ULUSLARARASI KIBRIS ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM-ÖĞRETİM VE ARAŞTIRMA ENSİTÜSÜ

Uluslararası İlişkiler Anabilim Dalı

SİBER GÜVENLİKTE ULUSLARARASI İŞBİRLİĞİ SORUNU

Uluslararası İlişkiler Yüksek Lisans Tezi

Burak DORUKOĞLU

Lefkoşa- 2019

ULUSLARARASI KIBRIS ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM-ÖĞRETİM VE ARAŞTIRMA ENSİTÜSÜ

Uluslararası İlişkiler Ana Bilim Dalı

SİBER GÜVENLİKTE ULUSLARARASI İŞBİRLİĞİ SORUNU

Uluslararası İlişkiler Yüksek Lisans Tezi

Burak DORUKOĞLU

Danışman

Yrd. Doç. Dr. Özker KOCADAL

Lefkoşa- 2019

ULUSLARARASI KIBRIS ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM-ÖĞRETİM VE ARAŞTIRMA ENSİTÜSÜ

TEZ ONAY SAYFASI

Uluslararası İlişkiler Anabilim Dalı'nda, 20153154 numaralı, Burak DORUKOĞLU'nun hazırladığı "Siber Güvenlikte Uluslararası İşbirliği Sorunu" konulu Yüksek Lisans tezi ile ilgili savunması yapılmış ve adayın çalışmasının başarılı olduğuna oybirliği ile karar verilmiştir.

Tez Savunma Günü: 23 Ocak 2019

Jüri üyeleri	**İmza**
1) Tez danışmanı Yrd. Doç. Dr. Özker KOCADAL	.....
2) Üye Yrd.Doç.Dr. Turan CAVLAN	.....
3) Üye Yrd.Doç.Dr. Sinan EVCAN	.....

Prof. Dr. Tahir ÇELİK

Enstitü Müdürü

BEYANNAME

Ad Soyad **:** Burak DORUKOĞLU

Tezin başlığı **:** Siber Güvenlikte Uluslararası İşbirliği Sorunu

Danışman **:** Yrd.Doç.Dr.Özker KOCADAL

Yıl **:** 2019

Yukarıda başlığı verilen ve tarafımca kaleme alınan bu tez çalışması içerisinde verilen tüm bilgilerin akademik kurallara ve etik davranışlara uygun olarak elde ettiğimi ve sunduğumu; bu çalışmaya özgün olmayan ve başka kaynaklardan aldığım bilgileri, akademik kuralların ve etik davranışların gerektirdiği şekilde, metinde ve kaynakçada eksiksiz olarak gösterdiğimi beyan ederim.

Bu tez çalışması; Uluslararası Kıbrıs Üniversitesi, Lisansüstü Eğitim, Öğretim ve Araştırma Enstitüsü tarafından saklanabilir ya da elektronik olarak sunulabilir.

Tarih: 23 Ocak 2019

İmza: _____

TEŞEKKÜR

Bu çalışmanın gerçekleştirilmesinde, çalışma konusunun belirlenmesinde ve çalışmanın hazırlanma sürecinin her aşamasında bilgilerini, tecrübelerini ve değerli zamanlarını esirgemeyerek bana her fırsatta yardımcı olan, güler yüzünü ve samimiyetini benden esirgemeyen, araştırmama vesile olan, katkı sağlayan, yönlendiren, yardım eden ve danışman hoca statüsünü hakkıyla yerine getiren Yrd. Doç. Dr.Özker KOCADAL'a, çalışmama ve eğitimime katkı sağlayan, desteklerini esirgemeyen, bilgi ve tecrübelerinden yararlandığım Sayın Hocalarım Doç. Dr. Ercan GÜNDOĞAN'a, Doç. Dr. Sertaç SONAN'a, Yrd. Doç. Dr. Nusret Sinan EVCAN'a, Yrd. Doç. Dr. Turan CAVLAN'a sonsuz teşekkürlerimi sunarım.

Beni bu günlere sevgi ve saygı kelimelerinin anlamlarını bilecek şekilde yetiştirerek getiren ve benden hiçbir zaman desteğini esirgemeyen kıymetli ailem başta olmak üzere, üç yıl boyunca değerli bilgilerini benimle paylaşan ve kullandığı her kelimenin hayatıma kattığı önemini asla unutmayacağım saygı değer manevi ablam ve hocam Yrd. Doç. Dr. Sevilay ATMACA'ya sonsuz teşekkürlerimi sunarım.

ABSTRACT

The global nature of the Internet and many security issues related to computer networks; considering the human dependence of internet technologies in daily life, business and state administration, today, cyber security is a global problem. Many states have faced the problem of creating military units with defense and offensive cyber capabilities. However, countries are making limited efforts in the diplomatic field to reduce the threat of cybercrime and promote cyber security around the world. In particular, many countries, particularly the USA, China, and Russia, the global powers of the twenty-first century, have recently faced each other because of cyberattack, hacking and espionage issues.

Cyber security has become one of the most important disciplines of the International Relations discipline and has become increasingly important. In recent years, the term "cyber" is one of the most common terms in the international security dictionary. The results of the survey and the public's response to the issue are that cyber threats are one of the critical threats on the international agenda, however, it shows that scientists have difficulty in addressing the effects of this framework and the potential theoretical perspectives to guide research. The study was conducted to seek an answer to the research question is ’’Is lnternational Cooperation Possible in Cyber Security?’’ The study uses a generalized analysis of the basics of both international and national interest perspective, the current views on this subject, past studies and approaches in the literature; it provides a conceptual perspective on the possibility of international cooperation in the cyber area and the development of a universal mechanism. The behavior of the existing actors in this field, the structure of cyber space, past events and the problems encountered by the states in the process of cooperation are analyzed and the work ends with the evaluation of the ethical situation in the field related to the conceptualization of norms.

Key words: *Cyber Security, Cooperation, Security Dilemma, EU, USA, China, Rusia.*

ÖZ

İnternetin küresel doğası ve bilgisayar ağlarıyla ilgili çok sayıda güvenlik sorunu; günlük yaşamda, iş dünyasında ve devlet yönetiminde internet teknolojilerine olan insan bağımlılığı göz önünde bulundurulduğunda, günümüzde siber güvenlik konusunun küresel bir sorun olduğunu ortaya koymaktadır. Birçok devlet, savunma ve saldırı siber yetenekleri olan askeri birimler oluşturma problemiyle karşı karşıya kalmıştır. Ancak, ülkeler siber suç tehdidini azaltmak ve dünya genelinde siber güvenliği teşvik etmek için diplomatik alanda sınırlı çaba göstermektedir. Özellikle, yirmi birinci yüzyılın küresel güçleri olan ABD, Çin, ve Rusya başta olmak üzere bir çok ülke son zamanlarda siber saldırı, hack ve casusluk sorunları yüzünden birbirleriyle karşı karşıya kalmışlardır.

Siber güvenlik, Uluslararası İlişkiler disiplininin en önemli ve çalışmaların giderek arttığı alanlarından biri haline gelmiştir. Son yıllarda "siber" terimi uluslararası güvenlik sözlüğünde en sık rastlanan terimlerden biridir. Anket sonuçları ve kamuoyunun konuya tepkisi, siber tehditlerin uluslararası gündemdeki kritik tehditlerden biri olduğunu, ancak bilim insanlarının bu çerçevenin etkilerini ve araştırmaları yönlendirecek potansiyel teorik bakış açılarını ciddi bir şekilde ele almakta zorlandıklarını göstermektedir. Çalışma, "Siber Güvenlikte Uluslararası İşbirliği Mümkün mü ?" araştırma sorusuna cevap aramak için yapılmıştır. Çalışma, hem uluslararası hem de ulusal çıkar perspektifi temellerinin genelleştirilmiş analizini, bu konudaki mevcut görüşleri, literatürde yer alan geçmiş çalışmaları ve yaklaşımları kullanarak; siber alanda uluslararası işbirliğinin ve evrensel bir mekanizma geliştirmenin olanaklılığı üzerine kavramsal olarak bir bakış açısı sunmaktadır. Bu alanda var olan aktörlerin davranışları, siber uzayın yapısı, geçmişte yaşanan olaylar ve devletlerin işbirliği yapma aşamasında karşılaştığı sorunlar analiz edilerek, normların kavramsallaştırılmasıyla ilgili alandaki etik durumun değerlendirilmesiyle çalışma sona ermektedir.

Anahtar Kelimeler: *Siber Güvenlik, İşbirliği, Güvenlik İkilemi, AB, ABD, Çin, Rusya.*

İÇİNDEKİLER

TEŞEKKÜR i
ABSTRACT ii
ÖZ iii
İÇİNDEKİLER iv
KISALTMALAR vii
TABLO LİSTESİ viii
ŞEKİLLER LİSTESİ ix
GİRİŞ 1
BÖLÜM 1 6
1.1 Uluslararası İlişkilerde Güvenlik Kavramı 6
1.2. GELENEKSEL GÜVENLİK ÇALIŞMALARI VE YAKLAŞIMLARI 8
1.2.1 Realizm ve Neorealizm Perspektifinde Güvenlik Anlayışı 8
1.2.2.Liberalizm ve Neoliberalizm Perspektifinde Güvenlik Anlayışı 10
1.2.1.Alternatif Teorik Yaklaşımlar ve Güvenlik Anlayışı 12
1.2.DEĞİŞEN GÜVENLİK KAVRAMI 17
1.3.1.Soğuk Savaş Döneminde Güvenlik Kavramı 17
1.3.2. Soğuk Savaş Sonrası Yeni Güvenlik Kavramları ve Konuları 19
1.4. SONUÇ 22
İKİNCİ BÖLÜM 23
SİBER GÜVENLİK KAVRAMI TARTIŞMALARI 23
2.1 SİBER GÜVENLİK 24
2.2. TEMEL SİBER GÜVENLİK KAVRAMLARI 25
2.2.1 Siber Uzay 25
2.2.2. Siber Saldırı 26
2.2.3. Siber Savunma 27
2.2.4. Siber Savaş 28
2.2.5. Siber Terörizm 28
2.2.6. Siber Casusluk 30
2.3. SİBER SALDIRI YÖNTEMLERİ 31
2.3.1.İnternet Servis Saldırıları 31
2.3.2 Kriptografik Saldırılar 32

2.3.3. Zamanlama Saldırıları 33
2.3.4.Trafik Analizi 33
2.3.5. Zararlı Yazılım Kullanımı 34
2.3.6. Yığın E-Posta Gönderme 35
2.3.7. İnternet Aracılığıyla Sosyal Mühendislik 35
2.4. ÜLKELER BAZINDA YAŞANMIŞ SİBER MÜCADELELER VE ULUSLARARASI İLİŞKİLERE ETKİLERİ. 37
2.4.1. İlk İnternet Savaşı: Çeçenistan- Rusya 37
2.4.2. ABD- Çin Arasında Yaşanan Siber Saldırılar 37
2.4.3. Körfez Savaşı 38
2.4.4. Estonya'ya Yapılan Siber Saldırılar 38
2.4.5. Suriye'ye Yapılan Siber Müdahale 40
2.4.6. Gürcistan'a Yapılan Siber Saldırılar 41
2.4.7. Stuxnet Solucan Virüsü 42
2.4.8. Shady RAT Olayı 44
2.4.9. Ukrayna'ya Yönelik Siber Saldırı 45
2.4.10.Rusya- Türkiye Siber Çatışmaları 47
2.5. SONUÇ 49
ÜÇÜNCÜ BÖLÜM 50
ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ 50
3.1. ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİNİN DEĞERLENDİRİLMESİ 50
3.1. AMERİKA BİRLEŞİK DEVLETLERİ 50
3.1.1. İlk Çalışmalar ve Strateji Belgeleri 50
3.1.2. Başkan Bill Clinton Dönemi 52
3.1.3. Başkan Barack Obama Dönemi 53
3.1.4. Süper Güç Perspektifinden; ABD- Çin Siber Rekabeti 56
3.2. ÇİN HALK CUMHURİYETİ 58
3.2.1. Doğu Asya'da Gelecek Dönemlerde Yaşanması Muhtemel Siber Çatışmalar 61
3.2.2. Bilgisayar Ağı Harekâtı Doktrini: "Wangdian Yitizhan" 61
3.2.3. "Yeşil Baraj Gençlik Eskortluk Projesi" (Green Dam Youth Escort) 62
3.2.4. Çin Casusluk Ünitesi (Unit 61398) 63
3.2.5. Altın Kalkan Projesi (Golden Shield Project) 65
3.3.RUSYA 66
3.3.1. Rusya'nın Siber Güvenlik Politikaları 66
3.3.2. Rusya'nın Enformasyon Savaşı Stratejileri 67

3.3.3. Gerasimov ve Hibrit Savaş Doktrini 68
3.3.4. Rusya'nın Siber Uzay Alanındaki Etkinliği 69
3.4. AVRUPA BİRLİĞİ 70
3.4.1. AB'de Siber Güvenlik ve Kritik Altyapı Kapsamındaki Gelişmeler 71
3.4.2. AB'nin Siber Güvenlik Stratejisi 72
3.4.3. Büyük Bir Siber Saldırı Durumunda AB Desteği 75
3.5. TÜRKİYE 76
3.5.1. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi 76
3.5.2. Türkiye'nin İlk Siber Güvenlik Strateji Belgesi 77
3.5.3. 2016-2019 Ulusal Siber Güvenlik Stratejisi 78
3.6. SONUÇ 80
BÖLÜM 4 81
SİBER UZAY'DA İŞBİRLİĞİ VE 81
ORTAK POLİTİKA ÜRETME SORUNU 81
4.1. ULUSLARARASI HUKUKUN VE SİBER NORMLARIN EKSİKLİĞİ 82
4.1.1. Yasal Çerçevelerin Geliştirilmesi 83
4.1.2. Siber Suçlar ve Siber Terörizm 85
4.1.3. Siber Saldırı Caydırıcılığının Zorluğu 87
4.2. ÜLKELER ARASINDA YAŞANAN GÜVENLİK İKİLEMİ 88
4.2.1. Siber Saldırıları Bir Devletin Gerçekleştirmesi veya Desteklemesi İhtimali 89
4.2.2. Siber Suçun Önlenmesi, Suçluların Araştırılmasına Yardım Edilmesi ve Suçluların İade Edilmesine Yönelik Çalışmaların Yetersizliği 90
4.2.3. Ortak Bir Tanımın Olmaması ve Mantıksal Çerçeve 92
4.3. Küresel Siyaset Açmazı: Ulusal Çıkarlar ve Egemenlik Hassasiyetlerin Yol Açtığı Dijital Altyapı Eksikliği 95
SONUÇ 99
KAYNAKÇA 106
ÖZGEÇMİŞ 122

KISALTMALAR

AB	**AVRUPA BİRLİĞİ**
ABD	**AMERİKA BİRLEŞİK DEVLETLERİ**
AET	**AVRUPA EKONOMİK TOPLULUĞU**
AGİT	**AVRUPA GÜVENLİK VE İŞBİRLİĞİ TEŞKİLATI**
ASEAN	**GÜNEYDOĞU ASYA ULUSLAR BİRLİĞİ**
AU	**AFRİKA BİRLİĞİ**
BM	**BİRLEŞMİŞ MİLLETLER**
BT	**BİLGİ TEKNOLOJİLERİ**
BTK	**BİLGİ TEKNOLOJİLERİ KURUMU**
CIA	**MERKEZİ İSTİHBARAT TEŞKİLATI (ABD)**
EC3	**AVRUPA SİBER SUÇ MERKEZİ**
EDA	**AVRUPA SAVUNMA AJANSI**
ENISA	**AVRUPA BİRLİĞİ AĞ VE BİLGİ GÜVENLİĞİ AJANSI**
EUROPOL	**AVRUPA POLİS TEŞKİLATI**
INTERPOL	**ULUSLARARASI KRİMİNAL POLİS TEŞKİLATI**
IP	**INTERNET PROTOCOL**
ITU	**ULUSLARARASI TELEKOMÜNİKASYON BİRLİĞİ**
KBRN	**KİMYASAL, BİYOLOJİK, RADYOAKTİF VE NÜKLEER**
NATO	**KUZEY ATLANTİK ANTLAŞMASI ÖRGÜTÜ**
NIS	**AĞ VE BİLGİ GÜVENLİĞİ**
OAS	**ORGANİZATİON OF AMERİCAN STATES**
OECD	**EKONOMİK KALKINMA VE İŞBİRLİĞİ ÖRGÜTÜ**
SCO	**ŞANGAY İŞBİRLİĞİ TEŞKİLATI**
SSCB	**SOVYET SOSYALİST CUMHURİYETLER BİRLİĞİ**
VPN	**VIRTUAL PRIVATE NETWORK**

TABLO LİSTESİ

Tablolar **Sayfa**

TABLO 1: Gücün Üç Türü …….12
TABLO 2: Geleneksel Terörizm ve Siber Terörizm Farkları …….29
TABLO 3: Birinci Seviye İnternet Zafiyetleri ve Temsili Saldırılar ……..32
TABLO 4: Stuxnet Virüs Solucanından Etkilenen Ülkeler ……43

ŞEKİLLER LİSTESİ

Şekiller **Sayfa**

ŞEKİL 1: Güvenliğin Katmanları 19
ŞEKİL 2: Beşinci Harekât Boyutu Olarak ‘Siber Uzay’ 25
ŞEKİL 3: Ülkeler Arasındaki Güvenlik Diyagramı..... 89
ŞEKİL 4: Politika Oluşturma ve Uygulama Diyagramı 94

GİRİŞ

İnternetin kullanılmaya başlandığı ilk dönemlerde kimlik doğrulama işlemlerinin ve normların geliştirilmesinin basit olduğu küçük bir topluluk olarak başlamasından itibaren büyük ölçüde bilgisayar uzmanlarının etki alanı olmuştur. Ancak, internetin toplumun tüm kesiminin kullanımına açılarak yaygınlaşması ve büyümesi her şeyi değiştirmiştir. İletişim yeteneklerinde görülen gelişim ile birlikte globalleşmenin bir neticesi olarak sosyal hayat ve küresel çevrede yaşanan çeşitlilik kapsamında bir dizi teknolojik gelişme gerçekleşmiştir. Önümüzdeki yıllarda gelinmesi muhtemel noktanın; her şeyin dijitalleştiği, uluslararası standartların ve protokollerin, insan yaşamının her alanına nüfuz ettiği bir e-dünya olacağı açıkça görülmektedir. Söz konusu yenilikler dâhilinde bilgi sistemleri ve ağları üzerinden üretilen zararlı yazılımlardaki artış; "siber güvenlik" ve "siber uzay" olarak nitelendirilen yeni terimlerin tartışılmasına neden olmuştur. Siber, sadece ticari ve sosyal faaliyetler için bir arena değil, aynı zamanda kültürel, siyasal, askeri, suç, hack ve terör ortamı da olmuştur.

Hükümetler, özel şirketler ve devlet dışı aktörler, kaynaklarını ve faaliyetlerini siber ortamda güvence altına almak için vazgeçilmez yetenekler geliştirmek için çaba sarf etmektedirler. Dış politika yapıcılar ve Uluslararası İlişkiler uzmanları, geleneksel güvenlik sorunlarından farklı olan siber alanın teknolojik ve yapısal özelliklerini anlamakta zorlanmaktadırlar. Onların arasında, siber tehditlerin potansiyel büyüklüğünü anlamanın anahtarı, internetin karmaşık bir ağ olması karakteridir. Siber tehditler, sivil ve askeri alanlar, devlet dışı ve devlet aktörleri ve hatta insan ve insan olmayan aktörler arasındaki farkları giderek daha fazla bulanıklaştırmasının yanı sıra, sürekli olarak gelişmektedir.

Siber güvenliğin, çeşitli açılardan uluslararası ilişkiler için büyük bir endişe kaynağı olduğu değerlendirilmektedir. Bilgisayar korsanlığı teknolojilerinin hızla yayılması sonucunda, birçok ülke ve uluslararası kuruluş, güvenlik önlemlerinin alınması ve fiziksel askeri güçler kadar yıkıcı olabilecek siber tehditlerin önlenmesi için çok taraflı işbirliğinin artırılmasına daha fazla odaklanmaktadır. Örneğin, İnternet yönetimi için siber güvenliğin tartışmalı alt alanlardan biri olduğu küresel bir çerçeve inşa etmek için çaba sarf etmektedirler; ancak henüz bu konuda fikir

birliğinin net olarak sağlandığı bir çerçeve oluşturulamamıştır. Özellikle, yirmi birinci yüzyılın küresel güçleri olan ABD, Çin ve Rusya başta olmak üzere birçok ülke son zamanlarda siber saldırı ve casusluk sorunları yüzünden birbirleriyle karşı karşıya kalmışlardır. Uluslararası ilişkilerde siber güvenlik konusu giderek önem kazanmakta ve devletlerin ilişkilerinde her iki taraftaki tehdit algılarını ciddi şekilde etkilemektedir.

Gelişmiş devletler, siber uzayda da etkin olma yarışı içerisine girmişlerdir. ABD, Çin ve Rusya başta olmak üzere bu alanda diğerlerinden önde ilerleyen devletler, yıllardan beri ürettikleri donanım, yazılım ve ağ teknolojilerini kullanarak casusluk imkânlarını ve askeri kapasitelerini maksimize etmek amacıyla planlamalar yapmaktadırlar. Ayrıca, bahse konu devletlerin, ülkelerinin siber güvenliğini tesis etmek amacıyla doktrinler ve stratejiler geliştirerek siber uzayı domine ettikleri görülmektedir.

Günümüzde yalnızca yüksek teknolojilere sahip devletler değil, gelişmekte olan ülkeler de siber uzay ve siber güvenlik konularında kapasite oluşturmaya yönelik ciddi çalışmalar gerçekleştirmektedirler. Bu bağlamda, Kuzey Kore'de "Unit 121" (Ünite 121) ismi verilen casusluk faaliyetleri başta olmak üzere, siber çatışmalara ve gerçekleşmesi muhtemel siber savaşlara karşı potansiyel güç oluşturmaya çalışan bir unsurunun olduğu bilinmektedir. (TRAC, 2018) Ayrıca siber alanda etkin olmaya çabalayan bir diğer ülke ise Hindistan'dır. Pakistan'la yaşadığı nükleer silah krizi ve Keşmir sorunu kapsamında Hindistan, 1999 yılından itibaren siber uzayı içerisine alan yeni güvenlik doktrinleri oluşturmaya ve siber güvenlik stratejileri benimsemeye başlamıştır. Hindistan, psikolojik operasyon, enformasyon harbi, elektro-manyetik dalga teknolojileri ve siber güvenlik alanında kapsamlı yapılara sahip alt birimler oluşturmuştur. Bunlarla birlikte, İran'da, Hindistan, Çin ve Rusya ile bilgi teknolojileri ve askeri alanda teknik destek ve eğitim alma, bilgi alışverişinde bulunma konularında ciddi işbirliği gerçekleştirerek siber güvenlik alanında önemli bir aktör konumuna erişmiştir (Kakar, 2018).

Siber tehdidin uluslararası doğası, devletlerin ve çeşitli uluslararası kuruluşların artan mücadeleyle en iyi şekilde nasıl başa çıkabileceği üzerine çalışmalar ortaya koyması gerekliliğini oluşturmuştur. Zira uluslararası örgütlere

örnek olarak NATO, bir siber saldırının 5. madde tehdidi olarak görülmesi gerekip gerekmediğini tanımlamakta zorlanmıştır ve siber güvenliğin yeni gerçekliğini yansıtmak için anlaşmaların güncellenmesi gerektiğini savunmuştur. Söz konusu gelişmeler ülkeler arasında uygulanabilir olumlu davranışlarla ve antlaşmalarla "Siber Güvenlikte İşbirliğini Sağlamak Mümkün mü?" sorusunu akla getirmektedir.

Bu araştırmada, Siyaset Bilimi ve Uluslararası İlişkiler alanındaki alan yazınından hareketle, siber güvenlikte uluslararası arenada işbirliği kapasitesi oluşturma çalışmalarının arka planında yaşanan zorluklar ve nedenleri incelenmiştir. Siber uzayda ortak politika üretme sorunu kapsamında, siber suçların önlenmesi, suçluların araştırılmasına yardım edilmesi ve suçluların iade edilmesine yönelik çalışmaların yetersizliği, siber saldırıları devletlerin destekleme veya gerçekleştirme ihtimalleri, siber caydırıcılığın zorluğu ve küresel siyaset açmazı bağlamında, ulusal çıkarlar ve egemenlik hassasiyetlerinin yol açtığı dijital altyapı eksiklikleri nedeniyle işbirliğini arttırmanın önündeki mevcut engeller ayrıntılı bilgilerle sunulmuştur.

Bu çalışmada ayrıca uluslararası ilişkiler alanında siber güvenlik konusu ele alınırken siber tehdit dâhil olmak üzere çok çeşitli konular incelenerek multidisipliner bakış ve değerlendirmeler yapılmıştır. Ulusal ve uluslararası yasal ikilemler, yönetişim sorunları, siber alan için rollerin ve sorumlulukların belirlenmesi, siber alanın militarizasyonu ve acil siber güvenlik tartışmalarına odaklanarak, hedefe cevap veren bir politika ve yasal mimarisinin oluşturulmasını desteklemek amaçlanmıştır. Siber alanın kendine özgü zorlukları ve geleceğe dönük yaklaşımlarıyla, farkındalık yaratmak ve konu hakkında geniş bilgiye sahip olmak için gerekli olan eleştirel düşünceyi oluşturmaya katkı sağlamaya çalışılmıştır.

Tarihi dökümanlar başta olmak üzere özellikle güncel dökümanlar kullanılarak tasarlanan bu çalışma, "güvenlik" ve "siber uzay" konuları ile sınırlıdır. Kuramsal perspektiften ise, 1950'lerde Neorealist teorisyen John Herz tarafından literatüre kazandırılan "*güvenlik ikilemi"* teorisi ile sınırlıdır. Bu çalışmada "tarihi araştırmalar tekniği" ve "tarama modeli" kullanılarak mevcut konuyla ilgili geçmişte olanlar da aktarılmıştır. Ayrıca çalışmada verilerin toplanması ve birleştirilmesi aşamasında, ilgili konular hakkında yazılmış yerli ve yabancı kitaplar ve makaleler taranarak, özellikle konunun yakın tarihi kapsayan bir konu olması nedeniyle elektronik ortamda bulunan haber, bilgi, makale, rapor ve güncel uluslararası web

sitesi yayınları (e-kaynaklar) da büyük ölçüde kullanılarak neden-sonuç ilişkisi çerçevesinde araştırma sorusuna cevap aranmıştır.

Çalışmanın birinci bölümünde, siber ortamda meydana gelen gelişmelerin neticesinde uluslararası ilişkilerde değişen güvenlik kavramının, öncelikli olarak disiplinde mevcut olan geleneksel perspektifteki realizm ve liberalizm açısından tanım ve temel anlamlandırmalarına yer verilecektir. Müteakiben, Alternatif Yaklaşımlar olarak da tanımlanan Eleştirel/Düşünümsel teorik yaklaşımların ve paradigmaların güvenliğin aktörleri ve boyutları çerçevesindeki katkıları incelenecektir. Daha sonra Soğuk Savaş sonrasında büyük bir evrim geçiren güvenlik kavramının yeniden tanımlanması ve biçimlendirilmesi sürecinde belirtilen yeni güvenlik sorunları ele alınarak, bunlardan son zamanlarda çokça kullanılan ve irdelenen siber güvenlik konusunun geldiği nihai noktanın anlaşılmasına ve farkındalık oluşturmaya katkıda bulunulmaya çalışılacaktır. Zira Uluslararası İlişkileri şekillendirdiği iddaa edilen realizm yaklaşımıyla askeri güce önem verilerek, onun dışında kalan tüm tehditler dikkate alınmamıştır. Her ne kadar konstrüktivizm, postmodernizm, eleştirel kuram ve alternatif yaklaşımlar gibi yaklaşımlar söz konusu anlayışı yıkmaya çalışsalar dahi hala askeri gücün disiplin içerisindeki başat konumunu koruduğu görülmektedir. Ancak, siber uzay kavramının ortaya çıkması sonucunda günümüzde ve gelecek zamanda da askeri alanın yanında devletler için siber güvenliğin de çok büyük önem arz edeceği yadsınamayacak bir gerçektir.

Çalışmanın ikinci bölümünde, siber güvenliği ve siber uzayı oluşturan unsurları tanımak ve analiz etmek amacıyla, siber saldırı, siber savunma, siber savaş, siber terörizm, siber casusluk kavramlarının oluşumu aktarılmıştır. Daha sonra, siber saldırı tekniklerinden en yaygın olanlarından bazıları irdelenerek saldırıların arka planında yaşanan gelişmeler ve günlük hayatta karşılaşılan örnekler aktarılmaya çalışılmıştır. Son olarak bu bölümde siber güvenliğin önemini vurgulamak amacıyla geçmiş de yaşanan siber çatışmalar ve saldırı olayları kronolojik çerçevede arz edilerek, devletlerin mevcut uluslararası sistemdeki baş aktör rolünü pekiştirmekte olduğu, ülkelerin siber alandaki teknolojileri askeri güçlerini geliştirmek amacıyla fırsat olarak kullandıkları ve siber ortamın anonim yapısının tehdit anlayışını asimetrik boyutlara taşıması bakımından uluslararası sistemi geçmişe göre daha

anarşik bir yapıya çevirdiği şeklindeki hipotezler analiz edilmiştir.

Çalışmanın üçüncü bölümünde uluslararası söz konusu etkileşimi analiz etmek amacıyla ABD, Çin, AB ve Türkiye'nin siber güvenlik stratejileri kronolojik biçimde analiz edilmeye çalışılmıştır. ABD'nin Soğuk Savaş döneminde Rusya ile girdiği askeri rekabet bağlamında geliştirdiği teknolojik imkânlar sayesinde sahip olduğu siber uzay araçları ve ABD'nin 1990'lı yılların sonlarına doğru ortaya koyduğu siber güvenlik stratejileri, başkanlık direktifleri ile birlikte değerlendirilmiştir. ABD'nin en büyük rakibi olarak görülen Çin Halk Cumhuriyeti'nin siber konsepti ve strateji planları ve "Süper Güç Perspektifinden; ABD-Çin Siber Rekabeti" de bu bölümde incelenmiştir. Uluslararası siber işbirliğine bakış açısı sunması bakımından bölgesel işbirliği olan, AB'nin siber güvenlik politikaları, bildirileri ve yayınlanan raporları çerçevesinde açıklanarak sunulmuştur. Bu kısımda ''AB'nin Siber Güvenlik Belgesi'' ana kaynağı oluşturmaktadır. Son olarak gelişmekte olan ülkeleri anlamak amacıyla, Türkiye'nin ulusal siber güvenlik konsepti analiz edilmiştir.

Çalışmanın dördüncü bölümünde ise, giderek daha yaygın, karmaşık ve zarar verici hale gelen siber tehditler ve saldırılar kapsamında, gelişen karmaşık tehdit ortamı ile karşı karşıya kalan uluslararası sistemin, ülkelerin toplu savunma, kriz yönetimi ve işbirliğine yönelik temel görevlerini yerine getirmek de yetersiz kalması hususunun nedenleri analiz edilmiştir. Günümüzde devletlerin, uluslararası arenada siber güvenliğin tesis edilmesine yönelik ortak bir anlayış ve yaklaşım oluşturamadığı görülmektedir. Bu kapsamda siber tehditlerin devlet sınırlarına ve örgütsel sınırlara meydan okuması sebebiyle, uluslararası güvenliği arttırmak için tüm ülkeler ve ilgili kuruluşların işbirliğini arttırması ve ortak mekanizmalar geliştirmesinin önemi tartışılarak, "**Siber Güvenlikte Uluslararası İşbirliği Mümkün mü?**" araştırma sorusuna cevap aranmıştır. Siber uzayda yaşanan bu belirsizliklere ilişkin bazı nedenler ve kaygılar bulunmaktadır. Bunlar arasında temel olanların, uluslararası hukukun yetersizliği, kritik altyapıların zayıflığı, atıfta bulunma zorluğu, savunma suçu avantajı, bilgi sistemlerinin zayıf giriş engelleri, uluslararası normların eksikliği ve kıtalararası açıklıklar nedeniyle uluslararası sınırları geçme kolaylığı olduğu değerlendirilmektedir. Bu nedenle, bu faktörler bir araya geldiğinde, politika yapıcılar ve araştırmacılar için siber çatışmanın diğer

alanlardaki çatışmalardan çok daha istikrarsız olması nedeniyle uluslararası işbirliğinin zorlukları açıklanmaya çalışılmıştır. Çalışma sonucunda siber uzayın doğası gereği, hâlihazırda ülkeler arasında yaşanan güvenlik ikilemi, rekabet ve çatışma ortamında gerekli işbirliği ve ortak politika üretiminin gerçekleştirilemediği ve işbirliği kapasitesinin arttırılmasının ülkelerin mevcut yaklaşımlarıyla mümkün olmayacağı cevabına ulaşılmıştır. Diğer taraftan sonuç bölümünde ise, "işbirliği" hususunda yapılan araştırma ve analizler sonucunda geleceğe yönelik çözümler üretmek amacıyla alternatif bir dizi çıkarımlar ve yaklaşımlarda bulunularak elde edilen bulgulara yer verilmiştir.

BÖLÜM 1

DEĞİŞEN GÜVENLİK KAVRAMI VE SİBER GÜVENLİK

Bu bölümde, güvenlik kavramı, kavramsal ve kuramsal anlamda irdelenerek, geleneksel güvenlik çalışmaları, realizm, liberalizm ve modern yaklaşımlar perspektifinden değerlendirilecektir. Soğuk Savaş ve sonrasındaki güvenlik konuları ile birlikte güvenlik aktörlerini de inceleyip güvenlik anlayışında gerçekleşen değişimler gösterilmeye çalışılacaktır.

1.1 Uluslararası İlişkilerde Güvenlik Kavramı

Güvenlik kelimesinin uluslararası alandaki İngilizce karşılığı ‘’security’ kelimesidir. Latin dilinde bulunan ‘securus’ kelimesinden türeyen söz konusu kelime, üzüntüden ve kaygıdan emin olma, tehlikeden korunmuş olma ve emniyetli durumda bulunma gibi anlamlara gelmektedir. Arnord Wolfer'e göre "elde edilen değerlere karşı tehdidin yok olduğu durum" olarak tanımlanmıştır. Kelimenin literatürde kullanımına 1432 yılından itibaren başlanmıştır (Glare, 2005). 17'nci yüzyılda ise merkantalizm akımı etkili olmuştur. İngiliz felsefeci Thomas Hobbes, güvenliği modern devletin merkezine yerleştirerek söz konusu kavrama yeni bir anlam yüklemiştir. Hobes'un bu teorisinin temelinde o yıllarda Avrupa'da ve İngiltere'de yaşanan iç savaşların etkisinin olduğu değerlendirilmektedir (M. Arends ve J. Frederik, 2009:6).

İkinci Dünya Savaşı sonrasında ise ABD eski başkanı Truman döneminde "Ulusal Güvenlik" (18 Ekim 1947) yasasının çıkarılması neticesinde "Ulusal Güvenlik" kavramı literatüre kazandırılmıştır. Bu kapsamda Ulusal Güvenlik salt

bir kavram olmaktan çok bir tartışma ve politika konusu olmuştur ve gelecek dönemde "ulusal güvenlik politikaları" tartışılmaya ve belirlenmeye başlamıştır. Neyin ya da kimin çıkarları? Sorularına verilen yanıtlar ulusal güvenlik konusunda genel yaklaşımları ve temel referansları oluşturmaktadır.

Güvenlik kavramı uluslararası ilişkiler disiplininde en fazla kullanılan kavramlardan biri olmaktadır. Bu nedenle tartışma konusu olarak önemli bir kavram olduğu değerlendirilmektedir. Realizm, uluslararası güvenlikte "gerçek"leri, devleti ve askeri gücü merkeze alarak tarafsız bir metodolojiyle analiz ettiği iddiasında bulunmaktadır. Wight ve Patomaki'ye göre, konu güvenlik kavramı olması sebebiyle büyük ölçüde klasik realizm ve neorealizm teorisyenlerinin varsayımları doğrultusunda şekillendirilmiştir. Fakat realizm ve neorealizm iddia ettikleri varsayımlarla hâlihazırda güvenlik haritasını gerçekçi yansıtmaktan uzaktır (Wight ve Patomaki, 2000:218).

Krause ve Williams'e göre,[1] geleneksel güvenlik çalışmalarında yapılan ana varsayımlar, devletlerin kendilerini güç politikasını esas alarak temel aktör olarak kabul etmesi ve uluslararası ilişkilerde çözülmesi gereken temel problemin devletler arası savaş olduğu düşüncesi üzerine oluşmaktadır. Bu kapsamda klasik güvenlik çalışmalarının, politik olarak askeri güç kullanımını ve kontrolünü inceleyen bir alan olduğu değerlendirilmektedir. 1980'lerde realizm/neorealizm'in tüm boyutlarının eleştiriye maruz kalması ve bazı teorisyenler tarafından askeri gücü esas alma mantığının bir yansıması olarak görülen Realist/ Neorealist güvenlik bakış açısının güvensizliğin zeminini hazırladığı iddia edilmiştir (Williams ve Krause, 1997). Bunun sonucunda güvenlik kavramını yeniden inceleyen yeni yaklaşımlar oluşmaya başlamıştır. Söz konusu yaklaşımlar güvenlik ve devlet kavramlarını ve aralarındaki bağlantıyı temel almak yerine bunları sorgulamıştır. Güvenlik çalışmalarında farklı sorular, cevaplar ve beklentiler oluşmaya başlamıştır.

Güvenlik konusunun daha net bir biçimde anlaşılması için incelenmesi

[1] Krause ve Williams'ın, klasik çalışmalara yaptıklara eleştirilerinin yer aldığı ''Eleştirel Güvenlik Çalışmaları'' isimli kitap klasik çalışmalar karşısında alternatif teorilerin gelişmesi adına önemli bir gelişme olmuştur (Akt: Şahin ve Şen, 2014:200).

gereken kavramlardan birisi de tehdittir. Tehdit kavramı güvenliğin zıt anlamlısı değildir. Fakat tehditler tam olarak tanımlanmadan güvenliğin tanımlanamayacağı ve söz konusu tehditlerin bertaraf edilmeden güvenli bir ortamın oluşturulamayacağı değerlendirilmektedir. Genelde ele alınan konu güvenlik değil güvensizlik algılamalarıdır. "kime karşı güvenlik?" veya "neye karşı güvenlik?" ve "ne kadar güvenlik?" sorularını cevaplamak ise hiçbir zaman basit olmamıştır ve söz konusu sorulara verilecek tek bir cevap da bulunmamaktadır. Bu nedenle, geçmişten günümüze güvenlik çalışmalarının sayısının artıp çeşitlenmesi öngörülebilmektedir.

1.2. GELENEKSEL GÜVENLİK ÇALIŞMALARI VE YAKLAŞIMLARI

1.2.1 Realizm ve Neorealizm Perspektifinde Güvenlik Anlayışı

Realist teorinin gelişmesinde önemli katkıları olan Niccolo Machiavelli, ulusların başlıca amaçlarını ve dış politikalarını tanımlarken, bir devletin güvenlik politikasının neler olduğunu da tanımlamıştır. Machiavelli mevcut uluslararası ortamda, devletlerin rekabet içinde olması sebebiyle ilişkilerinde çıkar çatışmasının hâkim olduğunu ve devletlerin birbirleri için birer tehdit durumunda olduğu görüşünü savunmuştur. Bu sebeple bir devletin mevcut varlığını muhafaza etmesi ve sürdürmesi için güçlü olması gerekmektedir (Dedeoğlu, 2008:38).

İngiliz filozof Thomas Hobbes'a göre insanlar doğası gereği bencildir. Güç ve iktidar hırsıyla hareket ederek kendi çıkarları peşinde koşmaktadırlar (Bull, 1981: 717). Hobbes'un görüşlerinden esinlenen Morgenthau, bu anarşi ortamından kurtulmanın tek çaresini, insanların kendini yönetme arzusundan vazgeçip bunu devlete devretmelerinde görmektedir. Devletlerinde bireylerden oluşan yapılar olmaları sebebiyle, çıkarlarına göre hareket ettiklerini ve güçlü olma çabası içinde olduklarını savunmaktadır (Dağı, 2013:73).

Realizm güvenlik kavramını ele alırken devleti baş aktör olarak görmektedir. Devlet yönetimine egemen olan ideoloji, devletin bekasının sağlanması üzerine kurulmuştur. Devletin bekasının sağlanması için en önemli araç güç unsurudur. Bu kapsamda devletlerin mevcut güç unsurları ve söz konusu güç unsurlarının uluslararası ilişkileri "güç mücadelesi'' üzerinden değerlendirilmektedir.

Realizm'e göre devletlerin güç unsurlarını belirleyen önemli faktörlerin başında askeri güç yer almaktadır. Coğrafi, jeopolitik, kültürel ve ekonomik unsurlar da önemli faktörler arasında bulunmaktadır. Uluslararası sistemi anarşik bir yapıya benzeten realizm devletlerin çıkar amaçlı davranışlarını sınırlandıran faktörün, söz konusu sistem içerisindeki diğer devletlerin güç kapasiteleri olduğunu değerlendirmektedir (Kalkan, 2012:203).

Klasik realizme göre devletler bekalarını sürdürmek zorunda oldukları uluslararası sistemde, güvenliklerini askeri güçlerini maksimize ederek gerçekleştireceklerini öngörmektedirler. Merkezi otoritenin olmadığı söz konusu ortamda çatışma ve rekabet meşrulaşmaktadır. Bu kapsamda uzun süreli kalıcı bir barıştan veya çatışma ortamından arınmış bir dünyadan söz etmek mümkün değildir (Baylis, 2008:72).

Neo-realist teorisyen Waltz, uluslar arasındaki etkileşimde güç dengesi kuramını insan doğasının bencilliği sebebiyle unsurların çıkar amaçlı etkileşimlerinden değil, mevcut sistemin anarşik yapısından kaynaklandığını savunur. Bu savına göre yapı, birimlerin etkileşimi sonucu ortaya çıkar ve beklenmeyen koşulları ifade eder. Neorealizm'in önemli temsilcilerinden Morgenthau, uluslararası ilişkileri "güç rekabeti" olarak tanımlamaktadır. Söz konusu güç elde etme mücadelesinde, devlet yöneticilerinin veya halkların ulaşmaya çalıştıkları hedefleri ne olursa olsun (özgürlük, refah, sosyal veya ekonomik idealler, güvenlik ya da gücün kendisi) içinde bulunulan politik ortamda bunları ancak güç ile elde edebilirler. Bu kapsamda güç, uluslararası ilişkilerde en temel amaçtır. Söz konusu güç ilişkilerinde güvenlik kavramı, "güvenlik ikilemi" olarak değerlendirilen yeni bir kavramın oluşmasına neden olmuştur. 1950'lerde Neorealist teorisyenlerden John Herz tarafından literatüre kazandırılan "*güvenlik ikilemi"* kavramı, devletlerin savunma amaçlı gerçekleştirdiği güvenlik önlemlerinin – gayri ihtiyari olarak- diğer devletlerin güvenliğini azalttığı durumları ifade etmektedir. Devletlerin birbirlerine olan güvensizlikleri doğrultusunda artan silahlanma neticesinde bir etki-tepki mekanizması oluşmaktadır. Bu mekanizma devletleri tehdit ve korku anlayışının giderek tırmandığı bir güvensizlik çıkmazına götürmektedir (Arı, 2014:184).

Bu kapsamda realistlerin yeni güvenlik konularını incelediğini söylemek

güçtür. Devlet en önemli ve başat aktör olarak değerlendirilmeye devam etmektedir. Söz konusu durumda güvenlik kavramı üzerine yapılan tanımlamalar dar kapsamda kalmaktadır. Devletin haricindeki aktörlerin askeri güç dengesine etki edebileceği anlayışı kabul görmemektedir. Güvenlik ikilemi ve anarşi kısır döngüsünün hüküm sürdüğü realizm odaklı uluslararası ortamda, işbirliği ve kalıcı barışın gerçekleştirilmesinin mümkün olmadığı değerlendirilmektedir.

1.2.2.Liberalizm ve Neoliberalizm Perspektifinde Güvenlik Anlayışı

Güvenlik tartışmalarının başlıca kaynaklarından bir diğeri de liberalizmdir. Liberalist teori insan merkezli güvenlik çalışmalarını temel almaktadır ve devletin dışında uluslararası kuruluşlar, sivil toplum örgütleri, çokuluslu şirketler ve bireyler gibi aktörleri de esas alarak incelemektedir. Jean Jack Rousseau, John Locke ve John Stuard Mill liberalizmin önemli düşünürleri arasında yer almaktadır (Birdişli, 2014:34). Literatürde bulunan çalışmaları incelediğimizde, liberalizmin kendi içinde farklı görüşlere ayrıldığı görülmektedir; ekonomik liberalizm, politik liberalizm sosyal liberalizm, muhafazakâr liberalizm, kültürel liberalizm bunlardan başlıcalarıdır.

Uluslararası ilişkiler analizlerinde önemli bir yer tutan güvenlik kavramını liberal siyaset felsefini temsil eden düşünürler de ele almıştır. Liberalizm kavramı uluslararası ilişkiler disiplinine, Birinci Dünya Savaşı sonrasında savaşın yıkıcı tarafının önlenmesi, uluslararası güvenlik ve barışın sağlanması çabaları sonucu kazandırılmıştır. Realizm ve liberalizm savunucuları arasında geleneksel bir anlaşmazlık söz konusudur. Realizm teorisi uluslararası ilişkilerin merkezine devleti yerleştirmiştir. Uluslararası sistemin bir çatışma ortamından oluştuğu varsayımı ile devletlerin farklı menfaatler elde etme çabaları sonucunda güç mücadelesi öncelikli güvenlik arayışlarına odaklanmıştırlar.

Liberalistler, realistlerden farklı olarak uluslararası ilişkilerde anarşi ve çatışma yerine işbirliği ve barış konuları üzerine yoğunlaşmaktadırlar. Liberalist teorisyenler uluslararası ilişkilerin gündeminin sadece güvenlik konularından ibaret olmadığı görüşünü savunurlar. Kant'a göre devletler, ebedi barışa ulaşmaları için siyasal ve ekonomik işbirliği içinde olmalıdırlar. Savaşarak ve askeri güç kullanarak diğer devletleri işgal etmenin sonucunda elde edilecek kısıtlı kazancın karşısında, toplu insan kayıplarının yaşandığı etik olmayan bir durum söz

konusudur. Liberalizm "mutlak kazanç" teorisini savunarak aktörlerin işbirliği yapmaları halinde, herkesin kazanç sağlayacağı görüşünü savunmaktadır (Caşın, 2007: 75).

Liberaller bireylerin özgürlüğünü diğer kavramların üstünde tutmakta ve ulusların bu özgürlüğü kısıtlamasına izin verilmemesi gerektiği görüşünü savunmaktadırlar. Devletler anarşi ortamında olsalar bile diğer devletlerle uzlaşma ve işbirliğinde bulunmayı öğrenmek zorundadırlar. Söz konusu süreç içerisinde devletler ekonomiden çevreye kadar pek çok konuda işbirliği yapmanın uzun dönem getirilerini inceleyerek bir değerlendirme yapmayı da öğrenmelidirler. Liberal anayasal bir devlet içsel olarak, vatandaşlarına karşı demokratik anlamda sorumludur. Devlet ekonomik piyasanın taleplerine saygı duymalı ve hukuk düzenine sahip olmalıdır. Liberaller söz konusu sınırları uluslararası düzeyde oluşturmak zor olsa da egemen devletlerin istikrar sağlayabilmesi için bunları oluşturması gerektiğine inanmaktadırlar (Griffiths, 2013:13). Smith'e göre, liberalizm aktörler arasındaki etkileşimde güç yerine rızayı temel alır ve sopa yerine havucu araç olarak kullanmayı tercih eder. Liberaller insan doğasını 'iyi' olarak değerlendirmektedir. Devletleri ve toplumları blok bir yapı olarak görmek yerine çoğul bir yapı olarak değerlendirmektedirler. Liberalizm de devlet odaklı güvenlik anlayışının aksine insan odaklı güvenlik anlayışına doğru bir değişiklik söz konusudur (M.Kauppi ve P. Viotti, 2016).

1980'lerin sonlarında SSCB'nin dağılmasıyla, liberal siyaset teorisine alternatif olarak neoliberalizm teorisi savunulmuştur. Teorinin en önemli kurucularından Robert Keohane ve Joseph Nye'nin argümanı, 'karşılıklı bağımlılık' kavramının realiteyi realizmden daha çok yansıttığı görüşüdür. Uluslararası örgütler ve uluslararası hukukun, ebedi barışın tesis edilmesinde etkili olabilecekleri, demokrasi, insan hak ve özgürlüklerinin korunması, serbest ticaret, kollektif güvenlik vb. konularına vurguda bulunarak dünya düzeyinde barışçıl ve işbirliği içinde bir yapının oluşturulabileceği görüşünü savunmaktadırlar (Arıboğan, 2007).

Nye, güç kavramını yumuşak güç ve sert güç olarak ikiye ayırmıştır. Bu iki farklı gücün birbiri ile yakın ilişki içerisinde olduğu ve birbirini sürekli beslediğini

değerlendirmektedir. Yumuşak gücü istenen sonuçlara varmak için başkasının üzerinde etki kurma (yaşam tarzı, siyasi ve demokratik normlar, kültürel ve evrensel değerler, vb.) sanatı olarak tanımlamıştır. Sert gücü ise askeri, ekonomik ve siyasi güç olarak tanımlamaktadır. Sert güçte caydırma, zorlama ve koruma davranışları görülürken yumuşak güçte hayranlık uyandırma ve gündem yaratma gibi davranışlar görülmektedir. Yumuşak güç sivil toplum örgütleri, medya, üniversiteler, finans ve iş dünyası gibi araçları kullanarak istenilen sonuçlara varma becerisi olarak tanımlanmaktadır. (Nye, 2005:75) Bu kapsamda Nye yeni güvenlik aktörlerinin önemini vurgulamıştır ve ulusal güvenlik kavramı ile ilişkilendirerek açıklamalarda bulunmuştur.

Tablo 1: Gücün Üç Türü

		Davranışlar	Temel Araçlar	Hükümet Politikaları
SERT GÜÇ	**Askeri Güç**	▪ Zorlama ▪ Caydırma ▪ Koruma	▪ Tehdit ▪ Kuvvet	▪ Zorlayıcı diplomasi ▪ Savaş ▪ İttifak
SERT GÜÇ	**Ekonomik Güç**	▪ Teşvik ▪ Zorlama	▪ Para verme ▪ Yatırım	▪ Yardım ▪ Rüşvet
	YUMUŞAK GÜÇ	▪ Hayranlık uyandırma ▪ Gündem yaratma	▪ Değerler ▪ Kültür ▪ Politikalar ▪ Kurumlar	▪ Kamu Diplomasisi ▪ İki taraflı ve çok taraflı diplomasi

Kaynak: (Nye J. , 2005:37)

1.2.1.Alternatif Teorik Yaklaşımlar ve Güvenlik Anlayışı

Güvenlik kavramını daha iyi anlamamıza yardımcı olacağını düşündüğümüz, belli başlı eleştirel uluslararası ilişkiler yaklaşımlarının güvenlik kavramına bakışını aşağıda inceleyeceğiz. Bu eleştirel okullar/yaklaşımlar şunlardır; Konstrüktivizm, Frankfurt Okulu ve Eleştirel Çalışmalar, Kopenhag Okulu ve Postmodernizm.

Eleştirel teorinin öncüsü olan Frankfurt Okulu, 1923 yılında Almanya'nın Frankfurt şehrinde bulunan Toplumsal Araştırmalar Enstitüsü'nde, siyaset bilimi, psikanaliz, sosyoloji, felsefe ve tarih gibi farklı alanlardan bir araya gelen akademisyenlerin modern topluma, pozitivizme ve aydınlanmaya yönelik eleştirileri sonucu kurulmuştur. Eleştirel çalışmalar, devlet merkezli tehdit anlayışları yerine,

toplumları ve insanları merkeze alarak toplumların ve bireylerin potansiyellerinin önündeki engelleri de incelemesi bakımından uluslararası ilişkiler disiplinine strateji ve jeopolitiğin dışında katkılar sağlamıştır. Eleştirel teorisyenler "özgürleştirme" kavramı üzerinde durmaktadırlar ve çalışmalarının içeriğini bu kavram oluşturmaktadır. Birçok eleştirel teorisyen kapitalizmi eleştirmekte ve hatta güvenlik ve kalıcı barışın sağlanamamasının önündeki tek engel olarak kapitalizmi görmektedir. Kapitalizm, maddi çıkarların olduğu eşitsiz gelir dağılımı, ekonomik istikrarsızlar ve ekonomik krizler, doğal kaynakların maddi kazanç sağlama amacıyla gerektiğinden fazla harcanması gibi olumsuz gelişmelere neden olması sebebiyle güvenlik problemlerinin temelini oluşturmaktadır (Uzgel, 2004).

Eleştirel güvenlik çalışmalarına göre güvenlik kavramının anlaşılmaz olması, tartışmalı doğasından değil, güvenliğin türetilmiş bir kavram olmasından kaynaklanmaktadır (Bilgin, Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları, 2010: 76). Güvenlik ne anlam ifade etmektedir sorusunun tüm mekânları ve tüm zamanları kapsayan bir cevabı yoktur. Bireylerin ve toplumların güvenlik anlayışları onların felsefi dünya görüşleri ve siyasi bakışlarından türemektedir. Booth güvenliği "tehditlerin yokluğu" olarak tanımlayarak güvenlik anlayışı için önemli bir referans oluşturmuştur (Booth, 1997:106). Eleştirel teorisyenler kapitalizme yaptıkları eleştirilerin haricinde, Soğuk Savaş sonrası dönemde güvenlik aktörlerinin ve tehditlerinin farklılaştığını savunarak klasik güvenlik çalışmalarını da (realizm, liberalizm, marksizm) eleştirmektedirler. Eleştirel teorisyenlere göre, hızlı nüfus artışı, göç, ırkçılık, küresel ısınma, çevre kirliliği ve doğal kaynakların kontrolsüz bir biçimde harcanması gibi olaylar tüm insanların ve toplumun ortak sorunlarıdır. Mabee(2003), geleneksel güvenlik çalışmalarına sadece devletleri ve devletlerin vatandaşlarının güvenliğini düşünmeleri sebebiyle karşı çıkmaktadır. Başka bir ifadeyle klasik güvenlik çalışmalarında, devletlerin hem güvenliği sağlaması hem de güvenlikte olması gereken tek aktör olmaları sebebiyle, tüm grupların veya ayrı ayrı bireylerin güvenliği ve en önemlisi olan 'evrensel güvenlik' göz ardı edilmektedir (Mabee, 2003:136).

Konstrüktivizm, sosyoloji, psikoloji ve siyaset bilimi gibi bilim dallarından etkilenerek ortaya çıkan inter-disipliner[2] bir yaklaşımdır. Konstrüktivizm yaklaşımında kimlik kavramı çok önemlidir. Konstrüktivistler uluslararası ilişkilerde, neorealistler gibi temel aktör olarak devletleri görmektedirler fakat güvenlik olgusunu, kimlik ve çıkar ilişkisini temel alarak analiz etmektedirler (Bozdağlıoğlu, 2007:149). "Wendt'e göre temel aktör olarak devletin alınmasının nedeni, Weber tarafından ifade edildiği biçimiyle, meşru şiddet kullanma tekelinin devlete ait olduğu konusunda uzlaşının sürmekte oluşudur. "Konstrüktivizm'e göre devletlerin çıkarları ve anarşi ortamı, söz konusu yapının devletlere dışarıdan dayattığı bir durum değildir. Devletlerin birbiri ile olan etkileşimi sonucunda kimlikleri oluşur ve oluşan bu yeni kimliğin niteliğine göre devletlerin çıkarları belirlenir (Wendt, 1995:74).

Konstrüktivizm, güvenlik kavramını genişletecek çalışmalarda bulunmuştur. Güvenliği sadece askeri güç bakımından açıklama çabası içerisinde bulunan geleneksel güvenlik çalışmalarına karşıdır. Bary Buzan'dan da etkilenen konstrüktivistler, sosyal ve ekonomik alanlarda çalışmalar yapmaktadırlar. Diğer adıyla inşacılar, güvenliğin sosyal boyutunu inceleyerek, bir devletin ulusal güvenlik siyasetini, hangi sosyal dinamiklerden etkilenerek belirlediğini ortaya koymaya çalışmaktadır. Bu kapsamda; "Etkileşim içindeki kültürler güvenliğin yeniden oluşumunu nasıl etkilemektedir ?" sorusuna yanıt aramaktadır (Çakmak, 2014:126).

Karl Wolfgang Deutsch'un öne sürdüğü "Güvenlik Toplulukları" kavramından da etkilenen bazı konstrüktivistler, tüm devletlerin halklarının evrensel bir toplum oluşturma duygusunu, bir kısım iletişimsel ve etkileşimsel faaliyetlerle geliştirerek, "ben" kavramı yerine ortak "biz" kavramı etrafında oluşan bağlılık ve sempati duyma düşüncesinin zamanla bağımlılık ve sorumluluk davranışlarına dönüşeceğini ve bu kapsamda söz konusu devletlerin ilişkilerine olumlu olarak yansıyacağını değerlendirmektedirler. Bu görüşe göre uluslararası güvenliğin sadece stratejik ya da askeri faaliyetlerde bulunarak değil, halklar arası oluşturulacak işbirliği alışkanlıklarına ve halkların karar alma sürecine dâhil olmaları sonucu devletlerinde olumlu davranışlarda bulunacağı değerlendirilmektedir (Kardaş,

[2] ''Ortak bir konuda, belirli disiplin bilgisine farklı disiplinlerin katkıda bulunmasıdır. Disiplinler sınırlarını zorlar ve karşılıklı bir etkileşim içine girerler''. (Garkovich, 1982:151-168) Akt: Akdoğan)

2007:138).

Çalışmamıza diğer bir alternatif yaklaşım olan postmodern teorilerin güvenlik yaklaşımlarını inceleyerek devam edeceğiz. Coşkun (2007)' a göre ilk olarak Fransa'da ortaya çıkan ve daha sonra ABD'de etkili olmaya başlayan postmodern çalışmalar, 1980'li yılların başından itibaren uluslararası ilişkiler disiplinine girmiştir. Önemli teorisyenlerinden bazıları; James Der Derian, Richard Ashley William Connoly, R.B.J. Walker ve David Campbell'dir (Coşkun, 2007). Postmodernizm sınıf dayanışması veya sanayileşme politikaları üzerine tartışılan yapıdan ziyade bilgi toplumuna yönelik bir değişimi analiz etmektedir. Postmodernizm' e göre ulusların sahip olduğu konum sorgulanmalı ve mevcut sistem ortadan kaldırılarak alternatif olarak bireyleri temel alan alternatif yaklaşımlar üzerinde çalışılmalıdır. Postmodern düşünürler devletler arasında düzenlenen sınırları eleştirmektedirler ve onlara göre söz konusu mevcut sınırlar tartışılarak alternatifleri düşünülmelidir. Postmodernizm, kültür, dil ve söylem olgularını analiz etmektedir. Çünkü bireylerin ve toplumların etkileşimleri dil ile gerçekleşir ve şekillendirilir. Postmodern teoride satır aralarını okuyup anlayabilme ve yorumlama gibi detaylar çok önemlidir. Bu detaylar sayesinde güç ilişkileri anlamlandırılabilir ve yapısı çözülerek bunların yerine alternatifleri oluşturulabilir (Özerdem, 2015:134).

Postmodernistler devletlerin 'yapay' güvenlik kaygıları oluşturduklarını savunmaktadırlar. Tarihin başlangıcından günümüze kadar geçen sürede, ulusların öncelikli var oluş sebebi, halklarının ve bir bütün olarak devletin güvenliğini sağlamak olmuştur. Bu kapsamda devletler var oluş sebepleri ile doğru orantılı bir biçimde bazı konuları güvenlikleştirmek istemektedirler (Mcdonald ve Bellamy, 2004:309). Soğuk Savaş yıllarında ABD ve SSCB blokları bir arada tutmak maksadıyla birbirlerini var olduklarından daha büyük bir tehdit olarak göstermekteydiler. Postmodernizm'e göre devletler kimliklerini ve ülke bütünlüklerini korumak adı altında bu yönteme başvurmaktadırlar (Yılmaz, 2015:170). Postmodernizm, kostrüktirivizm ve eleştirel teori birbirlerine benzer yaklaşımlarda bulunmuşlardır. Yeni güvenlik aktörleri çerçevesinde yapılan bir çalışmanın söz konusu üç teoriden hangisi içinde değerlendirilmesi gerektiği konusunda, karmaşa yaşanmasının sebebinin bu yaklaşımların birbirine olan

benzerliği olduğu değerlendirilmektedir.

Danimarka'nın Kopenhag şehrinden ismini alan Kopenhag Okulu, Centre for Peace and Conflict Research'te görev yapan ve aralarında Waever ve Buzan gibi akademisyenlerinde bulunduğu güvenlik üzerine çalışmalar yapan bir gruptur. Huysmans'a göre okulun çalışmalarının temel dinamiği; güvenlik kavramını askeri yaklaşımdan soyutlarken, tutarsız olmaktan da korumaktır (Bilgin, 2011:399-412). Kopenhag Okulu'nun güvenlik çalışmalarının popüler olma sebeplerinden en önemlisi Soğuk Savaş'ın sona ermesi ile değişen uluslararası sistemdeki güvenlik ortamını anlamamızı sağlayan yeni analiz araçları sunmasıdır. Kopenhag Okulu'nun literatüre kazandırdığı kavramlar Güvenlikleştirme ve Ters Güvenlikleştirme, Bölgesel Güvenlik Kompleksi, Güvenlik Sektörleri'dir. Aralarında Buzan'ın da bulunduğu Kopenhag Okulu olarak tanımlanan teorisyenler, "Güvenlik: Yeni Bir Analitik Çerçeve" isimli kitap ile literatüre güvenlik sektörleri kavramını kazandırmışlardır. Bu kapsamda klasik askeri güvenliğin haricinde politik, ekonomik, toplumsal ve insani ve çevresel güvenlik kavramlarıda literatüre girmiştir. Buzan'a göre güvenliğin boyutu değiştirilmeli ve insanların, grupların ve devlet dışı oluşumlarında güvenlik kaygılarını kapsayacak şekilde genişletilmelidir (Buzan ve diğerleri, 1998).

Waltz'un düşüncelerinden etkilenen Kopenhag Okulu teorisyenleri güvenlikleştirme kavramını oluştururken geleneksel güvenlik anlayışının iki temel kavramını baz almıştır; hayatta kalma ve varoluşsal tehdit (Waltz, 2001). Bu kapsamda Kopenhag Okulu Waltz'un neorealist düşüncelerine yakınlaşmaktadır. Herhangi bir varoluşsal tehdit algılanmasına müteakip güvenlikleştirme faaliyetini gerçekleştiren aktör, söz konusu tehdidin ortadan kaldırılması için ihtiyaç duyulan tüm önlemlerin alınmasını meşrulaştırmış olur. Bu açıdan güvenlik politik bir süreçtir ve güvenlikleştirme amacındaki aktörler herhangi bir olguyu ya da konuyu tehdit olarak kurgulayabilirler.

Kopenhag Okulu'na göre güvenlik, bir grubun ya da bir toplumun bir konuyu nasıl güvenlik tehdidi haline getirdiği ile ilgilidir. Taureck'(2006)'e gore; tüm söylemsel güvenlik oluşturma süreçleri başarılı bir güvenlikleştirme ile neticelenmeyebilir. Güvenlikleştirme sürecinin başarıya ulaşması için üç aşama vardır. Bunlardan ilki hayati öneme sahip bir tehdit unsurunun olmasıdır. İkincisi,

söz konusu tehdidin kaldırmasının acil bir durum olarak değerlendirilmesidir. Üçüncü aşama ise söz konusu tehdidin yok edilebilmesi için olağanüstü tedbirler alınması gerekliliğinin kabulüdür. Son aşamada olağanüstü tedbirler diye tabir edilen faaliyetlerin gerçekleştirilebilmesi için belli bir ölçüde kamuoyunun da desteğine ihtiyaç vardır. Kopenhag Ekolü'nün güvenlikleştirme argümanı söz edimi teorisi üzerine kurulmuştur. Bir şey söylemek veya bir şey yapmak gibi anlamlar ifade eden söz edimi kuramının kurucularından John Searle'ye göre iletişim yalnızca kelimelerle aktarılmaz, ses tonu, jest, aktarım hızı, dilin biçemi gibi birçok etken iletişim kurulmasında önemli rol oynar. Söz ediminde dinleyicinin düşünce, duygu ve eylemini nasıl etkileyeceğini hâlihazırdaki koşullar belirler. Tehdit algılamasında da nesnenin bilgisi, teşhis ve tespiti olmasa da var olabileceği varsayımını tartışmaya açan bu yaklaşım, problemlerin ancak bizim bildiğimiz ve tespit ettiğimiz sürece güvenlik tehdidi olarak anlaşıldığı, aksi takdirde mevcut problemin herhangi bir sorun olarak değerlendirilebileceğini ya da tehdit sorunu olarak görülmeyebildiğini ifade eder. Başka bir ifadeyle mevcut sorunlar kendiliklerinden tehdit teşkil etmezler, mevcut aktörler onları güvenlikleştirme eğilimine giderler (Taureck, 2006) (Arı, 2014:184).

1.2.DEĞİŞEN GÜVENLİK KAVRAMI

İnsanlık tarihinin başlangıcından günümüze kadar geçen sürede akademik alanda yapılan çalışmalar incelendiğinde güvenlik kavramını genişleten iki temel anlayış bulunduğundan söz edilebilir. Bunlardan ilki Soğuk Savaş Dönemi'nin başlangıcında çıkarlar ve tehditler kapsamında ele alınan güvenlik anlayışıdır (klasik güvenlik çalışmaları). İkincisi Soğuk Savaş'ın sona yaklaştığı dönemde yapılan çalışmalardır. Söz konusu çalışmalar güvenlik kavramına sadece sonuçlar üzerinden bakmak yerine olayların nedenlerini de sorgulamaya başlamıştır. (Alternatif Güvenlik Çalışmaları ve Eleştirel Güvenlik Çalışmaları). Güvenliğin tarihsel arka planını incelemek amacıyla çalışmamız Soğuk Savaş Dönemini ve sonrasını ele alarak gerçekleştirilmiştir.

1.3.1.Soğuk Savaş Döneminde Güvenlik Kavramı

Soğuk Savaş döneminde güvenlik konusunda, iki büyük güç olan Sovyetler Birliği ve ABD arasında politik, askeri ve ekonomik rekabet ortamının

biçimlendirdiği stratejik güvenlik yaklaşımları üzerine çalışmalar yapılmıştır. Caydırıcılık ve nükleer silahlanma konuları temelinde şekillenen stratejik güvenlik, bir güvenlik kategorisi olarak değerlendirilmektedir. Buzan ve Hansen (2009)'e göre; bu dönemde güvenlik çalışmalarının temel konularının, teknolojik ve nükleer devrim, iki süper gücün (ABD ve SSCB) politikaları, uluslararası alanda yaşanan gelişmeler, akademik tartışmalar, araştırma fonları ve düşünce kuruluşları olduğu değerlendirilmektedir (Buzan ve Hansen, 2009).

2'nci Dünya Savaşı bitiminden 1991 yılına kadar devam eden ve Soğuk Savaş Dönemi olarak adlandırılan süreçte ABD ve SSCB arasındaki anlaşmazlık boyutları büyürken, her iki tarafında nükleer silaha sahip olması, caydırıcılık ve karşılıklı tehdit anlayışlarının niteliğini de değiştirmiştir. Bu kapsamda nükleer silahların kullanılması durumunda dünya çapında yaratacağı yıkıcı etkiler, SSCB ve ABD'nin bir taraftan nükleer silahlanmaya devam etmelerine, diğer yandan da konvansiyonel silah, araç ve teçhizatlarını geliştirmelerine neden olmuştur. (Erhan, 2002)

Geçmişte yaşanan iki dünya savaşı sonrası güvenlik anlayışının, iki farklı düzlemde geliştiğini değerlendirmek mümkündür. Bunlardan ilki ulus-devlet güvenlik anlayışıdır. Söz konusu savaşlar sonucunda revize edilen uluslararası sistemde devletler iki gruba ayrılmıştır. İki grup da kendi belirledikleri değişkenleri farklı ideoloji ve sistemlerle açıklarken düzenleme yaparak değiştirmiştir. Bir grup aktör örgütlenmiş (Avrupa Konseyi, Kuzey Atlantik Paktı, Varşova Paktı ya da AET gibi) sisteme geçerken, diğer grup örgütsüz (Bağlantısızlar, Bloklar gibi) şekilde uluslararası sistemdeki varlıklarını devam ettirmiştirler. Bu nedenle her iki grubun da tehdit algılamaları değişmiştir. Rakip devletler, karşıt rejimler, toprak bütünlüğünü tehdit eden yayılmacı güçler, nükleer silaha sahip olan devletler bunlara örnek olarak verilebilir. İkinci düzlem ise, güvenlik kavramının küresel boyutudur. Az gelişmişlik, silahlanma yarışı, nükleer tehditler, çevre kirliliği, uluslararası olumsuz faaliyetler (mafya, terörizm, organize suç örgütleri, AİDS, insan ve uyuşturucu madde kaçakçılığı, göç, kara para aklanması) gibi başlıca yeni kavramlar tehdit anlayışlarına dâhil olarak, devletlerin ve toplumların güvenlik literatürünü genişletmiştir (Dedeoğlu, 2008:38) (Toklu, 2006) (Sander, 2004).

Şekil 1: Güvenliğin Katmanları

Kaynak: (Yılmaz S. , 2014)

1.3.2. Soğuk Savaş Sonrası Yeni Güvenlik Kavramları ve Konuları

1990 yılında Sovyetler Birliği'nin dağılması, mevcut uluslararası sistemde ve güç dengelerinde önemli bir dönüşüm ve yeni bir tartışma döneminin başlamasına neden olmuştur. Küreselleşme dönemi diye de adlandırılan bu süreçte askeri yaptırımların geçerliliğinin azalması, serbest ekonominin önem kazanması, milletleri bir araya getiren etnik kimliklerin güçlenmesi, ulus devlet öneminin belirli amaçlara ulaşmak için yetersiz kalması gibi gelişmelerle, uluslararası göç, uluslararası terörizm, kitle imha silahları, enerji güvenliği, çevre ve siber güvenlik gibi yeni tehditler ve güvenlik anlayışları ortaya çıkmıştır.

Bunlardan en önemlilerinden biri "uluslararası terörizm" dir. Terörizm kavramının tanımında olduğu gibi, bütün devletler tarafından kabul gören bir ''uluslararası terörizm'' tanımı da bulunmamaktadır. Genel anlamda uluslararası

terörizm, birden fazla ülkede terörizm faaliyetlerinin gerçekleştirilmesi anlamına gelmektedir (Altuğ, 1995:14). Uluslararası terörizmin tüm devletler tarafından kabul gören bir tanımının olmamasının nedeni, bir devlet/taraf için terör örgütü olanın, diğer bir devlet/taraf için demokrasi kahramanı ya da tehdit olarak algılanmamasıdır (Kuyaksil, 2004:92). Terör örgütlerinin varlıklarını sürdürebilmesinin ve önemli konularda eğitim, teşkilatlanma, finans sağlama gibi faaliyetleri gerçekleştirebilmesinin, genellikle başka ülke veya gruplardan alacağı desteğe bağlı olduğu değerlendirilmektedir (Ersoy, 2004:330).

Uluslararası İlişkilerde ülkeler birbirlerine karşıt güç olarak terörü, bir aktör olarak kullanmaktadırlar. Terörü araç olarak kullanan ülkeler çıkar sağlamak, ülkeyi istikrarsızlığa sokmak, baskı yapmak, anlaşamadığı bir konuda ikna etmek gibi amaçlar güdebilirler. Sistem içerisinde bulunan güçlü devletler egemen olmak ve diğer ülkeleri baskı altında tutmak, güçsüz devletler ise diplomatik yollarla gerçekleştiremediklerini, savaşacak yeterli güçlerinin olmaması veya riskli olması gibi durumlarda terörü bir dış politika aktörü olarak kullanmaktadırlar. Ülkeler, terör örgütlerine etkileşimde bulunduğu devletle olan ilişkileri oranında destek verir ya da mücadele eder. Terörizme destek veren ülkeler "dolaylı savaşı" tercih ederler. Bu kapsamda uluslararası terörizmin uluslararası güvenliği tehdit eden önemli bir sorun olduğu değerlendirilmektedir. Terör ve terörizmle mücadele her zaman uluslararası işbirliği söylemlerinin olduğu ancak bu söylemlerin eyleme dönüşmediği bir alandır (Urhal, 2009:346).

Bunlarla birlikte disiplinde, Kitle İmha Silahları da yeni güvenlik konularından birisi olarak ortaya çıkmıştır. Kitle İmha Silahları dünyaya ve insanlara verebileceği olası zararlar nedeniyle konvansiyonel silahlarla karşılaştırılamayacak boyutta tehlikeli silahlardır. Kitle İmha Silahları terimi, kimyasal, biyolojik, radyolojik ve nükleer silahları kapsamaktadır. Söz konusu kavram, literatürde kelime grubunun baş harflerinden oluşan bir kısaltma olan KBRN şeklinde ifade edilmektedir (Erdurmaz, 2003:27).

KBRN silahları, " uzun zaman süren savaşları kısa sürede bitirmek için" bilim ve teknoloji aracılığıyla insanlar tarafından üretilen, yalnızca yıkıcı değil neredeyse tüm dünyayı yok etme gücüne sahip silahlardır. Bu silahlar, uluslararası sistemde caydırıcı olabilme ve güçlü gözükebilmek amacıyla her geçen gün geliştirilerek daha

öldürücü seviyeye getirmek için çalışılmıştır. Kalıcı barış için KBRN silahlarının yasaklanması ve silahsızlanma faaliyetleri kısır döngü şeklinde devam etmektedir. Devletler kitle imha silahlarının, elinde bulunduran tarafa üstünlük sağlayacağını değerlendirmektedir ve söz konusu silahları üretmek konusunda kararlılık göstermektedirler. Fakat aynı kararlığı dünya barışını sağlamak amacıyla kitle imha silahlarının yasaklanması, sınırlandırılması veya tamamen ortadan kaldırılması hususunda göstermemektedirler. Eleştirel güvenlik teorisyenlerine göre, silahsızlanma sürecinin dünya barışı için temel bir ihtiyaç olduğu değerlendirilmektedir. Ancak söz konusu durum devletler için mevcut güçlerinin azalması ve kendilerini güvensiz bir durumda hissetmeleri olarak değerlendirilmektedir (Touraine, 1997:333).

Değişen güvenlik anlayışı kapsamında ele alınan güvenlik konularından birisi de enerji güvenliğidir. Silinir ve diğerleri (2012)'ne göre; mevcut uluslararası düzende, karşılıklı bağımlılığın zorunlu hale geldiği, devletlerin alt yapı yatırımları ve ekonomik hassasiyetlerinin de önemli ölçüde arttığı değerlendirilmektedir. Enerji arzının ve enerji pazarının güvenliği stratejik bir öneme haizdir ve enerji güvenliği sistemdeki tüm aktörler için kritik bir konu haline gelmiştir. Devletler enerji bağımlılığını enerji güvenliği ile ilişkilendirmektedirler ve amaçları enerji bağımsızlığını kazanmaktır. Söz konusu kazanım ulusal güvenliğin bir aşamasıdır. Aktörlerin ana amaçlarından bir diğeri de enerji bağımlılığı ve enerji güvenliğini dengede tutmaktır. Enerji güvenliğine yönelik uluslararası işbirliği ve ortak strateji geliştirilmeye çalışılırken NATO, Uluslararası Enerji Ajansı gibi örgütlere de roller verilmektedir. Örneğin NATO'nun askeri kuvvetleri, Akdeniz'de enerji arzının tehlikeye girmemesi için 2000 yılından beri aktif görevler icra etmektedir (Silinir ve diğerleri, 2012:146).

Enerjinin sınırlı olması, zor bulunması ve giderek artan enerji ihtiyacı devletleri ve insanları tedirgin etmektedir. Ayrıca günümüzde enerjinin, devletlerin dostluklarını veya düşmanlıklarını belirleyen çok önemli ve stratejik bir madde olduğu değerlendirilmektedir. Enerji politikalarını, savunma ve güvenlik politikasından, ekonomi politikasından, sanayi politikasından kısacası diğer tüm politikalardan bağımsız düşünmek mümkün değildir. Enerji güvenliğini dikkate almadan bu politikaları belirlemek neredeyse imkânsızdır. Tarih boyunca yaşanan

çatışma ve anarşi olaylarını, antlaşmaları, savaşları, ekonomik ilişkileri ve terör olaylarını enerji politiği ile incelemek zorunlu hale gelmiştir. Bu kapsamda enerji yalnızca bir fizik konusu olmaktan çıkarak, değişen güvenlik anlayışı için önemli bir kavram haline dönüşmüştür (İlbaş, 2014:11).

Bunların haricinde, Bilgi ve İletişim Teknolojisi (BİT), küresel güvenliğe karşı en kritik modern zorluklardan birini sunmaktadır. Tehdit değerlendirmeleri, bir sonraki büyük uluslararası krizin, kritik altyapı veya askeri lojistik ağlarını tahrip etmek için BİT'leri araç olarak kullanan bir devlet veya terörist gruptan kaynaklanabileceği tahmin edilen, asimetrik savaşların çoğalmasına neden olan ve (yani, farklı askeri yeteneklere sahip olan uluslar veya gruplar arasındaki çatışmalar) devletlerin uluslararası siber davranış kurallarını ve normlarını geliştirilmesini gerektiren ''siber güvenlik'' konusu, çalışmamızın ana konusu olması nedeniyle detaylı bir biçimde ikinci bölümde ele alınarak incelenecektir.

1.4. SONUÇ

Günümüzde "güvenlik" konusu Uluslararası İlişkiler disiplininde yer alan temel çalışma alanlarından birisidir. 2'nci Dünya Savaşı'na kadar gerçekleştirilen güvenlik çalışmaları sadece askeri tarihle sınırlandırılmıştır. Savaş sonrası güvenlik konusu farklı açılardan ele alınmaya başlanarak stratejik planlama çalışmaları gerçekleştirilmeye başlanmıştır. Soğuk Savaş döneminde ise, iki kutup arasında yaşanan nükleer rekabet, güvenlik anlayışına realist bakış açısını kazandırmış ve kitle imha silahlarının caydırıcılık konusunda nasıl kullanılabileceği çabalarına odaklanılmıştır.

Sovyetler Birliği ve ABD arasında 1962 yılında yaşanan Küba Füze Krizi ve müteakip dönemde ABD'nin yaşadığı Vietnam yenilgisi sonucunda uluslararası sistemde güvenliğin değerlendirilmesinde, askeri gücün yeterli ve geniş kapsamlı olmadığı düşünülmüş ve Eleştirel/Alternatif Güvenlik çalışmaları ortaya çıkmıştır. Küreselleşmeden etkilenen birçok lokal sorun kendi çerçevesinden taşarak ulusötesi olma eğilimi göstermiş ve aktörler çeşitlenerek artmıştır. Söz konusu gelişmelere bağlı olarak güvenlik konusunda çalışan uzmanlar birçok farklı disiplinle etkileşime girerek, güvenlik konularını çok boyutlu irdeleme ve yaklaşım geliştirme çabası içine girmişlerdir. Bu kapsamda, çalışmamızda ele alınan siber güvenlik konusunun da aralarında yer aldığı günümüz güvenlik konuları çok sayıda teori, yaklaşım ve ekol

içeren multidisipliner bir yapıya bürünmüştür.

İKİNCİ BÖLÜM

SİBER GÜVENLİK KAVRAMI TARTIŞMALARI

Bilim insanları teknolojinin uluslararası güvenlik konusundaki etkilerini gittikçe daha fazla ciddiye alırken, hükümetin ve diğer paydaşların benimsemesi gereken uygun politika yanıtlarının yanı sıra tehdidin seviyesi ve niteliği konusunda da anlaşmazlıklar devam etmektedir. En belirgin olarak, ilgili alanların uzmanları siber savaşın gerçekleşip gerçekleşmeyeceğini tartışmaktadırlar. İnternet 1990'ların ortalarında ticarileşmesinden bu yana hızla genişlemiştir. Günümüzde insanların büyük bir bölümü teknolojiye erişime sahiptir. Ayrıca, kullanılan tüm araç ve nesnelerin internete bağlı olmasını zorunlu kılan ağ sistemleri, dijital araçların kötü amaçlar için kullanılmasına olan ekonomik ve politik teşvikleri de arttırmıştır. Bu nedenle siber güvenlik, devlet düzeyinde dikkat çekmiştir. Buna paralel olarak, konuyla ilgili yayınların akademik, politika, endüstri ve askeri kurumlar tarafından çoğaltılması hususu, Uluslararası İlişkiler disiplini dâhilindeki araştırmacıları; özellikle güvenlik çalışmaları ve stratejik çalışmalar alt alanları, teknolojinin ulusal ve uluslararası güvenlik üzerindeki etkilerine giderek daha fazla odaklanmalarına neden olmuştur. Zira bunlara güç, egemenlik, küresel yönetim ve menkul kıymetleştirme gibi ilgili kavramlar üzerindeki etkisinin incelenmesinin de dâhil olduğu değerlendirilmektedir. Bu kapsamda siber güvenlik ve bilgi güvenliğinin anlamları son derece tartışmalı bir yapıya bürünmüştür. Kavramların geniş tanımları, siber savaş, siber saldırı, siber çatışma, siber terörizm, siber suç ve siber casusluk dâhil olmak üzere çok çeşitli siber tehditleri ve siber riskleri içerirken, daha dar kavramsallaştırmalar ağlarla ilgili daha teknik yönlere odaklanmaktadır. Zira disiplininin dışına çıkmamak için çalışmamızın bu bölümünde siber saldırı, siber savunma, siber savaş, siber terörizm, siber casusluk kavramlarının oluşumu aktarılmıştır. Daha sonra, siber saldırı tekniklerinden en yaygın olanlarından bazıları irdelenerek saldırıların arka planında yaşanan gelişmeler ve günlük hayatta karşılaşılan örnekler aktarılmaya çalışılmıştır. Son olarak bu bölümde siber güvenliğin önemini vurgulamak amacıyla geçmiş de yaşanan siber çatışmalar ve saldırı olayları kronolojik çerçevede arz edilmiştir.

2.1 SİBER GÜVENLİK

Konu hakkında günümüze kadar yapılan çalışmalar incelendiğinde, güvenlik kavramlarına ilişkin birçok konuda olduğu gibi "siber güvenlik" kavramı hakkında da net bir tanım yapılamadığı görülmektedir. Bu nedenle siber güvenlik kavramından once "siber" kavramını tanımlamamız gerekmektedir. Siber kelimesi ingilizce "cyber" kelimesinden dilimize uyarlanmıştır. Söz konusu kavram adını sibernetik kelimesinden almıştır. Sibernetik kavramı ise ilk olarak 1834 yılında Fransız matematikçi Andre Ampere tarafından kullanılmıştır. Sibernetik kavramına güncel anlamda manasını veren ise 1948 yılında kumandalı otomatik sistemlerin üstüne "Cybernetics" isimli eseri yayınlayan Norbert Wiener olmuştur (Eren, 2017:19). Klimburg (2012), siber kelimesini "bilgisayar ağlarına ve internete ait olan şeklinde" ifade etmiştir. Siber kelimesi sanal gerçeklik olarak da bilinmektedir (Klimburg, 2012).

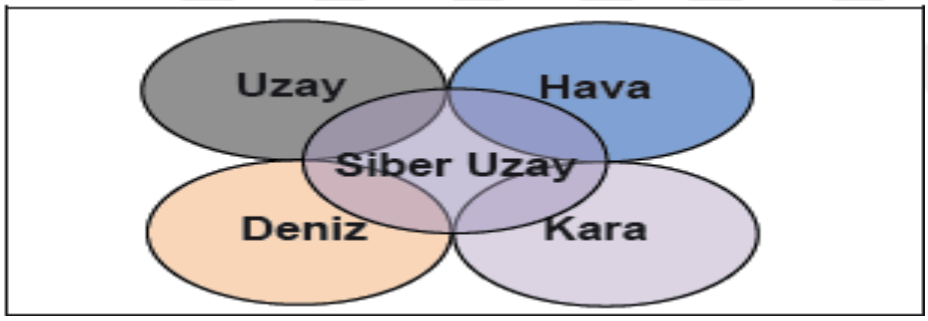
Siber güvenlik kavramı ise siber ortamda bulunan bilginin güvenliği ve bilginin bulunduğu cihazın güvenliği konuları ile birlikte kullanılmaktadır. Söz konusu bilgi güvenliğinin sağlanabilmesi için erişilebilirliğinin, gizliliğinin ve bütünlüğünün birlikte sağlanması gerekmektedir. Siber güvenlik kavramı da bu noktada devreye girerek bu bileşenlerin tek tek korunması için önlemler geliştirmektedir. Canbay ve diğerleri (2009) siber güvenliği, kullanıcı, kuruluş ve kurumların var oluşlarına ait özelliklerini siber ortamda bulunan güvenlik tehlikelerine karşı koruma amacıyla kullanılan, kılavuzlar, araçlar, güvenlik teminatları, eğitim ve teknolojiler risk yönetim yaklaşımları, politikalar ve bu amaç için gerçekleştirilen faaliyetlerin bütününe verilen bir isim olarak tanımlamaktadırlar. Siber saldırılar, düşük maliyetlerle kısa zamanda farklı sektörlere yönelik olarak gerçekleştirilmektedirler. Bu saldırılar sonucunda ülkelerin önemli altyapılarına kalıcı hasarlar verilmesi ve ülke ekonomilerinin zarar görmesi gibi sorunlar ortaya çıkmaktadır (Canbay ve diğerleri, 2009). Bu çerçevede siber güvenliğin önemli bir güvenlik konusu haline geldiği değerlendirilmektedir. Ayrıca siber güvenlik, güvenlik konularının birbiri içine geçtiğini göstermesi açısından da önemlidir. Bu kapsamda çalışmamızın ilerleyen kısımlarında siber güvenlik kavramının ortaya çıkış sürecini açıklamanın yerinde olacağı değerlendirilmektedir.

2.2. TEMEL SİBER GÜVENLİK KAVRAMLARI

Bu alt başlıkta siber güvenlik kapsamında bilinmesi gereken; siber uzay, siber saldırı, siber savunma, siber savaş, siber terörizm ve siber casusluk konuları açıklanacaktır.

2.2.1 Siber Uzay

Günümüzde beşinci boyut olarak adlandırılmakta olan "siber uzay" boyutunun uluslararası alanda yeni ve karmaşık bir ortam olduğu değerlendirilmektedir. Siber uzay(siber ortam) kavramının uluslararası kabul görmüş bir tanımı bulunmamaktadır. Literatürde yapılan bir tanıma göre siber uzay: "iletişim ağları, internet, enerji hatları ağları, kapalı askeri ağlar, yazılım alt yapılı telsizler, cep telefonları, insansız hava araçları sistemleri, uydu sistemleri gibi birçok donanım ve yazılım elemanlarının var olduğu ortam" şeklindedir. Siber ortamın birçok ülkede uzay, hava, deniz, kara gibi bir askeri harekât alanı olarak değerlendirildiği görülmektedir (Şekil-2.) (Akyazı, 2013).



Şekil 2: Beşinci Harekât Boyutu Olarak 'Siber Uzay'

Siber ortamın tartışma konusu olarak anlaşılması, ülkelerin iç politikada ve dış politikada sahip oldukları değerlere ilişkin bir zemin oluşturmasıdır. Güvenlik genel olarak anlaşıldığı üzere yalnızca tehlikeden veya tehdit ortamından uzak olmak değildir. Aynı zamanda herhangi bir düşmanın var olmasıyla da ilgilidir. Siber ortamda taraflar farklı amaçlarla birbirleriyle mücadele etmektedirler. Siber ortamın(siber uzay) uluslararası sistem içerisinde bir harekât alanı olup olmadığına yönelik en büyük tartışma, dijital ortamda bulunan tüm araçların fişinin çekilmesi veya ağ sistemindeki bağlantının sağlanamaması durumunda sona ereceği ve göreceli olduğu değerlendirilmektedir (Güntay, 2017:85).

2.2.2. Siber Saldırı

Siber saldırı, yasal veya yasal olmayan kuruluşların, yetkili hükümet kurumlarının, şirketler veya bireylerin, teröristlerin taktik ve operasyonel amaçlarına ulaşmak için siber uzayda uyguladıkları saldırı faaliyetleridir. Söz konusu saldırılar siber ortamda aktif olarak kullanılan donanım, yazılım ve alt yapıları hedef alır. Gerçekleştirilen saldırıları analiz etmek için muhtelif aşamalar vardır. Bunların en önemlileri yapılan saldırının amacı, saldırı şekli, etkileri, ahlakilik ve yasallık boyutlarıdır. Saldırıların amaçları değişiklik gösterebilir(hırsızlık, ideolojik vb.) Saldırılar pasif veya aktif olabilir. Pasif saldırılar hedef sistemin bilgi akışını, zamanlamasını, davranışlarını ve özelliklerini öğrenmeye yöneliktir. Aktif saldırılar ise sistemi devre dışı bırakma veya ona nüfuz etme amaçlıdır. Gerçekleştirilen saldırıların etkileri hedef sistemin unsurlarını, taciz etmeye, hırsızlığa, sistemi değiştirmeye veya sisteme zarar vermeye kadar değişiklik gösterebilir. Söz konusu saldırılar mevcut kanunlara göre yasal veya yasal olmayabilir. Saldırıda bulunulan bilginin sahibinin, kişilik hakları da ahlaki açıdan değerlendirilmesi gerekmektedir. Bilgi diğer kavramlarla kıyaslanıldığında, sahibinin haberi olmadan çalınabilen, paylaşılabilen ve kötüye kullanılabilen bir mülktür. Diğer mülkler çalındığında sahipleri onun kaybolduğunu anlarlar. Bilgi çalındığında ise çoğu zaman fark edilmez çünkü bilgi hâlihazırda eksilmemiştir veya ortadan kaybolmamıştır.

Canbek ve Sağıroğlu (2007)'ye göre;''bilgi ve bilgisayar güvenliği sistemini aşma, atlatma veya kırma yöntemlerini kullanarak, durdurma, bilgiyi ele geçirme, zafiyete uğratma, zayıflatma ya da tamamen bitirme, siber saldırı olarak adlandırılır." (Sağıroğlu ve Canbek, 2007: 2). Siber saldırılar, başka bilgisayarlara sızarak hack etme işlemini gerçekleştirecek ileri düzey yazılım ve programlama bilgisi olan uzmanlar tarafından, öncelikle sızılacak cihazların işletim sistemlerinde veya kullanıcısı tarafından kullanılan uygulamalarında, zayıf nokta veya bir açıklık bulunarak yapılmaktadır. Siber saldırılar, kurum çalışanları, teknoloji ya da endüstri casusları, profesyonel suçlular veya dış devletler tarafından gerçekleştirilebilir. Söz konusu saldırıları gerçekleştiren insanlar için ''bilgisayar korsanı'' kavramını kullanmanın daha uygun olacağı değerlendirilmektedir. Bu kavram yalnızca kötü amaçlı saldırganlar için değil iyi amaçla hizmet edenleri de kapsamaktadır.

Bilgisayar korsanları internetin ilk kullanılmaya başladığı zamanlarda saldırıları yalnızca dikkat çekme, idealistlik veya hobi amaçlı yaparken, günümüzde muhtelif birçok amaca ulaşmak için farklı saldırılar gerçekleştirilmektedir. Siber saldırı artık bir sektör olarak karşımıza çıkmaktadır. Bu kapsamda yapılan saldırı metotları da hızlı bir biçimde karmaşıklaşarak artma eğilimi göstermektedir (Keskin, 2008:242).

2.2.3. Siber Savunma

Siber saldırı kavramıyla birlikte açıklanması gereken diğer bir kavram da siber güvenlik kavramıdır. Literatürde siber saldırı ve siber güvenlik kavramları hakkında genel kabul görmüş tanımlar bulunmamaktadır. Siber güvenlik kavramı, bilgi güvenliği, bilgisayar ve elektronik cihaz güvenliği gibi kavramlar ile benzer anlamlarda kullanılmaktadır. Bilgi güvenliği kavramı genellikle kurumsal ve kişisel verilerin güvenliğini temel alan bir kavramdır. Bilgisayar güvenliği kavramı ise bilişim sistemlerindeki tüm aktörlerin güvenliği olarak değerlendirilmektedir. Söz konusu iki kavramda ortak öğeler içermektedir fakat odak aldıkları konular bakımından farklılık gösterebilmektedirler.

İnternetin vazgeçilmez bir araç olması ve bilgi sistem teknolojilerinde yaşanan gelişmelerle, siber ortamda bulunan tehdit ve saldırıların artması sonucunda uluslararası sistemin daha karmaşık bir yapıya dönüştüğü görülmektedir. Bu nedenle siber güvenlik ve savunma konusunun bireysel, kurumsal, ulusal ve uluslararası kapsamda önemli konular arasında yerini aldığı değerlendirilmektedir (Arslan, 2018:2). Goodrich ve Tamassio (2010)'a göre; siber savunma kavramının tanımı bilişim sistemleri ve temel malzemesi olan bilgi üzerinden yapılmaktadır. Siber ortamın güvenli olabilmesi için bilgi gizliliği(confidentiality), erişilebilirliği (avaliability) ve bütünlüğünün (intergrity) sağlanması gerekmektedir. Bilgi gizliliği sadece bilmesi gereken kişilerin bilmesi ve erişebilmesi anlamına gelmektedir. Erişim kavramı bilgi sistemlerinde bir şekilde muhafaza edilen bilginin yalnızca yetkili kişiler tarafından görüntülenmesi, doküman olarak çıktı alınabilmesi ve hatta bazı kritik bilgilerin varlığından bile yalnızca yetkili kişilerin haberdar olması gibi anlamları ifade eder. Söz konusu 'bilginin bütünlüğü' kavramı ise elde bulundurulan bilginin kısmen ya da tamamen silinmemiş, değiştirilmemiş veya yok edilmemiş olması gibi anlamları ifade etmektedir (Goodrich ve Tamassio, 2010).

2.2.4. Siber Savaş

Savaş normları ve savaşı önlemeye çalışan evrensel kurallar, bilgi sistem teknolojileri gelişmeden önce belirlenmiş olması nedeniyle siber saldırılar karşısında yetersiz kalmaktadır. Bazı teorisyenler siber savaşa gereğinden fazla önem verildiğini ve gerçekleştirilen bir siber saldırının savaş nedeni sayılamayacağını, devlet tarafından gerçekleştirilen siyasi bir siber saldırının casusluk, sabotaj veya tahrip amaçlı bir saldırı gibi değerlendirilerek konvansiyonel silahların kullanıldığı gerçek bir savaş doğurmayacağını savunmaktadırlar (Yayla, 2014:195). Fakat gelişen teknoloji ile birlikte siber saldırılar askeri operasyonların neredeyse tamamını etki edebilecek niteliklere sahiptir. Düşman unsurlarının iletişim ve bilgi sistemlerinin kesilmesi, istihbarat toplamak, düşman birliklerinin pozisyonlarını saptamak, akıllı silah sistemlerine etkide bulunmak gibi kavramlara etki etmektedir. Bu kapsamda siber savaş, devletlerin bilgi teknolojilerine giderek artan bağımlılıkları ve ulusal hassasiyetler neticesinde yeni bir savaşı ifade etmektedir (Keskin, 2008:242).

Herbert Lin (2010)'a göre siber savaş; düşmanın iletişim ağları veya bilgisayar sistemlerine ve bu ağlarda ya da sistemlerde bulunan bilgiyi, programları ve araçları bozmak, değiştirmek, geriletmek veya yanıltmak amacıyla gerçekleştirilen hereket ve harekâtlardır. Söz konusu saldırılar kişiler, özel kurumlar, devlet dışı aktörler veya devletler arasında meydana gelebilecek siber savaşların gerçekleşebileceği yeni savaş boyutu (domain) olarak değerlendirilmektedir (Lin, 2010:63).

2.2.5. Siber Terörizm

Bilgisayar ağlarının ve bilgi sistemlerinin yaygınlaşması, internetin her alanda zorunlu hale gelmesi ve devletlerin güvenlik sistemlerinde söz konusu teknolojilerin kullanılması nedeniyle, teröristler ve terör grupları tarafından da bilgi sistem teknolojileri yoğun bir biçimde kullanılmaktadır. Gelişmiş haberleşme vasıtalarını kullanan terör örgütleri elemanlarını daha kolay kontrol altında tutabilmekte ve en üst seviyede gizliliği gerçekleştirmektedirler. Teknolojideki yaşanan bu gelişmeler yalnızca güvenlik güçlerinin veya devletlerin, terör örgütlerinin haberleşmesini izlemesi değil, terör örgütlerinin de söz konusu teknolojiyi kullanarak devletlerin veya güvenlik birimlerinin haberleşmesini izleyerek buna yönelik tedbirler geliştirmesine imkân vermiştir. Dünyanın birçok ülkesinde güvenlik teşkilatları ve firmaları siber teröristlerin yaptıkları saldırıları

zamanında tespit etmeye hatta önlem almaya çalışmaktadırlar. (Andress ve Winterfeld, 2011:198), siber terörizmi şu şekilde tanımlamaktadır; "bilişim sistemleri kapsamında, elektronik iletişim araçlarını, programlarını ve yazılımlarını kullanarak, ulusal bütünlüğe ve çıkarlara zarar vermeyi amaçlayan eylem ve etkinliklerdir.".

Tablo 2: Geleneksel Terörizm ve Siber Terörizm Farkları

Konular	**Klasik Terör**	**Siber Terör**
Anlam Bakımından	Topluma ve mevcut siyasal rejime mesaj göndermek için terörizm bir araçtır.	Gerçekleştirilen eylemlerle topluma, hedef alınan organizasyona ya da devlete zarar vermek için terörizm bir amaçtır.
Risk Analizi	Eylemi yapan grup ya da kişi yaşamsal ve hukuksal riski üstlenmektedir.	Herhangi bir yaşamsal veya hukuksal risk olmadan etkili bir saldırı gerçekleştirilmiş olur.
Etki Alanı	Saldırının gerçekleştirildiği bölge ile sınırlıdır.	Ulusal veya uluslararası alanlarda etkili olabilecek eylemler olabilir.
Propaganda	Verilmesi amaçlanan mesaj bölgesel.	Verilmesi amaçlanan mesaj küresel olabilir.
Tespiti ve Denetimi	Tespit etmek, kontrol altına almak, takip etmek, yok etmek kısmi olarak mümkün.	Siber saldırıları ve siber teröristleri belirlemek, kontrol altında tutmak veya yok etmek neredeyse imkansız.
Kullanılan Araç	Silah ve bomba gibi fiziksel saldırı araçları.	Radyo frekansı, virüs, e-bomba, yazılım gibi sanal araçlar.
Uygulanacak Ceza	Suçun cinsine göre uygulanması gereken ceza açık ve nettir.	Suçun niteliğinden kaynaklanan hukuki boşluklar mevcuttur.

Kaynak: (Kara ve diğerleri, 2018:2)

Gelecekte karşılaşılabilecek en büyük tehlikenin, bilgi teknolojisinde yaşanan gelişmelerin terörist eylemlere daha kötü sonuçlara neden olabilecek yepyeni bir boyut kazandırabileceği görüşünün olduğu değerlendirilmektedir. Bilgi sistemine nüfuz eden siber teröristler sisteme müdahale ederek güvenlik, ulaşım, bankacılık

gibi birçok sektöre zarar verebilmektedirler. Bir enerji üretim veya nükleer santralin bilgi sistemine bilgi ağı kullanılarak gönderilebilecek hatalı bir komutun oluşturacağı zararın, söz konusu tesisin bombalanması sonucu meydana gelebilecek tüm zararlardan daha büyük olacağı değerlendirilmektedir. Bu eylemi gerçekleştiren aktörün tespit edilmesi ve yakalanması da çok zordur (Acar, 2007:372).

Bu kaygılardan dolayı, 1995 yılında Paris'de gerçekleştirilen terörizm başlıklı Dışişleri Bakanları Konferansı'nda, terör örgütlerinin bilgi ve haberleşme sistemlerini ve siber uzayı kullanarak gerçekleştirecekleri kasıtlı siber saldırılarla mücadele etmek amacıyla uluslararası işbirliği yapılmasını kararlaştırmışlardır. 1997 yılında da Avrupa Polis Teşkilatı (EUROPOL), devletlerin güvenlik teşkilatlarına, internette yasadışı bilgi bulunduran alanların incelenmesi, ülkelerin iç hukuklarının tasnif edilerek uyumlu hale getirilmesi ve gerektiğinde işbirliği yapılması için bildirimde bulunmuştur. Söz konusu işbirliği çalışmaları çeşitli aktörler tarafından muhtelif zaman ve yerlerde gerçekleştirilmeye devam etmektedir. Siber ortamda terörist saldırılarda kullanılabilecek taktik ve tekniklerin, yeryüzünü en ince detaylarına kadar gösteren harita ve krokilerin, fotoğrafların, bomba ve el yapımı patlayıcıların nasıl üretildiğini gösteren formüllerin bulunduğu bilinmektedir (Örgün, 2001:49-59).

2.2.6. Siber Casusluk

Casusluk kelimesi Arapça kökenli bir kelimedir ve "tecessüs" yani merak duyma, kendini ilgilendirmeyen konuları belli etmeden öğrenmeye çalışmak olarak tanımlanmaktadır. Casusluk anlamına gelen "espiyonaj" kelimesi ise Fransızca kökenli bir kavramdır. Ayrıca Türkçe kullanılan "ispiyon" kelimesi de Fransızca "espionnage" kelimesinden gelmektedir. "Kont-espiyonaj" kelimesi ise istihbarat ve istihbarata karşı koyma anlamlarını taşımaktadır. İstihbarat faaliyetleri geçmişte olduğu gibi günümüzde de siyasi, güvenlik, ekonomik vb. alanlarda hâlihazırda gerçekleşen teknolojik gelişmelerin de katkılarıyla önemli bir alan olma özelliğini korumaktadır (Avcı, 2004:6-7).

Casusluk, başka birey, kurum veya devletlerin muhafaza ettiği sırları veya bilgileri gizli yöntemlerle elde etme faaliyetleridir. Herhangi bir aktör(birey, örgüt, devlet) adına ve faydasına, gizli faaliyetlerde bulunan, istihbarat toplayan veya istihbarata karşı koyma amacı için çalışan özel olarak görevlendirilen kişilere de ajan

veya casus ismi verilmektedir (Tezsever, 1999:165-167).

Siber casusluk kavramı ise İngilizce "cyber spying" ya da "cyber espionage" olarak bilinmektedir. Keleştemur (2015)'e göre; siber casusluk faaliyeti ilk zamanlarda kişisel maksat ve niyetler için gerçekleştirilmekteydi. Önceleri çeşitli virüs yazılımları ile kullanıcı bilgisayarlarına nüfuz etmek ve onların parolalarını ele geçirmek gibi amaçlar için gerçekleştirilirken, zamanla siyasi, ekonomik ve askeri güç bakımından avantaj elde etmek için kullanılmaya başlamıştır. Günümüzde siber casusluk yapılarak diğer devletlerin bilgi sistemlerinde bulunan tüm bilgilerin ele geçirilebileceği ve hatta ülkelerin konvansiyonel savaş planları ve stratejilerinin ele geçirilebileceği değerlendirilmektedir. Siber casusluk faaliyetleri siber güvenlik için oldukça önemli bir etkendir (Keleştemur, 2015:312).

Siber casusluk eylemleri yasal olmayan yöntemlerle gerçekleştirilmektedir. Rakip devletlerin bilgi sistemlerine yasadışı metotlarla sızarak herhangi bir izin veya müsaade olmaksızın şahıs, grup veya devlete ait gizli bilgi ve belgelerin sızdırılması faaliyetleridir. Çoğunlukla dijital ortamda saklanan ve çeşitli devlet adamlarına ait olan bilgi, belge, görüntü, video veya ses kaydı gibi dosyalar ele geçirilerek rakip ülkeye şantaj yapılabilir. Bu kapsamda söz konusu ülkenin harekât ve etki alanının kısıtlanabileceği değerlendirilmektedir (Güven, 2013).

2.3. SİBER SALDIRI YÖNTEMLERİ

2.3.1.İnternet Servis Saldırıları

İnternet ortamında bulunan bilgisayarlar, internet servis ve protokolleri aracılığıyla birbirlerine bağlanarak iletişim kurmaktadırlar. Kullanılan bu protokollerin ve servislerin zayıf noktaları veya bu servisleri oluşturan yazılımlardaki açıklıklardan faydalanarak bilgisayarlara saldırı yapılabilmektedir. Bu protokollerin çok eski olmasından kaynaklanan mantık hataları bulunmaktadır. Saldırganlar mevcut zafiyetleri kullanarak çeşitli metotlarla saldırılar gerçekleştirebilmektedirler. Günümüzde bilgi güvenliğine verilen önemin artması ile birlikte, bahse konu protokollerden bazıları yeniden düzenlenerek revize edilmiştir. Fakat yine de mevcut zafiyetler saldırı düzenleyenlerin hedefi olmaktan kurtarılamamıştır.

Tablo 3: Birinci Seviye İnternet Zafiyetleri ve Temsili Saldırılar

İnternet Servisi	Zafiyetleri	Temsili Saldırılar
SMTP	*Adreslerin başlıkları ve kaynakların doğrulanması işleminin olmaması	*Sahte bir mail adresi ile e posta mesajı aldatmacası *E-postanın yetkisiz bir biçimde yeniden yönlendirilmesi. *E-posta bombardımanı
TCP/IP	*IP adreslerinin yetkisiz ve güvenliksiz transfer edilmesi. *Yetersiz sınır koruma	*Basit bir şekilde yakalanan paketler, IP adreslerinin hedefini ve kaynağını ifşa eder, trafik takip edilebilir. *Yetkili bir bilgisayar veya kullanıcı gibi kendini gösterme(Masquerading) *SYN saldırıları *Ölümcül ping *Oturum çalma
FTP	*ANONYMOUS ve GUEST kullanıcı isimlerine izin verilmesi *Saldırganlara, kurumlara kısıtlı da olsa giriş müsaadesi sağlanması	*İlk girişte bulunan sistem kaynakları hakkındaki bilgiler ilerisi için kaynak oluşturur. *Saldırgan FTP faaliyetlerine erişme hakkı elde edebilir.
WWW	* Güvenliksiz HTTP adreslerinin aktif içerikleri kabul etmesi	*Ortadaki adam saldırısı *Aktif içerikler kötü niyetli yazılımlar içerebilir *Çerez ismi verilen verilerle, söz konusu sitede yapılan faaliyetler izlenebilir.

Kaynak: (Çifci, 2017:93)

2.3.2 Kriptografik Saldırılar

Kriptografik saldırılar, bir algoritma ya da basit yöntemler aracılığıyla şifrelenmiş veri veya mesajların okunabilmesi için, şifrenin çözülmesi amacıyla gerçekleştirilen saldırılardır. Saldırılar gerçekleştirilirken hedef kriptografik sistem

araştırılır ve daha sonra mevcut sistemin zayıf tarafları incelenerek şifre kırılmaya çalışılmaktadır. Üzerinde durulması gereken nokta, kriptonun algoritmasından ziyade elde bulundurulan mevcut anahtarın güçlü olması gerekliliğidir. Saldırılar çoğunlukla anahtar varyasyonları oluşturan dağıtıcılar ve üreticilere gerçekleştirilmektedir. Mevcut sistemlerde herhangi bir açıklık bulunması durumunda saldırgan, anahtar tahmini yapabilmektedir. Ayrıca rastgele rakam üreticilerinin tekrar eden karakteristiğinin çözülmesi durumunda da anahtar tahmini gerçekleştirmek mümkün olabilmektedir. Kriptografik saldırılar çok eski bir istihbarat faaliyetidir. 1'inci Dünya Savaşı ve 2'nci Dünya Savaşı dönemlerinde gerçekleştirilmiş olan bu saldırılar sonucunda, birçok hassas ve önemli bilgi elde edilerek bu vesileyle savaşın seyrini değiştiren gelişmeler yaşanmıştır (Bıçakçı K. , 2013).

2.3.3. Zamanlama Saldırıları

Bilgisayarların aynı anda birden fazla işlemi yürütmesine eşzamanlı çalışma ismi verilmektedir. Ancak bilgisayarlar bazı durumlarda eşzamanlı işlem yürütmek yerine, mevcut işlemleri belirli bir sıra dâhilinde yürütmektedirler. Bu durumda bir işlemin başlaması için diğer işlemin sona ermesi gerekmektedir. Bu çalışma sistemine ise eşzamansız çalışma adı verilmektedir. Örneğin herhangi bir belgenin ya da dokümanın yazıcıdan çıktı alınması işlemi için çeşitli görevlerin sırayla işleme alınması gerekmektedir. Bu tür durumlarda işletim sistemleri mevcut istekleri bekletir ve yazıcıya (printer) ulaşılabilir olduğunda, öncelik sırasına göre istekleri gerçekleştirir. Bilgi sistemleri bu tür durumlarda kaynaklara erişebilmeye odaklı bir biçimde eşzamansız olarak çalışmaktadır (Benzer, 2014:28).

Eşzamansız çalışma işlemi sırasında, bellekte bekleyen verilerin değiştirilmesine dayanan saldırı şekline eşzamansız saldırı denilmektedir. Örneğin bir programla yapılan çalışma işleminin sonuçlarını yazıcıdan çıktı almak için sıradaki işlemlerin tamamlanmasının beklenildiği esnada, söz konusu yazılım konusunda bilgi sahibi olan kişiler bellekte bekleyen mevcut veriler üzerinde istedikleri biçimde silme, değişiklik veya ekleme yapabilme imkânlarına sahiptirler (Yazıcıoğlu, 1997).

2.3.4.Trafik Analizi

Trafik analiz yönteminde iletişimler yakalanarak analiz edilmekte ve iletişim ağlarından bilgi çıkarılmaktadır. Gerçekleştirilen bu analiz işlemi esnasında gelen-giden verinin içeriğinden daha ziyade söz konusu verinin metadatası veya örüntüsü

incelenerek sonuç elde edilmektedir. Trafik analiz yöntemi genellikle ağ tarama yöntemi ile karıştırılan bir yöntemdir. Bu işlem ile hedefin faaliyetleri hakkında bilgi toplanmaktadır. Trafiğin çok fazla olduğu bölgeler tespit edilerek, hedefin bir eylem aşamasına geçebileceği tespit edilebilmektedir. Ayrıca bu bölgelere gerekli saldırılar gerçekleştirilebilir ve hedef sistemlerdeki önemli veriler ele geçirilebilir. Özellikle ülkelerin silahlı kuvvetlerinin askeri istihbarat teşkilatları tarafından uygulanarak düşman faaliyetleri hakkında bilgi elde etmek amaçlanmaktadır. Örneğin belirli bölgeler arası trafiğin fazla olması durumu, bu bölgeler arasında organizasyonel bir ilişkinin bulunmasına; trafiğin olmaması durumu, bir şeylerin beklendiğine veya planın sonuçlandırıldığına; çok fazla trafik olması durumunun, planlama yapıldığına dair anlamlara gelebileceği değerlendirilmektedir (Çifci, 2017:93) (Keleştemur, 2015:312).

2.3.5. Zararlı Yazılım Kullanımı

Bir bilgi sistemine saldırmanın metotlarından bir diğeri de mevcut sisteme zararlı herhangi bir yazılım (Truva atı, solucan, virüs) yüklemek ya da yüklenmesini sağlamaktır. Bunlardan en önemlisi olan virüs kavramı anlam değişimine uğrayarak tüm zararlı yazılımları kapsar bir duruma gelmiştir. Ancak bilgi sistemlerinin kullanılamaz hale getirilmesi, sistemlere sızılması veya verilerin bozulması gibi işlemleri gerçekleştiren birden fazla zararlı yazılım vardır. "Virüs" ise bunlardan sadece biridir. Söz konusu diğer zararlı yazılımların birbirleri ile olan aralarındaki farklılıklar isimlerine yansımıştır. Bunlardan Truva atı, tarihteki bir olaya atıf olarak ve olaya benzerliği ile değerlendirilmektedir. Tüm zararlı yazılımların hedeflerine göre farklı sistemleri mevcuttur. Truva atı, hedef sistemin özelliklerine göre kurgulanır ve bilgiyi ele geçirmeye yönelik yazılır. Solucanlar ise sistemleri kullanılamaz hale getirmek için, sistemlere bulaşırlar ve sürekli kendilerini yayma becerileri gösterirler. Bunlara en iyi örnek 2010 yılında gerçekleştirilen ve İran'ın nükleer tesislerinin de hedef alındığı Stuxnet siber saldırısıdır (Fruhlinger, 2018).

Bazı durumlarda her hedef için farklı bir zararlı yazılım üretilmesine ihtiyaç duyulabilmektedir. Bu nedenle siber ordularda ve istihbarat birimlerinde görev yapan, alanında profesyonel olduğu değerlendirilen yazılım uzmanları çalışmaktadır. Söz konusu kuruluşlarda ve teşkilatlarda yazılım uzmanları ve siber güvenlik uzmanları koordineli bir biçimde çalışmakta, talep edilen yazılımın oluşturulması

aşamasında birlikte hareket etmektedirler. Üretilen yazılımın hedef sisteme sızdırılması sonucunda uzaktan erişim imkânıyla hedef sistem hakkında önemli bilgi ve belgeler ele geçirilmektedir. Ayrıca söz konusu yazılımlar yalnızca bilgisayarlar için değil, tüm akıllı telefon veya elektronik cihazlar içinde benzer metotlarla çalıştırılabilmektedir. Zararlı bir yazılım cep telefonlarımıza bulaşmasına müteakip, telefonun tüm yönetimi karşı tarafın eline geçmektedir. Telefonumuzun hafızasındaki mesajlardan, resimlere kadar tüm içerikler saldırganın eline geçmektedir (Keleştemur, 2015:312).

2.3.6. Yığın E-Posta Gönderme

Yığın e-posta gönderme işlemleri günümüzde de neredeyse her gün karşılaştığımız spam mail ismi verilen toplu olarak farklı kişilere gönderilen e-postalardır. Bulk mail ve Junk mail gibi farklı isimlerle de adlandırılmaktadır. Bu eylemi gerçekleştirebilmek için yüz binlerce web sitelerinden, elektronik bültenlerden, müşteri listelerinden, sosyal medyadan, haber gruplarından vb. e-mail adreslerini içeren işletmelerden veri tabanı satın alınmaktadır. Müteakiben çoğunlukla reklam amaçlı olarak, veritabanındaki e-mail kullanıcılarına toplu olarak e-mail gönderilmektedir. Ancak yığın e-mailler bazı durumlarda kasıtlı bir biçimde zararlı yazılımlarla birlikte gönderilmektedir. Söz konusu e-mailler tanımadığımız kişiler veya hesaplardan geldiği için, bağlantıyı açmadan direk gelen kutusundan silmek gerekmektedir. Bu özelliklere sahip e-mailler içeriğinde bulunan zararlı yazılımlar, mevcut sistemde güvenlik programının olması durumunda otomatik olarak tespiti sağlanarak bloke edilmektedir (Alfred, 2016).

Popescu (2013)'ün belirttiği üzere; internet üzerindeki e-mail trafiğinin yaklaşık % 75 'i yığın e-maillerden oluşmaktadır. (Popescu, 2013) Yığın e-mail göndermek için kullanılan servis sağlayıcılarında pek çok çevrimiçi servis aracı bulunmaktadır. Bunların dışında mevcut yazılım sistemlerinde kolayca bulunabilecek programlarda basit bir biçimde yığın e-mail gönderilmesine imkân tanımaktadır. Söz konusu yığın e-maillerden korunmak için tarayıcınızın e-posta istemcisi ile uyumlu bir biçimde çalışan güvenlik programlarını kullanmak gerekmektedir.

2.3.7. İnternet Aracılığıyla Sosyal Mühendislik

Sosyal mühendislik saldırıları genellikle bilgisayar kullanıcısına, bir bilgisayara veya ağa erişmek amacıyla ihtiyaç duydukları bilgileri vermeleri için

çeşitli psikolojik püf noktaları kullanan saldırganlar tarafından gerçekleştirilmektedir. Sosyal mühendislik saldırılarını düzenleyenlerin amacı, kullanıcıları istediklerini vermeleri için kandırmaktır. Sosyal mühendislik saldırılarından korunmanın çok zor olduğu belirtilmektedir. Çünkü tek başına donanım veya yazılımla korunmak mümkün değildir. Yeterli zaman, sabır ve kararlılığa sahip bir sosyal mühendisin, bir işletmenin sistemindeki zayıf noktaları en nihayetinde tespit edeceği değerlendirilmektedir (Çifci, 2017:93).

Günümüzün bilgi çalışanları tarafından kullanılan hizmetler, karmaşık sosyal mühendislik saldırıları için zemin hazırlamaktadır. Kişisel cihazları işyerlerinde ve kurumlarda kullanma yönünde artan eğilim, iş ortamlarında çevrimiçi iletişim ve işbirliği araçlarının kullanımı sorunu daha da arttırmaktadır. Küresel olarak faaliyet gösteren kurumlarda, ekipler artık coğrafi olarak bir arada bulunmamakta, ancak eşzamanlı çalışmaktadırlar. Sanal ortamda gerçekleştirilen iletişim araçları(e-posta, IM, Skype, Dropbox, Linkedln, Lync, vb.) giderek artmaktadır. Bu araçlar potansiyel sosyal mühendislik saldırıları için yeni zemin ve şablonlar oluşturmaktadır. Krombholz ve diğerleri (2014)'ne göre; New York Times ve RSA gibi şirketlere yapılan son saldırılar, sosyal mühendislik saldırılarının etkili ve evrimsel bir adım olduğunu göstermektedir (Krombholz ve diğerleri, 2015:113).

Söz konusu saldırılar neticesinde kullanıcıların bilgi sistemlerine kötü amaçlı yazılımlar yüklenebilmektedir. Kimlik avı e-postalarındaki veya kimlik avı web sitelerindeki bağlantılar veya ekler farklı kötü amaçlı yazılımlar içerebilir (örneğin, anahtar günlüğü, fidye yazılımı ve kripto para birimi madenciliği gibi kötü amaçlı yazılımlar). Kullanıcılar bu bağlantıları tıklarsa veya bu ekleri açarsa, aygıtları kötü amaçlı yazılım tarafından enfekte olabilir, bu da veri sızmasına, veri kaybına veya diğer finansal kayıplara yol açabilmektedir. Ticari markalar, patentler, ticari sırlar, vb. dâhil olmak üzere fikri mülkiyet, bir şirketin başarısı için çok önemlidir. Kurbanlardan elde edilen bilgilerle gerçekleştirilen kimlik avı ve yemleme saldırıları, milyonlarca hatta milyarlarca araştırma ve geliştirme maliyetini temsil edebilecek ve hatta şirketin geleceğini tehdit edebilecek fikri mülkiyet hırsızlığına neden olabilmektedir. Ayrıca saldırıya uğrayan bir organizasyon düşünüldüğünde, bu tip saldırılar markanın itibarını zedeleyebilmekte, müşteri verilerinin korunmasını sağlayamadığından müşterilerin güvenini kaybetmelerine neden olabilmektedir

(CISA, 2018).

2.4. ÜLKELER BAZINDA YAŞANMIŞ SİBER MÜCADELELER VE ULUSLARARASI İLİŞKİLERE ETKİLERİ

2.4.1. İlk İnternet Savaşı: Çeçenistan- Rusya

1994 yılında Rus birlikleri Çeçenistan'ın Grozni kentine operasyon düzenlediler. Ağır silah, araç ve gereçlerle şehre giren Rus askerleri Çeçenistan'ın direnişinin kısa sürede sona ereceğini değerlendirmekteydiler. Ancak gerçek muharebe beklentilerle uyuşmadı ve Soğuk Savaş sonrası dönemde ilk kez askeri bir çatışma internet ortamına yani siber ortama yansımış oldu. Çeçenler neredeyse tüm medya imkân ve kabiliyetlerini ve özellikle interneti araç olarak kullanıp bilgi savaşının ilk örneklerini gerçekleştirerek, savaş ortamında meydana gelen olayları Rusya Federasyonu aleyhine yansıtarak etkili bir propaganda yapmıştır. Bu kapsamda Rusya Federasyonu uluslararası kamuoyu açısından da söz konusu savaş esnasında, insanlık dışı yollara başvuran ve savaş suçu işleyen bir ülke olarak kabul edilmiştir. Bu propaganda internetin ve bilgi sistemlerinin savaş ya da harekât alanı olarak kullanıldığı ilk örneklerden birisi olarak literatüre geçmiştir (Bıçakçı ve Aydın (ed.), 2013).

Söz konusu olay için "ilk internet savaşı" tabiri yapılmaktadır. Fakat bu olayda görüldüğü üzere, Çeçenlerin gerçekleştirdiği mücadelenin bir siber savaştan ziyade siber uzay boyutunda propaganda işlevi gördüğü değerlendirilmektedir. Psikolojik harp enstrümanı olan internet aracılığıyla konvansiyonel muharebe içerisinde bulunan devletin ve savaşı takip eden uluslararası kamuoyunun zihni karıştırılarak, bahse konu devletin itibarının sabote edildiği görülmektedir.

2.4.2. ABD- Çin Arasında Yaşanan Siber Saldırılar

2001 yılında bir Çin savaş uçağı ile ABD Hava Kuvvetleri'ne ait bir casus uçak Güney Çin Denizi semalarında çarpıştı. Bu olay sonucunda birçok ülkenin bilgisayar korsanı "ABD'nin saldırgan tutumlarına karşı kendilerini koruma harekâtı" başlattılar. Honkers Union isminde bir grup Çinli hackerlar Beyaz Saray'ın resmi sitelerini saatler boyunca kapattılar. Ayrıca bu saldırılar neticesinde Kaliforniya Adalet Bakanlığı'nda bulunan bilgisayarlar da virüs gönderilerek

kullanılamaz hale getirilmiştir. Çin savaş uçağı ile ABD casus uçağının havada çarpışması neticesinde Çin savaş uçağı düşmüş, ABD'ye ait casus uçak ise hasar alarak Hainan Adası'na zorunlu iniş yapmak zorunda kalmıştır. Söz konusu olay The New York Times gazetesi tarafından "World Wide Web War I" olarak tanımlanmıştır (Smıth, 2001).

2.4.3. Körfez Savaşı

20 Mart 2003 tarihinde ABD Irak'ı işgal etmeden önce, siber unsurları tarafından Irak Savunma Bakanlığı'nın kapalı devre bilgisayar ağlarına sızdığı ve e-posta sistemi üzerinden Irak askerlerine savaşa başlamadan teslim olmaları yönünde tavsiye içerikli e-posta mesajı gönderdiği belirtilmektedir (Clarke ve Knake, 2012):

"Bu ABD Genelkurmayından size gönderilen bir mesajdır. Bildiğiniz üzere, yakın bir gelecekte Irak'ı işgal edeceğiz. Birkaç yıl önce yaptığımız gibi, sizi tamamen imha edecek bir güçle bunu gerçekleştireceğiz. Size ve askerlerinize zarar vermek istemiyoruz. Amacımız Saddam'ı ve iki oğlunu devirmektir. Zarar görmek istemiyorsanız, tanklarınızı ve zırhlı araçlarınızı sıraya dizerek terk edin. Kendinizi kurtarın. Siz ve askerleriniz evlerinize dönün. Bağdat'ta gerekli rejim değişikliği gerçekleştirildikten sonra siz ve başta Irak birlikleri yeniden göreve çağırılacaktır."

Söz konusu mesaj Irak birliklerinde güveni sarsmıştır ve toplumda bir kaos ortamı oluşturmuştur (Bayraktar, 2015:143). Bu e-maili alan birçok Irak askerinin silah bırakarak ABD ordusu ile savaşmayı tercih etmediği ve ABD uçaklarının Irak ordusuna ait tankları kolaylıkla imha ettiği belirtilmektedir. Konvansiyonel savaşın yanında siber taarruzun da kullanıldığı ilk savaş olarak tanımlanan Körfez Savaşı, gerçekleştirilen siber saldırılar sonucunda Irak askeri birliklerinin güçsüzleştirilmesiyle daha kolay bir şekilde kazanılmıştır (Keleştemur, 2015:312).

2.4.4. Estonya'ya Yapılan Siber Saldırılar

2007 yılında Rusya ve Estonya arasında bazı anlaşmazlıklar yaşanmıştır. Bu anlaşmazlıkların önemli nedeni, 1947 yılında Sovyetler Birliği'ni ve Kızıl Ordu askerini hatırlatmak amacı ile Tallinn Meydanı'na dikilen Rus heykelinin, 2007 yılında Estonya hükümeti tarafından kaldırılması olduğu değerlendirilmektedir.

Estonya, “Avrupa’nın bilgi sistemi en çok gelişen devleti” olarak tanımlanmaktadır. 1991 yılında bağımsızlığını kazanan Estonya’da bu dönemde halkın yarısının temel telefon hatlarına erişim imkânı mevcuttu. Yeni Estonya hükümeti bu konudaki eksikliği tespit ederek, bilgi teknolojileri ve telekomünikasyon alanlarında Ar-Ge çalışmalarını arttırdı. Günümüzde kullanılan Skype’ın oluşturulmasında kullanılan yazılımın patenti Estonya ülkesine aittir. 2006 yılında dünyada ilk kez Estonya hükümeti elektronik ortamda oy kullanma yeniliğini vatandaşlarına sunmuştur. Bu dönemde artık vatandaşların %60’a yakını günlük ihtiyaçlarının büyük bir kısmını interneti kullanarak karşılamak zorunda kalmıştır. Ülkedeki bankacılık hizmetlerinin yaklaşık %96’sı internet üzerinden gerçekleştirilmektedir. Her vatandaşın bankalara ve devlet kurumlarına internet üzerinden bağlanmasına olanak sağlayan ülkede, 345 devlet kurumu sanal dünyada yer almaktadır Ancak bilgi sistem teknolojilerinde önemli gelişmelerin yaşandığı bu süreçte Estonya devletinin, siber savunma ve internet güvenliği üzerine gerekli tedbirleri almadığından alt yapı konusunda zayıf olduğu değerlendirilmektedir.

27 Nisan- 18 Mayıs 2007 tarihleri arasında söz konusu alt yapı zafiyetinden yararlanılarak ilk kez bir ülkeye yönelik olarak sistematik ve çok taraflı siber saldırılar gerçekleştirilmiştir. Siber taarruzların ilk dalgasında finans merkezlerinin ve bankalarının, hükümet kurumlarının, ulaşım alt yapılarının, güvenlik ve medya kuruluşlarının internet siteleri geçici süre ile kullanım dışı bırakılmıştır. Bu dönemdeki saldırılara Estonya devleti tarafından bir takım önlemler alınmaya çalışılsa da başarılı olunamamaştır. 06 Mayıs 2007 tarihinden itibaren gerçekleştirilen ikinci dalgada, finans ve bankacılık sistemleri hedef alınmıştır. Bu saldırılar daha organize ve gelişmiş bir biçimde gerçekleştirilmiştir ve bir milyondan fazla botnet kullanılmıştır. Bu süreçte NATO üyesi olan Estonya devletindeki internet erişimi sekteye uğratılarak birçok eşzamanlı kritik işlemler gerçekleştirilememiştir. Bu kapsamda Avrupa’nın en gelişmiş bilgi teknolojilerine sahip olan ve bu sistemleri yoğun olarak kullanması sebebiyle kendisine “E-Stonia” latifesi (Lesk, 2007) yapılan bu Avrupa ülkesinde devlet otoritesi büyük ölçüde sarsılmıştır (Traynor, 2007:5).

Siber saldırıların kaynağının ve yerinin tespit edilmesi çok zor hatta bazılarının imkânsız olduğundan söz konusu Estonya saldırılarının Rusya tarafından gerçekleştirilip gerçekleştirilmediği ispat edilememiştir. Ancak yaşanan bu süreçte Rusya'daki bazı internet sayfalarında Estonya ülkesindeki internet sitelerine nasıl saldırı düzenlenebileceğine dair bilgiler yer almıştır. Bu bilgilerle amatör bilgisayar kullanıcılarının da siber saldırılara katılması sağlanmıştır (Cavelty, 2012). Estonya devletinin, bu siber saldırılardan sonra ülkede yaşayan 1200 Rus vatandaşını tutuklaması sonucunda, ülkedeki Rus azınlığın gerçekleştirdiği sokak gösterileri yaklaşık olarak 3 ay sürmüştür. Bu gösterilerde beş kişi hayatını kaybetmiştir (News BBC, 2008).

2.4.5. Suriye'ye Yapılan Siber Müdahale

2007 yılında İsrail bir Suriye radarına karşı siber saldırıda bulunmuştur. Bu saldırı literatürde "Operation Orchard" harekâtı olarak yerini almıştır. Bu olayda İsrail jetleri, Türkiye-Suriye sınırına 120 km mesafede bulunan bir binayı bombalamıştır. Clarke (2012) bir çalışmasında, söz konusu binanın uzun süren çalışmaların eseri olan Kuzey Kore- Suriye ortak nükleer tesisi olduğunu belirtmektedir. Bu tesis bir gece içinde yok edilmiştir (Clarke ve Knake, 2012).

Bahse konu İsrail siber saldırısını Friedman ve Singer şöyle açıklamaktadırlar: (Friedman ve Singer, 2014) 2006 yılında Suriye hükümetinden üst düzey bir bürokrat Londra seyahati esnasında taşınabilir bilgisayarını otel odasında bıraktı. Otel odasından ayrıldığında İsrail istihbarat teşkilatı ajanları otel odasına girdi ve siber saldırı amaçlı bir Truva atını söz konusu bilgisayara yüklediler. Suriyeli yetkilinin bilgisayarında bulunan fotoğraflar İsrailliler tarafından incelendiğinde, bir insanın zayıf bilgisayar güvenliğinin çok ciddi sonuçlara neden olabileceği durumu ortaya çıkmıştır. Fotoğraflardan birisinde Suriye Atom Enerjisi Kurumu başkanı Ibraham Othman ve Kuzey Kore devletinin nükleer proje çalışma liderlerinden birisi olan Chon Chibu'nun aynı karede yer aldığı tespit edildi. Anlaşıldığı üzere Suriye, Kuzey Kore'nin desteğiyle nükleer bomba üretiminde önemli bir element olan plütonyumun işlenmesi için al Kibar'da gizlilik içerisinde bir tesis inşa etmekteydi. 6 Eylül 2017 tarihinde 7 İsrail savaş uçağı Suriye hava sahasına girerek fotoğraflarla yeri tespit edilen tesisi füzelerle vurarak yerle bir

ettiler. İsrail savaş uçaklarının Suriye hava sahasında kaldıkları süre içerisinde, hava savunma sistemleri hiçbir reaksiyon göstermemiştir."

Düzenlenen savaş uçağı saldırısı Suriye radarları tarafından tespit edilememiştir. Yapılan incelemede İsrail'in Suriye hava savunma ağına sızması sonucu bir yazılım vasıtasıyla radar izleme merkezine aktarılan görüntüyü değiştirdiği tespit edilmiştir. Saldırıyı yapan İsrail uçaklarının görüntüsünü, Suriye hava savunma sistemleri yetkililerine her şey normalmiş gibi izlettirdiği anlaşılmıştır. İsrail devletinin Suriye hava savunma radarlarının kontrolünü ele geçirmesini sağlayan bu siber saldırıdan anlaşılacağı üzere, siber taarruz ile radarları etkisiz hale getirmek, klasik silahlı saldırı düzenlemeyerek çeşitli risklere girmekten tasarruf sağlanabileceği anlamına gelmektedir. Bu kapsamda söz konusu olay siber taarruzların, askeri hedeflere gerçekleştirilen klasik saldırılarla koordineli bir biçimde kullanılabileceği görüşüne de örnek teşkil etmektedir (Hilal, 2018:174).

2.4.6. Gürcistan'a Yapılan Siber Saldırılar

Rusya tarafından 7 Ağustos 2008 tarihinde Gürcistan'a yönelik olarak gerçekleştirildiği iddia edilen siber taarruzlar, Rus ordusunun konvansiyonel saldırısını desteklemek amacıyla planlanması konusunda, Gürcistan ile Rusya arasındaki geleneksel savaşı, uluslararası ilk hibrit savaş örneği durumuna getirmesi açısından önemlidir. Söz konusu olayı daha iyi anlamak için tarihsel arka planını incelemek gerekmektedir. Bilindiği üzere Güney Osetya ve Abhazya, Sovyetler Birliği'nin dağılmasından sonra de facto bağımsız bölgeler halinde varlıklarını sürdürmüşlerdir. 2008 yılında gerçekleşen bazı milliyetçi provokasyon neticesinde, 7 Ağustos 2008'de Gürcistan Silahlı Kuvvetleri ülkenin toprak bütünlüğünü sağlamak amacıyla Güney Osetya'ya karşı operasyona başlaması neticesinde, Rus askeri birlikleri de Osetya sınırlarına girmişlerdir. Rusya müteakip harekâtta Gürcistan'ı işgal etme planlarını gerçekleştirmeye başlamıştır. Rusya ve Gürcistan arasında yaşanan çatışma ortamının arka planında Gürcistan'ın Batı Blok'una yakınlaşması ve NATO'ya tam üye olma çabalarının olduğu birçok kaynakta belirtilmektedir. Gürcistan'a yapılan siber taarruzlar 8 Ağustos 2018 tarihinde Estonya saldırılarına benzer biçimde devletin kritik altyapılarını hedef alan ''DDoS'' taarruzları şeklinde başlamıştır ve spam e-posta şeklinde devam etmiştir. Bu saldırıların gerçekleştirildiği

siteler incelendiğinde, söz konusu sitelerin ABD vatandaşlarına ait çalınan kredi kartlarıyla Rusya ve Türkiye'de açıldığı belirlenmiştir (Goble, 2009:191).

Gürcistan'a gerçekleştirilen siber saldırılar, Estonya'ya yapılan saldırılardaki gibi devletin hükümet, finans ve medya sektörlerini kullanılamaz hale getirmek amacıyla yapılmıştır. Fakat bahse konu dönemde Gürcistan nüfusunun yalnızca %11'inin internet kullanması nedeniyle yani Gürcistan'ın Estonya'ya kıyasla ağlanma ve e-devlet kapasitesi düşük olduğu için söz konusu saldırılar kısmen etkili olmuştur. Ayrıca siber saldırılar yapıldığı dönemde Gürcistan devletinin NATO üyeliği hâlihazırda gerçekleşmediği için güvenlik konusunda ittifaktan doğrudan yardım alamamıştır fakat NATO'nun siber güvenlik uzmanlarından söz konusu saldırılara karşı koyma konusunda doğrudan destek almıştır. Bunun neticesinde Gürcistan hükümetinin siber verilerini üçüncü ülkelere taşımasıyla söz konusu siber saldırılar yaklaşık bir hafta içerisinde sona erdirilmiştir (Bıçakçı S. , 2012:103).

Tıkk (2010)'a göre; Gürcistan'a yapılan siber saldırılardan çıkartılabilecek önemli bir sonuç, literatürde genel kabul görüldüğü üzere bu siber saldırıların hibrit savaş niteliğine sahip olan ilk sıcak çatışma olduğu görüşüdür. Rusya, askeri birliklerin operasyonlarının hemen öncesinde Gürcistan'ı siber taarruzlarla yıpratarak işgale hazırlamaya çalışmıştır. İlerleyen dönemde Rusya, Gürcistan ve Estonya siber saldırılarından kazandığı tecrübe ile 2012 yılında yeni bir savaş stratejisi oluşturmuştur. Gerasimov doktrini veya Hibrit savaş konsepti diye adlandırılan bu strateji Rusya tarafından 2014 yılında Ukrayna'ya yönelik icra edilen askeri harekât sırasında tüm yönleriyle uygulanmıştır (Tıkk, 2010).

2.4.7. Stuxnet Solucan Virüsü

2010 yılı Haziran ayında Stuxnet isimli bir virüs solucanın İran'ın nükleer tesislerindeki bilgi sistemlerine etki yaparak çalışmaları sekteye uğrattığı tespit edilmiştir. Bu zararlı solucanın, Siemens marka komuta sistemlerini etkilediği bildirilmiştir. Stuxnet virüsünün İran'ın Natanz ve Buşehr nükleer tesislerini etkilediği iddia edilmektedir. İran devlet yetkilileri bu solucan virüsünün çalışanların bilgisayarlarına bulaştığını ve yaklaşık 30 bin civarında bilgisayarın etkilendiğini belirtmiştir. Söz konusu saldırı, siber taarruzların yıkıcı etkisini gösteren önemli bir

olay olarak değerlendirilmektedir (Çifci, 2017:93).

Stuxnet saldırısı ile SCADA sistem (merkezi denetleyici kontrol ve veri toplama sistemi) olarak adlandırılan, endüstriyel merkezi sistemleri hedef alınmıştır. Solucan, Finlandiya ve İran'da üretilen 708-1310 Hertz frekans aralığında çalışan çeviricileri odak almaktadır. Bu çeviricileri bulduğu zaman çıkış frekansını yüksek miktarda artırarak sistemin arızalanmasına neden olmaktadır. Söz konusu çeviriciler sadece İran'da değil diğer ülkelerde de bulunmaktadır (Shearer, 2010).

Tablo 4: Stuxnet Virüs Solucanından Etkilenen Ülkeler

Ülkeler	Etkilenen Bilgisayar Yüzdesi
İran	58,85
Endonezya	18,22
Hindistan	8,31
Azerbaycan	2,57
ABD	1,56
Pakistan	1,28
Diğer	9,2

Kaynak: (Shearer, 2010)

Karmaşık bir yapıya sahip olan virüs solucanı sadece devlet desteğiyle ve devlet kurumunda çalışan uzmanlar tarafından yazılabileceği iddia edilmektedir. Virüsün, normal kullanıcıların bilgisayarlarına etki etmediği belirtilmiştir. İran'ın kapalı ağ sistemi olarak kullandığı nükleer santral sistemine harici USB bellek kullanılarak (tesiste çalışan bir personel tarafından kasıtsız veya kasıtlı olarak) bulaştırıldığı değerlendirilmektedir. Solucan virüs, bulaştığı bilgisayar sistemlerine ait verileri kaydederek, "todaysfutbol.com" ya da "mypremierfutbol.com" adreslerine göndermiştir. Bu kapsamda bu zararlı solucan yazılımını yazanlar, birçok devletin önemli endüstriyel sistemlerine ait kritik verileri ele geçirmiştir. Stuxnet solucanının Çernobil'e benzer bir nükleer faciaya neden olabileceği iddia

edilmektedir (Associated Press, 2012).

The New York Times (2011)'de yazılan bir makalede, İsrail'in Necef Çölü'nde bulunan gizli ve çok iyi bir biçimde korunan nükleer üssünde, İran'ın nükleer tesislerinde bulunan sistemlerle aynı özelliklere sahip sistemler kurularak siber taarruz testlerinin yapıldığı ileri sürülmektedir. Söz konusu testlerin İsrail ve ABD tarafından ortaklaşa yapıldığı, İngiliz ve Almanların da yardım ettiği belirtilmektedir (David E. Sanger ve diğerleri, 2011).

Stuxnet solucanı yalnızca bilgisayarların değil; endüstriyel merkezi kontrol sistemlerinin ve kapalı ağ sistemlerinin hedef alınması ve söz konusu saldırıda başarılı sonuç alınması bakımından literatürde önemli bir yere sahiptir. Siber saldırılar için önlem almayan ve en kritik bilgi sistem unsurlarını dahi ithal eden devletler için dikkate alınması gereken bir uyarı niteliğindedir. Bu saldırıdan sonra İran'da siber güvenlik alanında çok ciddi bir kurumsal yapılanma başlamıştır ve İranlı siber korsanlar tarafından 2012-2013 yıllarında ABD'ye yönelik önemli saldırılar gerçekleştirilmiştir (Çifci, 2017:93).

2.4.8. Shady RAT Olayı

Shady RAT, 2006 yılında başlayan ve 5 yıl süre ile devam eden siber casusluk eylemidir. Ağustos 2011'de McAfee elektronik güvenlik firması tarafından yazılan raporda saldırıların Çin tarafından gerçekleştirildiği öne sürülmektedir. Siber saldırılarda ABD, Tayvan, Hindistan, Vietnam ve Güney Kore'nin de bulunduğu ülkelere ait yaklaşık 60 civarında savunma sanayi firmalarının sistemlerine sızılarak veri çalındığı belirtilmektedir. McAfee'ye göre siber saldırılar devlet destekli gerçekleştirilmiştir. 5 yıl boyunca süren veri çalma işlemleri ile endüstriyle alakalı patentleri içeren petabytelarca bilgi çalınmıştır. Devlet sırlarının, doğal kaynaklarla enerji üretimi yapan firmalardan araştırma planlarının, teknoloji firmalarından tasarım planlarının çalındığı belirtilmektedir (Sterling, 2011).

2.4.9. Ukrayna'ya Yönelik Siber Saldırı

Rusya'nın Ukrayna'ya ilk müdahalesi 23 Şubat 2014 tarihinde Rus askeri birliklerinin, Ukrayna ve Kola Yarımadası sınırında 150 bin askerin gerçekleştirdiği bir tatbikat ile başlayan bir süreçtir. Söz konusu tatbikatın güç gösterisi yapmak amacıyla icra edildiği değerlendirilmektedir. Ayrıca bu süreçte, Rusya meclisi Kırım'a gerçekleştirilmesi planlanan askeri harekâta izin veren bir yasayı 1 Mart 2014 tarihinde onaylamıştır (Gürcan, 2014).

Bununla birlikte, Ukrayna devlet yetkilileri tarafından 2014 yılı Şubat ayının sonlarından itibaren, mevcut mobil telefon operatörlerinin ve internet hatlarının saldırıya maruz kaldığını, büyük oranda sistemin geçici olarak kullanılamaz hale geldiğini ve Ukraynalı milletvekilleri ve üst düzey kamu yetkililerine ait akıllı cep telefonlarının "hacklendiği" ifade edilmiştir. Bu gelişmelere ilave olarak "CyberBerkut" isminde, Rus devleti yanlısı olması ile tanınan bir hacker grubu tarafından, Ukrayna Savunma Bakanlığı'na, Ukrayna resmi sitelerine, NATO'nun Ukrayna ile ilgili faaliyet gösteren internet erişimlerine, medya kuruluşlarına siber saldırılar düzenlenmiştir. Söz konusu siber saldırıların, Gürcistan ve Estonya'ya yapılan siber saldırılara kıyasla daha karmaşık planlandığı ve daha etkili olduğu görülmüştür. Siber ataklarda kullanılan "Snake/Uroboros" virüsü, Ukrayna'nın resmi kurumlarına gerçekleştirilen saldırılarda son derece etkili olmuştur (Weedon ve Galante, 2014).

Kelly (2014)'e göre; Ukrayna devletine yapılan siber taarruzların diğerlerine göre etkili olmasının bir diğer sebebi ise, Ukrayna'nın mevcut internet altyapısının nitelikleriyle ilgilidir. Ukrayna hükümetlerinin sınırlandırıcı çabalarına rağmen, Ukrayna'nın liberal ve özgür internet kullanım politikası mevcuttur. Ayrıca küresel internet sistemi ile bağlantısı hem uydu üzerinden, hem de karasal bir yapıyla sağlanmaktadır. Bu sebeple de hem küresel internet sistemiyle çeşitli bağlantılarla erişim halinde olan, hem de internet kullanım politikaları gereği serbestlik ilkesi bulunan Ukrayna'nın, Rusya tarafından gerçekleştirilen siber saldırılar sırasında internet trafiğini dış dünyaya kapatmaya yönelik çalışmaları başarısız olmuştur. Bunun neticesinde bahse konu siber taarruzlar etkili bir biçimde gelişmiş ve yaygınlaşmıştır (Kelly, 2014).

Mevcut siber taarruzlarla eş zamanlı bir biçimde, Rusya istihbarat servisinin kışkırtmaları ile eylem yapmaya teşvik edilen Rus taraftarı sivil protestocular Sivastopal şehrinde sokak eylemleriyle Rusya'ya bağlanma isteklerini dile getiren mitingler düzenlemeye başlamışlardır. Diğer yandan, Kırım'da bulunan Rusya yanlısı Russkoye Yedinto Partisi, Kırım'da bulunan Rusların güvenliğini sağlamak iddiasıyla iki hafta gibi kısa bir sürede 10 bin silahlı kişiden oluşan bir örgüt oluşturduğunu ilan etmiştir. Söz konusu grupların organize bir şekilde ve bu kadar kısa bir sürede silahlanmaları dikkate alındığında, Rusya istihbarat servisi ve Rus özel kuvvetleri ile dolaylı bir şekilde irtibatta oldukları değerlendirilmektedir.

Darıcalı (2017)'ye göre; mevcut siber saldırılar ile yıpratılan Ukrayna'ya yönelik konvansiyonel savaş başlamadan önce, Kırım'ın küresel sistemden ve Ukrayna'dan izole edilmesi amaçlanan planlama devreye sokulmuştur. 18-28 Mart 2014 tarih aralığında yoğunlaşacak biçimde, Ukrayna'nın resmi GSM operatörü olan Ukrtelecom'un mevcut altyapısı çökertilerek, bu sayede Kırım'da bulunan mobil cihazların çatışmanın başlangıç günlerinde aktif olarak kullanılması engellenmiştir. İnternet kısmen yavaşlatılmış, kritik altyapıları kullanılmaz hale getiren siber ataklar gerçekleştirilmiş, Karadeniz'de bulunan Rus donanma gemilerinden Kırım'daki radyo ve televizyon yayınlarını kesecek sinyaller gönderilmiştir ve "kimliği tespit edilemeyen şahıslar" tarafından Kırım'daki tüm haberleşme ağı optik kablo alt yapısı tahribata uğratılmıştır. Bunların haricinde 2015 yılı Aralık ayında Ukrayna'nın Prykarpatyalenego Bölgesi'ndeki bir enerji santraline siber saldırı düzenlenmiştir ve bu sebeple söz konusu bölgede belirli bir süre elektrik kesintisi yaşanmıştır. Ukrayna Savunma Bakanlığı tarafından yapılan konuya ilişkin açıklamada; "yaşanan elektrik kesintilerinin siber saldırılar nedeniyle gerçekleştiğinin değerlendirildiği, saldırıların arkasında Rusya devletinin olabileceği ve araştırmaların devam ettiği' kamuoyuna bildirilmiştir. Rusya" tarafı ise mevcut konuyla ilgili olarak hiçbir açıklama yapmamıştır (Darıcılı, 2017:112).

Uluslararası ilişkiler disiplini açısından incelendiğinde, Ukrayna'ya yapılan ve Rusya tarafından gerçekleştirildiği iddia edilen bahse konu siber saldırılar, Rusya'nın hibrit savaş kapsamında oluşturmaya çalıştığı yeni nesil savaş konseptinin başarılı bir uygulaması olarak değerlendirilmektedir. Ukrayna'ya düzenlediği siber müdahale

sonucunda Rusya, yaklaşık 20 yıl öncesinde geliştirmeye başladığı siber güvenlik hedefleri ile uyumlu bir biçimde ve son derece etkili bir siber taarruz kapasitesine ulaştığını somut bir şekilde ortaya koymuştur. Bu saldırı Rusya'nın sahip olduğu imkân ve kabiliyetlerin başta ABD ve ayrıca diğer ölçekte tüm devletler içinde dikkate alınması gereken bir tehdit haline geldiği değerlendirilmektedir. Rusya'nın bahse konu siber potansiyelinin, diğer ülkelerin de siber ortamda ulusal savunma ve taarruz kapasitelerini geliştirmelerine ve daha kapsamlı planlamalar yapmalarına sebep olduğu da değerlendirilmektedir.

2.4.10.Rusya- Türkiye Siber Çatışmaları

24 Kasım 2015 tarihinde Türkiye'nin hava sahasını ihlal eden bir Rus savaş uçağının Türk F-16'ları tarafından vurularak düşürülmesi sonucunda, Rusya ve Türkiye arasında önemli boyutlara ulaşan siyasi bir gerginlik dönemi başlamıştır (BBC, 2016). Söz konusu siyasi gerginlik, 13 Aralık 2015 tarihinde Türkiye'ye yapılan siber saldırılarla ile yeni bir boyut kazanmıştır. Bu saldırılarla "tr" uzantılı web sayfaları hedeflenerek, e-devlet sistemi, kamu kurumları ve bankacılık sistemleri gibi kritik elektronik altyapıların yıpratılması hedeflenmiştir. Söz konusu siber taarruzlar "DdoS" atakları şeklinde gerçekleştirilmiştir (Kolcu, 2015).

Siber ataklar devam ettiği sırada Anonymous isimli hacker grubu 23 Aralık 2016 tarihinde internete bir video servis ederek söz konusu saldırıları üstlenmiştir. Bu videoda; "siber atakların Anonymous hacker grubu tarafından gerçekleştirildiği, saldırının Türkiye hükümetinin Irak ve Şam İslam Devleti (DAEŞ)'e destek vermesine bir misilleme olarak yapıldığı, DAEŞ örgütüne mensup teröristlerinin Türkiye'de tedavi edildiği, Türkiye'nin DAEŞ'e finansal destek verdiği ve petrol aldığı ve siber saldırıların uzun bir süre devam edeceği" belirtilmiştir. Ancak bu paylaşımın Rusya istihbarat servisi tarafından planlı bir şekilde gerçekleştirilen "sahte bayrak (false flag)"[3] yani algı operasyonu olduğu değerlendirilmektedir (Darıcılı, 2017:112).

Bu kapsamda "DdoS" siber saldırılarının kimin tarafından planlandığı ve

[3] False Flag Operation: İstihbarat servislerinin ya da gizli örgütlerin halkı yönlendirmek, kışkırtmak, bölücü ve yıkıcı etki yaratmak amacıyla, kendi yaptıkları operasyon ve faaliyetleri hedefteki kişiler veya kurumlar gerçekleştiriyor gibi göstererek kamuoyunu aldatmak için gerçekleştirdikleri gizli planlamalara verilen isimdir. (Rationalwiki, 2017)

gerçekleştirildiği net bir şekilde ortaya koyulamamasına rağmen, Türkiye'ye yapılan bu siber saldırının yaklaşık 400.000 civarında internet sitesini etkileyecek potansiyelinin olması, bu sitelerin kamu kuruluşları,üniversite, e-devlet, askeri veya yerel şirket siteleri gibi kritik yapıların hedeflenmesi, Türkiye ve Rusya arasında uçak düşürülmesi faaliyetine bağlı olarak gelişen gerginlik ortamı ve siber saldırılar ile Türkiye'de bulunan tüm bilgi sistemleri değil de sadece ".tr" uzantılı sitelerin hedeflenmesi, gerçekleştirilen saldırıların yalnızca mesai saatleri içerisinde gerçekleşmesi, Rusya'nın buna benzer siber saldırılar kapsamındaki olumsuz intibası saldırının Rusya devleti ile bağlantılı bir şekilde gerçekleştirildiği ihtimalini arttırmıştır (Murcia, 2015).

Teknik açıdan değerlendirilecek olursa, gerçekleştirilen siber saldırılar basit bir formatta hazırlanmıştır. Bunun nedeninin arka planı gizleyerek, söz konusu saldırıyı bir hacker grubu tarafından gerçekleştirilmiş gibi göstermeye çalışma amacı olduğu değerlendirilmektedir. Fakat siber atakların haftalarca sürmesi için güçlü bir motor sistemine sahip donanımlara ihtiyaç duyması, bu potansiyelde sunucuların amatörler tarafından uzun süreli çalıştırılmasının teknik açıdan mümkün olmaması ve söz konusu teknik kapasitenin yalnızca bir devletin desteği ile gerçekleştirilecek düzeyde olması nedeniyle saldırının Rusya devletinin desteği ile gerçekleştiği tahmin edilmektedir (BBC, 2015).

Türkiye maruz kaldığı siber saldırılara cevap olarak, yurtdışı internet trafiğini keserek yurtdışından "tr" uzantılı internet sitelerine ulaşımı engellemiştir. Bunun haricinde Türkiye, saldırı döneminde hizmet veren kurumları siber saldırılardan korumak için saldırıya maruz kalan kurumun operatörünü değiştirerek kamu hizmetinin sürekliliğini sağlamaya çalışmıştır. Ayrıca saldırıya maruz kalan DNS Server'larını geçici olarak Hollanda'ya kopyalayarak siber saldırıların boyutu hafifletilmeye çalışılmıştır (Darıcılı, 2017:112). Arslan (2015)'e göre; söz konusu siber saldırılara Türkiye gündeminde yeterli önem gösterilmemiştir. Söz konusu durum Türk kamuoyunun siber saldırı, siber savaş ve siber güvenlik gibi kavramlara olan yabancılığı ile ilgilidir. Türkiye'deki internet kullanıcıları için, internet öncelikle sosyal medyanın kullanılması, e-posta haberleşmesi ve oyun oynamak gibi basit işlemlerin gerçekleştirilmesi anlamına gelmektedir (Arslan, 2015).

Uluslararası ilişkiler disiplininden ele alındığında Türkiye'ye yapılan siber saldırılar, Rusya'nın tarih boyunca Gürcistan, Estonya, Kırgızistan, Litvanya ve Ukrayna'ya yönelik olarak gerçekleştirmiş olduğu siber saldırılar ile benzer nitelikler içermektedir. Bütün bu siber saldırılarda olduğu gibi Türkiye'ye yapılan saldırı da "DdoS" atakları olarak, Türkiye'nin kritik altyapılarına zarar vermeye yönelik olarak planlanmıştır. Siber saldırıların başlangıcı uçak düşürme olayının hemen sonrasıdır. Bu kapsamda söz konusu saldırı ile Rusya'nın siber potansiyelini kullanarak, Türkiye'yi ekonomik tedbirler ve diplomatik baskılarla birlikte zor duruma sokmak istediği değerlendirilmektedir. Bu saldırılara ilave olarak Rusya'nın Türkiye'ye yönelik olarak basın, kamuoyu ve sosyal medyayı da kullanarak psikolojik bir savaş başlattığı da görülmektedir. Bu süreçte Rusya'nın bilgi ve haberleşme savaşı enstrümanlarını kullanma açısından ulaştığı yeni boyutu göstermesi bakımından da ayrı bir analiz yapılmasının literatüre katkı sağlayacağı değerlendirilmektedir.

2.5. SONUÇ

Bilgi/Enformasyon savaşlarının artarak devam ettiği günümüzde, özellikle elektronik ve teknolojik istihbarat başta olmak üzere koruyucu güvenlik tedbirlerinin önemi daha da artmıştır. Bilgi ve haberleşme güvenliğini sağlamanın en önemli aşaması, haberleşme araçlarının emniyet ihtiyacını ve sistemlere yönelik tehdit unsurlarını belirleyerek analiz işlemleri gerçekleştirmektir. Söz konusu tehdit unsurları, elektronik ve diğer araçlara nüfuz etmeyi, gizlilik dereceli bilgilere ulaşmayı, iletişim akışını kesmeyi, bilgi sisteminin içerisine yanlış veya sahte bilgi sokmayı amaçlamaktadır.

İnternet ve bilgi sistemlerinin yaygınlaşması, bilgisayarların taşınabilir sistemlere dönüşmesi ve akıllı telefon teknolojisi sayesinde, internetin oluşturduğu imkân ve kolaylıklar günlük yaşamın ötesine taşınarak ekonomi, askeri ve siyasal boyutlarda da yeni bir güç ve tehdit kavramının ortaya çıkmasına neden olmuştur. Ayrıca söz konusu durum güvenlik yaklaşımlarında ve tartışmalarında "siber güvenlik", "siber uzay", "siber saldırı", "siber terörizm" şeklinde tanımlanan yeni kavramların da ortaya çıkmasına neden olmuştur. Siber saldırılar gerçekleştirilirken kullanılan saldırı metotları basit yazılımlardan oluşmaktadır. Bunların bir kısmı siber korsanlar tarafından gerçekleştirilirken bir kısmı da bazı ülke hükümetlerinin zımni

onayı ve desteği ile yapılmaktadır. Ancak, internetin sınırsız doğası sayesinde, bu grupların birçoğunun konumunu ve saldırıları gerçekleştiren olduğunu tespit etmek çok zordur. Günümüz güvenlik tehditlerinin kapsam ve ciddiyetleri genişlemiş ve siber güvenliğin gelecekte uluslararası çatışmaları nasıl tanımlayacağı tüm toplum tarafından merak edilen bir yaklaşım konusu olmuştur.

ÜÇÜNCÜ BÖLÜM

ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ

3.1. ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİNİN DEĞERLENDİRİLMESİ

Siber ortamın tek bir rejim tarafından yönetilmesi durumunun geçerli olmadığı günümüzde, ülkelerin uluslararası bir anlaşma yaparak siber uzayı kontrol altına almaktan kaçınmaları, gevşek bir işbirliği durumunu tercih etmeleri ve siber ortam kaynaklı saldırılara karşı koyabilmek amacıyla hükümetlerin giderek daha fazla ekonomik yatırım yapmaları neticesinde siber uzayda yaşanan gelişmelerin ülkelerin uluslararası ortamdaki rolünü ve sorumluluğunu azaltmadığı, bunun aksine arttırmakta olduğu değerlendirilmektedir.

Bahse konu değerlendirmeler ve gelişmeler kapsamında, çalışmamızın bundan sonraki aşamasında sırasıyla ABD, Çin, Rusya Avrupa Birliği ve Türkiye'nin siber güvenlik stratejileri karşılaştırmalı biçimde ve geçmiş de yaşanan örnek olayların detaylarını incelemek suretiyle analiz edilecektir. Söz konusu analizler sonucunda siber ortamda gerçekleşen gelişmelerin, uluslararası ilişkiler literatürü açısından yeni bir güvenlik kavramı olarak görülmesinin ve geniş kapsamlı analiz çalışmalarının yapılmasının gerekliliği belirtilmeye çalışılmıştır.

3.1. AMERİKA BİRLEŞİK DEVLETLERİ

ABD'nin 20. yüzyılın başlarından itibaren askeri, siyasi, kültürel ve ekonomik alanda gerçekleştirdiği önemli gelişmeler sonucunda, günümüzde bilgi teknolojileri alanında dünyanın lider ülkesi olduğu değerlendirilmektedir. Bu alandaki gelişmişlik düzeyinin dolaylı olarak siber uzayda da ABD'nin öncü ülkelerden biri konumuna gelmesine zemin hazırladığı değerlendirilmektedir.

3.1.1. İlk Çalışmalar ve Strateji Belgeleri

ABD'nin siber güvenlik stratejisinin temelleri 1930'lu yıllara

dayandırılmaktadır. Bu yıllarda tarihte ilk işlevsel bilgisayar olduğu değerlendirilen ve Alman Deniz Kuvvetleri'nin 1920 yılında ürettiği "ENİGMA" isimli kripto cihazının muadili, ABD tarafından 1930'lu yıllarda ''SIGIBA'' ismi ile üretilmiştir. 1940'lı yıllarda ABD'de ''Atanasoff Berry Computer'' şirketi tarafından ilk dijital elektronik bilgisayar icat edilmiştir. 1950 yılında ise "International Business Machines (IBM)" şirketi bilgisayar dili olan "FORTRAN"ı oluşturmuşlardır, ayrıca bu yıllarda ilk bilgisayar çipleri de ABD tarafından kullanılmaya başlanmıştır (Bıçakçı S. , 2012:103).

Bu gelişmelerle birlikte, ABD, SSCB ile teknoloji alanında rekabet edebilmek amacıyla 1958 yılında "İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency/ARPA)'nı kurmuştur. ARPA bünyesinde yapılan çalışmalar balistik füze savunması, uzay araştırmaları ve dünya üzerinde nükleer çalışma yapılan coğrafi koordinatların tespit edilmesi gibi konuları da kapsamaktadır. 1967 yılında ARPA'ya hizmet veren ve çalışma yürüten bilim insanlarını bir araya getiren bir ağ teknolojisinin oluşturulmasıyla birlikte, bahse konu projenin internet tarihinin temellerini attığı değerlendirilmektedir. Ayrıca bu çerçevede ARPA projesi, ARPANET olarak isimlendirilmiştir (Rouse, 2017).

Ayrıca 1962 yılında yaşanan Küba Krizi sonucunda, olası bir nükleer savaş çıkması durumunda gerçekleştirilecek saldırılardan ARPANET'in etkilenmemesi için ne gibi önlemler alınmasının gerektiği şeklinde çalışmalar yapılmaya başlanmıştır. Bu çalışmalar sonucunda Paul Baran'ın, fiziksel saldırılar sonrasında elektrik bağlantısı sağlayarak iletişimi sürdürebilecek bir ağ altyapısının oluşturulabileceği görüşünü ortaya koyması büyük bir buluş olan internetin temellerini atılmasına neden olmuştur. Farklı noktalarda çalışan ağlar belirtilen sisteme göre düzenlenmiştir. Müteakiben söz konusu ağ alt yapısı ile birbirine bağlı olan ARPANET, öncelikle İngiltere'de bulunan ticari ağ ve Fransa'da bulunan araştırma ağı ile birleştirilmiştir. Bu kapsamda internetin ülkeler arası boyutlara ulaşan çekirdek altyapısı oluşturulmuştur. İnternetin kullanılmaya başlanmasına müteakip ise 1970 yılında ''creeper'' ismindeki virüs ve aynı zamanda ilk bilgisayar solucanı olan yazılım tarafından ARPANET olumsuz bir şekilde etkilenmiştir. Bahse konu solucan siber uzayda, ilk olası tehdit ve siber saldırı aracı olarak değerlendirilmiştir (Thomas, 1974).

Avrupa Nükleer Araştırma Örgütü'nde çalışan araştırmacıların, siber uzaydaki bilgiye kolayca erişebilmek amacıyla geliştirdiği "world wide web" yani kısaltması "www" olan format ile birlikte, internet ortamında bilgisayarlar ve diğer tüm dijital cihazlar tarafından sunulan web sayfalarının tasarlanması ve ziyaret edilmesi gibi imkânlar sağlanarak internetin ilk olarak ABD olmak üzere, uluslararası alanda da hızla gelişmesine olanak sağlanmıştır. Söz konusu gelişmelerin uzantısı olarak, 1997 yılında Stanford Üniversitesi'nde öğrenci olan Sergey Brin ve Larry Page isimli iki genç, tarihte ilk arama motoru olan "google"ı kurmuşlardır (Toprak, 2015).

Bu kapsamda çalışmamızın birinci bölümünde belirttiğimiz üzere realist teorinin politik köklerini insan doğasında arayan, uluslararası ilişkileri temel olarak "güç" ve doğrudan bu terimle örtüşen "çıkar" kavramı çerçevesinde açıklayan bir teori olduğu unutulmamalıdır. Ayrıca Waltz'un; uluslararası sistemin anarşik bir süreçten oluştuğunu ve mevcut sistemde devletlerin egemenliğini ve güvenliğini muhafaza etmeyi amaçla dıklarını, söz konusu anarşik yapının devletler arasında güvensiz bir ortam oluşmasına zemin hazırladığı ve mevcut bu durumun da ülkelerin uzun süreli işbirliği yapmalarına engel teşkil ettiği düşüncesini hatırlatmak gerekmektedir. ABD'nin Soğuk Savaş yıllarında Rusya ile giriştiği askeri, ekonomik, bilimsel ve uzay alanlarındaki büyük rekabetin sonucu olarak, realist varsayımlara uygun biçimde, söz konusu iki ülkenin işbirliği imkânları kısıtlanmış, silahlanma kapasitelerine büyük yatırımlar gerçekleştirmelerinin önü açılmış ve tüm bunların neticesinde uluslararası sistem daha güvensiz bir yapıya bürünmüştür. ABD'nin, Rusya ile yaşadığı bahse konu rekabette avantaj sağlamak amacıyla günümüze kadar uzanan modern ağ teknolojilerinin kökenlerini oluşturan teknik ve bilimsel gelişmeleri teşvik etmek suretiyle, siber ortamın oluşturulmasına da önemli katkılar sağladığı değerlendirilmektedir (Darıcılı, 2017:112).

3.1.2. Başkan Bill Clinton Dönemi

ABD 1990 yılından itibaren siber güvenlik konusunda çok sayıda belge, strateji, resmi plan ve doktrin ortaya koymuştur. Bunlardan, dönemin ABD başkanı Bill Clinton tarafından 1995 yılında yayınlanan "13100 Numaralı Başkanlık Direktifi" siber güvenlik konusuna dikkat çeken ilk resmi belge olduğu için önemi büyüktür. Söz konusu belgenin büyük bir bölümünün de gizli tutulmasıyla birlikte,

belgede Bill Clinton, başsavcılık makamından devletin kritik altyapılarına ve ağ sistemlerine gerçekleştirilmesi muhtemel herhangi bir siber saldırıya karşı mevcut hazırlık durumunu inceleyen bir çalışma yapmasını istemiştir. Müteakiben yapılan çalışma sonucunda hazırlanan raporda, geçmişte yaşanan siber saldırıların gücünün hâlihazırda ABD'nin kritik altyapılarını bütünüyle çökertecek seviyede olmadığı fakat sistemlere zarar verebileceği belirtilmiştir. Ayrıca bu raporda kritik alt yapıların olası siber saldırılara karşı korunması amacıyla, kamu ve özel sektörlerin birlikte hareket etmesi gerekliliğine vurgu yapılmıştır (Clinton, 1998).

ABD'nin federal bir sistemle yönetilmesi ve mevcut bu sistemin oluşturduğu birbirinden bağımsız karar mekanizmalarının var oluşu, siber güvenlik konusunda faaliyet gösteren kuruluş ve kurum miktarının çokluğu, devlet yönetiminde iktidara gelen hükümetlerin değişen politika öncelikleri gibi nedenlerle, ABD'nin 1990'lı yılların başından itibaren siber güvenlikle ilgili çok sayıda belge, strateji, resmi plan, başkanlık emri ve doktrin ortaya koyduğu görülmektedir. Söz konusu resmi belgelerden süreçleri belirleyici ve önemli olanları çalışmamızda analiz edilmeye çalışılacaktır.

Bu belgeleri ve ABD başkanlarını da ele alarak konuyu inceleyecek olduğumuzda; Clinton'ın başkanlık döneminde yani 1993-2001 yılları arasında yapılan siber güvenlik çalışmalarında, uluslararası siber suçlarla mücadele, kritik alt yapıların korunması ve siber güvenlik konusunda ülkeler arasında işbirliğinin gerçekleştirilmesi gibi hususlara vurgu yapıldığı görülmektedir. George Bush döneminde yani 2001-2009 yılları arasında ise ABD'nin siber güvenlik konusunda, bu alanı askeri güç olarak kullanma ve siber uzayı militarize etme amaçları içeren çalışmalarının olduğu görülmektedir. 11 Eylül'den sonra ise ABD hükümetinin kendisini küresel terörün etkisi altında olan bir savaş ortamında bulması nedeniyle, belgelerle sabit olan siber güvenlik çalışmalarında siber ortamın ABD askeri, politik ve ekonomik gücüne destek sağlayan bir alan olduğu değerlendirilmiştir.

3.1.3. Başkan Barack Obama Dönemi

2009 yılı sonrasında başkan Obama döneminde yapılan çalışmalarda, önceki dönemlere nazaran siber savunma stratejisi geliştirmek amaçlanmıştır; ABD siber güvenlik sisteminin merkezileştirilmesi, siber ortamda uluslararası işbirliğinin sağlanması, siber farkındalığın arttırılması, siber suçlarla mücadele edilmesi, siber

casusluk faaliyetlerinin karşı tedbirler alarak önüne geçilmesi gibi çalışmalar hazırlandığı görülmektedir. Obama yönetiminin siber güvenliğe verdiği önem ve hassasiyet çevresinde; siber tehditlere karşı savunma cephesi kurularak güvenlik açıklıklarının azaltılması, ağ güvenliğinin muhafaza edilmesi, siber saldırıları engelleme noktasında hükümet ve özel sektör ortaklarının birlikte hareket etmesi gibi hususlarda önemli ilerlemeler kaydedilmiştir (Bisson, 2015).

ABD'nin resmi siber kurum ve kuruluşları oldukça karmaşık bir yapıya sahiptir. Bahsettiğimiz bu karışık yapının ABD'nin âdem-i merkeziyetçi yönetim şeklinden kaynaklandığı değerlendirilmektedir. ABD'nin siber güvenlik konusunda faaliyet gösteren kurumları, "ABD Savunma Bakanlığı", "ABD İç Güvenlik Bakanlığı" ve "ABD Gizli Servisleri" olmak üzere üç yapıdan oluşmaktadır. Bunların haricinde, bazı resmi kurumların görev alanlarına yönelik olarak sorumlulukları da bulunmaktadır. Eyalet yönetimleri, devlet tarafından hizmete sunulan siber güvenlik ağı dışında, kendi siber güvenliklerini geliştirmek amacıyla farklı yapılanmalar kurarak aktif bir biçimde savunma çeşitliliklerini arttırmayı tercih etmektedirler (Çifci, 2017:93).

Bunlarla birlikte ABD'nin siber güvenlik politikalarını belirleyen eyalet ve federal yasaları hakkında ciddi bir tartışma söz konusudur. Bahse konu tartışmaların üç boyutu bulunmaktadır. Taraflardan birincisi siber güvenlik çalışmalarının ABD'nin güvenliği ve ekonomik refahı için elzem olduğunu belirtmekte ve bu çalışmaları desteklemektedirler. Tartışmaların diğer bir boyutu ise siber güvenlik kanunlarını desteklemekte, fakat bu alanda inisiyatifin devletten ziyade, kritik altyapıların ve ağların büyük bir bölümünü elinde bulunduran özel sektörde olması gerektiğini iddia etmektedirler. Tartışmanın son boyutunda ise siber güvenlik yasalarının ve ilgili yasalarla uygulanan kısıtlamaların yaratıcılığı öldürdüğünü, bilimsel buluşlara engel olduğu ve maliyetlerin yükselmesine sebep olarak özel kuruluşların rekabet gücünü azalttığı görüşünü savunmaktadırlar (Kirby, 2005).

Ayrıca ABD'nin teknolojik kapasitesiyle doğru orantılı olarak e-devlet alanındaki gelişmişlik düzeyinin diğer ülkelere göre çok önde olduğu görülmektedir. Bu alandaki ilk yasa olan ve 2012 yılında revize edilen yönetim yasasını 2002 yılında kabul etmiştir. Günümüzde de geçerliğini koruyan bu yasa ABD'nin e-devlet oluşumundaki eyalet yapıları ve federal yapı arasındaki eşgüdümü sağlaması, e-

devlet sisteminin güvenliğini muhafaza etmesi bakımından önemlidir. (En.wikipedia, 2018) 2012 yılında ise bu yasa "Dijital Hükümet Stratejisi" adı altında gözden geçirilerek yenilenmiştir. Bu revize işlemi kapsamında ABD yönetimlerinin en verimli ve uygun teknolojiye sahip olmayı hedeflemeleri ve özel kuruluşların yeni teknolojik buluş ve gelişmeleri sağlaması hususunda teşvik edilmesi temel amaçlar olarak belirlenmiştir (State.gov, 2012).

Bu kapsamda 11 Eylül 2001 tarihinde ortaya çıkan ve müteakiben devam etmesi kuvvetli muhtemel olan uluslararası terör saldırıları ve tehditlerinin de etkisiyle ABD'de siber güvenlik alanını düzenleyen yasalar, 2009 yılına kadar çok sıkı bir denetim rejimini içermiştir. 2009 yılı ve sonrasında ise Başkan Obama ve yönetimi ile birlikte, siber güvenlik konularını kapsayan yasalarda daha liberal bir eğilim gerçekleşmiştir ve daha çok internet ortamını düzenleyen, kamu ve özel kuruluşlar arasındaki uyumu ve işbirliğini arttırmayı hedefleyen yasalar gündeme gelmiştir. Darıcılı (2017)'ye göre; ABD ulusal siber güvenlik stratejisine etkileri bakımından, bahse konu sıkı denetim yönetiminden daha liberal bir rejime geçiş ile ilgili tartışma konularına 2013 yılında yaşanan "Edward Snowden Olayı"[4] olarak tanımlanan gelişmelerin etkisinin büyük olduğu değerlendirilmektedir (Darıcılı, 2017:112).

Bu belgenin ABD dış politikası ve siber ortam ilişkisi açısından ele alınması durumunda belgede ortaya konulan amaçların Başkan Obama ve yönetiminin uluslararası ilişkilerde müzakere yanlısı davranan bir strateji oluşturdukları belirtilebilmektedir. Söz konusu belgenin değerlendirilmesi bağlamında, Obama iktidarının siber güvenlik konusunda tekilci ve sert politikalar sürdürmeyi tercih eden Bush iktidarından farklı bir yaklaşım sergilemiş olduğu da açık bir biçimde görülmektedir.

Ayrıca 2011 yılında yayınlanan *"Siber Ortam İçin Uluslararası Strateji: Ağlanmış Bir Evren'de Güvenlik, Refah ve Açıklık / International Strategy for Cyberspace: Security, Prosperity and Openness in a Networked World isimli belgede*

[4] 20 Mayıs 2013 tarihinde Edward Snowden isminde Amerikalı bir genç, NSA'daki bilişim uzmanlığı görevi kapsamında elde ettiği gizli bilgi ve belgeleri The Guardian Gazetesi'ne vermiştir. Söz konusu gazete bu belgeleri yayımlamıştır ve bu bilgiler tüm dünyada deprem etkisi yaratmıştır. Bu gelişmelerın ardından Snowden bir dönem Çin Halk Cumhuriyeti'ne daha sonrada Rusya'ya sığınmıştır. (Biography.com, 2014)

ABD: uluslararası seviyede siber saldırılarla mücadele etmek için gerekli çabayı harcayacağını, internet sistemlerinin genişlemesini ve uluslararası işbirliği gerçekleştirilerek yönetilmesi hususunu destekleyeceğini, internet özgürlüğünün temel önceliği olduğunu ve ekonomik refah için enformasyon teknolojilerinin geliştirilmesinin büyük öneme haiz olduğunu" dünya kamuoyuna bildirmektedir (Obama, 2009). "ABD Savunma Bakanlığı Siber Strateji/ *The Department of Defence Cyber Strategy*" isimli belge, 23 Nisan 2015 tarihinde yayınlanmıştır ve söz konusu belge ABD'nin en son ilan ettiği siber güvenlik stratejisi niteliğindedir. Bu belge ile ABD Silahlı Kuvvetlerine "Ağ teknolojileri ve bilgi sistemleri ile gizli siber bilgilerini savunma, siber saldırılara karşı ülkenin çıkarlarını koruma, gizli siber ve askeri operasyonları planlama ve bahse konu operasyonları koordine etme" görevleri verilmiştir (E.Zheng, 2015).

3.1.4. Süper Güç Perspektifinden; ABD- Çin Siber Rekabeti

Siber güvenlik sorunları son zamanlarda ABD-Çin ilişkileri için hem gerilim hem de potansiyel işbirliğinin ana kaynağı haline gelmiştir. Yirmi birinci yüzyılda iki ülkenin dünya hegemonyası yarışması siber güvenlik alanındaki yarışmanın gerisinde kalmıştır. Aslında, uluslararası ilişkiler teorilerine göre, önde gelen sektörlerdeki rekabet dünya siyasetindeki genel hegemonik rekabeti yansıtmaktadır. Son birkaç yılda, önde gelen bir sektör olarak siber güvenlik (veya genel olarak BT ve İnternet) genel ABD-Çin ilişkileri içinde en önemli konulardan birsi haline gelmiştir. Bu mevcut güç rekabeti siber alanın artan stratejik öneminin altını çizmektedir. Haziran 2013'te, Amerika Birleşik Devletleri Başkanı Barack Obama ve Çin Cumhurbaşkanı Xi Jinping, siber güvenliğin iki güç arasındaki en büyük sorunlardan biri olduğu konusunda fikir birliğine varmıştır (Kaiman, 2014).

ABD'nin teknolojik hegemonyası konusundaki korkusu nedeniyle Çin, ABD'nin, Çin'i internette bilgi paylaşmaktan ve bilgisayar korsanlığını kolaylaştırmak için yazılımında arka iç mekan oluşturmaktan mahrum bırakarak hegemonyasını sürdürmek için teknolojik avantajlarını kullandığını iddia etmektedir (Swaine, 2013). Çin, özellikle ABD siber güvenlik teknolojilerine olan yoğun bağımlılığın politik dezavantajlara ve Çin'in güvenliğine yönelik askeri tehditlere neden olacağından endişe duymaktadır (Lu, 2013). Aslında, ABD teknolojik şirketleri Çin pazarında siber güvenlik için büyük teknolojileri tekelleştirmişlerdir.

Bu şirketlerin ABD Vatanseverlik Yasası da dâhil olmak üzere ABD yasalarına tabi olduğu konusundaki farkındalık, Çin'de politika yapıcılar ve sıradan kullanıcılar tarafından ABD'ye bağımlılıklarının çok büyük bir dezavantajı olduğunu değerlendirmelerine yol açmıştır. Çin hükümeti tarafından yapılan internet güvenlik incelemesiyle ilgili soruları yanıtlayan Çin Dışişleri Bakanlığı sözcüsü Qin Gang, "Yabancı şirketleri veya ortak girişimleri görüşmek için önemli bir ön koşulun, Çin'in ulusal çıkarlarına uygun olması ve Çin'in yasalarına ve düzenlemelerine uymak zorunda olduğunu söylemiştir." (Xinhua, 2014). Bu kapsamda, ABD'nin güvenlik söylemleri siber alandaki serbest bilgi akışına yönelik neoliberal görüşlere dayanırken, Çin'deki söylemler küreselleşmiş İnternet'in egemenlere büyük tehdit oluşturduğu hegemonik ve milliyetçi devlet egemenliği vizyonlarından oluşmaktadır.

Siber alanın karmaşıklığı, Uluslararası İlişkiler Kopenhag Güvenlik Araştırmaları Okulu tarafından sunulan "menkul kıymetleştirme" teorisini benimsemeyi makul kılmaktadır (Buzan ve diğerleri, 1998). Barry Buzan'a göre, belirli konuların menkul kıymetleştirilmesi "önemli siyasi etkilere sahip olmak için yeterli derecede dikkat çeken bir varoluşsal tehdidin kesişmeyen kurulması" ile oluşturulmuştur (Buzan ve diğerleri. 1998, 25). Siber güvenlik sorunları, en azından şimdiye kadar siber alandaki güvenlik tehditlerinin, gerçek tehditlerin peşinden gitmesinden ziyade söylem oluşturma meselesi olma eğiliminde olduğu anlamında tipik bir güvenlikleştirme örneğidir. Siber saldırganların kimliklerini, yerlerini ve giriş yollarını engelleyen bir mesafede faaliyet gösterebileceği için, suçluların suçlu oldukları kanıtlanmak yerine tahmin edilmektedir. Bu görüşe göre, ABD-Çin siber çatışması ve internet politika sürtünmeleri, siber alanda güvenlik söylemlerini meşgul etmeye yönelik yarışmaya dayanmaktadır. Bunun nedeni, rekabetin sadece fikirsel farklılıklarla değil, aynı zamanda gerçekliğin geleceğini etkileyen çıkar çatışması ile yakından ilişkili olmasıdır. Zira siber güvenlik uzun zamandır onlarca devlet kurumu ve geleneksel şirketler tarafından fazlasıyla politikleştirilmeye çalışılmıştır. Diğer yandan, iki ülke grubunun küresel siber güvenlik yönetimi için rekabet ettiği görülmektedir: Mevcut model, internetin daha açık ve özgür olması gerektiğine inanan Batı ülkeleri tarafından yönlendirilmiştir. Ancak son yıllarda, Rusya, Çin ve diğer gelişmekte olan ülkeler de dâhil olmak üzere bir devletler

koalisyonunun neden olduğu zorluklar organize edilmekte ve internet daha devlet kontrolünde bir vizyona sahip konuma getirilmeye çalışılmaktadır. Öte yandan, ABD ve Çin yirmi birinci yüzyılda iki farklı küresel güç olarak siber güvenlik konusunda rekabet etmektedirler. Teknik standartlarda siber güvenliğe farklı yaklaşımlar, düzenleyici politikalar ve güvenlik söylemleri iki dünya güçleri arasında çelişmektedir ve bu farklılıkların gelecekte daha geniş bir gerginliğe sıçraması muhtemeldir.

3.2. ÇİN HALK CUMHURİYETİ

Çin Halk Cumhuriyeti son yıllarda modern teknolojiye sahip silahlar geliştirmek ve kullanmak için çok sayıda çalışma gerçekleştirerek; kara, hava, deniz, uzay ve siber alanda askeri harekâta katkı sağlayacak ve koordine edebilecek alt yapı sistemleri ve modernizasyon çabası içine girmiştir. Bu çalışmaları neticesinde özellikle gelişmiş bir enformasyon yeteneği kazanarak, rakip ülkelerin bilgi akışını kontrol etme ve muharebe alanında etkinliğini sürdürme üzerine odaklanmıştır (Jinghua, 2018).

Çalışmamızın ilk bölümünde devletler tarafından siber taarruzlar uygulanarak rakip ülkelerin haberleşme, iletişim, lojistik ve komuta kontrolünü fonksiyonlarını yerine getiremez hale getirme yönünde bir siber stratejinin mevcut olduğu aktarılmıştır. Bu kapsamda, Çin Halk Cumhuriyeti'nin resmi belgelerinde, siber savaş gücünün geliştirilmesi yönünde bir stratejinin benimsendiği ifade edilmektedir. Çin Halk Cumhuriyeti'nin 2010 yılında yayınladığı Savunma Raporu'nda da ülkenin milli savunmasında ve çıkarlarında siber güvenlik konusunun önemi açıkça vurgulanmıştır (Hjortdal, 2011). Çin'in siber güvenlik stratejisinde, kapasitesi güçlü bir düşman devlete karşı bilgi üstünlüğünü sağlayabilmek ve karşı koyabilmek için enformasyon harbinin kullanılması öngörülmektedir. 2010 yılı başta olmak üzere, dünyadaki birçok devlet kurumlarına ve özel kuruluşlara ait bilgisayar sistemlerine girilerek siber saldırılar gerçekleştirilmiştir. Söz konusu bu saldırıların büyük bir çoğunluğunun başlangıç noktasının Çin Halk Cumhuriyeti olduğu belirlenmiştir. Söz konusu bu saldırıların temelde bilgi sistemlerinden veri çalma ve siber casusluk amaçlı gerçekleştirildiği tespit edilmiştir. Bu kapsamda gerçekleştirilen veri çalma işlemlerinde kullanılan yöntemlerin, yüksek seviyede teknik beceri gerektirmesi ve karmaşık olması nedeniyle sistemlere zarar vermek amacıyla saldırmak içinde

kullanılabilmesi, mevcut tehdidin çok büyük boyutlarda tezahür edebileceğini de ortaya koymaktadır.

Siber saldırı tekniklerinin Çin Halk Cumhuriyeti'ne üç temel alanda hizmet edebileceği değerlendirilmektedir; siber saldırı kabiliyetlerini, konvansiyonel bir savaşta kuvvet çarpanı olarak kullanarak avantaj sağlanması, rakip devletlerin internet ağı tabanlı iletişim, ticari ve lojistik faaliyetlerini kısıtlayabilme imkânı ve son olarak da siber casusluk yöntemi ile diğer ülkelerden veri çalma faaliyetleridir. Çin Halk Cumhuriyeti'nin bilgi ve internet ağı işlemlerindeki önemli stratejilerinden birisi de, elektronik harp ve kinetik silahları kullanarak gerçekleştirdiği bilgisayar ağı harekâtı ile hedef ülkenin bilgi sistemlerinde ''kör noktalar'' oluşturarak, ihtiyaç halinde bu noktaları sızma noktası olarak kullanmaktır. Çin Halk Cumhuriyeti'nin siber uzayla ilgili çalışmaları Rusya'nın çalışmaları ile benzerlik göstermektedir. Ayrıca Çin Halk Cumhuriyeti, "Law of Armed Conflict (Silahlı Çatışma Hukuku)" gibi uluslararası sözleşmelerin siber uzayda da uygulanmasına ve buna benzer ABD tezlerine muhalif görüşlere sahiptir (Çifci, 2017:93).

Bunlarla birlikte Çin Halk Cumhuriyeti ordusu, seferberlik durumunda düşman ülkelere karşı bilgi üstünlüğü sağlamak amacıyla muhtelif siber savaş araçlarının aktif olarak kullanılması için donatılmakta ve eğitilmektedir. Bahse konu siber harp stratejisini uygulamak için ihtiyaç duyulan insan gücünü karşılamak amacıyla, özel sektör, endüstri, akademi ve ticari çevrelerinden de yararlanmanın yollarını aramaktadır. Çin ordusu ve Çinli siber korsanlar arasındaki ilişkiyi, net bir biçimde ortaya çıkaracak açık kaynak bilgileri bulunmamakla birlikte, anılan tarafların aralarında işbirliği yaptığına dair delillerin var olduğu iddia edilmektedir. Çin Halk Cumhuriyeti'nin siber saldırı kabiliyetini, karmaşık saldırılar şeklinde ve uzun zamanlı bir biçimde, ABD başta olmak üzere, birçok gelişmiş ülkenin devlet ve sanayi kurumlarını hedef alarak, veri hırsızlığı ve istihbarat toplama faaliyetlerini desteklemek amacıyla kullandığı değerlendirilmektedir. Bilgi sistemlerine yapılan siber saldırılar incelendiğinde, saldırıların gerçekleştirildiği nihai noktaların büyük bir çoğunluğunun, henüz açığa çıkarılmamış sistem zafiyetlerini kullanan Çinli siber korsanlara ait olduğu tespit edilmiştir (Clarke ve Knake, 2012).

Çin Halk Cumhuriyeti'nin ABD'den internet ağı üzerinden çaldığı iddia edilen casusluk faaliyetleri incelendiğinde, bunların ABD'nin uzay programlarına,

milli savunmasına ve sivil teknoloji endüstrisine yönelik türden olduğu, ABD savunma ağlarına, ABD'nin stratejik planlarına, lojistik ve diğer kritik kabiliyetlerine yönelik olarak istihbarat toplamak amacıyla gerçekleştirildiği rapor edilmiştir. ABD'li siber güvenlik uzmanları, Çin Halk Cumhuriyeti ve ABD arasında yaşanması muhtemel bir siber savaşta, Çin Halk Cumhuriyeti'nin siber saldırı imkânlarını kullanarak ABD'nin resmi kurumlarına, askeri haberleşme ağına ve ABD ile müttefik olan ülkelerin iletişim ağlarına siber saldırı düzenleyebileceğini öngörmektedirler. Bu siber saldırıların temel olarak, gerçekleştirilen mevcut saldırı sürecinde ABD'ye zaman kaybettirmek ve askeri birliklerin etkinliğini azaltmayı hedeflediği değerlendirilmektedir (Schwartz, 2018). Çin'in rakip ülkelere karşı uygulamayı planladığı siber saldırı stratejilerine ya da hangi siber saldırıları savaş nedeni olarak kabul ettiğine dair, açık kaynaklarda yer alan bilgi veya herhangi bir doküman mevcut olmamakla birlikte, Çin Halk Cumhuriyeti'nin casusluk faaliyetlerini gerçekleştirmek amacıyla, Küba'da iki adet siber ağ istasyonu kurduğu; bu istasyonların birinden ABD Savunma Bakanlığı'na ait haberleşme ve iletişim unsurlarının dinlendiği, diğerinden ABD'nin internet trafiğini izlediği iddia edilmektedir. Söz konusu casusluk faaliyetlerinden eski ABD Savunma Bakanı Robert Gates'in çalışma bilgisayarının da etkilendiği belirtilmektedir. Ayrıca Çinli siber korsanların, ABD Ekonomi Bakanlığı müsteşarının Pekin ziyareti sırasında dizüstü bilgisayarından da veri çalındığı iddia edilmektedir (Alperovitch, 2018) (Schwartz, 2018).

2009 yılında Kanadalı siber güvenlik uzmanları, Çin Halk Cumhuriyeti'nin bazı ülkelere ait konsolosluklardaki bilgisayarlara ''GhostNet'' isimli bir yazılım yerleştirdiğini tespit ettiler. Söz konusu yazılım bilgisayar kullanıcısının haberi olmadan bilgisayarın mikrofonunu veya kamerasını açıp, ortamdaki bulunan görüntü ve sesleri Çin'de bulunan bir sunucuya gizlice göndermekteydi (Arnold, 2009). Ayrıca Çin, Microsoft ve Cisco'nun donanım ve yazılımlarını piyasaya göre daha uygun fiyatlarla satmaya ve Cisco yönlendirici devrelerini korsan olarak üreterek piyasaya sürmüştür. Bahsedilen korsan ürünleri ABD Silahlı Kuvvetleri'ne ait bazı kurum ve kuruluşlarında satın aldığı ortaya çıkmıştır. Bahse konu cihazların siber saldırı esnasında ABD'nin kritik alt yapılarını ve askeri ağlarını kullanılamaz hale getirmek amacıyla kullanılabileceği tespit edilmiştir. Cisco ve Microsoft ürünlerinin

açıklıklarını bilen Çin Halk Cumhuriyeti, kendine ait kritik kurumlarda ve askeri bilişim sistemlerinde yüksek güvenlik özelliği bulunan ve "Kylin" olarak adlandırılan kendi işletim sistemlerini geliştirmiştir. Kylin işletim sistemi, Çin Halk Cumhuriyeti Milli Savunma Üniversitesi tarafından üretilmiş olup, Unix tabanlı işletim yazılımının daha güvenli duruma getirilmiş son sürümüdür. Benzer gelişmeyi, Linux ile ABD'de CIA'de gerçekleştirmiştir (Cendrowski, 2015) (Danchev, 2009).

3.2.1. Doğu Asya'da Gelecek Dönemlerde Yaşanması Muhtemel Siber Çatışmalar

Siber uzay, kritik alt yapılar, bilişsel ve fiziksel alanlar arasındaki stratejik etkileşimler ve karşılıklı bağımlılıklardaki ileri derecedeki karmaşıklık nedeniyle siber savaşın, gelecekteki çatışmalarda geleneksel kinetik güç kullanımına meydan okuyacağı değerlendirilmektedir Örneğin, Doğu ya da Güney Çin Denizi'ndeki operasyonel erişimin sağlanmasında, ABD ordusu, kritik öneme sahip C4ISR sistemlerinin güvenlik, güvenilirlik ve bütünlüğünün yanı sıra giderek daha savunmasız hale gelecek olan savaş destek ve lojistik sistemlerini güvence altına almak zorunda olacaktır. Elektromanyetik nabız ve yüksek güçlü mikrodalga silahlarından kaynaklanan tehditler de dâhil olmak üzere elektronik savaşın diğer ortaya çıkan biçimlerinin yanı sıra siber tehditler de vardır. Bu sistemler üzerinde gerçekleştirilecek karmaşık bir siber saldırı, ABD'nin devlet kurumlarının ve askeri birliklerinin operasyonel görevlerini yerine getirme yeteneklerini kısıtlayacağı değerlendirilmektedir (Raska, 2017).

Siber destekli çatışmaların teknolojik değişimlere paralel olarak gelişeceği değerlendirilmektedir. Gelecek nesil savaşın karakterini değiştirmeye devam edecek yeni nesil robotların, yapay zekânın ve uzaktan kontrol edilen sistemlerin giderek artması, gerek sivil gerek de askeri açıdan, siber uzay ve bilgi teknoloji alanları, küresel güç olarak değerlendirilen Çin, Rusya ve ABD'nin silahlı kuvvetleri de dâhil olmak üzere, geleneksel silahların yanı sıra eş zamanlı olarak hedef alınabileceği değerlendirilmektedir.

3.2.2. Bilgisayar Ağı Harekâtı Doktrini: "Wangdian Yitizhan"

Çin Halk Cumhuriyeti, "Entegre Bilgi Ağı Elektronik Harbi" ismi verilen bilgi harbi stratejisine geçerek; siber saldırıları ve elektronik taarruz metotlarını

birlikte gerçekleştirebilen ordu birimleri teşkil etmiştir. Söz konusu stratejiye Çince “绿 坝 · 花季 护航” (Wangdian Yitizhan) ismi verilmiştir. Bahse konu stratejide, hedef ülkenin mevcut tüm bilgi sistemlerinin tesir altına alınması üzerine odaklanılmamaktadır, başta komuta kontrol olmak üzere lojistik akışlarının ve CIS4R sistemlerinin düğüm noktaları hedef alınmaktadır. Hedef devletin Muhabere, Komuta, Kontrol, İstihbarat, Bilgisayar, Keşif ve Gözetleme sistemlerine bilgisayar ağı harekâtı ve elektronik harp harekâtını eşzamanlı bir biçimde uygulanması esasına dayanan bu strateji, Çin Halk Cumhuriyeti'nin saldırıya dönük siber savaş yeteneğinin temelini oluşturmaktadır. Bu strateji, çatışmanın ilk aşamalarında siber saldırı araçlarının geniş bir biçimde düşman devlete karşı uygulanmasını esas almaktadır (Wortzel, 2011).

Çin Halk Cumhuriyeti, elektronik harp silahları, siber silahlar, uydular ve diğer uzay araçlarına karşı kullanmak amacıyla teknolojik silah geliştirmek için geniş çaplı ve büyük bütçeli AR-GE çalışmaları yapmaktadır. Çin devletinin mukabil uzay silahları içerisinde, yüksek hızlarla fırlatılan ve uydulara doğrudan nüfuz ederek kısa sürede kullanılamaz hale getiren kinetik silahları mevcuttur. 2007 yılı Ocak ayında, görev süresini tamamlayan Çin'e ait bir meteoroloji uydusu bu yöntemle imha edilmiştir. Çin Halk Cumhuriyeti bahse konu silahların yanı sıra yüksek güçlü mikrodalga sistemleri, lazer sistemleri ve elektromanyetik darbe silahlarına benzer yönlendirilmiş enerji araçları ve silahları da geliştirmektedir (Mizokami, 2018).

3.2.3. “Yeşil Baraj Gençlik Eskortluk Projesi” (Green Dam Youth Escort)

Resmi Çin medya kaynaklarına göre, Yeşil Baraj Gençlik Eskortu (GDYE) yazılımı, Windows işletim sistemlerinin içeriklerinin kontrolünü sağlamaya ve genç Çin vatandaşlarının internet ortamındaki sağlıksız bilgileri görmelerini engellemeye yöneliktir. Ancak, eleştirmenler, GDYE'nin bilgisayar korsanlarının GDYE ile kurulan bilgisayarların kontrolünü ele geçirmelerini sağlayan ciddi güvenlik açıkları olduğunu ve yazılımın casus yazılım ve kötü amaçlı yazılım işlevselliği taşıdığını değerlendirilmektedir. Eleştirmenler ayrıca, söz konusu yazılımın bilinmeyen amaçlar için uzak sunuculara iletilmek üzere kullanıcı verilerini ve tuş vuruşlarını toplamak üzere tasarlandığını da iddia etmektedirler. GDYE, 2009 yılında Çin Halk

Cumhuriyeti'nde satılan her bilgisayarda yüklü bulunması şart koşulmuştur. Yazılım, bilgisayarın her açılış işleminde yasaklı sitelere erişimi engellemekte, veritabanını otomatik olarak kaydetmekte ve kullanıcıya ait kişisel bilgileri toplamaktadır. Bu yazılımla genç kullanıcıların pornografik içeriklere karşı korunmasının amaçlandığı ileri sürülmektedir. Diğer yandan erişimi engellenen anahtar kelimelerinin %15'inin porno, yüzde %85'inin politik içerikli olduğu iddia edilmektedir (Li ve diğerleri, 2010). Yazılımda ABD firmalarından çalındığı ileri sürülen kodlar olması nedeniyle, 2010 yılında, yazılımı geliştiren firmaya ve Çin Halk Cumhuriyeti'ne 2 milyar dolarlık tazminat davası açılmıştır ancak firma tüm iddiaları reddetmiştir (Softpedia, 2015). Bahse konu yazılımda güvenlik açıklıkları ve hatalar tespit edilmesi ve Çin devletinin yazılım için verdiği mali desteği sonlandıracağını duyurması ve bu yazılım planının uluslararası medya tarafından gördüğü ilgi ve merak yoğunluğu karşısında aniden rafa kaldırıldığı tahmin edilmektedir (MacKinnon, 2009).

3.2.4. Çin Casusluk Ünitesi (Unit 61398)

Ünite 61398 resmi olarak, Halk Kurtuluş Ordusu Genelkurmay Başkanlığı 3. Dairesi'nin 2. Bürosu olduğu değerlendirilmekle beraber resmi Çin askeri açıklamalarında neredeyse hiçbir yerde bulunmamaktadır. Ancak grubu inceleyen istihbarat analistleri, Çin bilgisayar casusluğunun merkezi unsuru olduğunu söylemektedirler. Ünite, 2011 yılında Virginia'daki bir sivil toplum kuruluşu olan 2049 Enstitüsünün güvenlik ve politika konularını ele alan "Project 2049" Enstitüsü tarafından "büyük olasılıkla politik, ekonomik ve askeri istihbarata odaklanan ABD ve Kanada'yı hedefleyen öncü varlık" olarak tanımlanmaktadır. Söz konusu 12 katlı binayı, Çin siber ordusuna ait siber korsanların karargâh olarak kullandığını belirten haberler 2013 yılında The New York Times gazetesinde çıkmıştır. Anılan haberde, Amerika menşeli firmalara ve devlet kurumlarına yapılan siber saldırıların izleri ve emareleri takip edildiğinde bu binaya ulaşıldığı, ayrıca ABD istihbarat servislerinde çalışan yetkililerinde söz konusu bilgileri teyit ettiği iddia edilmektedir. Söz konusu siber korsanların, Coca-Cola gibi şirketlerden terabaytlarca veri çaldığı, Amerika Birleşik Devletleri'nin elektrik altyapısı, gaz hatları ve su işleri gibi kritik altyapısına dâhil olan şirketlere de saldırı düzenlediği belirtilmektedir. ABD'li siber güvenlik uzmanlarına göre, Kuzey Amerika'daki petrol ve doğalgaz boru hatlarının yüzde 60'ından fazlasına uzaktan erişimi olan bir şirkete de siber saldırı gerçekleştirilmiştir.

Ünitenin, bilgisayar kodları gizli şirket ve devlet veri tabanlarını koruyan bilgisayar güvenlik firması RSA'ya da saldıranlar arasında yer aldığı belirtilmektedir. Çin Halk Cumhuriyeti Bakanlık sözcüsü Hong Lei ise, siber saldırıların kesinlikle devlet tarafından gerçekleştirilmediğini ve bu durumun yasal olmayacağını belirtmiştir (Senger ve diğerleri, 2013).

Uluslararası Mandiant güvenlik şirketi tarafından, yayınlanan detaylı bir raporda, Çinli siber korsanlar tarafından gerçekleştirilen söz konusu siber saldırıların izlerinin nasıl sürüldüğü belirtilmektedir. Ayrıca bu raporun, Çin Halk Cumhuriyeti ve Kuzey Kore gibi kapalı bir ülke yapısında dahi siber saldırı iz ve emarelerine nasıl ulaşıldığını göstermesi açısından çok önemli olduğu değerlendirilmektedir. Çin'e ait bahse konu birimin varlığı ve operasyonları bir Çin devlet sırrı olarak kabul edilirken, ABD İstihbarat Komitesi Başkanı Mike Rogers, Mandiant raporunun "İstihbarat Komitesi'nin çalışmaları ile tamamen tutarlı olduğunu" belirtmiştir (McWhorter, 2013).

2014 yılında ABD Pensilvanya Mahkemesi'nin oluşturduğu büyük bir jüri, bilgisayar korsanlığı, ekonomik casusluk ve ABD nükleer güç, metal ve güneş enerjisi ürünleri endüstrisindeki altı şirkete ait verileri çalma eylemleri nedeniyle beş Çinli askeri subayı suçlamıştır. İddianamede, sanıkların bilgisayarlarına yetkisiz erişimi sürdürmek ve devlete ait işletmeler de dâhil olmak üzere Çin'deki rakiplerine faydalı olacak bu kurumlardan bilgi çalmak için Amerikan kurumlarının bilgi sistemlerine sızdıkları iddia edilmiştir. Jüri de bulunan bazı üyelerin iddialarına göre, komplocular Çinli şirketler için özellikle yararlı olacak ticari sırları çalmıştır. Bazı iddialara göre ise, saldırganlar aynı zamanda, ABD'nin savaş stratejisine ve savunma sanayisine ait hassas bilgileri de çalmıştır. ABD Başsavcısı Eric Holder, "Bu, Çin ordusunun üyeleri tarafından ekonomik casusluk iddia eden bir dava ve bu tür bir hacking için devlet aktörüne karşı ilk suçlamaları temsil ediyor." demiştir. "Bu durumda çalınan ticari sırların ve diğer hassas iş bilgilerinin önemi büyüktür ve failleri ağır şekilde cezalandırılmalıdır. Küresel pazardaki başarı, sadece bir şirketin yenilik yapma ve rekabet etme yeteneğine dayanmaktadır. Bu İdare, Amerikan şirketlerini yasadışı bir şekilde sabote etmeye ve serbest piyasanın işleyişinde adil rekabetin bütünlüğünü baltalamaya çalışan herhangi bir ulusun eylemlerini hoş görmeyecektir. "(The United States Department of Justice, 2014). Çin Halk

Cumhuriyeti ise gerçeği yansıtmayan delillerle davanın açıldığını ve ABD-Çin ilişkilerinin bozulmasına yönelik çalışmalar olduğunu iddia ederek söz konusu davayı kınamıştır (Harris, 2013).

3.2.5. Altın Kalkan Projesi (Golden Shield Project)

Altın Kalkan Projesi'nin amacı, Çin Halk Cumhuriyeti hükümeti tarafından ulusal güvenliği sağlamak amacıyla, Çinli kullanıcıların zararlı olan sitelere erişiminin engellenmesi veya bu sitelere erişimin kısıtlanması ve internet erişiminin filtrelenmesi projesidir (Rajeck, 2017). Kullanıcıların hızla artmasından dolayı Çin hükümeti, vatandaşların uygunsuz olarak kabul edilen içeriğe erişememelerini sağlayacak yöntemleri uygulamak amacıyla; Çin hükümetine yönelik suç faaliyeti, pornografi, müstehcenlik ve benzer içerikleri bulunduran sitelere erişimi engellemiştir. Bu strateji yürütülürken, IP Engelleme, IP Adresini Yanlış Yönlendirme ve Veri Filtreleme olmak üzere üç temel yöntem kullanılmıştır. Altın Kalkan Projesi sayesinde uygulamaya konulan kuralları, düzenlemeleri uygulamak ve kurallara uyulduğundan emin olmak için Çin hükümeti tarafından istihdam edilen 50.000'den fazla çalışan bulunmaktadır (Jones, 2014).

Çinli kullanıcıların büyük bir çoğunluğu Büyük Güvenlik Duvarı'nı atlamak için, sanal özel ağları (VPN) ve proxy'leri kullanmayı tercih etmektedir. VPN'ler, bilgisayarlar kullanıcılarının tam güvenliğini sağlayamamakla beraber, tüm ağlara uzaktan ve kısmen güvenli bir şekilde bağlanılmasına izin vermektedirler. Çin'de bulunan internet kullanıcılarından %25'inin güvenlik duvarını aşmak için vekil kullandığı bilinmektedir. Bu Çinli kullanıcılar, dünyanın dört bir yanından gelen haberleri takip edebilmek için Büyük Güvenlik Duvarı'ndan geçmek istemektedirler. Bununla birlikte, son yıllarda, söz konusu güvenlik duvarını aşmak daha da zorlaşmaktadır. Çin devleti tarafından onaylanmış VPN'lerin kullanımı sayesinde, özel yapım VPN'lerin kullanımı daha zor ve bazı durumlarda imkânsız hale gelmektedir. Bu VPN'lerin satın alınması ve Çin hükümetinin kullanıcıların faaliyetlerini görmesini sağlamak çok pahalıdır. Apple firması, hükümetin bu teşvikinden dolayı geçen sene Çin App Store'dan 674 adet VPN uygulamasını kaldırmak zorunda kalmıştır (Bloomberg, 2018).

Çin'deki VPN'lere getirilen kısıtlamalar nedeniyle, ülke içindeki şirketler, özellikle de yabancı şirketler birçok sorunla karşı karşıya kalmaktadır. Çin'in Altın

Kalkan Projesi'ni uygulama gerekçelerinden biri, bilgi akışını kontrol etmektir. Çin Halk Cumhuriyeti'nin izlediği bu vizyonu 'siber egemenlik' olarak adlandırmak mümkündür. Yani Çin hükümetinin internet kullanımı ve mevcut bilgi üzerinde tam kontrolü bulunmaktadır. Bazı yabancı şirketlerin ve ülkelerin büyükelçiliklerinin VPN'lerin kullandığı ağlar nedeniyle, bu şirketler sorun yaşamaktadırlar. Holloway (2018)'e göre; mevcut durum değerlendirildiğinde Çin hükümetinin tutarsız bir süreç ortaya koyduğu görülmektedir. Dünya Ticaret Örgütü, Çin'in bilgiyi sansürleme hakkına sahip olduğunu bilmektedir, ancak Çin hükümetinin yabancı şirketlere ticari erişimi engellemesine engel olamamaktadır. Bu durum, bahse konu yabancı şirketlerin Çin pazarında serbest ticaret yapmasına engel olarak dünyanın başka yerlerinde başarılı olan uygulamalarının Çin pazarında faaliyete geçirilmesi işleminin önüne geçmektedir (Holloway, 2018). Diğer taraftan bu sistemin özelliği, gerçekleşmesi muhtemel bir siber saldırıda veya herhangi bir siber tehdit algılandığında, Çin Halk Cumhuriyeti siber ortamının kapatılarak dış dünyadan tecrit edilebilmesidir (Clarke ve Knake, 2012).

3.3.RUSYA

3.3.1. Rusya'nın Siber Güvenlik Politikaları

Rusya devletinin siber güvenlik politikaları, Sovyet döneminden günümüze kadar etkinliği artan bir biçimde genişletmektedir. SSCB döneminde, Rus istihbarat servisinin gerçekleştirdiği operasyonların önemli bir kısmının, Batı bloğunda gerçekleşen teknolojik gelişmeleri takip ederek casusluk yöntemiyle bu buluşları Sovyet yönetimine aktarmaktan oluştuğu bilinmektedir. Kontrolsüz bilginin hükümet ve toplum için bir tehdit oluşturduğu görüşünü savunan Rusya hükümetlerinin siber uzay konusundaki stratejisinin temelleri, Bilgi ve İletişim Teknolojileri'ni, askeri doktrinlere entegre etme konusunda önemli teşvikler ve çalışmalardan oluşmaktadır. 1998 yılından itibaren Rusya, Birleşmiş Milletler Genel Kurulu'nda BİT'lerin güvenliğe olan etkileriyle ilgili açıklamalarda bulunmuştur. Ayrıca 2011 yılında da Uluslararası Bilgi Güvenliği Davranış Kurallarını geliştirmek için Çin ile ortaklık kurmuştur. Rusya askeri doktrininde, ulusal çıkarlarını desteklemek, bilgi harbini yürütmek ve hibrit savaşlarda siber saldırıları etkin biçimde kullanmak için araştırmalar gerçekleştirerek, planlama ve stratejiler oluşturmaktadır (Darıcılı, 2017:137).

Diğer taraftan Rusya, ABD ile yaşadığı askeri rekabet çerçevesinde sahip olduğu teknolojik ve kritik ağ altyapısını adeta bir etki-tepki bağlantısı şeklinde geliştirmiştir. Bu nedenle, hem siber uzayda hem de ABD silahlı kuvvetleri ile genel stratejik, operasyonel ve taktiksel avantajlarla mücadele etmektedirler. Bununla birlikte ABD, konumlandırma, navigasyon, keşif, gözetim, uydu iletişimi ve hava durumu izleme gibi fonksiyonlar için hayati önem taşıyan uzay varlıklarına ve destekleyici altyapılarına karşı artan siber tehditlerden endişe duymaktadır. İnternetin açık, uluslararası ve merkezi olmayan doğası, ABD'nin egemenliğine karşı önemli açıklar yaratmaktadır. Bu kapsamda siber saldırıların gerçekleştirildiği özel siber altyapı, yeni bir tür askeri silah olarak değerlendirilmektedir. Ayrıca modern silahların üretilmeye çalışıldığı günümüzde, artan bu silahlanma yarışının önemli etkilerinin ortaya çıkacağı politika yapıcılar tarafından iddia edilmektedir. Bu silahlanma yarışında düşmana karşı somut avantajlar elde etmek için yeni teknolojiler oluşturulmaktadır. Teknolojiye ek olarak, siber alanda operasyonların tüm çatışmalarda kullanılmasına izin verecek olan yenilikçi kavramlarla ilgili tartışmalar gerçekleştirilmektedir (Snyder, 2018).

3.3.2. Rusya'nın Enformasyon Savaşı Stratejileri

Rusya Federasyonu, özellikle son yıllarda siber alanda güvenliğin sağlanmasına özel önem göstermiştir. Başta askeri alanda olmak üzere siber komuta sistemi oluşturma konusunda ciddi çalışmaları mevcuttur. Bu tür birlikler ve kurumlar ülkenin bilgi güvenliğinden sorumlu konumdadır. Bu siber organizasyonların görevleri, dışarıdan gelen tüm bilgilerin izlenmesini, işlenmesini ve siber tehditlerle mücadeleyi içermektedir. Ayrıca siber alanda güvenliğe adanmış, "social.ligainternet.ru" adresinde bulunan bir sosyal ağ mevcuttur. Rusya'da söz konusu ağa herkes katılabilmektedir. Böyle bir sosyal ağ oluşturmanın amacı, siber güvenlik ile ilgilenen tüm vatandaşları bir tematik platformda birleştirmektir. Hâlihazırda, bu ağa sadece Rusya bölgelerinden değil, BDT ülkelerinden de binlerce insan kayıtlıdır. Ayrıca Avrupa ve ABD'den de katılımın sağlanması amacıyla projenin İngilizce versiyonu da bulunmaktadır (Yakushev, 2013). Rusya Federasyonu'nun siber güvenlik stratejisi bağlamında, bilgi silahlarının geliştirilmesi ve kullanılması, bilgi savaşının hazırlanması ve yürütülmesinin yanı sıra bilgi terörizmi ve siber suçu içeren "tehdit üçlüsü" formülü olarak adlandırılan stratejik

çalışmalar mevcuttur. Strateji, devletin özel işletme, akademik topluluk ve Rusya Federasyonu vatandaşları ile birlikte bu tür tehditlerle çalışma konusundaki faaliyetlerinin bir vizyonunu oluşturmaktadır. Stratejinin başarılı bir şekilde uygulanmasının nihai sonucunun, siber tehditlere ve zorluklara karşı güvenlik alanındaki devlet ve vatandaşlar arasındaki etkileşimin şeffaf, anlaşılabilir, iyi işleyen bir örgütsel, teknik ve düzenleyici altyapısının oluşturulması olacağı varsayılmıştır (Nikolayevich, 2017).

3.3.3. Gerasimov ve Hibrit Savaş Doktrini

Çalışmanın ikinci bölümünde, Rusya tarafından gerçekleştirildiği iddia edilen, Estonya, Gürcistan, Ukrayna ve Türkiye siber saldırılarında "hibrit savaş" ve "melez savaş" şeklinde bazı kavramlar belirtilmiştir. Rusya Silahlı Kuvvetleri Genelkurmay Başkanı Valery Gerasimov tarafından oluşturulan "Gerasimov Doktrini" bu kavramların bir parçasıdır. Söz konusu doktrinde Gerasimov, askeri müdahalelerin son adım olduğunu belirterek ondan önce, ekonomik, politik, bilgi ve siber uzay alanlarında mümkün olan her şey gerçekleştirildikten sonra fiziksel askeri müdahalelerin icra edilmesi gerektiğini belirtmiştir. Bahse konu böyle bir operasyon Ukrayna'da yapılmıştır. Zira iletişimin bastırılması ve kontrollerin etkisiz hale getirilmesi, yerel ayaklanmaların kışkırtılması gibi kritik hamleler sadece Kırım'da uygulanmakla kalmayarak birçok devlete karşı icra edilmiştir. Bazı politika uzmanlarına göre; Ukrayna'daki olaylar Sovyet sonrası alanda Kremlin'in politikasının bir parçası olarak görülmektedir. Batı ülkelerinin Çeçenya, Transdniestria ve Gürcistan'daki savaşa durgun tepki vermesi, Rusya'nın siyasi liderliğini aktif olarak öne çıkartarak, yeni araçlar ve yöntemler kullanma isteğini arttırmıştır. Ayrıca Rusya Milletvekili Dmitry Belotserkovets, Rusya'nın kendi doğal Sivastopol'unda da hibrit savaş unsurlarını aktif olarak kullandığını, Rus yanlısı örgütleri desteklediğini ve finanse ettiğini belirtmiştir. Bunlarla birlikte, Alman Marshall Vakfı uzmanı Bret Schafer, Rusya'nın Ukrayna'da edindiği deneyimi Batı ülkelerine karşı karma bir savaş yapmak için kullandığını ifade etmektedir. Schafer; "Amerika Birleşik Devletleri'ndeki Rus etkisini Twitter üzerinden izleyen Hamilton, 68 projenin, Rus trolleri tarafından gerçek zamanlı olarak dağıtılan konuları, etiketleri ve bağlantıları tanımlamasını sağlayarak, Kremlin'in gündeminde ne

olduğunu görmemizi sağlıyor ” şeklinde açıklama yapmıştır. Buna ek olarak Bret Schafer, bu alanda sadece Kremlin'in eylemlerine tepki vermenin haricinde, söz konusu mücadeleyi eğrinin ilerisine götürmenin gerekli olduğunu belirtmiştir (Yanevsky, 2017).

3.3.4. Rusya’nın Siber Uzay Alanındaki Etkinliği

Rusya'nın siber uzay alanının kontrolüne odaklanması, Bolşeviklerin bilgi vermemek amacıyla, kitleleri biçimlendirmek kapsamındaki faaliyetlerini gerçekleştirmek için kitle iletişim araçlarını kullanmaya çalıştıkları Sovyet dönemine kadar dayanmaktadır. Müteakip dönemlerde ise, Rus Hükümeti 2000 yılında oluşturduğu “Bilgi Güvenliği Doktrini” isimli resmi belgelerde belirtildiği üzere devletin dış müdahaleye karşı korunmada güçlü bir rol alması gerektiğini savunarak siber güvenliğini iç istikrarla ve ulusal güvenlikle ilişkilendirmiştir. Zira yaklaşık son on yılda yaşanan olaylar; Ukrayna ve Gürcistan'daki devrimler, Arap Baharı ve 2014 yılında Ukrayna Cumhurbaşkanı Viktor Yanukoviç'in görevden alınmaması, Rusya'nın siber uzay alanındaki artan tehdit algılamasına katkıda bulunarak, geniş kapsamlı bilgi teknolojileri gözetimi ve kontrolü için gerekçeler oluşturmuştur. Maurer ve Hinck’e göre, Rusya'nın siber uzayda öne çıkma nedenlerinden biri de suçlu bilgisayar korsanlarının yakalanması konusundaki başarısı olduğu değerlendirilmektedir. Eski Sovyet ülkeleri, az meşru ekonomik fırsatlara sahip, yüksek eğitimli, teknik olarak yetenekli bireylerin geniş nüfuslarına sahiptir; bu durumun, bazı ülkelerde artan hackleme ve suç işlemleri gibi olumsuz faaliyetlere dönüşmesine yol açtığı değerlendirilmektedir. Devlet ve suç korsanları arasında; korsanların eski Sovyet ülkeleri içindeki insanları hedeflemeyecekleri ve Rus devletinin kriminal faaliyetlerine katılacaklarını açıkça belirten pazarlığa dayanan bir ilişki bulunmaktadır. Bu güvenlik toleransı, Rus güvenlik hizmetlerinin yetenek ve kabiliyetlerini geliştirmekte ve rakip ülkeler karşısında göreceli avantajlar elde etmektedir (Maurer ve Hinck, 2018).

Rusya’nın siber uzay alanındaki etkinliğini açık biçimde ortaya koyan iki önemli siber olay olduğu değerlendirilmektedir. Bunlardan ilki ‘’Yahoo’’ skandalıdır. Yahoo’nun 2013’te başlayan bir dizi güvenlik ihlalinden büyük çoğunluğu ABD vatandaşlarından oluşan üç milyar hesabın etkilendiğini kabul etmesinden sonra gelmiştir. Müdahalenin Rus devleti tarafından desteklendiği iddia

edilmektedir, ancak bunu ispatlamak için çok az kanıt bulunmaktadır. Ayrıca söz konusu olay, 2016 yılına kadar kamuya açıklanmamıştır. 2016 yılında söz konusu şirket müşterilerine bilgi sızıntısı olduğunu duyurmuştur. Bu veriler kullanıcı adlarını, e-posta adreslerini, telefon numaralarını, doğum günlerini ve şifreleri içermektedir. Şirket, siber saldırıların "devlet destekli bir oyuncudan" geldiğini açıklamıştır, ancak birçok siber güvenlik uzmanı konu hakkında şüphelerini dile getirmiştir (Zapryanov, 2016).

İkinci önemli olay, Moskova'nın 2016 yılında gerçekleştirilen ABD seçimlerine müdahalesidir. Bu olayın, Batı ülkelerine Rusya'nın siber uzaya ilişkin görüş ve davranışlarıyla ilgili varsayımlarını tekrar gözden geçirmeleri için önemli bir farkındalık yaratma çağrısında bulunduğu değerlendirilmektedir. Bir dezenformasyon örneği olan saldırılar; Petersburg'daki "profesyonel korsanlar" örgütü, sosyal medya platformlarını manipüle ederek partizanlık alevlerini körükleyebildiklerini ve ABD'nin siyasi bölünmelerini kötüleştirebileceklerini göstermiştir. ABD Adalet Bakanlığı'nın 2018 yılında yayınladığı iddianamesinde anlatıldığı üzere, İnternet Araştırma Kurumu (IRA) bir dizi kampanya yürüterek "Amerika Birleşik Devletleri'ne karşı enformasyon savaşı" gerçekleştirmiştir. Söz konusu saldırılarda, YouTube, Facebook, Instagram ve Twitter gibi programlar da etkin biçimde kullanılarak, son derece partizan içerikler yayınlanmıştır. Zira geniş kitlelere yayılan yanıltıcı bilgiler, Rus hükümetinden destek alarak, ABD siyasi sisteminde anlaşmazlığa yol açmış ve karışıklığa neden olmuştur (Berlinger ve Santos, 2018).

3.4. AVRUPA BİRLİĞİ

NATO, Birleşmiş Milletler, AGİT gibi uluslararası kuruluşlar kendi içlerinde çalışma grupları ve komiteler bulundurmakta, siber güvenlik ve siber uzay alanında gerçekleşen gelişmeleri yakından takip etmekte, bu konularda araştırmalar yaparak gerçekleşmesi muhtemel siber tehditler karşısında önlemler almaya çalışmaktadırlar. Çalışmamızın bu kısmında, AB'nin siber güvenlik stratejisi nitelik bakımından değerlendirilmeye çalışılacaktır. Bununla birlikte siber tehditler ve siber saldırılar kapsamında önlem almaya çalışılırken karşılaşılan sorunlar, Avrupa Birliği'nin siber güvenliği tesis etme yönünde geliştirdiği politikalar ve sonuçları incelenecektir. Çalışmamızın bu kısmında amaç, AB'nin siber güvenlik stratejisini güvenlikleştirme

bakımından değerlendirerek, söz konusu bu stratejilerin hangi temellere dayandığını ve nasıl oluştuğunu tespit etmektir.

3.4.1. AB'de Siber Güvenlik ve Kritik Altyapı Kapsamındaki Gelişmeler

Avrupa Birliği'nin, uluslararası ortamda siber güvenliğin tesisi hususunda önemli bir aktör olduğu değerlendirilmektedir. AB kendi bünyesinde de kritik altyapıların korunmasını ve siber güvenliğin sağlanmasını önemli konular olarak görmekte ve bu doğrultuda stratejiler geliştirilmektedir.

Kritik altyapı, tahrip edilmesi veya zarar görmesi gibi durumlarda kendisine bağlı yapıların veya sistemlerin de önemli seviyede kesintiye uğraması ve zarar görmesine neden olan yapılar şeklinde tanımlanmaktadır (Westby, 2004). Kritik altyapıların kullanılamaz hale getirilmesi gibi durumlar, ülke vatandaşlarının güvenliği, sağlığı ve ekonomik refahı gibi temel yaşam ilkelerine olumsuz tesir edebileceği gibi hükümetin ve ülke ekonomisinin işleyişi üzerinde de önemli etkiler doğurmaktadır. Bu nedenle kritik bilgi ve ağ altyapıları ülkelerin siber saldırılara karşı savunmasında ve gerçekleştirilmesi muhtemel siber saldırılar karşısında önlem alınması konusunda büyük öneme sahiptir. Bu kapsamda AB'nin kritik olarak değerlendirdiği sektörler 2001 yılında yayınlanan 574/2001 sayılı bildiride açıklanmıştır. AB kritik altyapıların ve ağ sistemlerinin belirlenmesinde kıstas olarak, etkilenen bölümün büyüklüğüne ve zamansal etkisine vurgu yapmıştır. Kritik altyapının kullanılamaz hale gelmesi durumunda, etkilenen coğrafi alanın uluslararası, ulusal veya yerel olması durumu söz konusudur. Büyüklük kapsam olarak, sıfır, asgari, orta ve azami büyüklük olarak derecelendirilerek ifade edilmektedir. Ayrıca politik faktörler bağlamında, söz konusu altyapılara gerçekleştirilen siber saldırılar sonucunda hükümetlere olan güvenin artması veya azalması hususundaki etkilerden de bahsedilmektedir. Zamansal etki ise, gerçekleştirilen bir siber saldırıdan etkilenilmesi durumunda söz konusu saldırının ne kadarlık bir zaman aralığında kayıplara yol açması durumu olarak ifade edilmektedir. Bu zaman aralıkları anlık, 24 saat, bir hafta, bir ay gibi periyotlar halinde belirlenebilmektedir (Avrupa Komisyonu, 2001).

2004 yılında Avrupa Toplulukları İletişim Komisyonu'nun yaptığı çalışmalarda, kritik bilgi ve ağ altyapıları yeniden tanımlanmıştır. Bununla birlikte söz konusu çalışmalar kapsamında kritik sektör ve alanlar tekrar değerlendirilerek,

kriterlerinin neler olması gerektiği konusu tartışılmıştır. Bu komisyon tarafından belirlenen yeni tanıma göre, ''kullanılamaz hale getirilmesi durumunda ülke vatandaşlarının, güvenliği, sağlığı ve huzuru üzerinde veya üye devletlerin yönetim organlarının işleyişi üzerinde önemli tesirlere yol açma ihtimali olan bilgi teknolojileri ve fiziksel ağları, varlıkları ve hizmetleri'' kritik altyapılar olarak ifade edilmiştir. Söz konusu tanımdan yola çıkarak Avrupa Birliği'nin kritik altyapı ağlarına olan bakış açısının, temel devlet hizmetlerini sağlayan kurumlardan, kritik olarak değerlendirilen ekonominin birçok sektörüne kadar uzandığını söylemenin mümkün olduğu değerlendirilmektedir. Güvenlikleştirme çalışmaları kapsamından değerlendirildiğinde de, bu tanımın yeteri kadar kapsayıcı olduğu ve birçok güvenlik konuları altında değerlendirilebileceği düşünülmektedir. Güvenlikleştirmenin etkisi, merkez aldığı konunun önem derecesine göre şekillenmektedir. Söz konusu kritik altyapılarda da merkez alınan konu, doğrudan devletin ve vatandaşın bekası olması nedeniyle, güvenlikleştirme çalışmalarında kritik ağ altyapılarının güvenliğine azami önem atfedilmesine neden olmaktadır (Avrupa Komisyonu, 2004).

Bu gelişmelerle birlikte yürütülen kurumsallaşma çalışmaları neticesinde 2003 yılında "Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Union Agency for Network and Information Security Agency)" kurulması kararı alınmıştır. Müteakiben 14 Mart 2004 tarihinde kısaltması "ENISA" olan ajans fiilen kurulmuştur. ENISA, Avrupa genelinde ve AB'ye üye ülkelerde üst seviyede bilgi ve ağ güvenliğinin sağlamak ve AB'nin siber güvenliğinin tesisi konusunda gerekli koordinasyonu sağlamak amacıyla faaliyet göstermektedir (Enisa, 2004).

3.4.2. AB'nin Siber Güvenlik Stratejisi

Avrupa Komisyonu'nda belirtildiği üzere, AB, siber uzayın açık ve özgür olduğunu kabul etmiştir. Komisyonun hazırladığı strateji belgelerinde temel haklar, hukukun üstünlüğü ve demokrasinin siber ortamda korunması gereken temel prensipler olduğu belirtilmiştir. Ayrıca, özgürlüğün ve modern yaşamın temellerinin artan bir biçimde yenilikçi ve sağlam internete bağlı olduğu belirtilmiştir. Normalde bilgi güvenliği ile ilişkili pek çok önlem alınmasına rağmen, siber güvenlik gerçekten dijital bilgilerin güvenliğini ele almaktadır. Bilgi güvenliği, her türlü bilgi güvenliğini ele alan ve kâğıt belgeleri, fiziksel güvenlik ve insan hatası ile dijital verilerin işlenmesini kapsayan daha geniş bir yaklaşımdır. Etkin bir siber güvenlik

duruşu elde etmek için kuruluşlar, tek başına donanım ve yazılım çözümlerinin onları siber tehditlerden korumak için yeterli olmadığını ve daha geniş bir bilgi güvenliği yaklaşımına ihtiyaç duyulduğunu bilmelidirler. Stratejide etkin bilgi güvenliğinin dört temel alanı; insanlar, devlet, süreç ve teknoloji olduğu belirtilmektedir (Eren, 2017:79) (İtgovernance.eu, 2013).

AB'nin Siber Güvenlik Stratejisi, Avrupa Komisyonu Başkanı, Avrupa Birliği Dış İlişkiler ve Güvenlik Politikası Yüksek Temsilcisi tarafından 2013 yılında yayınlanmıştır. Söz konusu strateji belgesi ile AB, AB ve uluslararası alanda siber güvenlik politikasının ilkelerini açıklığa kavuşturmuştur. Bu belgede, Ortak Güvenlik ve Savunma Politikasının (CSDP) çerçevesiyle ilgili siber savunma politikası ve yeteneklerinin geliştirilmesi, üye devletlerin savunma ve ulusal güvenlik çıkarlarını destekleyen bilgi sistemlerinin siber esnekliğini arttırmak için, siber savunma kabiliyetinin geliştirilmesinin "karmaşık siber tehditlerden tespit, müdahale ve iyileşmeye odaklanması gerektiği" görüşü öne sürülmektedir. Ayrıca kritik siber varlıkların korunmasında gelişmiş sinerji, araştırma ve geliştirme kapsamında hükümetler, özel sektör ve AB'deki akademilerin yakın işbirliği ile desteklenmesi gibi konularda teşvik edilmesi gerekmektedir. Strateji kapsamında, AB siber savunma politikasını geliştirmek için siber savunma eğitimleri ve tatbikatları yapılarak, etkili savunma yetenekleri kazanmak ve işbirliği alanlarını belirlemek gibi konular üzerinde önemle durulmuştur. NATO dâhil olmak üzere uluslararası ortaklar arasında diyalog ve koordinasyon gibi hususları teşvik etmek amacıyla çalışmaların başlatılacağı ifade edilmiştir (European Defency Agency 2017).

Avrupa Komisyonu, siber güvenlik için endüstriyel ve teknolojik kaynaklar geliştirmek konusunda; "yenilikçi ve ileri teknoloji ürün ve hizmetlerini sağlayan dünya çapında liderlerin birçoğunun AB dışında yer aldığı" hususunun göz önünde bulundurarak, özel sektöre teşvik sağlamak için üye ülkeleri "Avrupa çapında yüksek güvenlikli ürünlere yönelik piyasa talebini" oluşturmaya davet etmiştir. Söz konusu durumun ancak yüksek seviyede siber güvenliği tesis etmekle oluşacağı hususu da ayrıca belirtilmiştir. Komisyon, Avrupa standardizasyon kuruluşlarının devam eden standardizasyon çalışmalarını desteklemek için tedarik zinciri güvenliğine odaklanan çalışma ile güvenlik standartlarının geliştirilmesini desteklemeyi hedeflemiştir. Avrupa Birliği için tutarlı bir uluslararası siber uzay politikası oluşturmak ve temel

AB değerlerini desteklemek amacıyla üye devletlerin, sivil toplum ve özel sektörün yanı sıra önemli uluslararası ortaklar ve kuruluşlarla olan ilgisini artırmak için tutarlı bir AB enternasyonal siber uzay politikasını oluşturan çalışmalar yapılması amaçlanmıştır (Trimintzios ve diğerleri, 2016).

AB, özellikle Avrupa Birliği, OECD, BM, AGİT, NATO, AU, ASEAN ve OAS gibi Avrupa Birliği değerlerini ve kurumlarını paylaşan üçüncü ülkeler olmak üzere siber konularda uluslararası ortaklara danışarak hareket etmeyi planlamaktadır. ABD ile işbirliği, özellikle, Edward Snowden tarafından ortaya konan ABD programlarıyla ilgili meseleleri ele almak için kurulmuş olan AB-ABD Siber Güvenlik ve Siber Suç Çalışma Grubu bağlamında daha da geliştirilecektir. AB vatandaşlarının kişisel verilerinin siber uzayı bir özgürlük alanı ve temel haklar olarak tanıması amacıyla AB, kurumsal sosyal sorumluluğu teşvik etmeli ve bu alanda küresel koordinasyonu geliştirmek için uluslararası girişimlerde bulunmalıdır. Ayrıca, şeffaflığı artırmak ve devlet davranışlarındaki yanlış algılama riskini azaltmak için yeni uluslararası yasal araçlardan ziyade, siber güvenlikte güven artırıcı önlemlerin geliştirilmesini teşvik etmelidir (Eren, 2017:81).

AB, Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme, Avrupa İnsan Hakları Sözleşmesi ve AB Temel Haklar Şartı'na internet ortamında da saygı gösterilmesinin ve siber uzayda uygulanmasının nasıl sağlanacağına odaklanması gerektiğine vurgu yapılmıştır. Stratejide AB'nin, hükümetleri ve özel sektörü içeren Kritik Bilgi Altyapısı Koruma (CIIP) ağlarını güçlendirmek için süregelen çabalarını yoğunlaştırması gerektiği de belirtilmiştir. Roller ve sorumluluklar kapsamında, siber tehditlerin sınır ötesi niteliği göz önüne alındığında, strateji, ulusal ve uluslararası siber güvenliği güçlendirmek için AB'deki NIS yetkili makamları, Bilgisayar Acil Müdahale Ekipleri (CERTs) ve kolluk kuvvetleri kurumları arasında paylaşılan bir sorumluluk önermektedir. NIS, kolluk kuvvetleri ve savunmayı kapsayan bir yaklaşımı önerilmiştir. AB düzeyinde, bir dizi kurum siber güvenlikle ilgilenmektedir. Söz konusu kurumlar sırasıyla, ENISA, Europol/EC3, EDA ve NIS şeklindedir. AB, bu kurumlar arasındaki koordinasyon ve işbirliği çalışmalarını gerçekleştirmekten sorumludur (Avrupa Komisyonu, 2013).

AB, normalde bilgi güvenliği ile ilişkili pek çok önlemi almasına rağmen, siber güvenliğin asıl olarak dijital bilgilerin güvenliğinin ele alması boyutunda, bilgi

güvenliği, her türlü bilgi güvenliğini ele alan ve kâğıt belgeleri, fiziksel güvenlik ve insan hatası ile dijital verilerin işlenmesini kapsayan daha geniş bir yaklaşımdır. Etkin bir siber güvenlik duruşu elde etmek için kuruluşlar, tek başına donanım ve yazılım çözümlerinin onları siber tehditlerden korumak için yeterli olmadığını ve daha geniş bir bilgi güvenliği yaklaşımına ihtiyaç duyulduğunu bilmelidir. Komisyona göre etkin bilgi güvenliğinin dört temel alanı insanlar, devlet, süreç ve teknoloji olarak değerlendirilmektedir (ENISA, 2015).

3.4.3. Büyük Bir Siber Saldırı Durumunda AB Desteği

Strateji belgesinde, siber tehdit ve siber saldırı durumlarında yapılacak müdahalelerin de ana hatları çizilmiştir. Olası bir saldırı durumunda, ENISA ve Europol aktif rol oynayarak endüstri paydaşları kurumlar ve AB'ye üye devletlerin kolluk kuvvetleri arasında koordine ve işbirliğini sağlamaya çalışacaklardır. İş devamlılığını ciddi boyutta etkileyen siber saldırılar gerçekleşmesi durumunda gerek üye devletler özelinde gerekse AB çapında gereken desteğin verileceği belirtilmiştir. Bu kapsamda uygulama açısından değerlendirildiğinde, bir siber saldırı olayı gerçekleşmesi durumunda olaydan etkilenen ve saldırıya maruz kalan üye devletlerin kolluk güçleri ile birlikte Europol'ün, söz konusu olayı açığa çıkarmak ve failleri tespit etmek maksadıyla her zaman işbirliği ve koordine içinde olacağı belirtilmiştir (Joın, 2017).

Ayrıca stratejide, devlet destekli bir siber saldırı veya siber casusluk olması durumunda da AB üyesi devletler ile dayanışma içerisinde olunarak, gerek sorumluların tespit edilmesi, gerekse kriz yönetimi konularında AB tarafından ihtiyaç duyulan tüm desteğin verileceği bildirilmiştir. Ulusal ve uluslararası güvenlik uygulamaları bağlamında da üye ülkelere erken uyarı mekanizması tesis etmek için gereken bilgilendirmenin yapılacağı belirtilmiştir. Siber saldırı veya siber tehdit kişisel bilgilerin ya da özel hayatın gizliliğinin ihlalini içeren bir durumu oluşturuyorsa bu durumda da, elektronik haberleşme sektörünün korunması ve kişisel verilerin işlenmesi ile ilgili" 2002/58/EC (Elektronik Haberleşme ve Gizlilik Direktifi) sayılı direktif" kapsamına veri koruma mekanizmalarının da dâhil edileceği belirtilmiştir. Üye devletlere yüklemiş olunan bu sorumluluklar, güvenlikleştirme aşamasında tehdidin tespit edilip, tanımlanmasından sonraki safhada gerçekleştirilecek önlemlerden olduğu değerlendirilmektedir. Zira gerek üye

devletler gerekse AB nezdinde alınan sorumluluklar hayati öneme haiz birimlerin güvenliğinin sağlanmasında kullanılacak metotları ve süreçleri kapsamaktadır. Kolluk kuvvetleri ve güvenlik güçleri boyutunda ele alınan bir konu olması konunun önemini açıkça ortaya koymaktadır. Bu kapsamda da sorumlulukların ve rollerin güvenlikleştirmenin beka perspektifinden değerlendirilmesinin gerekliliğini hissettirmektedir (Cox ve diğerleri, 2002).

3.5. TÜRKİYE

Türkiye'nin, siber güvenlik stratejisi hakkında bilgi sahibi olunabilmesi amacıyla öncelikli olarak, siber güvenlik ve siber uzay ile ilgili ilk strateji belgesi olma özelliği bulunan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın" yayınlanmasına kadar geçen süreçte gerçekleştirilen siber güvenlik çalışmalarının kısa bir analizi yapılarak, müteakiben söz konusu planın stratejik eylem başlıkları altında siber güvenlik sorumluluk ve görevlerin paylaşımı, kamu kuruluş ve kurumları, sivil teşebbüsler ve üniversiteler tarafından 2018 yılına kadar gerçekleştirilen çalışmalar ve faaliyetler incelenecektir. Gerçekleştirilen çalışmalar ve faaliyetler değerlendirildikten sonra, Türkiye'nin siber güvenlik stratejisi hakkında en güncel belge olma özelliği bulunduran, 2016 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın yayınladığı, 2013-2014 Eylem Planındaki faaliyetlerin icra edilirken karşılaşılan güçlükler, gerçekleşme dereceleri ve geleceğe yönelik değerlendirmeler dikkate alınarak tasarlanan, Türkiye'nin stratejisini açıklamak adına önemli olduğu değerlendirilen, 2016-2019 Ulusal Siber Güvenlik Stratejisi analiz edilecektir.

3.5.1. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

2017 yılı verilerine göre Türkiye nüfusunun yüzde 57,4'ü internet kullanmaktadır. Bu kapsamda Türkiye'de dünya üzerinde gerçekleştirilen siber saldırılardan etkilenmesi sebebiyle, gerek siber uzayda etkin konumda olabilmek gerekse siber saldırılara karşı kendini koruyabilmek amacıyla çalışmalar gerçekleştirmeye başlamıştır. Türkiye, 2009 yılında siber güvenlik konularını kapsayan ilk çalışma olarak değerlendirilebilecek "Ulusal Sanal Ortam Güvenlik Politikası'nı" oluşturmuştur (Çubukçu ve Bayzan, 2013:160). Bahsedilen politikayla Türkiye, muhtemel siber saldırılardan korunmayı amaçlayarak, siber ortamın

güvenlik aşamalarının ve kriterlerinin belirlenmesini hedeflenmiştir.

Türkiye'nin siber güvenlik faaliyetleri, Bakanlar Kurulu'nun 2012 yılında almış olduğu *"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı"* ile resmi boyuta ulaşmıştır. Bahse konu karar kapsamında Türkiye'de siber güvenliğin tesis edilmesine ilişkin strateji, politika ve eylem tasarıları ve planları hazırlamak, bu alanda koordinasyonunu sağlamak görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına (UHDB) verilmiştir. Ayrıca Türkiye'de siber güvenlik konularını kapsayan usul, esas ve standartların onaylanması, bu alanda alınması gereken önlemlerin belirlenmesi, hazırlanan, rapor, plan, program ve bunların koordinasyon işlemlerinin sağlanması amacıyla birçok üst düzey yöneticilerinde aralarında bulunduğu Siber Güvenlik Kurulu oluşturulmuştur. Siber Güvenlik Kurulu'nun ortaya koymuş olduğu strateji, politika ve planların, tüm kamu kuruluş ve kurumları tarafından uygulanması, yerine getirilmesi ve belirlenen standartlara, usul ve esaslara uyulması yükümlülükleri getirilmiştir (UHDB, 2017).

3.5.2. Türkiye'nin İlk Siber Güvenlik Strateji Belgesi

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", Türkiye'nin ilk siber güvenlik eylem planı olarak Siber Güvenlik Kurulu üyeleri tarafından kararlaştırılmıştır. Söz konusu plan yedi ana başlıktan oluşmaktadır ve bu planda siber güvenliğin tesisi amacıyla gereken yasal düzenlemelerin gerçekleştirilmesi, kolluk kuvvetlerine yardımcı olacak faaliyetlerin yürütülmesi ve siber saldırılara karşı koymak amacıyla Ulusal Siber Olaylara Müdahale Organizasyonu'nun kurulması gibi önemli kararlar alınmıştır. Belirlenen strateji ve hedefler çerçevesinde yedi gün yirmi dört saat esasına göre çalışılarak siber saldırı ve sabotaj olaylarına yönelik uyarı, alarm mekanizmaları oluşturularak siber saldırıların önlenmesinde gerek ulusal gerekse uluslararası koordinasyonun sağlanması amacıyla ve Telekomünikasyon İletişim Başkanlığı'nın (TİB) yönetiminde faaliyetlerini sürdürmek üzere, Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur (Resmi Gazete, 2015c). 2014 yılında kurulan USOM, uluslararası ve ulusal düzeyde siber uzayda ortaya çıkan tehditler ve siber saldırıları değerlendirerek, sözü edilen tehditlerin tespit edilmesi ve saldırıların bertaraf edilmesi amacıyla özel kuruluşlar

dâhil, kamu kurum ve kuruluşları arasındaki koordinasyonu sağlamaktadır. Bunlarla birlikte, ulusal ve uluslararası siber güvenlik tatbikatları düzenlenerek, devlet kurumlarının siber saldırılara karşı hazırlığının ve farkındalığının arttırılması faaliyetleri de Ulusal Siber Olaylara Müdahale Merkezi'nin görevleri arasında yer almaktadır. Ancak 17 Ağustos 2016 tarihinde Türkiye'nin resmi gazetesinde yayımlanan 671 sayılı Kanun Hükmünde Kararname (KHK) ile Telekomünikasyon İletişim Başkanlığı'nın kapatılması sonucunda USOM faaliyetlerini BTK bünyesinde sürdürmeye devam etmektedir (USOM, 2017).

USOM'un haricinde elektronik ve haberleşme alanındaki koordinasyonu ve işbirliğini gerçekleştirmek üzere 10 Eylül 2014 tarihinde sektörel ve kurumsal "Siber Olaylara Müdahale Ekibi (SOME)" kurulmuştur. Kurumsal SOME'ler kurumlarına dolaylı olarak ya da doğrudan gerçekleştirilen veya gerçekleştirilmesi muhtemel siber ataklara karşı gerekli önlemleri almak amacıyla uyarı, bilgilendirme ve koordinasyonu sağlarken, Sektörel SOME'ler enerji, finans, ulaştırma, elektronik haberleşme ve su yönetimi sektörleri gibi kritik olarak değerlendirilen altyapıların güvenliğini sağlamak amacıyla faaliyetlerini gerçekleştirmektedir. Kurumsal SOME'ler gerçekleşmesi olası siber saldırılara karşı gerekli tedbirleri alma ve bu tür siber olaylara karşı müdahalede bulunacak mekanizmayı oluşturarak, bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler (BTK, 2017).

3.5.3. 2016-2019 Ulusal Siber Güvenlik Stratejisi

2013 yılında Türkiye'nin ilk siber güvenlik strateji belgesi oluşturulmuş ve planlanan stratejinin büyük bir çoğunluğu uygulanmıştır. Ancak, küresel dünyada büyük bir hızla ilerleyen teknolojik gelişmeler ve yeni siber araçlarla daha hareketli bir yapıya bürünen siber ortamda, siber güvenlik kapsamında yeni sistemlerin oluşturularak, alternatif tedbirlerin alınması ihtiyacı ortaya çıkmıştır. Türkiye'de yeni bir strateji ve güvenlik belgesi oluşturmak için gerçekleştirilen çalışmalar çerçevesinde, çeşitli sivil toplum ve kamu kuruluşlarındaki uzman personelin de katılımıyla''*Ortak Akıl Platformu''* gerçekleştirilmiştir. Söz konusu platformda Türkiye'nin siber güvenlik alanındaki zayıf ve güçlü yönleri ele alınarak stratejik amaçları güncellenmiş ve gelecek dönemlerde gerçekleştirmesi gereken faaliyetler

belirlenmiştir. Bu kapsamda *"2016-2019 Ulusal Siber Güvenlik Eylem Planı*" ve "*2016-2019 Ulusal Siber Güvenlik Stratejisi"* yayımlanmıştır (Türkiye Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016).

Bu stratejide, Türkiye'de siber güvenliğin sağlanması yönünde hedefler ve politikalar belirlenirken Asya, Amerika ve Avrupa'dan bir çok sayıda devletin siber güvenlik stratejileri analiz edilerek bu devletlerin siber güvenlik hedef, kapsam ve öncelikleri dikkate alınmış ve bu yönde alternatif bir strateji belgesi hazırlanmıştır. Ancak, diğer devletlerin siber güvenlik stratejileri değerlendirildiğinde olası bir siber saldırı olayında, oluşan tehditler ve bu tehditleri bertaraf edecek eylemler uygulanırken uygulanan yöntemlerin ve risklerin birçok devlette farklılık göstermediği görülmüştür. Birçok devlette aynı olan yöntemleri incelediğimizde, öncelikle siber güvenliğin tesis edilmesinin yalnızca devletin değil eşzamanlı olarak, bireyler başta olmak üzere tüm kuruluş ve kurumlarının görevi ve yasal sorumluluğu olduğu ve bu sebeple bilgi paylaşımı ve işbirliğinin gerekliliği vurgulanmıştır. Ayrıca "Uluslararası Siber Güvenlik Operasyon Merkezleri" arasında üst düzey siber saldırı yönetimi mekanizmaları ve mutlak işbirliğinin olmasının gerekliliğine yer verilmiştir. Devletlerin stratejilerinde yer alan riskleri değerlendirdiğimizde öncelikle siber konulara hâkimlik ve uzman personel bağlamında yetersizliğin neden olduğu, kamu kurumları ve özel teşebbüsler arası koordinasyon eksikliği siber alanda gerçekleşen saldırılara karşı başarısız olunması durumunu arttırdığı değerlendirilmektedir. Bu kapsamda, bahse konu strateji belgesinde siber güvenlik ve bilgi sistemleri alanında uzman personel yetiştirilmesi ve bu alanda çalışma yapmak, uzmanlaşmak isteyen öğrenci, araştırmacı ve personellerin gerekliliği vurgulanmıştır (Yüksel, 2016) (UDHB, 2016).

Türkiye'de stratejik plan kapsamında, toplumu ve kritik altyapıları etkileyebilecek tehditleri ve riskleri azaltmaya yönelik eylem planlarının oluşturulması planlanmaktadır. Bu nedenle Türkiye stratejisinde, toplumu ve kurumları öncelikle maddi açıdan zarara uğratan siber saldırılar ve siber suçlarla etkin mücadele edilmesi ve siber suçlular için ihtiyaç duyulan hukuki düzenlemelerin yapılmasının gerekliliği belirtilmiştir. Aynı zamanda toplumun tüm kesiminin siber saldırılara ve tehditlere maruz kalma ihtimali bulunduğundan, toplumun her

kesiminin siber güvenlik ve siber ortam unsurlarının bilincine sahip olması amacıyla modern çalışmalar gerçekleştirilmesi planlanmıştır. Bunlarla birlikte siber güvenlik, milli güvenlik ile bütünleştirilerek mevcut kritik ağ altyapılarına herhangi bir siber saldırı olması durumunda meydana gelebilecek zararın azaltılması yönünde hedefler belirlenmiştir (UDHB, 2016:15).

Türkiye'nin siber alandaki mevcut konumu, çok iyi bir seviyede olmamakla birlikte, gelişmiş ülkelere kıyasla, olması gereken normal seviyenin de aşağısında olduğu değerlendirilmektedir. Geçmişte yaşanan siber saldırılarda devlet kurumlarına ait internet sayfalarına erişim yavaşlamış ve hatta işlem yapılamaz boyutlara ulaşmıştır. Söz konusu durum bankacılık ve finans sektöründe de mevcut olup siber saldırıya maruz kalındığında kriz yönetimi sağlanamadığı için bankaların müşterileri bankacılık işlemlerini gerçekleştirememektedir. Türkiye'nin, söz konusu eksikliklerin farkına varıp özeleştiri yaparak, Estonya örneğinde olduğu gibi olası bir siber saldırıda büyük zararlar meydana gelmeden, ihtiyaç duyulan tedbir ve önlemleri alması gerekmektedir.

Türkiye'de siber ortamın güvenliğinin sağlanması noktasında başarıya ulaşılabilmesi için, öncelikle kritik altyapı ağlarına internet erişimi sağlayan cihaz ve sistemlerde, yerli üretim ürünlerin, yazılımların, işletim sistemlerinin, güvenlik duvarlarının ve antivirüs programlarının kullanılması gerekmektedir. Milli üretim donanım ve yazılım ürünleri kullanılmadığı müddetçe Türkiye'nin siber ortamda başarılı olmasının mümkün olmadığı değerlendirilmektedir. Çünkü ithal edilen donanım veya yazılımlar, bünyesinde önceden kasıtlı bir biçimde yerleştirilmiş olan zararlı yazılımlar veya arka kapılar nedeniyle siber korsanların açık hedefi olmaktadırlar. Türkiye'nin yerli üretim donanım ve yazılımlara sahip olabilmesi için, Türkiye'de bulunan üniversiteler nezdinde, çeşitli kuruluşlar ve kurumlar ile AR-GE faaliyetleri gerçekleştirilerek siber alanda önemli adımlar atılması gerekmektedir.

3.6. SONUÇ

Hükümetler, modern toplumların finansal sistemlerden nakil ağlarına kadar her alanda bilgisayar sistemlerine giderek artan derecede bağımlı olduklarını bilmektedir. Hükümetlere göre, söz konusu bilişim sistemlerinin kapatılması ya da

zarar verilmesi için virüs ya da diğer araçlarla korsanlar kullanılmakta ve bu silahların hedef üzerinde konvansiyonel silahlardan daha fazla tesir oluşturma kapasiteleri bulunmaktadır. Geleneksel askeri saldırıların aksine, herhangi bir bölgeden, iz ve emare bırakmadan anında bir siber saldırı başlatılabilir. Ayrıca, siber saldırılarda; geleneksel saldırı gibi, faillerine kesin olarak ulaşılması veya misilleme yapılması son derece zor olmaktadır.

Sonuç olarak, hükümetler ve istihbarat teşkilatları, hayati altyapıya (bankacılık sistemleri veya elektrik şebekeleri gibi) yönelik dijital saldırıların, (Whittaker, 2017) saldırganlara bir ülkenin geleneksel savunmasını atlatmanın bir yolunu sağlayacağından ve ülkelerin bilgisayar güvenliğini artırmak için sürekli bir güvenlik ikilemi yaşayacağından endişe duymaktadır.

Bununla birlikte devletler strateji belirlerken, siber savaş yeteneklerinin, askerleri riske atmak zorunda kalmadan rakip devletler üzerinde etkide bulunmak için yeni bir yol sunan fırsatlarını da görmektedirler. Rakiplerinin siber silahlarına karşı savunmasız olma korkusu ve bu araçları dünyadaki kendi duruşlarını güçlendirmek için kullanma isteği, birçok ülkeyi siber silahlanma yarışına sürüklemektedir.

BÖLÜM 4

SİBER UZAY'DA İŞBİRLİĞİ VE ORTAK POLİTİKA ÜRETME SORUNU

Çalışmamızın bu bölümünde, siber güvenlik alanındaki farklı öz düzenleme türlerinin teorik ve pratik sonuçları analiz edilecektir. Son yirmi yılda, siber güvenlik ve kritik bilgi altyapısının korunmasına yönelik yaklaşımlar, kamu-özel işbirliğinin gerekliliği, çok yönlü stratejiler ve endüstrinin bilgi ağlarının güvenliğini sağlamada oynadığı önemli rolün tanınması üzerine dayanmaktadır. Bununla birlikte, politika gündeminin zirvesindeki siber güvenlik vurgusunun arttırılmasıyla, birçok hükümet ve akademisyen, özel sektörün bilgi ağlarında devlet müdahalesi olmadan kabul edilebilir güvenlik düzeyi sağlamadaki olası başarısızlığı ile ilgilenmektedir. Konseptin bu kayması, güvenlik olaylarının zorunlu olarak raporlanması ve bilgi, güvenlik standartları ve uygunluk prosedürlerinin paylaşılması zorunluluklarının tanımlanması şeklinde siber güvenliği yasama önerilerini

beraberinde getirmiştir. Bu gelişmeler, siber güvenlikteki dengenin aşağıdan yukarıya toplumun her kesiminde gönüllü yaklaşımlardan ve işbirliğinden daha yoğun bir düzenlemeye kaydırılması konusunda birçok kaygı uyandırmaktadır. Bu bölüm, belirttiğimiz dizinlerin olumsuz sonuçlara yol açabileceğini ve siber güvenliği sağlamanın en iyi yolunun, işbirliği ve sanayi ile hükümetler arasında güven oluşturmak için mevcut kanalların evrimi olduğunu açıklamaktadır.

Jervis (2011)'e göre; uluslararası anarşi ve güvenlik ikilemi, egemen devletler arasında işbirliğini zorlaştırmaktadır. Güç dengesi sistemlerinin birlikte hareket etme biçimine dönüşmesi, büyük antihegemonik savaşlardan sonra ortaya çıkma eğilimindedir. Bu tür savaşlar, güç dengesi sistemini destekleyen varsayımları çürütmekte ve aktörlerin kazancını işbirliğini teşvik edecek şekilde değiştirmektedir. ''Güvenlik İkilemi Altında İşbirliği" kapsamında geliştirilen mantık şu şekilde ifade edilmektedir; büyük koalisyon dağılırsa ortaya çıkacak maliyetlerin artması nedeniyle, devletler birbirleriyle işbirliği yapmak için daha fazla teşvik oluşturmaktadırlar, bu durumda devletlerin diğerlerinin gerçekleştirebileceği saldırılardan korkması için daha az neden bulunmaktadır. İşbirliği, her bir devletin başkalarının ne yaptığını görme yeteneğini artıran mekanizmalarla daha da kolaylaştırılmaktadır (Jervis, 2011:1).

4.1. ULUSLARARASI HUKUKUN VE SİBER NORMLARIN EKSİKLİĞİ

Rusya'nın ABD'nin 2016 yılında yapılan cumhurbaşkanlığı seçimlerini Donald Trump'a doğru çarptırmaya yönelik siber müdahaleleri, 2015'te Ukrayna'nın elektrik sistemini bozan anonim siber saldırıları ve İran'daki santrifüjü tahrip eden ''Stuxnet" virüsünü içeren bir dizi siber saldırı, siber uzayda yaşanan çatışmalarla ilgili endişeleri arttırmıştır. 2017 yılında gerçekleştirilen Münih Güvenlik Konferansı'nda Hollanda Dışişleri Bakanı Bert Koenders, Birleşmiş Milletler Uzmanlar Grubunu (GGE) desteklemek için Siber İstikrar Komisyonu adı altında yeni bir uluslararası Küresel Komisyon oluşturulduğunu bildirmiştir (S.Nye, 2017).

Şubat 2017'de Hollanda'da Küresel Siber İstikrar Komisyonu ''Global Commıssıon On The Stabılıty Of Cyberspace'' kurulmuştur. Başkan Marina Kaljurand komisyonun hedefini, "siber uzayda devlet ve devlet dışı aktörler tarafından gerçekleştirilmesi istenen davranışlara rehberlik edecek normlar ve

politika önerileri geliştirerek uluslararası barışı, güvenliği ve istikrarı artırmak" olduğunu belirtmiştir. Söz konusu komisyonun 19-20 Eylül 2018 tarihinde Singapur'da gerçekleştirdiği toplantıda[5], katılımcılar tarafından altı adet evrensel norm belirlenmiştir. Bu normların, küresel bir toplum olarak siber istikrarı ve işbirliğini gerçekleştirmek amacıyla hükümet, özel sektör ve sivil toplum içindeki karar vericilere yardımcı olacağı değerlendirilmiştir. Siber alanın birbirine bağlı doğası, küresel topluluğun üzerinde anlaşabileceği ''yolun kuralları" nı belirlemeyi gerektirmektedir ve bahse konu çaba bu yönde gerçekleştirilen önemli bir adım olarak nitelendirilmektedir. Ayrıca, söz konusu komisyon toplantısında bulunan BM Genel Sekreteri Müsteşarlığı ve Silahsızlanma İşleri Yüksek Temsilcisi Izumi Nakamitsu,''Tüm paydaşlar siber uzayda neyin kabul edilebilir, neyin kabul edilemez olduğu hakkındaki küresel bir anlayışı ilerletmek için normlar ve neyi temsil ettikleri üzerine tartışmaya devam etmelidir" şeklinde bir çağrıda bulunmuştur (GCSC, 2018).

4.1.1. Yasal Çerçevelerin Geliştirilmesi

Siber uzayda özel aktörlerin sayısının artması ile uluslararası hukukun uygulanması da önemli bir sorun olarak karşımıza çıkmaktadır. Hukuk da kural yapmak önemli bir faktördür, ancak bu kurallar zorunlu ihtiyaçlar çerçevesinde değilse belirli bir zaman sonra önemini yitirmektedir. Bu konu her durum için geçerlidir; uzayda, dünyada ya da siber uzayda çoğu mesele yorum ve değerlendirmeye açıktır. Sadece sorunların yaşandığı istisnai durumlarda, bir kuralın geçerliliğini ve uygulanabilirliğini "test etmek" gerekir. Tüm kavramlar üzerinde akademisyenler, öncelikle kuralların insanların davranışlarına ve insan doğasına uygun olup olmadığını tartışmaktadırlar. Genellikle, bu kurallara uyulmamasının sonucunda bir yaptırım olabileceği bilgisinin olduğu varsayılmaktadır. Yaptırım

[5] Söz konusu toplantı, devletlere siber alanda ortak strateji ve normlar sunması açısından yakın geçmişteki önemli gelişmelerden biridir. Önerilen normlar Birleşmiş Milletler Silahsızlanma Araştırmaları Bürosu (UNODA), Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR), Birleşmiş Milletler Genel Sekreteri Dijital İşbirliği, Üst Düzey Kuruluşu Organizasyonu'nun üst düzey temsilcileri tarafından tartışılmıştır. Avrupa Güvenlik ve İşbirliği (AGİT) ve Avrupa Birliği'nden siber koordinatörler ve Avustralya, Belçika, Kanada, Estonya, Finlandiya, Fransa, Almanya, Macaristan, Hindistan, Japonya, Kenya, Meksika, Hollanda, Yeni Zelanda, Norveç, Polonya, Singapur, İsviçre, Birleşik Krallık ve Amerika'dan üst düzey yetkililer toplantıya katılmışlardır. Asya-Pasifik Ağ Bilgi Merkezi (APNIC), FIRST, ICANN, Microsoft, JP Morgan Chase ve S dâhil olmak üzere sivil toplum ve özel kuruluşlar da toplantıda temsil edilmiştir.

uygulanırken söz konusu kuralın ihlal edildiğinin tespiti çok önemlidir. Siber uzayda da ülkeler tarafından kabul gören yasal bir sistem olabileceği değerlendirilmektedir. Ancak hâlihazırda siber olaylara müdahale kapsamında, uluslararası arenada bu konu açık ve net bir biçimde ortaya konulamamaktadır. Bu nedenle siber alanda otoriteyi kurmak ve işletmek için, bir sistem tarafından desteklenen kuralları oluşturmak ve gerekirse yaptırımlar uygulamak gerekmektedir (Metcalf, 2018). Siber saldırıların, fiziksel ve ekonomik zararlara neden olmasının yanı sıra, büyük yıkımlara ve ölümlere de neden olabilecek kabiliyetlere ulaştığı değerlendirilmektedir. Bu kapsamda, yüksek teknolojinin ulaştığı boyutlar ve imkânlar değerlendirilerek olası siber saldırı senaryoları oluşturulmakta ve devletler tarafından söz konusu saldırılara karşı önlem alma ve strateji geliştirme çalışmaları üretilmekte iken, diğer taraftan hukuk disiplininde oluşması muhtemel sorunlar tartışılmaktadır.

Yayla (2014)'e göre; uluslararası ortamın doğasında gerçekleşen iki önemli değişim ve etkileşim; BM Güvenlik Antlaşması'nda öngörülemeyen kritik sorunların oluşmasına neden olmuştur. Bunlardan ilki, yaşanan teknolojik gelişmelerle birlikte mevcut silah kavramında ve silah sistemlerinde yaşanan değişimdir. Zira BM Güvenlik Antlaşması, bilişim çağı öncesi bir antlaşmadır ve siber ortamın imkânlarını ve boyutlarını öngörememiştir. Bilgi sistemlerinde yaşanan gelişmeler, birçok hukuk kurallarını ve BM Güvenlik Antlaşması'nı çağ dışı olarak nitelendirilecek bir durumda bırakmıştır. Diğer değişim ise, siber güvenlik konusunun ve tehdit yaklaşımlarının farklılaşan yapısı ve bu durumun uluslararası toplum tarafından anlaşılması hususunda yaşanan değişimdir. Siber güvenlik kavramı, artık ulusal çerçevede değerlendirilecek boyutu aşmış ve uluslararası boyuta geçmiştir. Siber ortamın mekân tanımayan doğası kapsamında, devlet dışı aktörler uluslararası ölçekte örgütlenerek, aynı zaman diliminde farklı ülkelere ya da kuruluşlara siber saldırı eylemleri gerçekleştirebilmektedirler. Zira bu noktada en önemli konu bahse konu siber saldırıların, can ve mal kayıpları gibi büyük yıkımları gerçekleştirebilecek boyutlara ulaşmasıdır. Söz konusu gelişmeler, siber tehditlere etkin bir biçimde müdahale etmek için, mevcut uluslararası antlaşmaların yetersiz kaldığını göstermektedir. Diğer taraftan ülkeler boyutunda, kuvvet kullanılmasının çerçevesini belirlemek için planlanmış olan BM sistemi, devlet harici aktörler tarafından yapılan saldırılar gibi sorunlarla etkin biçimde ilgilenmede önemli

derecede zorluklarla karşılaşmaktadır (Yayla, 2014:184).

Siber ortam artık birçok ülkede kara, hava, uzay ve deniz gibi çatışma ve askeri harekat bölgesi olarak nitelendirilmektedir. Bu kapsamda gelecek yıllarda, dünyanın büyük olasılıkla e-dünyaya dönüşmesi durumu düşünüldüğünde siber saldırıların çok büyük yıkımlara neden olacağı için siber güvenlik hususunda gerekli tedbirlerin alınmasına elzem bir biçimde ihtiyaç duyulmaktadır. Alınacak tedbir ve önlemler başarılı olabilmesi için küresel ölçekte gerçekleştirilmesi gerekmektedir. Uluslararası çapta koordinasyon ve işbirliği sağlanarak ortak kabul ve anlayışların oluşturulması, problem sahalarının çözülmesi ve önlenmesi, önlenemese bile meydana geldikten sonra asgari zararla ve hızla çözülebilmesi konularında yapılacak çalışmalar büyük önem arz etmektedir. Bu bağlamda, bütün devletlerin katılım sağlayacağı sözleşme ve antlaşmalar sayesinde uluslararası bir hukuk çerçevesinin geliştirilmesi ve bu hukuki çerçeve içerisinde emniyet ve yargı unsurlarının etkin ve hızlı çalışabilme durumlarının tesis edilmesi öncelikli ihtiyaçlardandır. Ayrıca siber uzayda da diğer alanlarla benzer olarak "silahlı çatışma hukuku"na benzer davranış standartlarına ve normlara sahip olunması gerekmektedir. Uluslararası siber güvenlik düzenlemelerini oluştururken literatürde yer alan diğer ortak alan düzenlemelerin ve işbirliklerinin örnek olarak alınabileceği değerlendirilmektedir. Ancak söz konusu çalışmalara tüm ülkeler katılım sağlayıp ısrarla takip etmezse gerçekçi ve etkin bir çerçevenin oluşturulması çok zordur.

4.1.2. Siber Suçlar ve Siber Terörizm

İnternet, suçlulara göreceli anonimliğe sahip saldırıların başlatılması için bir yol sağlayarak suçların işlenmesini kolaylaştırmıştır. İletişim ve ağ altyapısının artan karmaşıklığı, siber suçların araştırılmasını zorlaştırmaktadır. Yasadışı faaliyetlere ilişkin ipuçları genellikle suçları tespit etmek ve delil toplamak amacıyla elenmesi gereken büyük miktardaki verileri içermektedir. **S**iber suçlular sıklıkla, temel olarak iyi bilinen teknik açıklardan yararlanmaktadırlar. Bununla birlikte, internet ve bilgisayar suçlarının çok karmaşık olabileceği ve yönetişim boşluğu göz önüne alındığında cezalandırılmasının özellikle zor olduğu da önemli bir gerçektir. Siber uzayı karakterize eden: siber suç baskısı, aktörler, motivasyonlar ve saldırının asıl kapsamı ile ilgili belirsizlik bağlamında, unsurların tespiti hususunda uluslararası koordinasyonu gerekmektedir. Siber suç grupları sınırlar arasında faaliyet

gösterdiğinden, devletler onlarla tek başına mücadele edemezler ve suçlular genellikle siber bir saldırıya atıfta bulunma, uluslararası soruşturmalar yürütme ve suçluları yabancı bir ülkede işlenen bir suçun adaletine getirme konusundaki doğal mücadeleden yararlanmaktadırlar (ICDF2C, 2015).

Siber suçlara karşı uluslararası işbirliğinde her ne kadar yetersiz kalsa da siber diplomasinin gerçekte iyi sonuçlar üreten bir alan olduğu değerlendirilmektedir. 60'tan fazla ülke tarafından imzalanan Avrupa Konseyi'nin 2001'deki Siber Suçlar Konvansiyonu Sözleşmesi (Budapeşte Konvansiyonu), ulusal temas noktalarının kurulmasını, ulusal uyumu uyumlaştırmayı zorunlu kılarak internet ve bilgisayar suçlarını ele alan ilk uluslararası anlaşmadır (GFCE, 2016). Ancak mevzuatın genişletilmesi, araştırma tekniklerinin uyumlaştırılması ve daha güçlü bir uluslararası işbirliğine ihtiyaç duyulmaktadır. Uluslararası toplumun tüm çabalarına rağmen, sözleşme bugün devletlere siber alanda kötü niyetli faaliyetleri ele alma biçiminde yükümlülükler yükleyen tek çok taraflı antlaşma olarak durmaktadır.

Bununla birlikte, ulus ötesi siber suçlara karşı uluslararası işbirliğini geliştirme amaçlı çok taraflı çabalar, Budapeşte Konvansiyonu'nun çok ötesine geçmektedir. Bir yandan, bu durum, siber suçun, devletlerin, yerel düzeyde ve uluslararası işbirliğini de içeren, yeterli bir potansiyele sahip olması beklenen ekonomik yükünün ciddiyetini yansıtmaktadır. Öte yandan, uluslararası toplum bu alanda bu kadar yüksek bir işbirliğine ulaşmışsa, bunun nedeninin siber suçun temel olarak geleneksel bir "kolluk kuvveti" yaklaşımıyla ilgilenilmesi gereken bir " kamu düzeni" meselesi olarak kabul edilmesi olduğu değerlendirilmektedir. Bu anlamda, uluslararası işbirliği kısıtlamanın tam aksine aslında ulusal egemenliği pekiştirmektedir: kolluk kuvvetleri ve adli uluslararası işbirliği, siber güvenliğin uluslararası işbirliğinin temel ve basit unsurlarıdır.

Genel olarak, siber suçların ulusötesi organize suç olarak anlaşılması durumu yaygındır. Geçmiş de yaşanan ulusötesi suç olayları değerlendirildiğinde; uluslararası işbirliğine karşıt olarak bulunan ulusötesi organize suç gruplarının, devletin otoritesine doğrudan bir meydan okuma oluşturduğu değerlendirilmektedir. Uluslararası suç örgütleri, dünya ekonomisine finansal bir yük getirmekte ve ayrıca uluslararası normları ve istikrarı aşındırmaktadır. Başkan Clinton, 50. yıldönümünde Birleşmiş Milletler Genel Kurulu'nda yaptığı açıklamada,

uluslararası suç güçlerinin "barış ve özgürlüğe yönelik küresel eğilimi tehlikeye attığını, kırılgan demokrasilere zarar verdiğini, gelişmekte olan ülkelerden gelen gücü azalttığını ve bu ülkelerle işbirliği inşa etme çabalarımızı tehdit etmektedir" şeklinde belirtmiştir (Rugge, 2018). Ancak, siber alan "belirsizlik alanı" dır ve siber suçun zararı, internet kullanıcıları arasında yarattığı güven kaybından ve dünya ekonomisine getirdiği maliyetlerden çok daha büyüktür. Kanun uygulayıcı bakış açısından değerlendirildiğinde siber suçlar aslında ulusal ve uluslararası güvenliği doğrudan etkilemekte ve geleneksel organize suçları aşan ölçekte bir olgu olduğu değerlendirilmektedir.

4.1.3. Siber Saldırı Caydırıcılığının Zorluğu

Nükleer silahların inanılmaz gücü, askeri bir strateji olan caydırıcılığa neden olmuştur. Orduların amacı, savaşları kazanmaktan ziyade onları önlemeye çalışmaya çevrilmiştir. Siber saldırılar başlı başına bir nükleer patlama ile karşılaştırılamaz, ancak yirmi birinci yüzyılda yaşanan siber savaş örnekleri gelecekteki uluslararası çatışmalarda başrol oynayacağı değerlendirilen siber tehditlerin ciddi boyutlara ulaştığını ortaya koymaktadır. Bu konuda, ulusal güvenlik planlayıcıları, reaktif, taktik siber savunmanın ötesine bakmaya başlayarak, uluslararası askeri caydırıcılığı da içerebilecek proaktif, stratejik siber savunma stratejileri geliştirmek amacıyla çalışmalar gerçekleştirmektedirler.

Libicki (2009)'a göre; siber savaşta, saldırganlar müthiş avantajlara sahiptir. Bu avantajlardan en önemlisi anonimlik kavramıdır. Saldırganın kimliği, konumu ve saldırının kanıtlanabilirliğinin açık bir biçimde ortaya koyulamaması gerçekleştirilen tüm suç eylemleri karşısında bilgisayar korsanlarına hiçbir yaptırım olmaması sonucunu doğurmaktadır. Ayrıca siber uzayda gerçekleştirilen faaliyetlerin inkâr edilebilirlik boyutu da uluslararası ilişkilerde bir endişe kaynağı olarak karşımıza çıkmaktadır. Zira bilgisayar korsanları gerçeği gizleyerek bir dizi uyuşmazlık algoritmaları oluşturabilmekte ve saldırıları kasıtlı bir biçimde üçüncü bir aktörün gerçekleştirdiği izlenimi yaratarak suçu başkasının üzerine atmaya çalışmaktadırlar. "Siber saldırılar cezasız kalabilecek bir biçimde yapılabilirse, saldırganın durması için caydırıcı bir neden bulunmamaktadır" (Libicki, 2009).

Bunlarla birlikte, Alperovitch (2011)'e göre; siber saldırıların tespitinin kesin ve net bir biçimde yapılması durumunda dahi, ''ceza ve caydırıcılık'' yönteminin

uygulanabilirliği çok zordur. Karar vericilerin karşı karşıya olduğu önemli bir karar; bir siber saldırı sonrasında misillemede bulunup bulunulmayacağının değerlendirilmesidir. Kritik durumlarda geleneksel silahlar kullanmak icap edebileceği değerlendirilmektedir. Ancak çatışmayı siber alan içinde tutmayan bir misillemenin orantılı güç kullanımı yasasına da aykırı olması sebebiyle gerçekleştirilmesi çok zordur. Zira bir siber karşı saldırının ise tesir açısından gereken hassasiyetten yoksun olacağı değerlendirilmektedir (Alperovitch, 3. Uluslararası Siber Çatışma Konferansı, 2011). Caydırıcılık için kesin tahminler sadece rasyonel rakipler için yapılabilmektedir. Siber uzayda aktörler siber saldırılarının maliyetine fazla önem vermeyen irrasyonel aktörleri her zaman caydıramaz. Varsayımlar, bu somut olmayan caydırıcılık konseptinin doğal bir parçasıdır. Ancak, uluslararası zeminde siber güvenliği sağlamak için gelecek vaat eden yöntemlere, geniş kaynaklar harcayarak etkili bir caydırıcı çerçevenin oluşturulması gerekmektedir.

4.2. ÜLKELER ARASINDA YAŞANAN GÜVENLİK İKİLEMİ

Güvenlik analizlerinde realist paradigmalar anlayışı dâhilinde gerçekleşen gelişme sürecinde, ortaya çıkan ''güvenlik ikilemi (security dilemma)'' kavramı temel olarak; bir devletin diğer bir devleti tehdit olarak görmesi sebebiyle silahlanması neticesinde, diğer devletin veya devletlerin de aynı şekilde karşılık vermesi sonucu oluşan bir kısır döngü süreci olarak tanımlanmaktadır (Arı, 2010:198). Günümüzde siber güvenlik konusunun ise, devletlerin, kurumların ve bireylerin gündeminde son derece önemli bir konu haline geldiği açıkça görülmektedir. Bu kapsamda güvenlik anlayışlarına yönelik olarak, siber uzay merkezli ve uluslararası siber ortamdan kaynaklanan yeni sorunlar ve bu sorunlara karşı devletlerin oluşturduğu güvenlik uygulamaları güvenlik ikilemi yaklaşımını daha karmaşık bir yapıya dönüştürmüştür.

Şekil 3: Ülkeler Arasındaki Güvenlik Diyagramı

Kaynak: (Krickovic, 2016)

Özellikle gelişmiş devletler siber uzayı askeri kapasitelerini arttırmak için yeni bir kabiliyet olarak değerlendirmektedirler. Hükümetler siber güvenliği göreceli avantajlar açısından incelemekte ve rakipleriyle tehditler karşısında önleyici ve işbirliği antlaşmaları yapmaktan çekinmektedirler. Otoriter hükümetler, devlet iktidarını ve hükümet otoritesini kontrol etme ve projelendirme konusunda anlaşma çalışmaları yürütürken, demokratik hükümetler direnç ve savunmaya odaklanmaktadırlar. Ayrıca, mevcut uluslararası sistemde iki teknik otorite grubu varlığı görülmektedir; Teknik imkân ve kabiliyetleri yüksek olanlar ve olmayanlar. Teknik açıdan yetenekli hükümetler terörizmle ilgili faaliyetlere odaklanmaktadırlar ve genellikle faaliyet sınırlayıcı anlaşmalara katılmaktadırlar. Yeterli teknik imkânlara sahip olmayanlar ise siber suç faaliyeti konusunda anlaşmalarla meşgul olmaktadırlar (Buchanan, 2017).

4.2.1. Siber Saldırıları Bir Devletin Gerçekleştirmesi veya Desteklemesi İhtimali

Son yıllarda ulus devletler tarafından başlatılan önemli siber saldırılar şunları içermektedir: Stuxnet (iddiaya göre İsrail ve ABD); Estonya karşısında DDoS saldırıları, Ukrayna'nın sanayi kontrol sistemlerine yönelik saldırılar ve ABD'de

seçime müdahale saldırıları (iddiaya göre Rusya tarafından); Ayrıca Çin, çoklu fikri mülkiyet hırsızlığı saldırılarıyla ve yakın zamanda (ve tartışmalı olarak) donanımları ''Supermicro'' sunucularına gizlemekle suçlanmaktadır (McCarthy, 2018).

Siber suçun uluslararası güvenlik için yarattığı en ciddi tehditlerden biri, devletlerin siber suçun geliştirdiği saldırı yeteneklerini kullanmak isteyebileceğinden kaynaklanmaktadır. Devletler, hedeflerini uluslararası arenada ilerletmek için, siber suç, istihbarat ve askeri müdahaleler sırasında operasyonel yeteneklerini doğrudan ilerletebilecek veya başlı başına büyük ağ operasyonlarını kapsayacak şekilde kullanılabilecek bilgisayar korsanlığı araçları ve teknikleri geliştirmektedir. Siber suç, devlete makul bir inkâr edilebilirlik sağlama konusunda da eşsiz bir avantaj sunmaktadır ve belirsizlik alanında gerçekleştirilen bu durumun, paha biçilmez bir operasyonel avantaj sağladığı değerlendirilmektedir. Bu anlamda, siber suç örgütleri gerek vekil olarak gerekse de başlı başına birçok devletin siber gücünü temsil etmektedir. Ayrıca bu durum, bazı devlet aktörlerinin, özellikle yabancı hedeflere karşı çalışıyorsa ve ihtiyaç halinde bir vekil olarak kullanılabiliyorsa, suç faaliyetlerinde bulunan siber yer altı unsurlarına belirli bir serbestlik sağladığını açıklamaktadır. Paradoksal olarak, bir devletin siber küresel arenadaki gücü, bir şekilde, sınırları dâhilinde faaliyet gösteren siber suçlulara karşı örtülü ve gönüllü toleransına da bağlı olarak değişmektedir (Rugge, 2018).

4.2.2. Siber Suçun Önlenmesi, Suçluların Araştırılmasına Yardım Edilmesi ve Suçluların İade Edilmesine Yönelik Çalışmaların Yetersizliği

Siber suç faaliyetlerinin çoğu uluslararasıdır ve bu nedenle ulusal savcılar ya da kolluk kuvvetleri uluslararası işbirliğini zorunlu kılmaktadır. Devletler 2000'li yılların başında siber suçla ciddi şekilde mücadele etmeye başlamıştır. Özellikle son birkaç yılda, bu enstrümanların benimsenmesinde, bağlayıcılıklarına göre veya bağlayıcı olmayan niteliklerine göre gruplandırılabilecek bir dizi tartışma yaşanmıştır. İlk grup, çok taraflı bir bakış açısıyla siber suçlarla başa çıkmak için harcanan en kapsamlı çabalardan birini içermektedir**: ''**Siber Suçlar Sözleşmesi'' ayrıca Budapeşte Sözleşmesi olarak da bilinmektedir. Taslak hazırlama sürecinin başlamasından üç yıl sonra 2001 yılında Avrupa Konseyi tarafından kabul edilmiştir. Bu, şu ana kadar kabul edilen en yaygın uluslararası bağlayıcı

araçtır. Sözleşmenin teknik kısıtlamaları bulunmakla birlikte, dijital kimliklerin çalınması, siber zorbalık veya siber terörizm gibi bir takım meseleleri içermemesi nedeniyle eleştirilmektedir. Avrupa Konseyi üye ülkeleri tarafından tasarlanıp kabul edilmesine rağmen, söz konusu sözleşme, Avrupa Konseyi üyesi olmayan ülkelere de açıktır (Sözleşme Amerika Birleşik Devletleri, İsrail ve Avustralya tarafından da onaylanmıştır) (Siber Suçlar Sözleşmesi, 2011).

Ancak, Gerhart (2017)'ye göre; siber suçların önlenmesinin, Budapeşte Konvansiyonu'nda önerilenlerden daha güçlü ve daha ayrıntılı bir yasal çerçeve gerektirmesi durumu, siber suçların yaygınlığı, genişleyen doğası ve sürekli evrim içinde olması, gerekli hükümlerin yenilenmesine ve periyodik güncellenmesi ihtiyacının oluşmasına neden olmuştur (Gerhart, 2017). Bu konuda Avrupa Birliği (AB), siber alanda meydana gelebilecek özel suç uygulamalarıyla mücadeleye yönelik çeşitli araçlar benimsemiştir. Bunlardan ilki, dolandırıcılıkla mücadele ve nakit dışı ödeme araçlarının sahteciliği konusunda 28 Mayıs 2001 tarihli AB Konseyi kararıdır (Official Journal, 2001). 12 Temmuz 2002'de, Avrupa Birliği, "ePrivacy" direktifini kabul etmiştir (European Parliament, 2002). Bahse konu direktif elektronik iletişim sektöründe kişisel verilerin işlenmesi ve gizliliğin korunması ile ilgilidir. Siber suç konusunda ise, üye devletlerin ceza suçlarının tespiti ve kovuşturulması durumunda elektronik iletişim haklarını kısıtlamak için yasal tedbirler almalarına izin vermiştir. Daha sonra AB, 2009 yılında ceza hukuku yaptırımlarını içerecek şekilde değiştirilen bilgi toplumu hizmetlerinin, özellikle elektronik ticaretin belirli yasal yönleri hakkında e-ticaret direktifini yeniden adlandırmıştır. Avrupa Birliği daha sonra bilgi sistemlerine yönelik saldırılara ilişkin direktif yayınlamıştır (European Parliament, 2013)(2013/40 / AB). Söz konusu direktif bilişim sistemlerine yasadışı erişim, yasadışı sistem müdahaleleri ve yasadışı veri girişimi ile ilgilidir ve yasadışı müdahale gibi yeni suçları da kapsamaktadır.

Bölgesel düzeyde, diğer kuruluşlar, siber suçun farklı kavramsallaştırılmasını sağlayan siber suçlarla mücadele için bağlayıcı araçlar benimsemiştir. 2001 yılında Bağımsız Devletler Topluluğu (BDT) , siber suçun "hedefin bilgisayar bilgisi olduğu suç eylemi" olarak tanımlandığı Bilgisayar Bilgisi ile İlgili Suçlarla Mücadelede İşbirliği Anlaşması'nı kabul etmiştir. (Fletcher ve diğerleri, 2016) Şangay İşbirliği Teşkilatı (SCO) bilgi güvenliğini 2009 yılında Yekaterinburg

Deklarasyonunda belirlenen önceliklerden biri olarak uygulamaya başlamıştır. Daha sonra, 2011'de kabul edilen "Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması", siber suçları ve siber güvenlik hükümlerini çok geniş çapta ele almaktadır (Rab, 2018).

Operasyonel ve kanun uygulama düzeyinde iki önemli ağ vardır: "INTERPOL" (Küresel Siber Suçlar Uzman Grubu) ve "EUROPOL" (Avrupa Siber Suçlar Merkezi) (EC3). Bu ağlar, uluslararası siber suç araştırmalarını ve operasyonlarını, kolluk kuvvetleri tarafından sahada kullanılacak olan harekete geçirilebilir istihbarat üretimi de dâhil olmak üzere, farklı kanallar aracılığıyla koordine etmeye yardımcı olmaktadır. Özellikle EC3'ün, siber düzeyde, AB ülkeleri arasında, bugüne kadar diğer alanlarda aynı düzeyde işbirliğini sağlayan kolluk kuvvetleri ile adli sektör arasında başarılı bir işbirliği sağladığı değerlendirilmektedir (Europol, 2013).

Uluslararası düzeyde devletlerin, bu olgunun üstesinden gelmeyi amaçlayan işbirliği ve karşılıklı adli yardım anlaşmalarını güçlendirmeye devam edeceği öngörülmektedir. Ancak, Dominioni (2018)'e göre; daha kapsamlı ve kapsayıcı bir sözleşmenin kabulü sorunlu olabilir. Nitekim Rusya 2010 yılında, Budapeşte Konvansiyonu'na desteğini sürdürmemeyi tercih ettiği için ABD, Kanada, İngiltere ve AB tarafından durdurulmuş olan Birleşmiş Milletler Siber Suçlar Kongresi için bir taslak önerisinde bulunulmuştur. Söz konusu tartışma, daha geniş bir biçimde egemenlik, içerik kontrolü ve ulusal güvenlik kavramlarıyla ilgili olması nedeniyle, işbirliği mekanizmalarının ve suç tipolojilerinin ötesine geçmektedir (Dominioni, 2018).

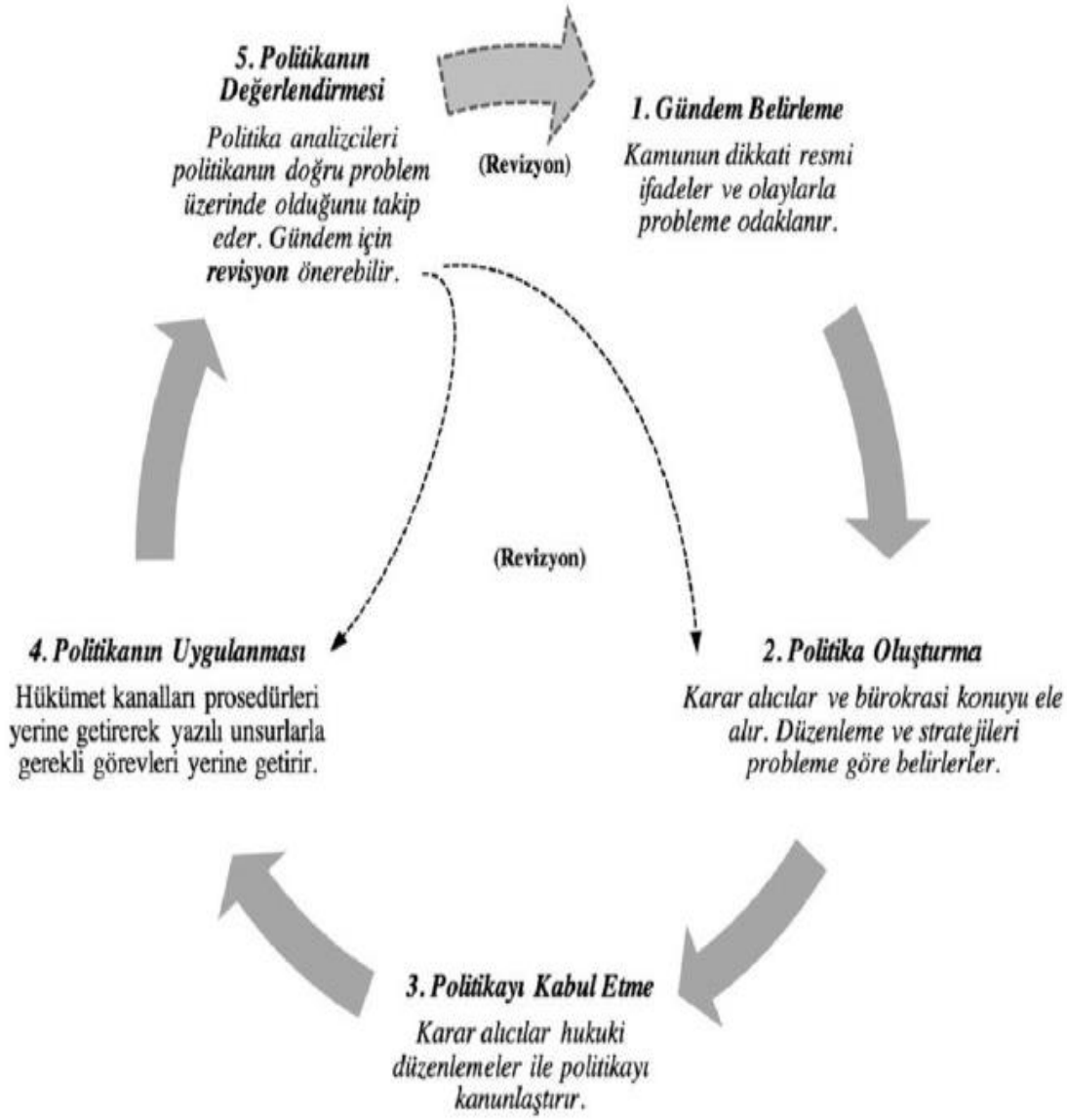
4.2.3. Ortak Bir Tanımın Olmaması ve Mantıksal Çerçeve

Net bir tanım olmadan, siber güvenlik birçok zaman çelişkili amaçlar için kullanılmaya devam edecektir. Terimin geniş uygulaması çalışmamızın üçüncü bölümünde de incelediğimiz ülkelerin stratejilerinde görüldüğü üzere, parçalanmış ve zıt yaklaşımlara yol açmış, ayrıca demokratik uluslarda gizlilik ve ifade özgürlüğü konusundaki son kısıtlamaları haklı çıkarmıştır. Devletler sorunu ulusal otorite altında tutmak için mücadele ederken, siber güvenlik göreceli olarak ülke vatandaşlarına karşı iyi olmasına rağmen, bireysel paydaşların çoğu bilgi güvenliğinin yetersiz kaldığını düşünmektedir. Bauer ve Eeten (2009)'e göre; bu

ademi merkeziyetçilik, belirli aktörlerin özel çıkarlarına cevap verdiğinden ve kamu yararına hizmet etmediğinden, alt optimal güvenlik seviyelerine yol açmıştır (Bauer ve Eeten, 2009).Siber güvenliğe kullanıcı odaklı bir yaklaşımın ise, bireylerin siber tehditlerle başa çıkmaya hazır olduklarını ve çevrimiçi haklarını kullanmadaki müdahalelere karşı korunmalarını garanti edeceği durumunu ortaya koymaktadır.

Siber güvenlik konusu, uluslararası ilişkiler terminolojisinde hâlihazırda ortak bir tanımı ve anlayışı bulunmaması nedeniyle önemli bir tartışma konusu olarak ele alınmaktadır. Hükümetler, siber güvenlik politikaları aracılığıyla güvenli çevrimiçi ortamlar oluşturmayı amaçlamaktadırlar. Ancak siber güvenlik, çevrimiçi ve çevrimdışı dünyada BİT güvenliğinin çeşitli yönlerini oluştururken, internet güvenliği siber güvenlik gündeminin yalnızca bir parçasıdır. Çoğu zaman ülkelerin stratejilerinde bir hedef olarak listelenen internet güvenliği, çevrimiçi tehditlerle başa çıkabilmek için bireylerin ve kuruluşların farkındalık, sorumluluk ve hazırlık kültürü ile ilgili kavramlardan oluşmaktadır. Ancak politika yapıcılar alana farklı açıdan bakmaktadırlar;

Şekil 4: Politika Oluşturma ve Uygulama Diyagramı



Kaynak : (The Texas Politics Project, 2016)

2005 Dünya Bilgi Toplumu Zirvesi'nde (WSIS) görüşülmesinin ardından, Bilişim Teknolojileri'nden sorumlu Birleşmiş Milletler ajansı olan Uluslararası Telekomünikasyon Birliği'ne (ITU) siber güvenlik alanında uluslararası çabaları koordine etme yetkisi verilmiştir. 2010 yılında Meksika'nın Guadalajara kentinde düzenlenen ITU Ortak Konferansı, bu görevi alınan 130 karar ile güçlendirmiştir. Söz konusu konferans tavsiye içerikli olmasının yanı sıra uluslararası alanda kullanılacak geniş bir siber güvenlik konseptini kapsayan

içerikleri bulunmayan devletler, karşılıklı ortak bir anlayış oluşturamadan siber güvenliği konuşmuştur (ENISA, 2012). Devletlerin internet yönetişimi alanındaki uluslararası otoriteyi pekiştirmeye ilgi göstermemesi veya Birleşmiş Milletlerin temel olarak politika yapıcılarına ulaşmaya odaklanarak sivil toplumu dâhil etmemesi durumu devletlerin bireysel ihtiyaçlarına göre politikalar belirlemesine neden olduğu görülmektedir. Zira bu süreçte, uluslararası zeminde güvenilir bir siber güvenlik tanımının oluşturulmasına çok az önem verilmiştir. Terimin anlaşılmasının ülkeden ülkeye değişmesinin nedeninin bu olduğu değerlendirilmektedir.

4.3. Küresel Siyaset Açmazı: Ulusal Çıkarlar ve Egemenlik Hassasiyetlerin Yol Açtığı Dijital Altyapı Eksikliği

Dünya genelinde siber saldırıların etkileri birçok sektörde de hissedilmektedir. Ortaya çıkan zararlar, doğrudan finansal zararların yanı sıra itibar sorunlarını da içermektedir. Bunlar, iş kaybı, beklenen hizmetleri sağlayamama, fırsat maliyetleri ve güven kaybı gibi sorunlardır. Stratejik ve Uluslararası Çalışmalar Merkezi'ne göre (2014), dünya ekonomisi 2014 yılında siber saldırılardan 445 milyar dolar zarar etmiştir. Devletler yaklaşık 100 milyar dolar zarar görmüştür. Almanya 60 milyar dolar, Çin 45 milyar dolar ve İngiltere 11,4 milyar dolar zarar ettiğini bildirmiştir. Rakip ülkelerin sırlarını ve fikri mülkiyetlerini arayan devletlerin casusları, kimlik bilgileri ve para çalmak isteyen örgüt mensubu suçlular veya teröristler, elektrik şebekelerine, su kaynaklarına veya diğer kritik altyapı sistemlerine saldırı gerçekleştirmektedirler. Ayrıca bazı siber korsanlar veya hacktivist gruplar siyasi veya sosyal bir açıklama yapmak amacıyla siber saldırı düzenlemektedir (Eckenrode ve Friedman, 2018).

Günümüz piyasasında gündemi ve gelişmeleri takip etmenin çoğu zaman şirketlerin siber riskini azaltmanın zorluklarına da katkıda bulunabileceği öngörülmektedir. Şirketlerin, siber güvenlik alanında gerçekleştireceği büyük bütçeli yatırımların uzun vadeli bir büyümeyi olumlu yönde geliştireceği unutulmamalıdır. Veri koruma, tüketicilerin şirketlerden önemle beklediği bir durumdur ve bu kapsamda yapılacak güvenlik yatırımları günümüzün büyüyen siber saldırı dünyasında rekabet avantajı oluşturabileceği değerlendirilmektedir (Peasley ve diğerleri, 2017).

Fikri mülkiyet hırsızlığı, ABD'ye yıllık altı yüz milyar dolara mal olmaktadır (Alexender, 2017). Ancak, daha da kötüsü, internette her gün gerçekleşen siber bilgi ve yeteneklerin tahsis edilmesi durumudur. Çin'in teknolojik yükselişi, büyük ölçüde Çin'in Amerika'nın özel sektörünü siber sömürüsüyle hızlandırmıştır. Çin'in fikri mülkiyet hırsızlığı nedeniyle ABD'ye karşı kazandığı rekabet avantajı fazlasıyla göz ardı edilemez boyuttadır. ABD hükümetinden yasa dışı yollardan avantajlı bilgiler alarak temel özel sektörlerini kolaylaştırmak Çin hükümetinin aktif bir politikası olmuştur (Kuchler, 2017). Bu nedenle, on yıl içinde Çin'in US Steel'in araştırma ve geliştirme koluna siber saldırısı, Apple'ın iCloud sunucularını hacklemesi ve F-35 tasarımlarının ele geçirilmesi sanayi sektörünün, teknoloji sektörünün ve savunma sanayi üretimlerinde büyük atılımlar gerçekleştirmesine neden olmuştur (Ling, 2016). Bu kapsamda, düşman siber faaliyetlerin maliyetlerinin düşük ve faydaların yüksek olduğu görülmektedir. Çalışan bir siber caydırıcılık teorisi olmadan ve siber sömürünün birçok yararıyla, büyük güçler birbirlerini büyük savaşa doğru itmeye devam edecektir.

Siber güvenlik ortamı gereği, saldırılara ve ihlallere karşı çok sık tepki göstermek gerekmektedir. Ancak, teknolojinin karmaşıklığı neticesinde günümüzde siber olaylara, bir sorun meydana geldikten sonra (bazen de uzun zaman sonra) yapılan işlemlerle müdahalede bulunulmaktadır. Siber saldırıları ele almak için en sık kullanılan teknoloji, önceki saldırı modellerine dayanan ''tehdit imzaları" kullanılarak gerçekleştirilmektedir. Ancak bu yaklaşımlar yeni tür saldırıların önlenmesinde sınırlı imkânlar sunmaktadır.

Teknolojinin hızlı evrimi sayesinde, her geçen gün siber tehditlerin, silahların, araçların sayısı ve kuvvetleri artmaktadır. Bu nedenle siber güvenliğin geleceği daha da karmaşık ve zorlu görünmektedir. Kuruluşlarda, günümüzde bulunan tehditlerin sayısı ile başa çıkmak için yeterli siber uzman bulunmamaktadır ve söz konusu dengesizliğin muhtemelen daha da kötüleşeceği öngörülebilmektedir. Gelecek zamanda ki bir senaryoyu değil de şimdiki durumun ilk aşamalarını açıklamak gerekirse, kamu ve özel sektör kuruluşları teknolojik bağlamda, siber güvenlik programlarını geliştirmek adına analitik ve otomasyon programlarını yeteri kadar kullanmamaktadırlar. Bu araçlar en önemli olayları ve varlıkları tanımlamaktadır. Örneğin, firmalar müşteri analitiklerinde normal yaklaşım

müşterileri değerlerine göre segmentlere ayırarak bunlardan en önemlilerine odaklanmakta ve bu müşterilerin ne alabileceklerini tahmin etmek için varyasyonlar üretmektedirler. Otomatik teklifler her müşterinin tercihlerine göre özelleştirilebilmektedir (Davenport ve Amjad, 2016). Bu kapsamda aynı teknolojilerin uluslararası alanda gerçekleştirilecek çalışmalarla, devletleri artan siber güvenlik problemlerinden kurtarabileceği değerlendirilmektedir. Bu tür bir öngörücü güç, devletlerin ve kuruluşların ortak güvenlik çabalarını, hedeflenmesi en muhtemel teknoloji ortamlarına odaklamalarına olanak sağlayacaktır.

İnternetin popülaritesi giderek artmakta ve siber güvenliği giderek daha da zorlaştırmaktadır. Bununla birlikte, 2018 yılı Kasım ayında yaklaşık 4 milyar kullanıcısı (İnternet Live Stats, 2018) olmasına rağmen "internetten hiç kimse sorumlu değildir". Bu kontrol ve güvenlik eksikliği, siber savaşın, siber casusluğun ve siber suçların üç ana zorluğuyla sonuçlanmaktadır. Bu tehditler farklı saldırganlardan gelmekle birlikte, belirli kullanıcılara yönelik gerçekleştirilebilmekte, hepsi aynı internet ağında çalışmakta ve çok sayıda internet kullanıcısına karşı felaket bir etkiye sahip olabilmektedirler.

Siber güvenlik, gün geçtikçe hem hükümetler hem de işletmeler için artan bir tehdit olarak ortaya çıkmıştır. Siber tehditlerin çok yavaş şekilde sınıflandırılması uluslararasında ve iş dünyası ile hükümetler arasında işbirliği olanaklarını sınırlamaktadır. Siber güvenlik karmaşık bir sorundur çünkü birçok alanda kesişmektedir. İnternetin ağ yapısı, siber güvenliği bariz bir şekilde uluslararası bir sorun haline getirmektedir. Özel sektörün elindeki aşırı miktardaki siber altyapı yoğunluğu, siber güvenlik tehditlerinin hem halka hem de özel sektöre zorluk teşkil ettiği anlamına gelmektedir. Bireylerin internete olan ihtiyaçlarının artması, siber güvenliğin, ulusal güvenlik ile bireysel özgürlükler arasındaki dengeyi de kapsadığı anlamına gelmektedir.

Bu artan risklerle ve tam anlamda siber güvenliğin sağlanmasının imkânsız doğası ile karşı karşıya kalan kamu ve özel sektörün anahtarı esnekliği arttırmaktır. Kamu ve özel sektör arasındaki ortak tehdit, ortak bir yaklaşım için güçlü fırsatlar sunmaktadır. Ancak iki büyük zorluğun bu işbirliğini sınırladığı düşünülmektedir. Birincisi, özel sektörün hükümetin katılımından korkması, mahremiyeti ve özel bilgilerin korunması konusunda endişe etmesidir. İkincisi,

hükümetin, siber yeteneklerini çok fazla sınıflandırması ve hassas bilgileri açığa vurmadan özel sektörle anlamlı bir şekilde paylaşamaması hususudur. Zira siber güvenlik ortamını daha iyi bir hale getirmek için gelişmiş düzenlemelere gerek duyulmaktadır; ancak hangi düzenlemenin en iyisi olacağı konusunda anlaşmazlıklar vardır. Bazıları, özel kullanıcılar arasında standardizasyon ve gönüllü sertifikalandırma yapılmasını savunurken, bazıları ise özel sektördeki oyuncular arasında oyun alanını düzleştirmek için daha özel bir düzenleyici yaklaşım gerektiğine inanmaktadır.

Siber tehdidin uluslararası doğası, çeşitli uluslararası kuruluşların artan mücadeleyle en iyi şekilde nasıl başa çıkabileceği sorusunu akla getirmektedir. Joyner (2010)'un aktardığına göre; NATO, bir siber saldırının 5. madde tehdidi olarak görülmesi gerekip gerekmediğini tanımlamakta zorlanmıştır ve siber güvenliğin yeni gerçekliğini yansıtmak için anlaşmaların güncellenmesi gerektiğini savunmuştur. Birçok araştırmacı, NATO'nun siber güvenlik uygulamasının sorunun profilini oluşturma ve tehditleri göstermede yararlı olacağı konusunda hemfikirken, diğerleri de NATO ve AB'nin uluslararası bir siber oyuncu olarak büyük bir rol oynama ihtimalinin düşük olduğu görüşünü öne sürmektedir (Joyner, 2010).

Bunlarla birlikte, siber uzayın oluşturulmasına yardım eden teknik topluluğun, hükümetler için siber güvenliği arttırmaya çalışmalarında yararlı bir araç olabileceği değerlendirilmektedir. Söz konusu teknoloji kuruluşları, güvenliğine ve refahına derinden bağlı kalmaya devam ederken, hükümetlerin kendi faaliyetlerine ve kültürlerine saygı göstereceğinden emin olabilirlerse, hükümetlere çözümler üretme konusunda yardım etmeye istekli olacakları değerlendirilmektedir.

Siber uzayda en güçlü ülkelerin hükümetlerinin bile tek başına siber mücadeleyi gerçekleştiremeyecekleri ve uluslararası alanda birlikte çalışan hükümetlerin bile özel sektörün katılımı olmadan başarılı olamayacakları değerlendirilmektedir. Devletlerin siber güvenlik konusunda ortak hedeflere ulaşabilmek ve siber tehditle mücadele edebilmek için karşılıklı şüphelerini aşmaları gerekmektedir. Zira küresel siyaset açmazı bağlamında, evrensel bir siber güvenlik mekanizması oluşturulurken; "sistemin merkezinde hangi devlet veya örgüt olacak ?" "finans desteğini kim hangi oranda sağlayacak ?" ve en önemlisi "hangi siyasi

yapı bu mekanizmayı denetleyecek?" gibi cevabı olmayan sorular ve belirsizlikler mevcuttur. Zira bu hususlar, ülkelerin etkin işbirliği gerçekleştirilememesinin ve bu konularda yaşadığı anlaşmazlıkların en önemli nedenleri olarak görülmektedir.

SONUÇ

1990 yılında Sovyetler Birliği'nin dağılması, mevcut uluslararası sistemde ve güç dengelerinde önemli bir dönüşüm ve yeni bir tartışma döneminin başlamasına neden olmuştur. Küreselleşme dönemi olarak da adlandırılan bu süreçte askeri yaptırımların geçerliliğinin azalması, serbest ekonominin önem kazanması, milletleri bir araya getiren etnik kimliklerin güçlenmesi, ulus devlet öneminin belirli amaçlara ulaşmak için yetersiz kalması gibi gelişmelerle, uluslararası göç, uluslararası terörizm, kitle imha silahları, enerji güvenliği, çevre güvenliği ve siber güvenlik gibi yeni tehditler ve güvenlik anlayışları ortaya çıkmıştır.

Uluslararası sistemde ABD, Çin Halk Cumhuriyeti ve Rusya gibi küresel güç olan ülkeler yeni nesil enformasyon savaşını ve siber saldırıları önemli bir stratejik savunma ve taarruz etme yöntemi olarak değerlendirmektedirler. Siber uzaydaki faaliyetlerin arkada iz bırakmadan ve kolay bir biçimde gerçekleştirilebilir oluşu da bu yöntemin kullanılmasını teşvik eden en önemli faktörlerden biridir. Ancak siber alanda yaşanan önemli gelişmeler yeni güvenlik tehditlerini de beraberinde getirmiştir. Artan bu risk ve tehditleri bertaraf etme konusunda ise devletlerin rolü önemli derecede artarken, iktidarda bulunan hükümetler bu konuda strateji geliştirmek zorunda bırakılmıştır. Bireylerin veya grupların gerçekleştirdiği siber taarruzlar ile uluslararası ortamın, neorealist varsayımlara uygun biçimde geçmiş dönemlerden daha belirsiz ve anarşik bir yapıya bürünmeye başladığı değerlendirilmektedir.

Bir ülkede oturan yalnız bir saldırganın, diğer ülkelerdeki internetteki tüm bilgisayarları tehdit eden bir işlemi anında gerçekleştirebilmesi gerçeği, birçok alan ve uzman kişi tarafından birlikte çalışılarak ele alınması gereken bir sorundur. Konuyla ilgili angajman kurallarının nasıl uygulanacağı ve saldırganlara veya eylemlerini düzenleyen uluslara nasıl ceza verileceği tartışılması gerekmektedir. Siber casusluk davranışlarıyla ilgili anlaşmalar gerçekleştirmek mümkün değildir ancak, siber alanda saldırganlığın artması riskini azaltmak amacına yardımcı olmak

için doktrinler geliştirmenin mümkün olduğu değerlendirilmektedir. Ayrıca kabul edilemez bir dizi siber eylemi ve bu tür eylemlerden kaçınmak için caydırıcı unsurları oluşturmak amacıyla birlikte çalışan küresel bir ortaklık oluşturulması şarttır.

Siber ortamın doğası gereği, tehdidin kaynağını, zamanını ve yerini belirsiz kılmasının, uluslararası ilişkileri Soğuk Savaş dönemine nazaran daha anarşik bir sisteme dönüştürdüğü sonucunu çıkarmak mümkündür. Ayrıca hâlihazırda siber ortamı düzenleyen ve denetleyen nihai ve kesin evrensel uluslararası hukuk kurallarının olmaması, siber ortamda ülkeler arasında işbirliğinin yerine rekabetçi ve çatışmacı politikaların kabul görmesi ve söz konusu rekabetin seviyesinin giderek artması gibi konular dikkate alındığında, mevcut uluslararası yapının geçmiş dönemlerden çok daha fazla güvensiz ve belirsiz bir durumda olduğu da iddia edilebilmektedir. Bunlarla birlikte benzer biçimde ülkelerin siber güvenlik strateji ve politikalarının genel olarak gizli olması, bu kapsamda bir ülkenin gerek rakip olduğu gerekse dost olarak nitelendirdiği bir ülkeye karşı gizli bir siber faaliyet gerçekleştirip gerçekleştirmediğinin net olarak bilinememesi de bahse konu anarşik yapının derinleşmesine sebep olan faktörler olarak karşımıza çıkmaktadır.

Siber ortamın oluşturduğu imkânların uluslararası yapı içerisinde devlet dışındaki aktörlerin(bireyler, medya destekli sosyal hareketler, baskı ve çıkar grupları, çok uluslu şirketler vb.) önemini ve çeşitliliğini arttırmasına rağmen, neo-realist teorilere göre siber ortamda yaşanan gelişmelerin eş zamanlı olarak devletlerin etkin rolünü daha da pekiştirdiği de düşünülmektedir. Bağımsız kabul edilseler dahi devlet dışındaki aktörlerin mevcut uluslararası sistemde kalıcı bir etki oluşturabilmeleri, ancak devlet destekli bir düzenlemeye dâhil edilmeleriyle mümkün olabilmektedir.

Nye (2010)'a göre, siber ortam kaynaklı gerçekleşen yeni gelişmelerin oluşturduğu potansiyel güç yayılması durumu ne olursa olsun asla devletlerin mevcut uluslararası sistemdeki başat aktör rolünü değiştiremeyecektir. Nye bu hipotezini, bir ülkenin kritik ağ altyapılarını bütünüyle kullanılamaz hale getirmeye yönelik bir siber saldırının düzenlenmesini sağlayan donanımın ve bu saldırıların maliyetlerinin hâlihazırda yalnızca devletlerin imkân ve kabiliyetleri ile karşılanabiliyor olması, tespitiyle desteklemektedir (S.Nye, 2010).

Özetle teknolojik gelişmelerin seviyesi ne olursa olsun geçmiş de olduğu gibi mevcut uluslararası sistemde de başat aktör devletlerdir. Siber ortamın karmaşık yapısı nedeniyle, devletler rakip devletler ya da devlet dışı aktörler tarafından gerçekleştirilmesi muhtemel siber saldırılara karşı siber güvenlik stratejileri bağlamında siber güvenlik kurumları ve siber ordular tesis etmekte, bunların dışında siber uzmanlar ve bilim insanları yetiştirerek gelişim göstermeyi amaçlamaktadırlar. Bu kapsamda gerek rakip devletlerden gerekse de diğer tüm aktörlerden gelebilecek siber tehditlerin yalnızca merkezi bir devlet oluşumu ile bertaraf edilebileceği ve etkin bir siber güvenlik sistemi gerçekleştirilebileceği değerlendirilmektedir. Ayrıca ulusal internet ve ağ teknolojilerinin, bu sistemleri denetleyen mekanizmaların ve tüm bunlarla örüntülü olarak planlanan siber güvenlik stratejilerinin devlet yönetimleri tarafından gerçekleştirildiği değerlendirildiğinde, uluslararası disiplinde belirtilen realist teorilerle uyumlu bir biçimde devletin temel aktör olduğu açıkça görülmektedir. Siber alanda yaşanan tüm bu gelişmeler de devletlerin mevcut uluslararası sistemdeki başat aktör rolünü pekiştiren etmenler olarak değerlendirilmesi gerekmektedir.

Bilgi iletişim teknolojisinde güvenliği, siber güvenliğin tesisi, siber alanda hukukun üstünlüğünü ve insan haklarının korunmasını güçlendirme ihtiyacının tanınmasıyla birlikte, "siber" kavramının dâhil olduğu her şey artık çok önemli hale gelmiştir. Bireylerin temel haklarına ve devletlerin ulusal (güvenlik) çıkarlarına değindikleri için, ortak çözümler konusunda uluslararası fikir birliğine varmak gittikçe zorlaşmaktadır. Bu ikilemin üstesinden gelmek için, en mantıklı yaklaşım, Budapeşte Siber Suçlar Konvansiyonu gibi hâlihazırda yürürlükte olan ve işleyen ortak standartlara ve özellikle de kapasite geliştirmeye yönelik geniş bir anlaşmaya varılan yaklaşımlara odaklanmaktır. Daha büyük bir koordinasyon öngören siber suçlarla mücadele alanı, tüm devletlerin eylemlerini en az iki yönde geliştirmesine ihtiyaç duymaktadır; hukuki müdahalenin arka planının geliştirilmesi ve tasarlanan normların ulusal mevzuata uygulanması, bilgi alışverişinin ulusötesi temelinin geliştirilmesi.

Ayrıca, teknoloji alanı ve teknoloji kısıtlamaları tarafından tanımlanan gereksinimlerin politika tasarım sürecine dâhil edilmesine her daim ihtiyaç duyulmaktadır. Fakat bu konudaki sorunlar, kısmen teknoloji ortamının karmaşıklığı ve dinamizmi, kısmen politikacıların yanıtının nispi yavaşlığı ve uzman bilgisini beklemek gibi faktörlerden oluşmaktadır. Bugünün ağları çeşitli ve kapsamlıdır. Bu nedenle teknoloji sağlayıcıları tek güvenlik mimarı olamazlar. Tüm paydaşlarla paylaşılan bir siber güvenlik bilincini oluşturmalıdırlar. Etkin işbirliği, etkili siber yönetişim için hayati öneme sahip olacaktır. Sanayilerin yaygın olarak kabul edilen güvenlik standartlarını oluşturmak için hükümetlerle birlikte çalışması gerekmektedir. Ayrıca, tüm paydaşları, endüstri güvenliğini artırmak için hayati bir kaynak olan açık kaynak güvenliğine daha fazla yatırım yapmaya teşvik etmeleri gerekmektedir. Standartlar üzerinde anlaşma, herhangi bir uluslararası güvenlik yaklaşımında önemli bir bağlantıdır. Sanayi kuruluşları, endüstrilere güvenlik konusunda net ve tutarlı bir rehberlik sağlayacak kapsamlı uluslararası standartlar geliştirmek için teknoloji sağlayıcılarla birlikte çalışmalıdırlar. Sanayi kuruluşları ayrıca tedarik zincirlerinin artık küresel olduğunu kabul etmek için hükümetlerle birlikte çalışmalıdır. Hükümetler, koordine edilmemiş ulusal standartların güvenlik sorunlarını çözmeyeceğini anlamalıdırlar. Ayrıca, farklı standartlara sahip olmak tedarik zincirlerini kıracak, teknolojik gelişmeleri engelleyecek ve iş yapma maliyetini artıracaktır. uluslararası standartlar son derece önemlidir. Standardizasyon sağlamak için, hemen hemen tüm ürünlerin doğrudan açık kaynak kodunu içermesi, yazılım geliştirmenin giderek daha önemli bir parçası olacaktır. Günümüzde, açık kaynak toplulukları, yeni teknolojinin güvenlik zorluklarına hızlı bir şekilde yanıt verecek personel ve finanstan yoksundur, bu nedenle açık kaynak yazılımının güvenlik özellikleri gerisinde kalmaktadır. Tüm paydaşların daha geniş yatırım yapması gerekecektir.

Kullanıcı bilinci oluşturma kapsamında, teknoloji kullanıcılarını ve toplumu korumak için, her şirket ve vatandaş, siber güvenlik, veri sahipliği ve mahremiyet konusunda daha fazla farkındalığa ihtiyaç duymaktadır. Dünyanın dört bir yanındaki büyük ülkeler, siber güvenlik konusunda halk eğitimini ulusal veri koruma ve gizlilik stratejilerinin önemli bir parçası haline getirmişlerdir. Hükümetler, siber suçları ve siber güvenlik tehditlerini kontrol etmeye yardımcı olmak için genel bilgi ve beceri

seviyelerini yükseltmeyi amaçlamaktadırlar. Halk kendini nasıl koruyacağını bilirse, bu bireylerin ve hatta bir bütün olarak ulusun siber kırılganlığını azaltacağı anlamına gelmektedir. AB, Avusturya, Hollanda ve Avustralya, gençleri siber güvenlik konusunda eğitmeyi ulusal siber stratejilerinde kilit bir önlem haline getirmiştir. Gençlere kendilerini korumak için ihtiyaç duydukları farkındalık ve becerileri vererek siber alandaki zafiyetleri en aza indirmeye çalışmaktadırlar

Hem ilkeleri hem de normları içeren zengin bir ortak bağlamın olmaması, çok paydaşlı topluluğun toplumsal ilişkilerle ilgili paylaşılan değerler üzerine inşa etmesini sağlayacak uyumlaştırılmış mekanizmaların ortaya çıkmasını geciktirmiştir. Politika yapıcıların ve teknolojistlerin hızlı bir şekilde gelişen teknoloji ortamına uyumlu, uygun siber güvenlik politikaları ve siber normlara yaklaşımlar geliştirmek için işbirliği yapmalarına ihtiyaç duyulmaktadır. İnternet'in küresel doğası ve dünya çapında her yerde bulunan siber uzay kullanımın birleşmesi gerekmektedir. Çeşitli disiplinler ve akademi, hükümet, sanayi ve sivil toplum kuruluşları siber güvenlik konusunda işbirliği konularını tartışmaktadır. Ancak, araştırma ve uygulayıcılar topluluğu daha somut ve sık sık alana özgü bir bağlantı kuracak bir mekanizma geliştirememiştir

Çok paydaşlı gruplar sıklıkla ilkelerin geliştirilmesine odaklanır çünkü yüksek düzeyde genelleme, farklı katılımcıların yakın görüşlerini oluşturmasına ilkeler ile izin vermektedir. Normlar, özellikle teknik normlar özel bilgi ve uzmanlığa sahip topluluklar tarafından gerçekleştirilmelidir. Kabul edilen politika ilkelerine dayalı teknik normlar ve en iyi uygulamaları tasarlamak gerekmektedir. Normlar ve ilkeler arasındaki ve teknoloji ile teknik arasındaki bağlantı politikası alanı oldukça soyuttur. Bu soyut durum fikir birliğini basitleştirmektedir, ancak, hem normları hem de prensipleri dikkate alan siber güvenlik politikalarının tasarımı ve uygulamaları hakkındaki tartışmaları karmaşıklaştırmaktadır.

Siber tehditler, kanunsuz, anarşik bir siber alandan kaynaklanan, küresel bir güvenlik sorunu olarak yaygın şekilde kabul görmüştür. Siber alanda uygun devlet davranışını neyin oluşturduğuna dair ortak anlayışlar geliştirmenin uluslararası güvenliği ve istikrarı sağlamak için kritik öneme sahip olduğu ortak bir inanışa dayanarak, bilinçli bir norm oluşturma gereksinimi ortaya çıkmıştır. Hükümetler, ikili görüşmeler ve çok taraflı istişareler yoluyla ortak davranış kuralları

oluşturmalıdır. Proaktif olarak deneyimlerini ve en iyi uygulamaları paylaşmalı ve siber saldırıları ve siber suçları engellemek için birlikte çalışmalıdırlar. Bu önlemler şeffaf, işbirlikçi ve açık bir ortamda güven inşa edilmesine yardımcı olacaktır. Ayrıca, casusluk bağlamında norm oluşturma çabaları, normların devlet davranışını şekillendirmedeki gücünü oluşturmaktadır. Bu normlar ortaya çıktıkça ve içselleştirildiklerinde, siber uzayda devlet uygulamalarını değiştirmeleri muhtemeldir.

Siber güvenlik ele alınırken siber tehdit dâhil olmak üzere çok çeşitli konuları inceleyerek multidisipliner bakış ve değerlendirme yapılması gerekmektedir. Ulusal ve uluslararası yasal ikilemler, yönetişim sorunları, siber alan için rollerin ve sorumlulukların belirlenmesi, siber alanın militarizasyonu ve acil siber güvenlik tartışmalarına odaklanarak, hedefe cevap veren bir politika ve yasal mimarisinin oluşturulmasını desteklemeyi amaçlayan yaklaşımlar geliştirmek gereklidir. Bu çalışmada da siber alanın kendine özgü zorlukları ve geleceğe dönük yaklaşımlarıyla, farkındalık yaratmak ve konu hakkında geniş bilgiye sahip olmak için gerekli olan eleştirel düşünceyi oluşturmaya katkı sağlanmaya çalışılmıştır.

Tüm bu bilgiler ışığında, siber tehditlerin devlet sınırlarına ve örgütsel sınırlara meydan okuması sebebiyle, uluslararası güvenliği arttırmak için tüm ülkeler ve ilgili kuruluşların işbirliğini arttırması ve ortak mekanizmalar geliştirmesinin önemi tartışılarak, "siber güvenlikte uluslararası işbirliği mümkün mü**?**" araştırma sorusuna cevap aranmıştır. Siber uzayda yaşanan bu belirsizliklere ilişkin bazı nedenler ve kaygılar bulunmaktadır. Bunlar arasında temel olanların, uluslararası hukukun yetersizliği, kritik altyapıların zayıflığı, atıfta bulunma zorluğu, savunma suçu avantajı, bilgi sistemlerinin zayıf giriş engelleri, uluslararası normların eksikliği ve kıtalararası açıklıklar nedeniyle uluslararası sınırları geçme kolaylığı olduğu değerlendirilmektedir. Bu nedenle, bu faktörler bir araya geldiğinde, politika yapıcılar ve araştırmacılar için siber çatışmanın diğer alanlardaki çatışmalardan çok daha istikrarsız olması nedeniyle uluslararası işbirliğinin zorlukları açıklanmaya çalışılmıştır. Çalışma sonucunda, "siber uzayın doğası gereği, hâlihazırda ülkeler arasında yaşanan güvenlik ikilemi, rekabet ve çatışma ortamında; gerekli işbirliği, ortak politika üretiminin gerçekleştirilemediği ve işbirliği kapasitesinin arttırılmasının ülkelerin mevcut yaklaşımlarıyla mümkün olmayacağı" cevabına

ulaşılmıştır.

Dijital dönüşümün topluma ve ekonomiye olan etkisi, siber güvenliği kritik bir iş konusu ve kalkınma aracı haline getirmiştir. Tek başına bir ülkenin veya kuruluşun bu zorlukla başa çıkamayacağı değerlendirilmektedir. Uluslararası işbirliği, çok yönlü, modern ve esnek siber güvenlik çözümlerinin anahtarıdır ve bu sektördeki insan sermayesinin krizi çözmenin alternatif bir yolu olduğu değerlendirilmektedir. Bununla birlikte, son olaylarda, siber saldırılar melez savaşın bir parçası olmuştur. Bu kapsamda BM, AB ve NATO gibi organlara ihtiyaç duyulmaktadır. Ancak, birlikte çalışabilirliği artırmak için ortak teknik standartlara ve siber faaliyetlerle ilgili normlara ihtiyaç duyulmaktadır. Siber diplomaside aktif olan çeşitli ülkeler ve az sayıda uluslararası şirket, giderek daha karmaşık ve kalabalık siber tehdit ortamlarını yönetmek için uygulanabilir normlar araştırmaktadırlar. Bununla birlikte, ticari avantaj sağlamak amacıyla siber özellikli fikri mülkiyet hırsızlığını yürütmemek dışında, devletler arasında henüz açık ve net bir biçimde ortaya çıkan bir fikir birliği veya kabul gören ilkeler bütünü bulunmamaktadır. Siber uzayda sorumlu devlet davranış normları, henüz emekleme dönemlerinde olsalar da, ulus devletler ve uluslararası kuruluşlar tarafından uzun vadede yürütülen gelecekteki siber operasyon türlerini önemli ölçüde etkileme potansiyeline sahiptir. Normlar, özellikle bir davranışı kodlayan veya kınayan biçimde, pozitif veya negatif olabilirler. Siber normların geleceği, siyasi ve kurumsal irade ile aynı fikirde olacak ve nihayetinde belirli devletlerin siber operasyonlarını yürütürken bu normları kabul veya göz ardı etme kararları ile revize edilebilecektir.

.

KAYNAKÇA

Acar, U. (2007:372). *Devlet Güvenliği İstihbarat ve Terörizm.* Ankara: Adalet Yayınevi.

Akyazı, U. (2013, 11 14). Uluslararası Siber Güvenlik Stratejisi ve Doktrinleri Kapsamında Alınabilecek Tedbirler. *6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı* (s. 216-220). Ankara: https://www.iscturkey.org/assets/files/2016/03/2013-paper105.pdf. İscturkey Web Sitesi: https://www.iscturkey.org/assets/files/2016/03/2013-paper105.pdf adresinden alınmıştır. Erişim Tarihi: 04.09.2018

Alexender, B. (2017, 08 15). https://www.nytimes.com/2017/08/15/opinion/china-us-intellectual-property-trump.html adresinden alınmıştır. Erişim Tarihi: 05.09.2018

Alfred, N. (2016, 09 29). *CNET*. https://www.cnet.com/news/aol-wants-to-save-the-internet-from-the-death-of-email/ adresinden alınmıştır. Erişim Tarihi: 10.09.2018

Alperovitch, D. (2011). 3. Uluslararası Siber Çatışma Konferansı. *"Siber Caydırıcılık Stratejisinin Oluşturulmasına Doğru".* Tallinn: IEEE Xplore.

Alperovitch, D. (2018, 11 08). *Bank İnfo Security.* https://www.bankinfosecurity.com/chinese-cyber-threat-nsa-confirms-attacks-have-escalated-a-11696 adresinden alınmıştır. Erişim Tarihi: 12.12.2018

Altuğ, Y. (1995:14). *Terörün Anatomisi.* İstanbul: Altın Kitaplar.

Andress ve Winterfeld, J. (2011:198). *Cyber Warfare.* Amsterdam: Elsevier.

Arı, T. (2014:184). *Postmodern Uluslararası İlişkiler Teorileri 2.* Bursa: Dora Yayıncılık.

Arıboğan, D. Ü. (2007). *Uluslararası İlişkiler Düşüncesi.* İstanbul: Bahçeşehir Üniversitesi Yayınları.

Arnold, J. (2009, 03 30). *It World Canada* . https://www.itworldcanada.com/blog/project-ghostnet-canada-and-google-saves-the-world-from-cyber-spying-again/54861 adresinden alınmıştır. Erişim Tarihi: 01.11.2018

Arslan. (2015, 12 24). *Türkiye'ye Siber Saldırının 10 günü: Ne oldu?* BBC News: https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan adresinden alınmıştır. 01.11.2018

Arslan, M. E. (2018:2, 11 01). *Siber Güvenlik ve Siber Saldırı Türleri.* s3.amazonaws: https://s3.amazonaws.com/academia.edu.documents/52122013/SIBER_GUVENLIK_VE_SIBER_SALDIRI_TURLERI.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1542705586&Signature=Q55fBKqviUymyxELSLZthb5iNF8%3D&response-content-disposition=inline%3B%20filename%3DSIBER_ adresinden alınmıştır. Erişim Tarihi:02.11.2018

Avcı, G. (2004:6-7). *İstihbarat Teknikleri-Aktörleri, Örgütleri ve Açmazları.* İstanbul: Timaş Yayınları.

Avrupa Komisyonu. (2001). *european commission.* ec.europa.eu: https://ec.europa.eu/health/documents/eudralex/vol-2_en adresinden alınmıştır. Erişim Tarihi: 05.11.2018

Avrupa Komisyonu. (2004). https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure adresinden alınmıştır. Erişim Tarihi: 07.11.2018

Bauer ve Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. 706-719.

Baylis, J. (2008:72). Uluslararası İlişkilerde Güvenlik Kavramı. *Uluslararası İlişkiler Dergis, 5*(8), 72.

Bayraktar, G. (2015:143). *Siber Savaş ve Ulusal Güvenlik Stratejisi.* İstanbul: Yeniyüzyıl Yayınları.

BBC. (2015) bbc.com: https://www.bbc.com/turkce/haberler/2015/12/151223_siber_saldiri adresinden alınmıştır

BBC.(2016)bbc.com: https://www.bbc.com/turkce/haberler/2016/01/160130_rusya_turkiye_ucak adresinden alınmıştır. Erişim Tarihi:01.11.2018

Benzer, R. (2014:28). Siber Suçlar ve Teorik Yaklaşımlar. H. M. Çakır ve Kılıç içinde, *Güncel Tehdit:Siber Suçlar* (s. 28). Ankara: Seçkin Yayıncılık.

Berlinger ve Santos, J. N. (2018, 10 04). *"İngiltere, 'Pervasız' Siber Saldırı İçin Rus Ordusunu Suçluyor".* https://edition.cnn.com/2018/10/03/uk/uk-russia-cyber-attacks-intl/index.html adresinden alınmıştır. Erişim Tarihi: 10.01.2019

Bıçakçı ve Aydın (ed.), S. (2013). *21. Yüzyılda Siber Güvenlik.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Bıçakçı, K. (2013). *Kullanışlı Güvenlik Ne ? Neden ? Nasıl ?* Bilgem: http://mcs.bilgem.tubitak.gov.tr/cryptodays/arsiv/kriptogunleri_2013/files/2013-sunumlar/Kemal-Bicakci.pdf adresinden alınmıştır. Erişim Tarihi:09.10.2018

Bıçakçı, S. (2012:103). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler, 9*(34), 219.

Bilgin, P. (2010: 76). Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları. *SAREM Stratejik Araştırmalar Dergisi, 8*, 76.

Bilgin, P. (2011:399-412). The politics of studying securitization? The Copenhagen School in Turkey . *Security Dialogue,* 399-412.

Birdişli, F. (2014:34). *Teori ve Pratikte Uluslaraası Güvenlik .* Ankara: Seçkin Yayıncılık.

Bisson, D. (2015, 02 17). *Tripwire*. https://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports/ adresinden alınmıştır. Erişim Tarihi: 09.11.2018

Bloomberg. (2018, 11 06). https://www.bloomberg.com/quicktake/great-firewall-of-china adresinden alınmıştır. Erişim Tarihi: 16.12.2018

Booth, K. (1997:106). Security and Self: Reflections of a Fallen Realist. *Critical Security Studies: Concepts and Cases*, 104-119.

Bozdağlıoğlu, Y. (2007:149). *Yapılandırmacı Yaklaşım(Konstrüktivizm).* Ankara: Platin Yayınları.

BTK. (2017, 12 15). *BTK*. https://www.btk.gov.tr/sektorel-siber-olaylara-mudahale-ekibi adresinden alınmıştır. Erişim Tarihi: 19.10.2018

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.* Oxford Scholarship.

Bull, H. (1981: 717). Hobbes and the International Anarchy. *Social Research: An International Quarterly, 48*(4), 717-738.

Buzan ve diğerleri. (1998). *Security: A New Framework for Analysis.* London: Lynne Rienner Publishers.

Buzan ve Hansen. (2009). *International Security Studies.* Cambridge: Cambridge Universty Press.

Canbay ve diğerleri.(2009). *cybersecurity*. http://www.cybersecurity.gov.tr/publications/sg.pdf adresinden alınmıştır. Erişim Tarihi: 01.10.2018

Caşın, M. H. (2007: 75). *Kürselleşmanin Avrupa Birliği Ortak Güvenlik ve Savunma Politikasına Etkisi.* İstanbul: Nokta Kitap.

Cavelty, M. (2012). Cyber- Allies Strengths and Weaknesses of NATO's Cyberdefense. *Dgap Journal*, 1-8.

Cendrowski, S. (2015, 02 26). *Fortune.* http://fortune.com/2015/02/26/why-china-is-making-life-miserable-for-big-u-s-tech/ adresinden alınmıştır. Erişim Tarihi: 24.11.2018

CISA. (2018). *www.us-cert.gov*. https://www.us-cert.gov: https://www.uscert.gov/ncas/tips/ST04-014 adresinden alınmıştır. Erişim Tarihi:27.11.2018

Clarke ve Knake, R.-R. (2012). *Cyber War.* New York: Ecco.

Clinton, B. (1998). *Fas.org*. https://fas.org/irp/offdocs/pdd/pdd-63.htm adresinden alınmıştır. Erişim Tarihi: 12.12.2018

Coşkun, B. D. (2007). Postmodern Yaklaşım . H. Çakmak içinde, *Uluslararası İlişkiler "Giriş, Kavram ve Teoriler "* (s. 192-193). Ankara: Platin Yayınları.

Cox ve diğerleri, P. (2002). https://eur-lex.europa.eu/eli/dir/2002/58/oj adresinden alınmıştır. Erişim Tarihi: 14.09.2018

Çakmak, H. (2014:126). *Uluslararası İlişkiler: Giriş, Kavramlar ve Teoriler.* İstanbul: Doğu Kitabevi.

Çifci, H. (2017:93). *Her Yönüyle Siber Savaş.* Ankara: Tübitak Kitaplar Müdürlüğü.

Çubukçu ve Bayzan, A.-Ş. (2013:160). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research*, 148-173.

Dağı, İ. (2013:73). *Devlet, Sistem ve Kimlik: Uluslararası İlişkilerde Temel Yaklaşımlar.* İstanbul: İletişim Yayınları.

Danchev, D. (2009, 05 13). *ZDNet.* https://www.zdnet.com/article/chinas-secure-os-kylin-a-threat-to-u-s-offensive-cyber-capabilities/ adresinden alınmıştır. Erişim Tarihi: 01.09.2018

Darıcılı, A. B. (2017:112). *Siber Uzay ve Siber Güvenlik.* Bursa: Dora Yayıncılık.

Davenport ve Amjad, T. A. (2016, 09 26). *Deloitte Insights.* https://www2.deloitte.com/insights/us/en/topics/analytics/future-of-cybersecurity-in-analytics-automation.html adresinden alınmıştır. Erişim Tarihi: 12.11.2018

David E. Sanger ve diğerleri. (2011). *https://www.nytimes.com.* The New York Times:https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html adresinden alınmıştır Erişim Tarihi: 09.10.2018

Dedeoğlu, B. (2008:38). *Uluslararası Güvenlik ve Strateji.* İstanbul: Yeniyüzyıl Yayınları.

Dominioni, S. (2018, 07 16). *Multilateral tracks to tackling cybercrime: an overview.* ISPI. adresinden alınmıştır. Erişim Tarihi: 29.12.2018

E.Zheng, D. (2015, 04 24). *Csıs.* Center For Strategıc&Internatıonal Studies: https://www.csis.org/analysis/2015-dod-cyber-strategy adresinden alınmıştır. Erişim Tarihi: 19.12.2018

Eckenrode ve Friedman, J.-S. (2018). *Deloitte Finansal Hizmetler Merkezi.* https://www2.deloitte.com/insights/us/en/industry/financial-services/state-of-cybersecurity-at-financial-institutions.html?icid=dcom_promo_featured|global;en adresinden alınmıştır. Erişim Tarihi: 22.12.2018

En.wikipedia. (2018). *En.wikipedia*. https://en.wikipedia.org/wiki/E-government adresinden alınmıştır. Erişim Tarihi: 17.12.2018

Enisa. (2004). *enisa.* https://www.enisa.europa.eu/about-enisa adresinden alınmıştır. Erişim Tarihi: 03.05.2018

Erdurmaz, A. (2003:27). *Orta Doğu'daki Kitle İmha Silahları ve Silahların Kontrolü.* Ankara: Ümit Yayıncılık.

Eren, M. (2017:19). *Avrupa Birliği'nin Siber Güvenlik Politikası.* İstanbul: Beta Basın Yayın Dağıtım.

Erhan, Ç. (2002). Soğuk Savaş Sonrası ABD'nin Güvenlik Algılamaları. *Uluslararası Güvenlik Sorunları Ve Türkiye,* 55-81.

Ersoy, Ö. (2004:330). Terör ve Organize Suçlarda Yakınlaşma ve İşbirliğinin İncelenmesi. *Polis Dergisi,* 328-339.

European Defency Agency 2017. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence adresinden alınmıştır. Erişim Tarihi:02.12.2018

European Parliament. (2002). https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML adresinden alınmıştır. Erişim Tarihi: 15.12.2018

European Parliament. (2013). https://www.ispionline.it/it/pubblicazione/multilateral-tracks-tackling-cybercrime-overview-20962 adresinden alınmıştır. Erişim Tarihi:23.12.2018

Europol. (2013). *European Cyber Crımecenter - EC3.* https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 adresinden alınmıştır. Erişim Tarihi:01.12.2018

Fletcher ve diğerleri. (2016). *The European Union as an Area of Freedom, Security and Justice.* https://research.utwente.nl/en/publications/introduction-the-european-union-as-an-area-of-freedom-security-an adresinden alınmıştır. Erişim Tarihi:06.12.2018

Friedman ve Singer, A.-P. (2014). *Cyber Security and Cyber War: What Everyone Needs to Know.* London: Oxfor University Press.

Fruhlinger, J. (2018). *csoonline.* https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html adresinden alınmıştır. Erişim Tarihi: 20.12.2018

GCSC. (2018, 11 08). *Küresel Siber İstikrar Komisyonu.* https://cyberstability.org/news/global-commission-introduces-six-critical-norms-towards-cyber-stability/ adresinden alınmıştır. Erişim Tarihi:02.12.2018

Gerhart, M. (2017, 06 27). *Imperva.* https://www.imperva.com/blog/the-evolution-of-cybercrime-and-what-it-means-for-data-security/ adresinden alınmıştır. Erişim Tarihi:01.10.2018

GFCE. (2016, 12 07). https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime adresinden alınmıştır. Erişim Tarihi:15.11.2018

Glare, P. (2005). *Oxford Latin Dictionary.* Oxford: Clarendon Press.

Goble, A. (2009:191). Defining Victory and Defeat : The Information War Between Russia and Georgia, In the Guns of August 2008: Russia War in Georgia. S. E. diğerleri. içinde New York: Armonk.

Goodrich ve Tamassio. (2010). *Introduction to Computer Security.* Wesley: Addison .

Griffiths, M. (2013:13). *Uluslarası İlişkilerde Temel Kavramlar.* Ankara: Nobel Yayıncılık.

Güntay, V. (2017:85). Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği. *Güvenlik Bilimleri Dergisi, 2*(6), 81-108.

Gürcan, M. (2014, 05 01). *Rusya'nın Ukrayna'daki Bulanık Savaş Konsepti.* academia.edu: https://www.academia.edu/11069073/RUSYANIN_BULANIK_SAVA%C5%9E_KONSEPT%C4%B0 adresinden alınmıştır. Erişim Tarihi: 01.12.2018

Güven, C. (2013). *Bal Tuzağı Bel Altı İstihbarat .* İstanbul: Timaş Yayınları.

Harris, P. (2013). *The Guardian.* https://www.theguardian.com/technology/2013/feb/23/mandiant-unit-61398-china-hacking adresinden alınmıştır. Erişim Tarihi: 22.11.2018

Hilal, T. (2018:174). *Siber Mücadeleye Giriş.* İstanbul: Kutlu Yayınevi.

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, *4*(2), 1-24.

Holloway, R. (2018, 02 06). *BaseCreative.* https://www.basecreative.co.uk/opinion/the-golden-shield-project/ adresinden alınmıştır. Erişim Tarihi: 05.10.2018

ICDF2C. (2015, 10 08). *7. Uluslararası Dijital Adli Tıp ve Siber Suçlar Konferansı (ICDF2C).* https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/7th-international-conference-digital-forensics-and-cyber-crime-icdf2c adresinden alınmıştır. Erişim Tarihi:01.11.2018

İlbaş, M. (2014:11). *Enerji-Politik Dünya ve Türkiye.* Ankara: Berikan Yayınevi.

İnternet Live Stats. (2018). http://www.internetlivestats.com/ adresinden alınmıştır. 01.12.2018

İtgovernance.eu. (2013). *İtgovernance.eu.* https://www.itgovernance.eu/en-ie/eu-cybersecurity-strategy-ie adresinden alınmıştır. Erişim Tarihi: 05.11.2018

Jervis, R. (2011:1). From Balance to Concert: A Study of International Security Cooperation. *Princeton University Journals*.

Jinghua, L. (2018). *carnegieendowment.org.* https://carnegieendowment.org/2018/10/19/chinese-perspective-on-pentagon-s-cyber-strategy-from-active-cyber-defense-to-defending-forward-pub-77540 adresinden alınmıştır. Erişim Tarihi: 27.12.2018

Joın. (2017). *Joınt Communication To The European Parlıament And The Councıl.* Consılıum:https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf adresinden alınmıştır. Erişim Tarihi: 13.12.2018

Jones, H. (2014, 09 03). *Searchengineland.* https://searchengineland.com/chinas-golden-shield-project-works-202282 adresinden alınmıştır. Erişim Tarihi: 03.11.2018

Joyner, J. (2010, 07 02). *The National Interest.* https://nationalinterest.org/commentary/natos-cyber-threat-3590 adresinden alınmıştır. Erişim Tarihi: 20.10.2018

Kaiman, J. (2014, 05 20). *theguardian.* https://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges adresinden alınmıştır. Erişim Tarihi: 14.11.2018

Kakar, H. (2018) Observer Research Foundatıon, https://www.orfonline.org/expert-speak/has-pakistan-started-losing-hybrid-war-kashmir-46027/ Erişim Tarihi: 09.12.2018

Kalkan, Ö. (2012:203). Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Okulu Çerçevesinde Tartışılması. *Turan Stratejik Araştırmalar Merkezi Dergisi, 4*, 202-208.

Kara ve diğerleri. (2018:2, 07 09). *Ağ Ekonomisin Karanlık Yüzü: Siber Terör.* edu.tr: http://kisi.deu.edu.tr/oguz.kara/Ag%20Ekonomisinin%20karanlik%20yuzu%20siber%20teror.pdf adresinden alınmıştır. Erişim Tarihi: 01.12.2018

Kardaş, T. (2007:138). Güvenlik: Kimin Güvenliği ve Nasıl ? *Uluslararası Politikayı Anlamak 'Ulus- Devlet'ten Küreselleşmeye',* 125-152.

Keleştemur, A. (2015:312). *Siber İstihbarat.* İstanbul: Level Kitap.

Kelly, S. (2014). *Freedom On The Net 2014.* freedomhouse: https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf adresinden alınmıştır. Erişim Tarihi: 10.10.2018

Keskin, B. (2008:242). *Elektronik Harp ve Sinyal Savaşları.* İstanbul: IQ Kültür Sanat Yayıncılık.

Kirby, C. (2005, 02 17). *Sfgate*. https://www.sfgate.com/business/article/Former-White-House-aide-backs-some-Net-regulation-2729985.php adresinden alınmıştır. Erişim Tarihi:12.12.2018

Klimburg, A. (2012). *National Cyber Security Framework Manual.* Tallin: NATO CCD COE Publications.

Kolcu, G. (2015). *Hürriyet.* hurriyet.com.tr: http://www.hurriyet.com.tr/teknoloji/onlar-saldirdi-biz-fisi-cektik-40030151 adresinden alınmıştır. Erişim Tarihi: 12.09.2018

Krickovic, A. (2016). Catalyzing Conflict: The Internal Dimension of the Security Dilemma. *Journal of Global Security Studies, 1*(2), 111-127.

Krombholz ve diğerleri. (2015:113). Advanced social engineering attacks. *Journal of Information Security and Applications,* 113-122.

Kuchler, H. (2017, 11 28). *Fınancıal Times.* https://www.ft.com/content/d23cc752-d3b0-11e7-8c9a-d9c0a5c8d5c9 adresinden alınmıştır. Erişim Tarihi: 04.11.2018

Kuyaksil, A. (2004:92). Türkiye'de Terör ve Terörün Kaynakları. *Polis Dergisi Terörle Mücadele Özel Sayısı, 10*(40), 89-108.

Lesk, M. (2007). The New Front Line Estonia Under Cyberassault. *IEEE Securty&Privacy*, 76-79.

Li ve diğerleri, F. (2010). *SpringerLink.* https://link.springer.com/chapter/10.1007/978-3-642-15506-2_4 adresinden alınmıştır. Erişim Tarihi: 05.09.2018

Lin, H. (2010:63). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*. Erişim Tarihi: 19.11.2018

Ling, J. (2016, 03 24). *Vıce News.* https://news.vice.com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty adresinden alınmıştır. Erişim Tarihi:05.12.2018

Lu, C. Y. (2013). Analysis of the Dilemma of the Current Global Governance of Cyberspace. *Contemporary International Relations* , 11.

M. Arends ve J. Frederik. (2009:6). Homeros'dan Hobbes ve Ötesine: "Güvenlik" Kavramının Avrupa Geleneğindeki Boyutları. *Uluslararası İlişkiler Dergisi, 6*(22), 3-33.

M.Kauppi ve P. Viotti. (2016). *Uluslararası İlişkiler Teorisi.* İstanbul: Nobel Akademik Yayıncılık.

Mabee, B. (2003:136). Security Studies and the 'Security State': Provision in Historical Context. *Internatıonal Relations, 17*(2), 136.

MacKinnon, R. (2009). *CircleID.* http://www.circleid.com/posts/20090608_chinas_green_dam_youth_escort_software/ adresinden alınmıştır. Erişim Tarihi:01.12.2018

Maurer ve Hinck, (2018). *"Rusya'nın Siber Stratejisi".* ıspı: https://www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835#nota6 adresinden alınmıştır. Erişim Tarihi: 10.01.2019

McCarthy, K. (2018, 10 22). *TheRegister.* https://www.theregister.co.uk/2018/10/22/super_micro_chinese_spy_chip_sec/ adresinden alınmıştır. Erişim Tarihi: 23.12.2018

Mcdonald ve Bellamy, A. (2004:309). Securing International Society: Towards an English School Discourse of Security. *Australian Journal of Political Science, 39*(2), 307-330.

McWhorter, D. (2013, 02 19). *FireEye.* https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html adresinden alınmıştır. Erişim Tarihi:12.11.2018

Metcalf, K. N. (2018, 10). *A Legal View on Outer Space and Cyberspace: similarities and differences.* CCDCOE: https://ccdcoe.org/multimedia/legal-view-outer-space-and-cyberspace-similarities-and-differences.html adresinden alınmıştır. Erişim Tarihi:21.12.2018

Mizokami, K. (2018, 11 09). *The Natıonal Interest.* https://nationalinterest.org/blog/buzz/russia-china-war-5-weapons-china-would-strike-35657 adresinden alınmıştır. Erişim Tarihi:21.12.2018

Murcia, M. (2015, 12 18). telegraph.co.uk: https://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation.html adresinden alınmıştır. Erişim Tarihi: 01.11.2018

NewsBBC.(2008).http://news.bbc.co.uk/2/hi/technology/7208511.stm adresinden alınmıştır. Erişim Tarihi: 15.12.2018

Nikolayevich, K. D. (2017). *Siber Uzay ve Askeri Çatışmalar: Terminolojiye Doktrinal Yaklaşımlar.* http://www.inf74.ru/safety/ofitsialno/zashhita-kiberprostranstva-v-raznyih-stranah/ adresinden alınmıştır. Erişim Tarihi: 10.01.2019

Nye, J. (2005:37). *Yumuşak Güç, Dünya Siyasetinde Başarının Yolu.* Ankara: Elips Kitap.

Nye, J. S. (2005:75). *Yumuşak Güç.* Ankara: Elips Kitapları.

Obama,B.(2009). *InterNatıonalStrategy*.info.publicintelligence.net:https://info.publicintelligence.net/WHInternationalCyberspace.pdf adresinden alınmıştır. Erişim Tarihi: 19.11.2018

Official Journal. (2001). https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32001F0413 adresinden alınmıştır. Erişim Tarihi: 25.09.2018

Örgün, F. (2001:49-59). *Küresel Terör.* İstanbul: Okumuş Adam Yayınları.

Özerdem, F. (2015:134). *Güvenliğin Gündeminden Çatışma, Ayrılıkçı Ayaklanmalar ve Terörizm.* Ankara: Nobel Kitap.

Peasley ve diğerleri, (2017). *DeloitteInsights.* https://www2.deloitte.com/insights/us/en/industry/retail-distribution/cyber-risk-

management-in-consumer-business.html adresinden alınmıştır. Erişim Tarihi: 10.10.2018

Popescu, A. (2013, 04 10). *Mashable*. https://mashable.com/2013/04/10/5-services-to-boost-email-productivity/#iPBx6_zLTiqr adresinden alınmıştır. Erişim Tarihi:10.10.2018

Rab, N. (2018, 07 19). *DıgıtalGuardian.* https://digitalguardian.com/blog/what-security-operations-center-soc adresinden alınmıştır. Erişim Tarihi: 05.11.2018

Rajeck,J.(2017).*Econsultancy*.https://econsultancy.com/freetrial/?utm_source=econsite&utm_medium=banner&utm_campaign=FreeTrialLaunch adresinden alınmıştır. Erişim Tarihi: 12.12.2018

Raska, M. (2017, 03 08). *AsiaTimes.* http://www.atimes.com/article/chinas-evolving-cyber-warfare-strategies/ adresinden alınmıştır. Erişim Tarihi: 21.11.2018

Rouse,M.(2017).*searchnetworking*. https://searchnetworking.techtarget.com/definition/ARPANET adresinden alınmıştır. Erişim Tarihi: 01.09.2018

Rugge, F. (2018). https://www.ispionline.it/en/pubblicazione/cybercrime-and-international-relations-20996 adresinden alınmıştır. Erişim Tarihi:12.12.2018

S.Nye,J.(2010).*CyberPower*.belfercenter: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf adresinden alınmıştır. Erişim Tarihi: 14.11.2018

S.Nye, J. (2017, 03 13). *euronews.* euronews: https://www.euronews.com/2017/03/13/view-conflicts-in-cyberspace-a-normative-approach-to-preventing-cyberwars adresinden alınmıştır. Erişim Tarihi:10.10.2018

Sağıroğlu ve Canbek. (2007: 2). Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 1-12.

Sander, O. (2004). *Siyasi Tarih 1918-1994* (s. 183). Ankara: İmge Kitabevi.

Schwartz,M.J. (2018). *bankinfosecurity.com.* https://www.bankinfosecurity.com/chinese-cyber-threat-nsa-confirms-attacks-have-escalated-a-11696 adresinden alınmıştır. Erişim Tarihi: 09.12.2018

Sengervediğerleri,(2013).*TheNewYorkTimes.* https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html adresinden alınmıştır. Erişim Tarihi: 27.10.2018

Shearer, J. (2010, 07 13). *Symantec*. Symantec.com: https://www.symantec.com/security-center/writeup/2010-071400-3123-99 (23.10.2018) adresinden alınmıştır

Silinir ve diğerleri. (2012:146). Enerji Güvenliği: NATO'nun Küresel Enerji Güvenliğindeki Rolü. *Batman Üniversitesi Yaşam Bilimleri Dergisi, 2*(1), 132-147.

Smıth,C.(2001). *Nytimes.* https://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html adresinden alınmıştır. Erişim Tarihi:25.11.2018

Snyder, B. (2018). *iz.ru.* https://iz.ru/791497/2018-09-21/tramp-utverdil-novuiu-strategiiu-ssha-po-kiberbezopasnosti Erişim Tarihi: 10.01.2019 adresinden alınmıştır

Softpedia. (2015). https://en.wikipedia.org/wiki/Green_Dam_Youth_Escort adresinden alınmıştır. Erişim Tarihi: 11.10.2018

State.gov. (2012). https://www.state.gov/digitalstrategy/ adresinden alınmıştır. Erişim Tarihi:02.11.2018

Sterling, B. (2011, 03 11). *Revealed: Operation Shady RAT*. wired.com: https://www.wired.com/2011/08/operation-shady-rat/ adresinden alınmıştır. Erişim Tarihi: 09.07.2018

Swaine, M. (2013). *Chinese Views on Cybersecurity in Foreign Relations.* http://carnegieendowment.org/files/CLM42MS.pdf adresinden alınmıştır. Erişim Tarihi: 01.12.2018

Taureck, R. (2006). Securitisation Theory and Securitisation Studies. *Journal of International Relations and Development*, 53-61.

Tezsever, S. (1999:165-167). *Milli Güvenliğimiz İçinde İstihbarat.* İstanbul: İ.Ü. Basımevi.

TheTexasPoliticsProject.(2016).https://texaspolitics.utexas.edu/archive/html/bur/features/0303_01/policy.html adresinden alınmıştır.Erişim Tarihi: 07.11.2018

The United States Department of Justice. (2014, 05 19). https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor adresinden alınmıştır. Erişim Tarihi: 29.10.2018

Thomas, R. H. (1974, 12 01). *Corewar*. http://corewar.co.uk/creeper.htm adresinden alınmıştır. Erişi Tarihi: 16.08.2018

Tıkk,E.(2010).*ccdcoe.org/publications/books.*ccdcoe: htttps://www.ccdcoe.org/publications/books/legalconsiderations.pdf (25.10.2018) adresinden alınmıştır

Toklu, V. (2006). *Uluslararası İlişkiler.* Ankara: İmaj Yayınevi.

Toprak,G.(2015,09 03). *Medyaakademi*. https://www.medyaakademi.org/2015/09/03/google-in-kurulus-oykusu-ve-gelisimi/ adresinden alınmıştır. Erişim Tarihi: 20.10.2018

Touraine, M. (1997:333). *Alt Üst Olan Dünya.* Ankara: Ümit Yayıncılık.

TRAC, (2018) Terrorism Research Analysıs Consortıum, https://www.trackingterrorism.org/group/unit-121-north-korean-cyberterrorists Erisim Tarihi : 03.09.2018

Traynor, I. (2007:5). Russia Accused of Unleashing Cyberwar Disable Estonia. *The Guardian,* 5.

Trimintzios ve diğerleri, P. (2016). *Report on Cyber Crisis Cooperation and Management.* Enısa.

Türkiye Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi.* http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf adresinden alınmıştır. Erişim Tarihi: 13.09.2018

UHDB. (2017, 05 08). *Ulusal Siber Güvenlik Çalışmalarının Yönetilmesi, Yürütilmesi ve Koordinasyonuna İlişkin Karar.* http://www.udhb.gov.tr/doc/siberg/SOME_BKK.pdf adresinden alınmıştır. Erişim Tarihi: 19.10.2018

Urhal, Ö. (2009:346). *Küreselleşen Dünyada Güvenlik.* Ankara: Adalet Yayınevi.

Uzgel, İ. (2004). *Ulusal Çıkar.* Ankara: İmge Kitabevi.

Waltz, K. (2001). *Man, the State and War: A Theoretical Analysis,* . New York: Columbia Universty Press.

Weedon ve Galante, J.-L. (2014, 03 12). *Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast.* Fireeye.com: https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html adresinden alınmıştır.Erişim Tarihi:11.12.2018

Wendt, A. (1995:74). Constructing International Politics. *Internatıonal Security, 20*, 74.

Westby, R. (2004). *International Guide to Cyber Security.* Chicago: American Bar Association.

Whittaker, Z. (2017, 06 12). https://www.zdnet.com/article/russian-malware-likely-to-blame-for-ukrainian-power-grid-attack/ adresinden alınmıştır. Erişim Tarihi: 15.11.2018

Wight ve Patomaki, H. P. (2000:218). After Postpositivism ? The Promises of Critical Realism. *International Studies Quarterly*(44), 218.

Williams ve Krause, K. (1997). *Critical Security Studies: Concepts and Cases.* London: UCL Press.

Wortzel, L. (2011). China: Warfare in the Information Age. *Asia Policy*, 101-105.

Xinhua. (2014). Http: // news.xinhuanet.com/world/2014-05/28/c1110904778.htm adresinden alınmıştır. Erişim Tarihi: 24.11.2018

Yakushev, M. (2013). *Siber Uzayda Savaş: Rusya İçin Dersler ve Sonuçlar.* http://bourabai.ru/telematics/infowar2.htm adresinden alınmıştır. Erişim Tarihi: 10.01.2019

Yanevsky, A. (2017). *"Rusya, Ukrayna'da edinilen tecrübeyi Batı ülkelerine karşı karma bir savaş yapmak için kullanıyor.".* https://www.golos-ameriki.ru/a/4085965.html adresinden alınmıştır. Erişim Tarihi: 10.01.2019

Yayla, M. (2014:195). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Harketlerden Farkı. *Hacettepe HFD*, 181-198.

Yazıcıoğlu, R. (1997). *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile.* İstanbul: Alfa Yayıncılık.

Yılmaz, M. E. (2015:170). *Toplumlar Arası Çatışmalarca Barışı İnşa Etmek Birleşmiş MilletlerBarış Güçleri ve Alternatif Uyuşmazlık Çözümü.* Bursa: Dora Yayıncılık.

Yılmaz, S. (2014). *Uzay Güvenliği.* İstanbul: Milenyum Yayınları.

Yüksel, M. (2016, 09 14). *Siber Tehdit.* http://sibertehdit.com/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani/ adresinden alınmıştır. Erişim Tarihi: 02.09.2018

Zapryanov,J.(2016). https://www.capital.bg/biznes/kompanii/2016/10/16/2844401_verizon_postavia_pod_vupros_sdelkata_s_yahoo/ adresinden alınmıştır. Erişim Tarihi: 10.01.2019

ÖZGEÇMİŞ

1. Adı Soyadı **:** Burak DORUKOĞLU

İletişim Bilgileri

Adres **:** Paşaalanı Mah.225.Sok.No:50/7 KARESİ/BALIKESİR

Telefon 0535 020 11 01

Mail : freemanbd@hotmail.com

2. Doğum Tarihi **:** 23.05.1988

3. Öğrenim Durumu : Yüksek Lisans Öğrencisi

Derece	Başlangıç	Bitiş	Üniversite
Lise	2002	2005	Zühtü Özkardeşler Lisesi/ BALIKESİR
Ön Lisans	2005	2007	K.K.K. Astsubay Meslek Yüksek Okulu / BALIKESİR
Lisans	2008	2011	Anadolu Üniversitesi, İşletme Fakültesi İşletme Bölümü/ ESKİŞEHİR
Yüksek Lisans	2015	2019	Uluslararası Kıbrıs Üniversitesi, Lisansüstü Eğitim Öğretim ve Araştırma Enstitüsü, Uluslararası İlişkiler Bölümü

4. Yabancı Dili ve Seviyesi **:** İngilizce/Intermediate