security, and Openness in a Networked World (2011). https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf /22.03.2019.

The White House (2013). Joint Statement on New Field of Cooperation in Confidence Building. https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0 /10.02.2020.

The White House, National Strategy to Secure Cyberspace (2003). https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf /20.03.2019.

The White House, National Security Strategy (2015). https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf /01.04.2019.

The White House, Presidency Of USA, Executive Order 13010-Critical Infrastructure Protection, https://www.hsdl.org/?abstract&did=1613 / 17.03.2019.

The White House, Presidential Decision Directive 63 on Critical Infrastructure Protection (1998). https://www.govinfo.gov/content/pkg/FR-1998-08-05/pdf/FR-1998-08-05.pdf /17.03.2019.

The White House, The National Strategy to Secure Cyberspace (2003). https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf /17.04.2019.

Turovsky, Daniil (2018). What is the GRU? Who gets recruited to be a spy? Why are they exposed so often?. https://meduza.io/en/feature/2018/11/06/what-is-the-gru-who-gets-recruited-to-be-a-spy-why-are-they-exposed-so-often 24.01.2020.

UN Organization, Deputy Director of New Threats and Challenges Department's Statement (2016). https://www.un.org/sc/ctc/wp-content/uploads/2016/12/Statement-by-DVF-on-special-joint-session-NY-Dec-2016.pdf 27.01.2020.

US CYBERCOMMAND, US Cyber Command History (2019). https://www.cybercom.mil/About/History/ 12.04.2019.

US Department of Homeland Security. (2015). ''National Strategy to Secure Cyberspace.'' https://www.dhs.gov/national-strategy-secure-cyberspace 14.01.2019.

Yangyue, Liu (2015). '' The Conceptual Underpinning of Cyber Security Studies.'' Massachusetts Institute of Technology (MIT), Research Paper, No: 2016-2, Pages 17-18. http://ssrn.com/abstract=2734336

Yılmaz, Seda, Şeref Sağıroğlu (2013). İscturkey.org https://www.iscturkey.org/assets/files/2016/03/2013-paper81.pdf /07.02.2019.

Zheng, Denise E. (2015). 2015 DOD Cyber Strategy. https://www.csis.org/analysis/2015-dod-cyber-strategy 03.04.2019.

Wearesocial.com. (2018). https://wearesocial.com/us/blog/2018/01/global-digital-report-2018 /30.01.2019.

Wiener, Norbert (1948). Cybernetics: Or Control and Communication in the Animal and The Machine. Cambridge: M.I.T. Press. https://en.oxforddictionaries.com/definition/cyber /10.01.2019.