T. C.

ULUDAĞ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRMALI ANALİZİ

(DOKTORA TEZİ)

ALİ BURAK DARICILI

BURSA - 2017

ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER
ENSTİTÜSÜ ULUSLARARASI
İLİŞKİLER ANABİLİM DALI

AMERİKA BİRLEŞİK DEVLETLERİ VE
RUSYA FEDERASYONU'NUN SİBER
GÜVENLİK STRATEJİLERİNİN
KARŞILAŞTIRMALI ANALİZİ
(DOKTORA TEZİ)

Ali Burak
DARICILI

BURSA
2017

T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRMALI ANALİZİ

(DOKTORA TEZİ)

Ali Burak DARICILI

Bursa 2017

T. C.

ULUDAĞ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRMALI ANALİZİ

(DOKTORA TEZİ)

ALİ BURAK DARICILI

Danışman:

Prof. Dr. Barış ÖZDAL

BURSA – 2017

T. C.

ULUDAĞ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Uluslararası İlişkiler Anabilim Dalı'nda 711316003 numaralı Ali Burak DARICILI'nın hazırladığı "Amerika Birleşik Devletleri ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi" konulu doktora çalışması ile ilgili tez savunma sınavı 07../07./ 2017 günü 14⁰⁰ - 16⁰⁰ saatleri arasında yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin/çalışmasının ....BAŞARILI..... (başarılı/~~başarısız~~) olduğuna .OYBİRLİĞİ..... (oybirliği/~~oy çokluğu~~) ile karar verilmiştir.

Prof. Dr. Barış ÖZDAL Uludağ Üniversitesi Üye (Tez Danışmanı ve Sınav Komisyonu Başkanı)	Prof. Dr. Fırat PURTAŞ Gazi Üniversitesi Üye
Doç. Dr. R. Kutay KARACA İstanbul Gelişim Üniversitesi Üye	Yrd. Doç. Sertaç SERDAR Uludağ Üniversitesi Üye
Yrd. Doç. Dr. Sezgin KAYA Uludağ Üniversitesi Üye	
	07../07./ 2017

Yemin Metni

Uludağ Üniversitesi Sosyal Bilimler Enstitüsü'ne arz ettiğim bahse konu doktora tez çalışmamın bilimsel araştırma, yazma ve etik kurallarına uygun olarak tarafımdan yazıldığına ve tezde yapılan bütün alıntıların kaynaklarının usulüne uygun olarak gösterildiğine, tezimde intihal ürüne cümle veya paragraflar bulunmadığına şerefim üzerine yemin ederim.

Adı-Soyadı : Ali Burak Darıcılı
Öğrenci No : 711316003
Anabilim Dalı: Uluslararası İlişkiler
Programı : Uluslararası İlişkiler
Statüsü : Doktora

SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS/DOKTORA İNTİHAL YAZILIM RAPORU

ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 15/06/2017

Tez Başlığı / Konusu: Amerika Birleşik Devletleri ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi / Bu tez çalışması, uluslararası ilişkiler açısından siber uzayın neden olduğu yeni tartışma konularını ele almak suretiyle, Amerika Birleşik Devletleri (ABD) ve Rusya Federasyonu (RF)'nun siber güvenlik stratejilerini karşılaştırmalı olarak analiz etmek amacıyla hazırlanmıştır. Çalışmadaki temel sorunsalımız ise ABD ile RF'nin, siber güvenlik stratejilerini belirleme sürecinde birbirleriyle bir etkileşim ve etki-tepki ilişkisi içinde olup olmadığı tartışmasına odaklanmıştır.

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 193 sayfalık kısmına ilişkin, 15/06/2017 tarihinde şahsım tarafından intihal tespit programından (Turnitin)*aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı % 18 'tir.

Uygulanan filtrelemeler:

1- Kaynakça hariç
2- Alıntılar hariç/dahil
3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi
ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.
Gereğini saygılarımla arz ederim.

15.06.2017
Tarih ve İmza

Adı Soyadı:	Ali Burak Darıcılı
Öğrenci No:	711316003
Anabilim Dalı:	Uluslararası İlişkiler
Programı:	Uluslararası İlişkiler
Statüsü:	☐Y.Lisans ☒Doktora

Danışma (Prof. Dr. Barış ÖZDAL)
*** Turnitin programına Uludağ Üniversitesi Kütüphane web sayfasından ulaşılabilir.**

19.06.2017

ÖZET

Yazar Adı ve Soyadı : Ali Burak DARICILI

Üniversite : Uludağ Üniversitesi

Enstitü : Sosyal Bilimler Enstitüsü

Anabilim Dalı : Uluslararası İlişkiler

Bilim Dalı :

Tezin Niteliği : Doktora Tezi

Sayfa Sayısı : 223 (CCXXIII)

Mezuniyet Tarihi : …. / …. / 2017

Tez Danışmanı : Prof. Dr. Barış ÖZDAL

AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRMALI ANALİZİ

Bu tez çalışması, uluslararası ilişkiler açısından siber uzayın neden olduğu yeni tartışma konularını ele almak suretiyle, Amerika Birleşik Devletleri (ABD) ve Rusya Federasyonu (RF)'nun siber güvenlik stratejilerini karşılaştırmalı olarak analiz etmek amacıyla hazırlanmıştır. Çalışmadaki temel sorunsalımız ise ABD ile RF'nin, siber güvenlik stratejilerini belirleme sürecinde birbirleriyle bir etkileşim ve etki-tepki ilişkisi içinde olup olmadığı tartışmasına odaklanmıştır.

Bu doğrultuda tezde ulaşılan sonuç, ABD ve RF'nin siber güvenlik stratejilerini şekillendirme süreçlerinde, birbirlerine yönelik tehdit algılamalarının önemli etkisi olduğudur. Zira ABD ve RF arasında siber uzay alanında günümüze kadar süre gelen rekabetinin kökenleri her iki devletin Soğuk Savaş dönemindeki ideolojik ve askeri çekişmesinin bir sonucu olarak şekillenmiştir. Bununla birlikte söz konusu iki devlet kısa ve orta vadede ağ teknolojileri kapsamında askeri kapasitelerini geliştirmek için etkili bir siber savunma ve saldırı kapasitesi yaratmaya çalışacaklardır.

Genel ve soyut olarak aktardığımız bu çerçeve içerisinde tez çalışmasının ilgi bölümlerinde:

- Teknoloji kültürlerinin Soğuk Savaş döneminde ABD ve SSCB arasındaki askeri rekabetin günümüz siber uzay alanının şekillenmesine yaptığı katkıların,
- 1990'lar başı ile birlikte küreselleşen, ticarileşen ve sivilleşen internet teknolojisinden ABD ve RF'nin askeri ve istihbari bir enstrüman olarak istifade etme arayışlarının,
- Sosyal medya imkânlarını her iki devletin bir enformasyon savaşı aracı olarak kullanmaya yönelik planlamalarının,
- ABD ve RF'nin bu yıllar ile birlikte şekillenmeye başlayan resmi siber güvenlik strateji belge ve doktrinlerinin,
- Ulusal siber uzay alanlarını denetleyen hukuki rejimlerinin ve ulusal siber güvenlik kurumlarının faaliyetlerinin analiz edilmesine odaklanılmıştır.

Anahtar Sözcükler: Neo-Realizm, Siber Güvenlik, Siber Uzay, Amerika Birleşik Devletleri, Rusya Federasyonu

ABSTRACT

Name and Surname : Ali Burak DARICILI

University : Uludağ University

Institution : Social Science Institution

Field : International Relations

Branch :

Degree Awarded : Ph. D

Page Number : 223 (CCXXIII)

Degree Date : …. / …. / 2017

COMPARATIVE ANALYSIS OF CYBER STRATEGIES ADOPTED BY UNITED STATES OF AMERICA, AND RUSSIAN FEDERATION

This thesis study aims at comparative analysis of cyber security policies adopted by United States of America **(**USA), and Russian Federation **(**RF), with consideration of new discussions originated from cyber space in the context of international relations. This work tries to find out whether there is an action-response relation between USA, and RF or not, in the course of setting cyber security strategies.

Accordingly, this study found out the fact that USA, and RF's mutual perception of threat on their countries, is decisive when they are setting cyber security strategies. It is because of that today's ongoing competition between USA, and RF in the field of cyber space, originates from ideological, and military competition between USA, and RF during Cold War. Besides, the two states will try to create an effective cyber defense and attack capacity in order to improve their military capacities in the short and medium term within the scope of networking technologies.

As we explained in general and abstract, in order to support arguments of this study, focus of related chapters of this thesis;

- Contributions of technology cultures to the shaping of today's cyberspace space in the Cold War-era military rivalries between the USA and the Soviet Union,
- Attempts of USA, and RF to benefit from internet technology as a means of military, and espionage, since it has been global, commercial, and civil by 1990s,
- Planning of social media facilities for the use of the two states as an information warfare tool by the state,
- USA, and RF's official cyber security strategy documents, and doctrines that started to be formed by then,
- Legal regimes governing national cyber space areas; and activities of national cyber security institutions.

Keywords: Neo-Realism, Cyber Security, Cyber Space, United States of America, Russian Federation

ÖNSÖZ

Siber güvenlik kapsamındaki çalışmalar ülkemizde genel itibariyle bilişim teknolojileri temelli teknik konular olarak kabul edilmektedir. Benzer ön kabulden hareketle sosyal bilimciler de siber güvenlik çalışmalarını teknik bir alan okuyarak, özellikle teknik altyapı bilgisi gerektiren bu tür çalışmalardan kaçınma eğilimi gösterebilmektedirler. Hâlbuki siber güvenlik ve siber uzay çalışmalarını sadece teknik bir alan olarak değerlendirmek, bizce meseleyi son derece dar bir bakış açısıyla ele almak anlamına gelmektedir. Siber güvenlik ve uzay, özü itibariyle elbette ki teknik meselelerdir. Ancak siber güvenlik ve siber uzay alanı temelli gelişmelerin bireylerin, kurumların ve devletlerin güvenliklerini yakından ilgilendirdiği, uluslararası sistemdeki aktörler arasındaki ilişkilere önemli ölçüde tesir ettiği, bu kapsamda da uluslararası ilişkiler disiplininin çalışma konuları dahilinde önemli sonuçlar elde ettiği de ortadır.

Söz konusu değerlendirmeleri de dikkate almak suretiyle, tez çalışmasına başladığım ilk anlardan itibaren çalışmanın başarıyla tamamlanabilmesi için ciddi desteğe ihtiyaç duyacağımı bilmekteydim. İhtiyacım olan desteği ise tez yazım sürecinde çalışmamın her satırı detaylı bir şekilde okuyarak değerlendiren, yönlendirmeleriyle çalışma şevkimi arttıran, hatalarımı düzelten değerli Hocam Prof. Dr. Barış ÖZDAL ile tezimdeki yazım hatalarımı sabırla düzelten kıymetli dostum Tarık DİLAVER ile ablam Figen DARICILI'dan buldum. Bu vesile ile anılanlara, ayrıca hayatım boyunca desteklerini ve sevgilerini her zaman hissettiğim değerli ailemin tüm fertlerine teşekkür ederim.

Ali Burak DARICILI

Ankara 2017

İÇİNDEKİLER

BİRİNCİ BÖLÜM

REEL POLİTİK PARADİGMANIN ULUSLARARASI İLİŞKİLER DİSİPLİNİNDE KURAMSALLAŞTIRILMASI

İKİNCİ BÖLÜM

AMERİKA BİRLEŞİK DEVLETLERİ'NİN SİBER GÜVENLİK STRATEJİSİNİN ANALİZİ

ÜÇÜNCÜ BÖLÜM
RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİSİNİN ANALİZİ

DÖRDÜNCÜ BÖLÜM

AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRILMASI

KISALTMALAR

Kısaltma	Bibliyografik Bilgi
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AGİT	Avrupa Güvenlik ve İşbirliği Örgütü
ARPANET	Advanced Research Projects Agency / Gelişmiş Araştırma Projeleri Ajansı
AT	Avrupa Topluluğu
APEC	Asia-Pasific Ekonomic Cooperation / Asya-Pasifik Ekonomik İşbirliği
BND	Bundesnachrichtendienst / Federal İstihbarat Servisi
BM	Birleşmiş Milletler
BDT	Bağımsız Devletler Topluluğu
BİT	Bilgi İletişim Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
Bkz.	Bakınız
C.	Cilt
CERN	European Organization for Nuclear Research / Avrupa Nükleer Araştırma Örgütü
çev.	Çeviren
CIA	Central Intelligence Service / Merkezi Haber Alma Servisi
CNSS	Cyber National Security Section / Siber Milli Güvenlik Bölümü
COMECON	The Council for Mutual Economic Assistance / Karşılıklı Ekonomik Yardımlaşma Konseyi
CSS	Cyber Criminal Section / Siber Kriminal Bölümü
CYBERCOM	Cyber Command / Siber Komutanlığı
DDoS	Distributed Denial Of Service / Servis Dışı Bırakma
der.	Derleyen
DHS	Department of Homeland Security / İç Güvenlik Bakanlığı
DNI	Director of National Intelligence / Milli İstihbarat Direktörü
ed.	Editör
ECS	Enhanced Cybersecurity Services / Geliştirilmiş Siber Hizmetleri
FAPSİ	The Federal Agency for Government Communications and Information / Federal Elektronik ve Sinyal İstihbarat Servisi
FBI	Federal Bureau of Investigation / Federal Araştırma Bürosu
FSB	Federalnaya Slujba Bezopasnosti / Federal Güvenlik Servisi
FSO	Federalnaya Sluzhba Okhrany / Federal Koruma Servisi
FSTEC	Federal Service for Technical and Export Control / Teknik ve İhracat Kontrolü Federal Servisi
GRU	Glavnoye Razvedyvatel'noye Upravleniye / Ana Askeri İstihbarat Servisi
haz.	Hazırlayan
ICS-CERT	Industrial Control System-Computer Readiness Team / Endüstriyel Kontrol Sistemi-Bilgisayar Hazırlık Ekibi
IŞİD	Irak Şam İslam Devleti

JCC	Joint Cyber Center / Ortak Siber Merkez
KGAÖ	Kolektif Güvenlik Antlaşması Örgütü
MC	Milletler Cemiyeti
md.	Madde
MOSSAD	İstihbarat ve Özel Operasyonlar Enstitüsü
MILNET	Military Net / Askeri Net
NATO	North Atlantic Treaty Organization / Kuzey Atlantik Antlaşması Teşkilatı
NATO CCD-COE	NATO Cooperative Cyber Defence Centre of Excellence / NATO Müşterek Mükemmelliyet Siber Savunma Merkezi
NCIJTF	National Cyber Investigative Joint Task Force / Ulusal Siber Araştırma Müşterek Görev Kuvveti
NCPS	National Cybersecurity Protection System / Ulusal Siber Koruma Sistemi
NCSD	National Cyber Security Division / Ulusal Siber Güvenlik Bölümü
NICIC	National Cybersecurity and Communications Integration Center / Milli Siber ve İletişim Entegrasyon Merkezi
NIPP	National Infrasture Protection Plan / Ulusal Altyapı Koruma Planı
NSA	National Security Agency / Ulusal Güvenlik Ajansı
NSS	National Security Service / Milli Güvenlik Servisi
ODTÜ	Orta Doğu Teknik Üniversitesi
RBN	Russian Business Network / Rus İş Ağı
RF	Rusya Federasyonu
RİS	Rus İstihbarat Servisleri
RSK	Rus Silahlı Kuvvetleri
p.	Page
pp.	Page to Page / Sayfadan sayfaya
s.	Sayfa
SABRE	Semi-Automatic Business Research Environment / Yarı Otomatik İş Araştırma Ortamı
SAGE	Semi-Automatic Ground Environment / Yarı Otomatik Yer Ortamı
SBU	Ukrayna Devlet Güvenlik Servisi
SOME	Siber Olaylara Müdahale Ekipleri
SORM	System for Operative Investigative Activities / Operatif Araştırmacı Faaliyetleri Sistemi
ss.	Sayfadan sayfaya
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
STRATCOM	Strategic Command / Stratejik Komutanlık
SVR	Sluzhba Vneshney Razvedki / Dış İstihbarat Servisi
ŞİÖ	Şangay İşbirliği Örgütü
TİB	Telekomünikasyon İletişim Başkanlığı
Ter.	Tercüme
UOMM	Ulusal Siber Olaylara Müdahale Merkezi
US-CERT	US Computer Emergency Readiness Team / ABD Bilgisayar Acil Durum Hazırlık Takımı

USOM	Ulusal Siber Olaylara Müdahale Merkezi
Vol.	Volume
yy.	Yüzyıl
vb.	Ve benzeri

GİRİŞ:

İnternetin sivil kullanıma açılarak yaygınlaşması; iletişim imkân ve kabiliyetinde görülen gelişim; küreselleşmenin bir sonucu olarak günlük ve sosyal hayatta yaşanan çeşitlilik; teknolojik yenilikler ile birlikte internet üzerinden yayılan zararlı yazılımlardaki artış; "*siber uzay*" ve "*siber güvenlik*" şeklinde tanımlanan yeni kavramların tartışılmasına neden olmuştur. Ticari, kültürel, askeri, siyasal, finans gibi önemli sektörleri de içine alacak şekilde ağ teknolojilerinin kullanımı ise muazzam bir hızla küresel ölçekte yaygınlaşmıştır. Bu sürecin varacağı nihai noktanın; istisnasız olarak her şeyin sayısallaştığı, uluslararası protokollerin ve standartların hayatın tüm evrelerine nüfuz ettiği bir e-devlet olacağını ifade etmek, mevcut gelişmelerin seyri dikkate alındığında abartılı bir değerlendirme olmayacaktır.

Bu kadar önemli olmasına rağmen literatürde siber uzay kavramının uluslararası kabul görmüş bir tanımı bulunmamaktadır. Çoğunlukla interneti ifade etmek için kullanılan bir kavram olarak analizlerde sıklıkla ele alınmaktadır. Gerçekte bu tabir bir bilim kurgu romanı ile oluşturulmuştur. Zira dünyada en çok okunan bilim kurgu romanlarından biri olan Neuromancer'in yazarı William Gibson gerçeklikle hiçbir ilgisi olmayan bu kavramı, kendisi ile yapılan bir söyleşi de ilk defa kullanmıştır. Gibson'a göre siber uzay *"milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir halüsinasyon"* ve *"tasavvur edilemez karmaşa"* şeklindedir.[1]

Bu etkileyici terim tanımı ne olursa olsun, günümüzde günlük hayattan, askeri ve ekonomik konulara kadar, ciddi ve derin anlamlara sahip bir biçimde karşımıza çıkmaktadır. Siber uzay, kimilerine göre birbirleri ile haberleşen bilgisayar teknolojileri için kavramsal bir çerçeve, kimilerine göre askeri doktrinde yeni bir cephe, kimilerine göre bütün ekonomik eko-sistemin büyüyüp geliştiği bilgiye dayalı bir alt katman, kimilerine göre ise dünya politik arenasında gittikçe önem kazanan yeni bir içerik anlamını taşıyabilmektedir. Bize göre ise en kapsamlı ve doğru tanım;*"internet, iletişim ağları, dış dünyaya kapalı askeri ağlar, enerji hatları ağları, cep telefonları yazılım altyapılı telsizler,*

[1] GIBSON William, **Neuromancer**, Ace Books, New York, 1984, p. 69.

elektronik komuta sistemleri, cep teflonları, uydu sistemleri, insansız hava araçları sistemleri gibi birçok yazılım ve donanım elemanları toplamı" şeklinde yapılabilecektir.[2]

Uluslararası ilişkiler açısından ise siber uzayı ABD ve RF'nin gerek yıllardan beri geliştirdikleri ağ teknolojileri ve bu teknolojileri kullanmak suretiyle askeri kapasitelerini ve espiyonaj imkânlarını maksimize etmek adına yaptıkları planlamaları gerekse ülkelerinin siber güvenliklerini sağlamak adına ortaya koydukları strateji ve doktrinler çerçevesinde domine ettikleri görülmektedir.

Uluslararası sistemde yer alan diğer devletlerin de elbette ki siber güvenlik stratejilerini geliştirmek adına sofistike planlamalar geliştirmeye gayret ettikleri ortadadır. Örneğin; ÇHC ve Kuzey Kore siber savunma alanına önemli yatırımlar yapan ülkelerin başında gelmektedirler. ÇHC günümüz itibarıyla önemli siber saldırı kapasitesine ve gelişmiş istihbarat alt yapısına sahip bir devlet olarak 2050 yılına kadar siber egemenliği hedefleyen ve düşman kuvvetlerinin altyapılarını etkisiz hale getirebilmeyi de içeren bir siber doktrin benimsemiştir.[3] Söz konusu doktrinde ÇHC *"rakiplerine karşı siber saldırı kapasitesini artırarak sadece fizik dünyada yapılan savaşların üstünlük için yeterli olmadığını kabul etmiştir*."[4] ÇHC, özellikle ABD ve RF gibi güçlü rakipleriyle siber alanda başa çıkabilmek için önemli çalışmalar yapmakta ve güçlü virüsler ile kötü amaçlı yazılımlar düzenleyerek düşmanlarının elektronik alt yapılarını çökertmeyi amaçlamaktadır.[5]

Sadece yüksek teknolojiye sahip ülkelerin değil, az gelişmiş ülkelerin de siber saldırı kapasite ortaya koymaya yönelik çalışmaları söz konusudur. Bu kapsamda, Kuzey

---

[2]AKYAZI Uğur, **Uluslararası Siber Güvenlik Stratejisi ve Doktrinler Arasında Alınabilecek Tedbirler**, 6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı, http://www.iscturkey. org/s/2226/i/ 2013-paper105.pdf, (14.04.2017).

[3]GÜRKAYNAK Muharrem ve İREN Adem Ali, "Siber Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt 16, No.2, 2011, s. 268.

[4]Ayrıntılı bilgi için bkz. United States-China Economic and Security Review Commission, **China's Proliferation Practices, And The Development Of Its Cyber and spaceWarfare Capabilities, United States-China Economic and Security Review Commission**, Washington, 2008, http://origin.www.uscc.gov/ites/default/files /transcripts/5.20.08HearingTranscript.pdf (15.02.2016), p. 1-5.

[5]Ayrıntılı bilgi için bkz. GÜRKAYNAK ve İREN, op. cit., ss. 268-269.

Kore Ordusu da *"Unit 121"* adında siber savaşa odaklanan ve olası bir savaşa karşı kapasitesini geliştirmeye çalışan bir birim kurduğu bilinmektedir.[6]

Siber güvenlik alanında etkinlik tesis etmeye çalışan bir diğer devlet ise Hindistan'dır. Hindistan, Pakistan'la yaşanan Keşmir Sorunu ve nükleer silah denemelerinde maruz kaldığı siber saldırılara önlem almak amacıyla sanal dünyada yaşanan rekabete kayıtsız kalamamış ve 1998 yılından itibaren siber savaşı da içine alan yeni güvenlik doktrini doğrultusunda güvenlik stratejisini belirlemiştir.[7] Bu güvenlik stratejisi kapsamında *"Ulusal Savunma Üniversitesi / National Defense University"* ve *"Savunma İstihbarat Birimi / Defense Intelligence Agency"* şeklinde bir kurumsal örgütlenmeye giden Hindistan, siber savaş, psikolojik operasyon, elektro-manyetik ve dalga teknolojilerinde uzman alt birimler kurmuştur.

2010 yılında, nükleer tesisleri, İsrail ve ABD kaynaklı olduğu tahmin edilen Stuxnet[8] isimli gelişmiş bir virüs tarafından fiziksel hasara uğratılan İran'da siber güvenlik kapasitesine sahip olma noktasında analiz edilmesi gereken önemli bir aktördür. İran, silahlı kuvvetleri ve üniversiteleri ile birlikte siber alanda teknoloji ve uzman geliştirebilecek kapasiteye çalışmak amacıyla planlamalar yapmıştır. Ayrıca bu konuda, RF ve Hindistan ile bilgi teknolojileri satın alma, askeri alanda teknik yardım temin etme ve eğitim desteği alma konusunda ciddi işbirliği geliştirmiştir.

Ancak bu devletlere göre bizce ABD ve RF'nin durumu daha farklıdır. Bu farklılık ise söz konusu iki devletin siber güvenlik stratejilerini belirleyen gelişmelerin 21 yy. başından bu yana karşılıklı olarak etkileşim halinde olmasından, adeta bir etki-tepki ilişkisi kapsamında planlanmasından ve bahse konu etkileşimin de uluslararası sistemde yer alan diğer aktörleri etkileyecek şekilde küresel siber uzay alanını şekillendirmesinden kaynaklandığı iddia edilebilir.

Bu çerçevede söz konusu etkileşimin ve etki-tepki ilişkisinin ortaya konması amacıyla tezin ilk bölümünde, siber uzayda meydana gelen gelişmelerin, ulusal düzeyde bir siber güvenlik sistematiğinin ve planlamasının geliştirilmesi noktasındaki öncü rolü

[6]The USA Air Force Law Review, **Cyber War Edtion**, http://www.afjag.af.mil/shared/media/document/AFD-091026-024.pdf, (17.02.2016), s. 133.
[7]GÜRKAYNAK ve İREN, op. cit., s. 269.
[8]BIÇAKCI Salih, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler**, Cilt.10, Sayı 40, Kış 2014, s. 108.

nedeniyle devletin uluslararası sistemdeki temel aktör pozisyonunu pekiştirmekte olduğu, devletlerin siber uzay alanındaki gelişmeleri askeri kapasitelerini geliştirmek adına yeni bir fırsat olarak okudukları, ayrıca da siber uzayın anonim yapısının tehdit kavramını asimetrik hale getirmek suretiyle uluslararası sistemi eskiye kıyasla çok daha anarşik hale dönüştürdüğü şeklindeki savlar analiz edilecektir. Bu kapsamda reel politik düşüncenin kökenleri ve temel yaklaşımları ile birlikte güvenlik kavramına yönelik paradigmaları ana hatlarıyla ele alınacaktır. Akabinde ise siber uzay ve siber güç kavramlarının tanımları ile bu kavramlara ilişkin bazı teorik analizler de irdelenecektir.

Tezin ikinci bölümünde ise ABD'nin 1900'ların başı itibarıyla ortaya koyduğu, özellikle de Soğuk Savaş döneminde Sovyetler Birliği ile girdiği askeri yarış çerçevesinde ciddi bir biçimde gelişimine katkı sağladığı teknolojik imkânların günümüz siber uzay teknolojilerine etkisi kronolojik bir yaklaşım ile analiz edilecektir. Bu bölümde ayrıca ABD'nin 1990'ların ikinci yarısından sonra planladığı siber güvenlik strateji belgeleri ve başkanlık direktifleri ile bu belgelerin belirlediği hedefler kapsamında kurulan siber güvenlik kuruluşları ve çıkartılan ulusal yasalar değerlendirilecektir. Bu değerlendirme esnasında, söz konusu kurumlar ile ulusal yasaların, 11 Eylül 2001 öncesi ve sonrası dönemde değişen tonu ve etkinliği irdelenmek suretiyle, ABD'nin siber güvenlik stratejisin günümüzdeki temel özellikleri irdelenecektir. Bu bölümde son olarak günümüzde de etkileri devam eden güncel gelişmeler analiz edilerek, ABD'nin siber güvenlik stratejisinin zaafları ve eksikleri ortaya konmaya çalışılacaktır.

Çalışmanın üçüncü bölümünde RF'nin siber güvenlik stratejileri kronolojik bir yaklaşımla analiz edilecektir. Bu analiz dâhilinde, Sovyet teknoloji mirası, Sovyet Ordusu'nun ağ teknolojileri alanındaki ilk planlamaları, SSCB'nin çöküşü sonrasında 1990'lı yıllar itibarıyla RF'nin siber güvenlik alanındaki öncü faaliyetleri incelenecektir. Sonrasında ise V. Putin iktidarı ile birlikte, RF'nin siber uzaydaki gelişmeleri askeri kapasitesini arttırmak adına ne şekilde kullanmaya gayret ettiği, bu çerçevede ortaya koyduğu siber güvenlik strateji belge ve doktrinleri detaylandırılmak suretiyle analiz edilecektir. Bu bölümde son olarak, Rus istihbarat ve güvenlik servislerinin siber güvenlik alanındaki faaliyetleri ile RF'nin komşularıyla ilişkilerinde sahip olduğu siber kapasitesini nasıl bir baskı aracı olarak kullanmakta olduğu örnek olaylar dikkate alınarak irdelenecektir. Bu değerlendirme çerçevesinde RF'nin sosyal medya imkânları ve 2010 yılı

sonrası kurduğu uluslararası medya kuruluşları vasıtasıyla elinde bulundurduğu yeni nesil enformasyon savaşı enstrümanlarının da analiz edilmesine gayret edilecektir.

Bu kapsamda önemle açıklamamız gereken husus, ABD ve RF'nin siber güvenlik stratejilerini analiz ettiğimiz başlıkların bazıların birbirleriyle uyumlu değilmiş gibi gözüktüğüdür. Bu uyumsuzluk her iki devletin siyasi, ekonomik, hukuki, teknolojik ve tarihsel gelişimi ile doğrudan bağlantılıdır. Zira Soğuk Savaş döneminde küresel düzeyde rekabet eden bu iki devlet, bugün siber güvenlik alanında tecrübe edilen muazzam teknolojik gelişmelerin de aslında temelini atmışlardır. Bununla birlikte 1990'ların yaşadığı ekonomik ve siyasi kriz ile birlikte SSCB'nin dağılması sonrasında RF'nin bu yıllar için siber güvenlik alanından pozisyon alması gecikmiştir. Öte yandan 2000'li yıllar ile birlikte RF'nin uluslararası sistemde gösterdiği aktif rol, siber uzayda da etkinliğini artırmasına neden olmuştur. Bu gelişmeler ve adımlar ise ABD tarafından bir tehdit olarak algılanmış, adeta bir etki-tepki ilişkisi içinde siber kapasitesini artırmaya yönelik strateji ve planlamalara hız vermesine neden olmuştur. Bu kapsamda süreç içinde her iki devletin siber saldırı ve savunma kapasitesini artırmaya yönelik çabaları, RF ve ABD'nin kendi iç siyasi, hukuki, ekonomik dinamikleri ve teknolojik gelişmişlik düzeyleri çerçevesinde şekillenmiştir.

Tezin dördüncü bölümde ise ABD ve RF'nin siber güvenlik stratejilerine ilişkin olarak çalışma kapsamında ortaya çıkan hususların karşılaştırmalı olarak ayrıntılı bir değerlendirmesi yapılacaktır. Bu bölümde ABD ve RF'nin:

- Siber uzayın günümüzdeki teknolojik gelişmişlik düzeyine ulaşmasına katkı sağlayan ve Soğuk Savaş döneminden bu yana devam eden ağ teknolojileri alanındaki rekabeti;
- Resmi siber güvenlik belge ve doktrinlerinde birbirlerine yönelik atıf ve tehdit değerlendirmeleri;
- Resmi belge ve doktrinlerinin açıklanması sonrasında karşılıklı olarak yapılan yeni hamleler ve işbirliği çabaları;
- Ulusal siber uzay alanlarına yönelik karşılıklı tehdit algılamaları;
- Birbirlerine yönelik siber saldırı ve casusluk faaliyetleri ve bunları engellemeye yönelik çabaları;

- RF’nin komşularına yönelik siber saldırıları ve bu saldırılara yönelik ABD’nin tepkisi;
- Edward Snowden, WikiLeaks Skandalı ve Demokrat Parti’nin e-posta haberleşme sisteminin hacklenmesi olayı kapsamında gerginleşen ABD ve RF ilişkileri analiz edilecektir.

BİRİNCİ BÖLÜM

REEL POLİTİK PARADİGMANIN ULUSLARARASI İLİŞKİLER DİSİPLİNİNDE KURAMSALLAŞTIRILMASI

Realist teori, siyasetin köklerinin insan tabiatında arayan, uluslararası politikayı temel itibarıyla "*güç*", bu terim ile etkileşim içinde olan "*çıkar*" kavramını merkeze alarak açıklayan, evrensel moral ilkelerinin devletlerin eylemlerine uygulanamayacağı görüşünü savunan düşünce biçimidir.[9] Bu kapsamda uluslararası ilişkilerin esas paradigması olarak kabul edebileceğimiz realizm, bu bilimin ana teorilerinin ve yaklaşımlarının da temelini oluşturmuştur.

1. Klasik Realizmin Temelleri

Realizm, uluslararası ilişkiler disiplini açısından kökenleri tarihin ilk dönemlerine kadar uzanan bir yaklaşımdır.[10] Realist teori, 2. Dünya Savaşı sonrasında on yıllar boyunca uluslararası ilişkiler disiplininde hakim kuram olarak kabul edilmiş ve kendisine yönelik eleştiriler yaklaşımlar ile birlikte uluslararası ilişkiler disiplininde yeni görüşlerin oluşmasına zemin yaratmıştır.[11]

Realist yaklaşımın savunduğu görüşlerin temelleri köklü bir düşünce geçmişine sahiptir. Bu kapsamda Thucydides'in Atina ile Sparta arasındaki Peloponezya Savaşları'nı anlattığı Melian Dialogue adlı eserinde güç dengesi kavramına yaptığı vurgu bu yaklaşım ile ilgili ilk tarihi perspektif olarak düşünülebilir. Daha sonra Niccolo Machiavelli, Prens adlı kitabında bir hükümdarın temel amacının gücünü artırmak olduğunu ve bu amaç için dini ya da etik ilkelere karşı kayıtsız olması gerektiğini yazmıştır. Thomas Hobbes, Leviathan adlı eserinde Leviathan'da doğa durumunda, yani insanlar devletleşmeden önce "herkesin herkese karşı savaş" halinde olduğunu söylemiştir. Otto Von Bismarck ise "*güç dengesi*" kavramını siyasi sahnede uygulayan ilk devlet adamı olarak tarihe geçmiştir.

---

[9] Ayrıntılı bilgi için bkz. MORGENTHAU J. Hans, **Politics Among Nations**, McGraw Hill Press, New York, 7th Edition, pp. 3-5, 2006.

[10] KOLASİ Krevis, "Soğuk Savaş'ın Barışçıl Olarak Sona Ermesi ve Uluslararası İlişkiler Teorileri", **Ankara Üniversitesi SBF Dergisi**, Cilt 68, No.2, 2013, s. 149.

[11] RÖVŞEN İbrahimov, **Uluslararası İlişkilerde Realistler ve Realizm Paradigması**, Qafqaz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, http://journal.qu.edu.az/article_pdf/1030_350.pdf, (12.11.2016), s. 1.

Söz konusu tarihi arka plan ile birlikte realizmin bir paradigma olarak uluslararası ilişkiler disiplininde 20.yy.'da ortaya çıktığı ifade edilebilecektir. Uluslararası ilişkiler disiplinin bir bilim dalı olarak ilk defa 1. Dünya Savaşı sonrası ele alınmaya başlandığı düşünüldüğünde, realist paradigmanın 2. Dünya Savaşı'nı engelleyemeyen ütopik yaklaşımlara karşı bir reaksiyon olarak, savaş başlamadan hemen önce gelişmeye başladığı, savaşın sonu ile birlikte de bu disiplinde hakim paradigma haline geldiği açıktır.[12]

Bu kapsamda realizm, devleti uluslararası ilişkilerin temel aktörü olarak kabul ederek, uluslararası ilişkileri ve uluslararası politikayı devletlerarasındaki mücadele süreci olarak ele alır. Realistler için insan; kötü, günahkâr, çıkarcı, saldırgan ve ilişkilerinde gücü ön plana alan olumsuz bir doğaya sahiptir. Klasik realizm, uluslararası politikayı da insan doğasıyla açıklamaktadır. Realizme göre; insan doğuştan kötü, aç gözlü ve hırslıdır. İnsanın yapısına dair bu olumsuz özellikler devletlerin yapısına da yansımıştır. Sürekli kapasitesini arttırma güdüsüyle hareket eden devletler, olanakları ölçüsünde diğer devletleri egemenliği altına almaya çalışırlar. Dolayısıyla böyle bir yapıda savaş ve çatışma olağan hale gelmektedir. Realizme göre devlet adamını yönlendiren unsurlar korku, kuşku, güvensizlik, üne kavuşma, prestij ve çıkar gibi unsurlardır. Bu kapsamda realist teoriye göre, devlet adamları diğer bir devletin/devletlerin güçlenmesine seyirci kalmamalı ve gerekirse bu süreci engellemek için savaşa başvurmalıdır.[13]

Diğer yandan realizmin uluslararası ilişkiler disiplininde etkinlik kazanmasında özellikle Hans J. Morgenthau'nun[14] katkıları oldukça kayda değerdir. Anılan, Morgenthau Politics Among Nations (Uluslar Arasında Politika) eserinde realist bir teori kurma amacını açıkça ifade etmiştir. Bu kitabında, Morgenthau: "*siyaset ve toplumun, kökleri insan doğasında bulunan objektif yasalarla yönetildiğini, uluslararası politikanın hareket noktasının, güç terimi ile tanımlanan çıkar kavramı olduğunu, gücün, uygulandığı zaman ve mekâna bağlı olarak farklılık gösterebildiğini, ancak politikanın özü olan çıkar kavramı zamandan ve mekândan etkilenmediğini, evrensel moral ilkeler, evrensel soyut formüller biçiminde, devletlerin eylemlerine uygulanamaz olduğunu"* ileri sürmüştür. Görüldüğü

[12] Ibid., p. 3.
[13] Ayrıntılı bilgi için bkz. ARI Tayyar, **Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya İşbirliği**, MKM Yayınları, Bursa, 2010, ss. 164-167.
[14] Almanya'nın Coburg şehrinde doğan Morgenthau, Berlin, Frankfurt ve Münih üniversitelerinde tarih, hukuk, ekonomi ve felsefe üzerine klasik Alman eğitimi almıştır. Anılan, II. Dünya Savaşı döneminde Nazi Almanya'sından kaçarak ABD'ye sığınan bir mültecidir.

üzere, realizm belli bir ulusun moral arzularını evreni yöneten moral yasalarla tanımlamaktan kaçınır. Realizmde insan doğası özcü (essentialist) bir anlayışla, yani değişmeyen ve bencil olarak tanımlamıştır.[15] Morgenthau, bu durumu "*animusdominandi (hükmetme arzusu)"* ifadesi ile tarif etmiştir. Ancak çıkış noktası insan doğasının bencilliği olmasına rağmen, realizmi realizm yapan devlete ilişkin varsayımlarıdır. Birincisi, devletler merkezi ve meşru bir hükümetin yokluğu tarafından tanımlanan anarşik bir dünyada temel aktörlerdir. Devletler anahtar analiz düzeyini temsil eder. Diğer devlet dışı aktörlerin varlığı yadsınamazsa da onlar devletlere göre ikincildir. İkincisi, devlet bütüncül (unitary) bir aktör olarak kabul edilmektedir.

Ayrıca Morgenthau, uluslararası ilişkiler alanında realizm çerçevesinde belirlediği altı temel ilkeyle de tanınmıştır. Söz konusu kitabının I. bölümünde yer alan bu ilkeler, birçok realist düşünürü etkilemiştir. Morgenthau'nun ortaya koyduğu klasik realizminin temel ilkeleri ise şu şekildedir:[16]

1. Siyasi realizm, genel olarak siyasetin köklerinin insan tabiatında bulunan objektifliğe yöneltildiğine inanır.

2. Uluslararası politika denen geniş alanda siyasal realizme yolunu bulmakta yardım eden en önemli odak noktası ise güç terimi ile ifade edilen çıkar kavramıdır. Uluslararası politikayı kavrayıp anlamaya çalışan akıl ile anlaşılması gereken gerçekler arasındaki bağlantıyı bu kavram sağlamaktadır.

3. Realizmin en temel kavramı olan güç şeklinde tanımlanan çıkar kavramı hiç değişmeyen ve sabit bir anlam içinde ortaya konulamaz. Çıkar fikri gerçekten de politikanın özüdür ve zaman ve yere bağlı değildir, onlardan etkilenmez.

4. Siyasal realizm siyasal eylemin moral öneminin farkındadır. Fakat çoğu zaman başarılı bir politikanın gerekleriyle ahlakın emirleri arasında giderilmesi güç bir gerilim olduğu görülmektedir. Realizm, evrensel moral ilkelerinin, evrensel soyut formüller biçimi içinde, devletlerin eylemlerine uygulanamayacağı görüşündedir ve bu ilkelerin zaman ve yer konusundaki somut şartlara göre ayıklanması gerektiğine inanır.

5. Siyasal realizm, belli bir ulusun ahlaki hareket edip etmediğini belirleyip

[15] Ayrıntılı bilgi için bkz. DONNELY Jack, **Realismand International Relations**, Cambridge University Press, Cambridge, pp. 7-16, 2000.
[16] Ayrıntılı bilgi için bkz. MORGENTHAU, op. cit., p. 5-16.

anlamakta dünya çapındaki moral yasaların ölçüt olarak alınması görüşünü kabul etmez. Gerçek ile kanaat arasında bir ayırım ve benzemezlik olduğuna inandığı gibi gerçek ile gerçek yerine konan şeylere tapınma arasında da ayrım olduğuna inanır.

6. Siyasal realizm ile diğer düşünce ekolleri arasında gerçek ve önemli bir fark vardır. Bununla beraber siyasal realizm, siyasal alanın kendi başına ve bağımsız bir alan olduğuna inanılır.

Bununla birlikte, Morgenthau'ya göre uluslararası alanda geçerli olan tek gerçek, güç unsurudur. Güçlü olan üstün duruma geçer ve sözünü geçirir. Bundan dolayı uluslararası arenada sürekli olarak bir güç mücadelesi hüküm sürer. Devletler durmadan kuvvet kazanmaya ve karşılarındakini güçsüz bırakmaya çabalarlar. Bu çabaların sonucu, ortaya uluslararası barışı koruyacak tek düzen olan *"güç dengesi"* çıkar. Uluslararası arenada geçerli tek gerçek güç yine de karşı bir güç tarafından dengelendiği zaman barış ve düzen hüküm sürer. Barışı başka türlü kurma ve koruma boşunadır. Morgenthau, bu konuda idealistler tarafından ileri sürülen *"ortaklaşa güvenlik"* ve *"dünya devleti"* gibi çözüm yollarının geçersiz olduğunu birçok örnekler ve savlar ileri sürerek ispata çalışır. Morgenthau, uluslararası hukuk, uluslararası ahlak gibi öğeleri, *"ulusal güç ve ulusal çıkar"* kavramları karşısında ancak ikinci derecede unsurlar olarak görür. Morgenthau'ya göre güç, politikada temel motiftir ve ekonomide kazanca yönelik davranış nasıl temel teşkil ediyorsa, politikada da güç aynı şekilde temel oluşturmaktadır. Dolayısıyla güç kayramı çözümlemelerde operatif anlamda nesnelliğe katkıda bulunmakta ve bu anlamda temel kavramlardan biri olarak disiplin terminolojisine yerleşmektedir.[17]

2. Klasik Realizm ve Güvenlik

Güvenlik: *"dışarıdan gelebilecek saldırılara karşı kendini koruyabilme yeteneğidir."*[18] Devletler açısından ise güvenlik: "*barış zamanında kendi değerlerini tehditlere karşı koruyabilme, savaş zamanı ise zafer kazanma gücüdür*."[19] Başka bir tanıma

[17] Ayrıntılı bilgi için bkz. Ibid., pp. 179-200.
[18] LUCİNA Giacomo, "TheEconomic Content Of Security", **Journal of Public Policy**, Vol.8, 1989, p. 151.
[19] BELLAMY Ian, "Towards a Theory of International Security", **Political Studies**, Vol.29, No.1, 1981, p. 102.

göre ise güvenlik; "*düşmanını karşılıklı paylaşım ve yanlış yönlendirmeler ile dost yapabilme yetkinliğidir."*[20]

Öte yandan söz konusu açık tanımlara karşın güvenlik kavramı ile ilgili olarak, herkes tarafından kabul gören, her dönem geçerli olan ve tanımlama yapılırken birçok etkeni dikkate alabilen bir yaklaşımın ortaya konulamayacağı da iddia edilebilir. Bununla birlikte güvenliğe ilişkin *"tehlikelerden ve korkulardan uzak kalma, bir tehdidin olmaması"* gibi ifadelerin birçok tanımda kullanılmış olması ortak bir anlayışın olduğunu da göstermektedir.[21] Bu itibarla güvenliğin, insanoğlu için temel değer olduğu ve kaybedildiğinde sahip olunan her şey kaybedilebileceği için insanların güvenliklerini tehdit edecek şeyleri ortadan kaldırmak için ellerinden gelenin en iyisinin yapmaya çalışacakları rahatlıkla ifade edilebilecektir.[22] Bu noktadan da hareketle, günümüz dünyasında ortaya çıkan gelişmeler dikkate alındığında ise güvenliği, bu çeşit bir ayrıma tabi tutarak birbirinden bağımsız alanlar gibi incelemenin çok doğru olmayacağı açıktır.

Klasik realist teori analizlerinde ise güvenlik kavramı en temel belirleyicidir. Realizm için temel aktör olan devletin gücü, güvenliği sağlama kapasitesi ile birlikte değerlendirilir.[23] Realist teori güvenlik analizlerine verdiği büyük önem ve uluslararası politikaya dair öne sürdüğü savlar ve kavramsallaştırmalar ile birlikte, güvenlik literatürüne ciddi katkıda bulunmuştur.[24]

Klasik realizm güvenliği, devletlerin askeri gücü ve ulusal çıkarları ile ifade etmektedir. Devletin temel amacı ise bekasının ve güvenliğinin sağlanması, çıkarının yerine getirilmesi şeklinde tanımlanmaktadır. Realizmin güvenlik anlayışı devletlerin sahip oldukları güç unsurları (askeri kapasite) ve bu unsurların uluslararası ilişkileri *"güç mücadelesi"* üzerinden şekillendirmesine dayanmaktadır.[25] Klasik realist paradigmada,

---

[20] Ayrıntılı bilgi için bkz. KOLODZIEJ Edward, **Security and International Relations**, Cambridge University Press, New York, pp. 15-30., 2005.

[21] Ayrıntılı bilgi için bkz. ÖZCAN A. Behiç, "Uluslararası Güvenlik Sorunları ve ABD'nin Güvenlik Stratejileri", **Selçuk Üniversitesi İİBF Sosyal ve Ekonomik Araştırmalar Dergisi**, No.22, 2011, ss. 447-448.

[22] MORGAN M. Patrick, **International Security Problemsand Solutions**, CQ Pres., Washington DC, p. 1, 2006.

[23]ÇETİNKAYA Şerif, "Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları", **21. Yüzyılda Sosyal Bilimler**,Sayı 2, Aralık/Ocak, Şubat 2011/2012, http://www.21yuzyildasosyalbilimler .com/assets/uploads/files/seref-cetinkaya-pdf_18032013.pdf, (15.01.2016), s. 247.

[24]SANDIKLI Atilla ve EMEKLİER Bilgehan, **Güvenlik Yaklaşımlarında Değişim ve Dönüşüm,** http://www.bilgesam.org/Images/Dokumanlar/0-81-2014040746sandikli_emeklier.pdf, (15.01.2016), ss. 3-4.

[25] KALKAN KÜÇÜKSOLAK Övgü, "Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Okulu Çerçevesinde Tartışılması", **Turan Stratejik Araştırmalar Dergisi**, Cilt 4, Sayı 14, İlkbahar 2012, s 204.

askeri-stratejik konular uluslararası politikada hâkimdir. Burada güvenlik konuları *"yüksek/birincil politika (highpolitics)"* olarak tanımlanırken, ekonomi ve sosyal konular *"alçak/ikincil politika (lowpolitics)"* olarak değerlendirilmektedir. Böylece savaş/güvenlik ile ilgili konulara ekonomi ve sosyal konulara göre öncelik verilir. Tüm bu varsayımlar realizmi devlet-merkezli (statist) bir teori yapmaktadır. Ancak realizmin belki de en önemli diyebileceğimiz iddiası güvenlik varsayımlarının evrensel olmasıdır. Realizmin diğer önemli bir varsayımı ise devletlerin tek tek güvenliğini sağlayacak bir merkezi otoritenin olmadığı uluslararası yapının anarşik yapısıdır. Realistlere göre, uluslararası yapıdaki istikrarsızlıklar devletlerin düvenliği için tehdit oluşturmakta olup, devletler olası tehditlere karşı destek sağlamak için ittifak anlaşmaları imzalayabilirler.[26] Ancak devletler güvenlikleri için bunlara çok fazla güvenmezler ve kendi güvenliklerini sağlayabilecek bir güce erişmeye çalışırlar. Realistler maksimum güce ulaşmak arzusuyla hareket eden tüm devletlerin birbirlerinin bu tür amaçlarına engel olmaya çalıştıklarını; bunun sonucunda ortaya çıkan güç dengesinin ise istikrarı sağlayan önemli bir unsur olduğunu iddia etmektedirler.[27]

Tüm realistler için uluslararası kurumlaşmanın güvenlik alanındaki işbirliğinin gelişmesine etkisi oldukça marjinal düzeydedir.[28] Realistler için uluslararası anarşik yapıda istikrarı ve güvenliği sağlayan, devletleri işbirliğine ve kurumsallaştırmaya yönelten en önemli faktör birbirlerini dengelemeye dönük davranışlardır. Güvenlik değerlendirmelerinde ise tüm realistler iç politika ile uluslararası politikayı birbirinden ayırarak ele almaktadırlar.[29]

Düzen kurucu merkezi bir otoritenin bulunmadığı anarşik uluslararası yapıda devletlerin çıkar odaklı davranışlarını sınırlandıran, sistem içerisindeki diğer devletlerin güç kapasiteleridir. Güç kapasitesinin azlığı veya çokluğu ise devletin güvenliği ile doğrudan orantılıdır. Dolayısıyla güç faktörleri devletlerin güvenliğini sağlayacak temel unsur olarak öne çıkmaktadır. Devlet bekasının güç faktörlerine bağımlı olduğu söz konusu sistemde güvenlik, askeri gücün maksimize edilmesi aracılığıyla sağlanmaktadır. Görüldüğü gibi realizm güvenliği doğal olarak güç ile ifade etmektedir. Diğer devletlere

[26] Ayrıntılı bilgi için bkz. ARI, op. cit., ss. 167-168.
[27] Ayrıntılı bilgi için bkz. KEGLEY Charles, **Neoliberal Challange to Realist Theories of World Politics: An Introduction**, St. Martin's Press, New York, pp. 1-24, 1995.
[28] ARI, op. cit. s.169.
[29] Ayrıntılı bilgi için bkz. STONE Alec, "What is a SupronationalConstitution? An Essay in IR Theories", **The Review of Politics**, Vol.56, No.3, 1994 Summer, pp. 441-473.

göre daha baskın yeterli bir güce sahip olan devlet daha güvenli olacaktır. Bu düşünceye göre askeri kaynaklar güvenliğin sağlanmasında esas çözüm yoludur.[30]

Realizmde devletin güvenliğinin tesis edilmesi, bireyin ve toplum güvenliğini sağlamanın temel yoludur. Devlet güvende oldukça, birey ve toplumda güvende olacaktır. Bu noktada, realizmin uluslararası sistemdeki güvensizlik ve belirsizlik durumuna vurgu yaparak, devletin güvenliğinin sağlanmasını analizlerde birincil öncelik verdiği ifade edilebilecektir. Realizmde devlet, uluslararası ilişkilerin tek ve hâkim aktörüdür.

Daha öncede ifade edildiği üzere, realist kurama göre anarşi ve güvensizliğin süreklilik kazandığı bir uluslararası ortamda güvende olmanın tek yolu, güç ve kapasite artırımına gitmektir. Realist teorisyenler, ulusal gücü artırma imkân ve kabiliyetine sahip tek aktör olarak ulus-devletleri görmekte; *"ulusal güvenlik"* söylemi üzerinden de sadece ulus-devletlerin güvenliğini dikkate almaktadır.[31] Realist paradigma için devletin güvenliğini ulusun ve dolaylı yoldan bireyin güvenliği ile eş tutulmalıdır.

Ulusal güvenliğin sağlanmasının temel yolu ise askeri gücün tesis edilmesi ve sürekli olarak askeri kapasitenin artırılmasıdır.[32] Realizmde devletin güvenliğinin tesis edilmesi, bireyin ve toplum güvenliğini sağlamanın temel yoludur. Devlet güvende oldukça, birey ve toplumda güvende olacaktır. Bu noktada, realizmin uluslararası sistemdeki güvensizlik ve belirsizlik durumuna vurgu yaparak, devletin güvenliğinin sağlanmasını analizlerde birincil öncelik verdiği ifade edilebilecektir.

3. Neo-Realizmin Temelleri

Neo-realizm, ilk defa Kenneth Waltz'un[33] Theory of International Politics (Uluslararası Politika Teorisi) adlı eseriyle gündeme gelmiştir. Neo-realizmin ortaya çıkışı, dünyada iç ve dış siyasi gelişmeleri birbirlerinden ayıran realizm yoğun eleştirilere maruz kaldığı ve en önemlisi de Vietnam Savaşı'nın gidişatı askeri gücün her zaman sonucu belirleyen olmadığını göstererek realizmin varsayımlarına olan inancı sarsıldığı 1970'li yıllara tekabül etmektedir.

---

[30]BUZAN Barry**, People, States and Fear, Great Britain, London**, Aktaran: Akın Alkan, 21. Yüzyılın İlk Çeyreğinde Karadeniz Güvenliği, Nobel Yayın Dağıtım, Ankara, s. 4, 2006.
[31]Ayrıntılı bilgi için. SANDIKLI ve EMEKLİER, op. cit., ss. 1-3.
[32]AYDIN Mustafa, "Uluslararası İlişkilerin 'Gerçekçi' Teorisi: Kökeni, Kapsamı, Kritiği", **Uluslararası İlişkiler**, Cilt 1, No.1, Bahar 2004, s. 39.
[33]Amerikalı siyasetçi, Kaliforniya Üniversitesi'nde ve Kolombiya Üniversitesi'nde okumuş ve Kore Savaşı'nda veteriner olmuştur. Anılan, neo-realizmin kurucusu olarak kabul edilmektedir.

Bu kapsamda realizmin gerek marksist gerekse liberal yazarlar tarafında çok ciddi anlamda eleştirildiği böyle bir zaman diliminde Waltz, realizmi inkâr edip yok saymayarak tam tersine realizmin zengin düşünce geleneğinden bilimsel bir teori kurma amacıyla realist geleneği tekrar canlandırmıştır. Tüm disiplini etkileyecek güçte bir girişimde bulunan Waltz, uluslararası politika teorisini o dönemin etkili düşünce akımlarında olan pozitivizm üzerine bina etmiştir.[34]

Waltz'ın devletlerin davranışlarının belirlenmesinde yapıya yaptığı vurgu nedeniyle "*yapısal realizm"* olarak da adlandırılan neo-realizm, hiyerarşik bir düzenin varlığının kabul edildiği devletlerarası bir yapıyı ön kabul olarak benimseyerek yapısal anlamda anarşik bir uluslararası sistemin var olduğunu öne süren bir uluslararası ilişkiler ekolüdür.

Bu çerçevede, Waltz'a göre: uluslararası yapı nedeniyle devletler benzer koşullarda kendi özel farklılıklarına rağmen aynı politikalar izlemektedirler. Aslında Waltz'a göre indirgemeci olan yalnız dış politikayı insan doğasına ve devletin kapasitesine dayandıran klasik realistler değil, aynı zamanda klasik liberaller ve marksistler de benzer şekilde indirgemecidirler. Waltz bu nedenle yapının dış politika üzerindeki sınırlandırıcı ve koşullandırıcı etkisine dikkat çekmektedir.

Konuyu daha derinlemesine ele almak istersek neo-realist yaklaşımda, iç siyasal sistemin temel kuralı hiyerarşi olmasına karşılık uluslararası sistemin ana ilkesi anarşidir denilebilir. Hiyerarşik bir yapıya sahip olan ulusal sistemde emir ve itaat ilişkisi hakimdir. Oysa uluslararası anarşik yapıda ast-üst ilişkisi ya da itaat eden-edilen ilişkisi söz konusu değildir. Bu noktada, Waltz'a göre güç dengesi süreklilik göstermektedir. Waltz'a göre ister iki kutuplu olsun isterse çok kutuplu olsun her ikisinde de güç dengesi sistemin ana özelliğidir. Çok kutuplu sistemlerde söz konusu olan karşılıklı bağımlılığın artması da istikrarı azaltan bir diğer unsur olarak değerlendirilmektedir. Waltz'a göre bu anarşik uluslararası sistemde her bir devletin öncelikli amacı egemenliği ve güvenliğini korumaktır.[35] Waltz uluslararası sistemi *"bir siyasi yapı ve etkileşim içinde bulunan öğelerden (uluslararası sistemde devletler) oluşan bir bütün"* olarak tanımlamıştır.[36] Waltz'ın bu bütüncül tanımı aslında realizme ters bir tanım olmayıp tam tersine realizmin

[34]KOLASİ, op. cit., s. 159.
[35]WALTZ Kenneth ve QUESTER H. George, **Uluslararası İlişkiler Kuramı ve Dünya Siyasal Sistemi**, Çev. Ersin Onulduran, SBF Yayınları, Ankara, ss. 19-32, 1982.
[36]WALTZ Kenneth, **Political Structures, Robert O. Keohane (Edt.), Neorealism and its Critics**, New York, Colombia University Press, p. 70, 1986.

üzerine bina edilen daha kapsayıcı bir tanımdır. Neo-realizme göre sistemin anarşik yapısı devletleri, var olmak için aynı mücadeleyi vermek zorunda bırakacaktır. Burada söz konusu olan *"aynılık"* devletlerin davranışlarında ya da sistemin yapısının empoze ettiği görevleri yerine getirme hususunda ortaya çıkacaktır. Fakat var olma mücadelesi içinde aynı fonksiyonları görmek, bu fonksiyonları eşit yetkinlikte yerine getirebilmek anlamına gelmez. Dolayısıyla, devletlerarasında farklılık da söz konusu olacaktır. Bu *"farklılık"* esas itibarıyla söz konusu sistemik fonksiyonları yerine getirme yetkinliğinde saklı olacaktır. Bu yetkinlik, devletlerin kapasitesine bağlı olduğundan her bir devlet, gücüyle orantılı olarak bu fonksiyonları yerine getirecektir.[37] Sonuçta güç, sistemin var olmak yolunda devletlere empoze ettiği fonksiyonları yerine getirme yetkinliği sağlayan bir araçtır.

Özetle neo-realizme göre, klasik realizmden farklı olarak, güç edinme isteği, insanın doğasından değil, uluslararası sistemin yapısından kaynaklanmaktadır. Bu noktada, *"neo-realizmi klasik realizmden ayıran en önemli unsurlardan bir diğerinin de gücün ulaşılacak bir amaç olmayıp gerektiğinde başvurulacak bir araç olduğu"* belirtilebilecektir. Neo-realizme göre devletlerin kapasiteleri bakımından bir sınıflandırılması söz konusudur ve bu sınıflandırma da büyük, orta ve küçük şeklinde kurgusal bir bakışla yapılmaktadır. Waltz'ın öne sürdüğü teorisinde göze çarpan tek eşitsizlik, devletlerin güç dağılımındaki eşitsizliktir. Bunun sebebi ise devletlerin uluslararası sistemde güç dağılımına göre konumlandırılmalarıdır. Devletlerin gücü derken kastedilen güç devletlerin sahip oldukları askeri ve ekonomik güçtür. Bu iki güç arasında da ekonomik güç çok daha önemlidir. Çünkü ekonomik gücün her zaman askeri güce dönüşebilme özelliği vardır.[38]

Devletin toplumsal ilişkilerden bağımsız bir aktör olduğu fikri, realist düşüncenin en önemli unsurlarından biridir ve iç politika/toplum ile uluslararası politika/dış toplum ayrımına dayanmaktadır. Klasik realistlerde ve neo-realistlerde bu görüşü desteklerler. Ancak klasik realistler için uluslararası güç mücadelesinin nedeni insan doğasında yatarken, Waltz ampirik olarak doğrulanamayacağı için bu görüşten kaçınmış ve güç mücadelesini uluslararası yapının özelliğine bağlamıştır. Bu farklılık da neo-realizmin belkemiğini oluşturmuştur. Waltz'a göre uluslararası sistem adem-i merkeziyetçi bir

[37]BOZDAĞLIOĞLU Yücel ve ÖZEN Çınar, "Liberalizmden Neoliberalizme Güç Olgusu ve Sistemik Bağımlılık", **Uluslararası İlişkiler**, Cilt 1, No.4, Kış 2004, s. 5.
[38]WALTZ Kenneth, **Theory of International Politics,** Chicago,Addison-Wesley Pub., p. 126., 1979.

yapıya sahiptir ve anarşiktir. Bu anarşik sistemde devletlerin amacı yaşamlarını sürdürebilmektir. Sistemin anarşik yapısı üzerindeki bu vurgu, devletlerin birbirlerini bir endişe ve korku kaynağı olarak gördüğü varsayımına dayanmaktadır. Devletler anarşik sistemde diğerlerine güvenemeyeceklerinden, ayakta kalabilmek için kendi yarattıkları *"araçlara"* veya *"düzenlemelere"* dayanmak zorundadır.[39]

Diğer yandan Waltz için iç politikayı, dış politikadan ayıran en önemli husus savaşın ve çatışmanın sürekli olması değil iç ve dış politikanın sahip oldukları farklı yapılardır. Birimlerin emir itaat ilişkisine tabii olduğu iç politikada yapının düzenleyici ilkesi hiyerarşiyken, merkezi bir gücün olmadığı uluslararası politikada yapının özelliği adem-i merkeziyetçi ve anarşiktir. [40]

Uluslararası politika, neo-realistler için belirli türden bir politikadır. İç politikadan farklı olarak, uluslararası politika merkezi bir devletin/hükümetin olmadığı bir ortamda cereyan etmektedir. Böylece anarşi kavramı, iç politikadaki kaos veya kargaşadan farklı olarak, merkezi bir devletin yokluğuna, veya hiyerarşik bir yönetimin yokluğuna işaret etmektedir. Aslında uluslararası politikada anarşi belirli türden bir düzene işaret etmektedir.[41] Hatta Waltz güç dengesine ve savaşa işaret ederek anarşinin erdemlerinden de bahsedebileceğini vurgulamıştır.[42] Bunun ne anlama geldiğine ise neo-realizm ve savaş hakkındaki varsayımları açıklanırken değinilecektir.

Waltz'a için kapasiteler dağılımı esastır. Çünkü güç devletin sahip olduğu bir özellikken, devletlerin güç dağılımı ise sistemin bir özelliğidir.[43] Diğer bir deyişle, uluslararası alanda değişim büyük güçlerin yükseliş ve çöküşüne bağlı olarak ve bu süreci takip eden güç dengesindeki değişimler sonucu meydana gelir.[44] Bu çapta bir değişimin tipik aracı ise büyük-güçler savaşıdır.[45] Yapıdaki değişim ise devletlerden beklenen davranışlarla ilgili beklentilerin değişmesine neden olmaktadır[46]

---

[39]Ayrıntılı bilgi için bkz. WALTZ Kenneth, **Anarchic Orders and Balances of Power,** Robert O. Keohane (der.), NeorealismanditsCritics,http://www.olivialau.org/ir/archive/wal8.pdf, (18.06.2016), pp. 1-2.
[40]Ayrıntılı bilgi için bkz. KOLASİ, op. cit., ss. 162-163.
[41]Ibid., p. 164.
[42]Ayrıntılı bilgi için bkz. WALTZ, "Theory of International …", op. cit., pp. 111-113.
[43]Ibid., p. 96.
[44]KOLASİ, op. cit., s. 164.
[45]JACKSON Robert ve SORENSEN Georg, "International Relations: TheoriesandApproaches", **Oxford UniversityPress**, p. 77, 2007.
[46]WALTZ, "Theory of International…**",** op. cit. p. 97

Waltz'a göre savaşlar: *"insan doğası, devletlerin yapısı ve uluslararası sistemin anarşik yapısından"* kaynaklanmaktadır. Ancak Waltz'a göre savaşların temel nedeni uluslararası anarşidir. Waltz'a göre savaş, savaşı engelleyecek herhangi birşey olmadığı için var olur. İşte bu temel varsayımdan devletlerin davranışları için önemli sonuçlar doğmaktadır.[47]

4. Neo-Realizm ve Güvenlik

Görüldüğü üzere klasik realist teori, güvenliği ulusal güvenlik kavramı üzerinden ve askeri güç ekseninde tanımlayarak, 2. Dünya Savaşı sonrası dönemde uluslararası ilişkiler disiplinin de hakim yaklaşım haline gelmiştir. Bu çerçevede klasik realist güvenlik paradigmasının temel ilgi alanı, devletlerin bekalarına yönelik tehditlerle mücadele etmek amacıyla geliştirmeleri gereken askeri imkân, kabiliyet, kapasite ve stratejiler şeklinde belirlenmiştir. Realist güvenlik perspektifinde tasarlanan ve Soğuk Savaş konjonktürüne egemen olan tehdit odaklı klasik güvenlik paradigması, *"iki süper güç arasındaki çekişmenin doğrudan silahlı çatışmaya dönüşmemesi durumu"* şeklinde özetlenebilecek daha sınırlı bir çerçevede inşa edilmiştir.

Neo-realist yaklaşıma göre ise uluslararası sistemin yapısı uluslararası aktörlerin davranış ve güvenliklerini belirlemektedir. Bu yönüyle neo-realizm, klasik realizmden farklı olarak güvenliğin kavramsal boyutunu genişletmiş ve güvenlik kavramı içine ulus-devlet yapılarının ile birlikte uluslararası sistemin güvenliği olgularını da dâhil etmiştir. Kısacası, realist çalışmalar ile ortaya çıkan klasik güvenlik yaklaşımları, neo-realist analizlerle olgunlaşıp şekillenmiştir.

Güvenlik analizlerinin reel politik paradigma anlayışı dahilindeki söz konusu olgunlaşma sürecinde, neo-realist kuramın güvenlik ikilemi *(security dilemma)* yaklaşımının da etkisi önemli olmuştur. Temel tanımıyla ise güvenlik ikilemi kavramı, bir devletin başka bir devletten tehdit algılayıp silahlanması durumunda buna tehdit algılanan devletin de aynı şekilde cevap vermesini ifade etmektedir. Güvenlik ikilemi modeline göre, bir devletin güvenliğini sağlamaya yönelik davranışları, mevcut ya da potansiyel düşmanlarının güvenliğini tehdit etmekte ve bu aktörleri tehlikeye sokmaktadır.[48] Buna göre A devletinden tehdit algılayan B devleti, A devletine karşı silahlanır veya ittifaklara

[47]WALTZ Kenneth, "**Man, the State and War**", Columbia University Press, New York, p. 232, 2001.
[48]ARI, op. cit., s. 198.

katılır; fakat B devletinin silahlanması bu kez A devletinin güvenlik kaygılarını ön plana çıkarır ve bu durum A devletinin de silahlanmasına yol açar. Bu durumda her iki devlet de birbirine karşı silahlanmış olur.[49] Soğuk Savaş döneminde aynı blokta yer almalarına karşın birbirini tehdit olarak algılayan Türkiye ve Yunanistan arasındaki silahlanma yarışı, güvenlik ikilemi modeline örnek teşkil etmektedir.[50]

Güvenlik ikileminde devletler uluslararası ilişkileri "sıfır toplamlı bir oyun" olarak değerlendirmektedirler. Devletler, uluslararası sistemdeki davranış kalıplarını "*nisbi kazanç*" varsayımına dayandırarak planlamakta ve nisbi kazanç varsayımına göre devletler, birbirleriyle ilişkilerinde "*ikimiz de karlı çıkacak mıyız?*" sorusu yerine "*kim daha karlı çıkacak?*" sorusunu yönelterek işbirliğinden kaçınmaktadırlar.[51]

Neo-realizm, anarşi olgusu ekseninde rekabetçi ve çatışmacı bir güvenlik bakış açısına sahiptir. Bu bakış açısının katılığına rağmen, neo-realist yaklaşımda işbirliği yapmanın sınırlılığı ve zorluğu ön plana çıkarmaktadır. Çünkü neo-realist paradigma için uluslararası sistemin yapısı anarşiktir ve bu güvensizlik ortamı, devletlerin uzun süreli işbirliği yapmasını engellemektedir.[52]

Waltz için devletlerin birincil amacı varlıklarını korumak yani savunmalarını sağlamaktır. Neo-realistler yaklaşıma göre her devlet, statükocu bir yaklaşımla sistemdeki konumunu sürdürebilir ve bu sürecin sonunda uluslararası sistemde ortaya çıkan güç dengesiyle de güvenliğini sağlayabilir. Güç dengesi yaklaşımı neo-realist güvenlik anlayışında esastır. Bu mekanizma uluslararası sistemin düzenleyici mekanizması şeklinde işlev görerek istikrarı sağlamakta ve uluslararası sistemin güvenliği ile birlikte devletlerin güvenliğini de tesis etmektedir.[53] Başka bir deyişle neo-realizme göre uluslararası aktörlerin davranış ve güvenliklerini belirleyen yapı uluslararası sistemdir.[54] Bu yönüyle neo-realizm, klasik realizmden farklı olarak ulus-devlet yapılarının güvenliği ile birlikte uluslararası sistemin güvenliğini de göz önünde bulundurarak güvenlik bakış açısını genişletmiştir. Kısaca, klasik realizmden farklı olarak neo-realizmin uluslararası sistemi incelemeye alarak güvenlik çalışmalarındaki analiz seviyesinin makro boyuta taşımıştır.

[49]Ayrıntılı bilgi için bkz. BİLGİÇ Ali, "Güvenlik İkilemi"ni Yeniden Düşünmek Güvenlik Çalışmalarında Yeni Bir Perspektif", **Uluslararası İlişkiler**, Cilt 8, No. 29, Bahar 2011, ss. 123-124.
[50]SANDIKLI ve EMEKLİER, op. cit., s. 8.
[51]WALTZ ve QUESTER, "Uluslararası İlişkiler Kuramı …", op. cit, s. 46.
[52]Ibid.
[53]WALTZ, "Theory of International …", op. cit, p. 47.
[54]Ayrıntılı bilgi için bkz. Ibid., p. 38-59

Bu noktada neo-realizm anarşi olgusu ekseninde rekabetçi ve çatışmacı bir güvenlik perspektifi öngörmekte ve devletarası işbirliğinin zorluğuna dikkat çekmektedir. Waltz bu kapsamda işbirliği devletlerin birbirlerini aldatma ihtimali ve göreli kazançlarına yönelik ilgisi ile şekillenmekte olduğunu değerlendirmekte ve uluslararası sistemin anarşik yapısı ve güvensizlik ortamı, devletlerin uzun süreli işbirliği yapmasını engellediğini ileri sürmektedir.[55]

Neo-realizmin güvenlik yaklaşımını realizmden farklılaştıran ve klasik güvenlik terminolojisini geliştiren bir diğer nokta, neo-realist anlayışın analizlerine ekonomik değişkenleri de eklemeleridir. Waltz, askeri-stratejik konuların yanı sıra ekonominin de artık uluslararası ilişkiler gündeminde belirleyici bir rol oynadığını belirtmiş ve bir bakıma ekonomik güvenlik üzerinde durmuştur. Waltz bu savına örnek olarak ise özellikle Vietnam Savaşı hedefe ulaşmada tek aracın askeri güç ve kapasite olmadığını gösterdiğini, ayrıca 1973-1979 petrol şoklarının uluslararası ekonomik faktörlerin de güvenliğin tesisinde dikkate alınması gerektiğini vurgulamıştır.[56] Pratiğin teori üzerindeki bu etkisi, neo-realistleri ekonomiye yönlendirmiş olsa da nihayetinde askeri-stratejik konulara odaklanan neo-realizmin ağırlık merkezini yine de *"high politics"* teşkil etmiştir.[57]

Görüldüğü üzere, 2. Dünya Savaşı sonrasında ABD ve SSCB'nin liderliklerindeki Batı ve Doğu Blokları arasında gerginlik ve kısmi çatışma biçiminde sürdürülen mücadele sırasında güvenlik esas olarak reelpolitik yaklaşımın düşünce çizgisinde tanımlanmıştır.[58] Kısacası, Soğuk Savaş döneminde tehdit algısı nettir. Tehditler nasıl planlanabileceği, nereden, hangi şekilde ve ne tür bir tehdit ile karşılaşılabileceği bilinmektedir. Soğuk Savaş döneminde, tehditlerin kaynağı devletlerdir. Yani devletler, uluslararası sistemin başat aktörleridir. Devletten, daha üstün bir siyasi otorite ve karar alma organı bulunmamaktadır.[59] Dolayısıyla devlet dışı aktörleri ilgilendiren tüm konular tali öneme sahiptirler. Güvenlik esas ve birincil öneme sahiptir. Özgürlük ile güvenlik arasında yapılacak sıralamada güvenlik önce gelmektedir.[60]

---

[55]BAYLIS John, "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler**, Cilt 5, Sayı 18, Yaz 2008, s. 74.
[56]Ayrıntılı bilgi için bkz. WALTZ, ""Theory of International …", op. cit, pp. 146-160.
[57]KAÇAR Gamze, **Güvenlik İkilemi**, http://www.tuicakademi.org/guvenlik-ikilemi/, (18.01.2016).
[58]ERDOĞAN İbrahim, "Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı", **Akademik Bakış**, Cilt 6 Sayı 12, Yaz 2013, s. 267.
[59]SNYDER Jack, "One World, RivalTheories", **ForeignPolicy**, No.145, November-December 2004, s. 59.
[60]Ayrıntılı bilgi için bkz. SANCAK Kadir, **Güvenlik Kavramı Etrafındaki Tartışmalar ve Güvenlik Kavramının Dönüşümü**, http://www.ktu.edu.tr/dosyalar/sbedergisi_69519.pdf, (15.01.2016), ss. 129-130.

Soğuk Savaş Dönemi'nin sona ermesiyle sistemde hâkim olan iki kutuplu yapı sona ermiş, ABD dünyada tek süper güç olarak kabul edilmiştir. Bu kapsamda dönemin ilk yıllarında ABD'nin "*öteki"* ya da *"düşman"* yaratma gayretleri söz konusu olmuştur. Bu gayretler doğrultu da ise*"medeniyetler çatışması, radikal İslam tehdidi ve haydut devletler (roguestates)*" gibi kavramlar uluslararası ilişkiler disiplininin analizlerinde sıklıkla tartışılmaya başlanmıştır.[61] Diğer yandan, bu kavramların 11 Eylül 2001'de ABD'de meydana gelen terör saldırıları ile birlikte meşrulaşması/meşrululaştırılması sonucunda güvenlik anlayışlarında da yeni yaklaşımlar söz konusu olmuştur.

Yeni güvenlik algılamalarında, devlet kaynaklı simetrik tehdit algısı önemini yitirmiş ve asimetrik tehdit kavramı ön plana çıkmıştır. Asimetrik tehdit kavramı: *"devlet dışı yapılar tarafından gerçekleştirilen ve saldırganın, muhatabı karşısındaki zayıflığına karşılık göreceli biçimde üstünlüklere sahip olması"* şeklinde tanımlanmıştır.[62] Asimetrik tehdit kavramının en önemli kaynaklığını ise *"terör saldırıları"* teşkil etmiştir. Bu dönemde terör saldırıları da klasik yapısından sıyrılarak, yeni bir boyut kazanmış ve etkileri bakımından 11 Eylül saldırıları örneğinde olduğu gibi küresel bir boyuta ulaşmıştır.

Soğuk Savaş'ın sona ermesi ile birlikte uluslararası güvenliğe yönelik tehditler çeşitlenmiş ve daha da derinleşmiştir. Örneğin kitle imha silahlarının yayılması sorunu önceki dönemde olduğu gibi Soğuk Savaş sonrası dönemde de temel güvenlik sorunlarından biri olmaya devam etmiş ancak terör örgütlerinin söz konusu silahlara ulaşma ihtimallerinin belirmesi bu sorunu yeni dönemde çok daha tehlikeli bir boyuta taşımıştır. Bu gelişmeler ışığında Soğuk Savaş sonrası dönemde, küreselleşme olgusuyla birlikte ekonomi, sosyal politikalar, siyaset, ideolojik yaklaşımlar, radikal dini akımlar, terörizm, çevresel sorunlar, internetin gelişimi ile birlikte iletişim alanında yaşanan değişimler ve bilimsel ilerlemeler dikkate alındığında, güvenlik yaklaşımları ile ilgili olarak da artık hiçbir şeyin eskisi gibi olmayacağını belirtmek kaçınılmaz olmuştur.

Bu dönemde güvenlik alanında küresel ekonomik krizler, yasadışı göç sorunu, etnik milliyetçi çatışmaların artması, salgın hastalıklardan kaynaklanan zorluklar, siber güvenliğe dair sorunlar yeni tehdit odakları olarak ortaya çıkmıştır. Yine bu dönemde bireyin özellikle devlete karşı güvenliği, toplumsal güvenlik, çevre güvenliği gibi

[61]Ayrıntılı bilgi için bkz. ARIBOĞAN Deniz Ülke, **Tarihin Sonundan Barışın Sonuna**, Timaş Yayınları, İstanbul, ss. 113–114, 2003.
[62]SANCAK, op. cit., s. 134.

konuların güvenlik alanına eklemlenmiştir. Son olarak Soğuk Savaş sonrası dönemde geleneksel güvenlik tehditleri içerisinde yer alan terör, savaş, organize suçlar gibi konular kabuk değiştirerek dönüşmüş, yeni formlarda tekrar ortaya çıkmışlardır.[63]

Ayrıca Soğuk Savaş sonrası dönemde artış kaydeden ve hızla gelişen bilgisayar ve iletişim teknolojisi, artık bilginin sadece saklandığı değil, işlendiği, kullanıldığı ve geliştirildiği en önemli ortam haline gelmiştir. Devletlerin yanı sıra kişisel ve kurumsal kullanıcılar tarafından da etkin şekilde kullanılan ağ teknolojileri ile birlikte bilgi daha çekici ve hedeflenebilir konuma ulaşmıştır. Ayrıca, 1980'ler itibarıyla hızla artan teknolojik gelişmeler akabinde Bilgi ve İletişim Teknolojileri (BİT)'nin hızla gelişmesi, 2000'li yıllarla birlikte BİT'lerin tüm dünya çapında yayılması, buna paralel olarak gerek kamu gerekse de özel kesimin uygulamalarını elektronik ortama aktarmaları, hayatı bir anlamda BİT'lere bağımlı hale getirmiştir. İnsanoğlu için çok büyük yararlar sağlayan siber ortamın tehdit, saldırı, cana ve mala zarar verme gibi amaçlarla kullanılması ve siber saldırılar dolayısıyla kişilerin ve devletlerin gördüğü zararların büyük boyutlara ulaşması güvenlik anlayışında değişikliklere yol açmıştır. Siber güvenlik konusu ise bireylerin, kurumların, devletlerin ve uluslararası kuruluşların gündeminin en önemli gündem maddelerinden biri haline gelmiştir. Bu itibarla güvenlik algılamalarına yönelik olarak siber uzay merkezli olarak ortaya çıkan yeni sorunlar gerek güvenlik uygulamalarına getirdiği yeni anlayış gerekse de bu alanda gerçekleşen gelişmeleri devletlerin askeri kapasitelerini artırmaya yönelik yeni bir imkân şeklinde değerlendirmeleri kapsamında bizce ayrıca irdelenmelidir.

5. Neo-Realist Perspektif Açısından Siber Uzay

İnternet, en basit tanımıyla, bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağıdır. 1985yılında kullanılmaya başlayan internet kelimesi, *"kendi aralarında bağlantılı ağlar"* anlamına gelen "*Interconnected Networks"* teriminin kısaltmasıdır. İnternet, günümüzde tartışmasız bir şekilde yaşamımızın ve güvenlik yaklaşımlarımızın ayrılmaz bir öğesi haline gelmiştir. Bugün dünyada dört milyara yakın insanın internet ulaşımına sahip olduğu, 2017 yılına gelindiğinde ise internete bağlanma kapasitesine sahip

[63] ERDOĞAN, op. cit., s. 266.

cihaz sayısının insan nüfusunda daha fazla olacağı tahmin edilmektedir.[64] Diğer yandan süreç içinde ticari, kültürel, askeri, siyasal, finans gibi tüm sektörleri de içine alacak şekilde ağ teknolojilerinin tüm dünyayı derinden etkileyeceği açıktır.

Görüldüğü üzere, bilgisayarın taşınabilir bir hale gelmesi ve akıllı cep telefonu teknolojisi ve internet erişimin yaygınlaşması ile birlikte, internetin yarattığı imkânlar ve kolaylıklar, günlük yaşamın da ötesinde siyasal, askeri, ekonomik yaşamda da yeni bir güç faktörünün ortaya çıkmasına neden olmuştur. Bu durum ayrıca güvenlik tartışmalarında ve analizlerinde siber uzay ve siber güvenlik şeklinde tanımlanan yeni kavramların da tartışılmasına yol açmıştır.

Siber uzay kavramının uluslararası kabul görmüş bir tanımı bulunmamaktadır. Çoğunlukla interneti ifade etmek için kullanılan bir kavram olarak analizlerde sıklıkla ele alınmaktadır. Gerçekte bu kavram tabiri bir bilim kurgu romanı ile insanların karşısına çıkmıştır. Dünya'nın en çok okunan bilim kurgu romanlarından biri olan Neuromancer'in yazarı William Gibson gerçeklikle hiçbir ilgisi olmayan söz konusu kavramı, kendisi ile yapılan bir söyleşide ilk defa kullanmıştır.[65] Anılana göre siber uzay: *"milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir halüsinasyon"* ve *"tasavvur edilemez karmaşa"* şeklindedir.[66]

Belirtildiği üzere siber uzayın üzerinde uzlaşılmış tek bir tanımı bulunmamaktadır. Buna karşın yapılan bazı tanımlar ise şu şekildedir. Siber uzay bir tanıma göre: *"internet, iletişim ağları, dış dünyaya kapalı askeri ağlar, enerji hatları ağları, cep telefonları yazılım altyapılı telsizler, elektronik komuta sistemleri, cep teflonları, uydu sistemleri, insansız hava araçları sistemleri gibi birçok yazılım ve donanım elemanları toplamı*" şeklindedir.[67] Diğer bir tanım ise *"hızla genişleyen, her biri farklı bir sayısal etkileşim ve iletişim yöntemi sağlayan birleşimlerdir*."[68] ABD Savunma Bakanlığı'na göre siber uzay: *"internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemci ve denetleyicileri de içeren, bilgi teknolojisi altyapılarının bağımsız ağlarından oluşan*

[64]DEMİRCİOĞLU Cemalettin, "Siber Uzayda Güç ve Güvenlik", **İdareci'nin Sesi**, Mart-Nisan 2014, http://www.tid.web.tr/ortak_icerik/tid.web/160/8%20Cemalettin%20DEM%C4%B0RC%C4%B0O%C4%9ELU.pdf,(10.02.2016), s. 39.
[65]Ibid., s. 40.
[66]GIBSON, loc.cit.
[67]AKYAZI Uğur, **Uluslararası Siber Güvenlik Stratejisi ve Doktrinler Arasında Alınabilecek Tedbirler,** 6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı, http://www.iscturkey.org/s/2226/i/2013-paper105.pdf,
[68]DODGE Martin ve KITCHIN Rob, **Mapping Cyberspace**, Routledge, London, 2001, s. 1.

küresel etki alanıdır". 2001 Kongre Araştırma Servisi Raporu'na göre siber uzay: *"insanların, bilgisayarlar ve telekomünikasyon aracılığıyla fiziksel coğrafya dikkate alınmadan tümden birbirine bağlı olması*" anlamına gelmektedir.[69]

Diğer yandan bu etkileyici kelime tanımı ne olursa olsun, günümüzde ise günlük hayattan, askeri ve ekonomik konulara kadar, ciddi ve derin anlamlara sahip bir kavram olarak karşımıza çıkmaktadır. Siber uzay, kimilerine göre birbirleri ile haberleşen bilgisayar teknolojileri için kavramsal bir çerçeve, kimilerine göre askeri doktrinde yeni bir cephe, kimilerine göre bütün ekonomik eko-sistemin büyüyüp geliştiği bilgiye dayalı bir alt katman, kimilerine göre ise dünya politik arenasında gittikçe önem kazanan yeni bir içerik anlamını taşımaktadır.[70] Bununla birlikte, siber uzayın insan, makine ve yazılım temelli hibrit bir yapısı söz konusudur ve kavramsallaştırılırken asla internet ile sınırlandırılmamalıdır.

Siber uzay şeklinde tanımlanan alanda meydan gelen bahse konu gelişmeler ile birlikte güvenlik çalışmalarında siber güvenlik başlığı altında yeni analizlerin de daha sık gündeme geldiği müşahede edilebilmektedir. Siber güvenlik kavramın da çeşitli kaynaklar tarafından yapılan farklı tanımları bulunmaktadır. Belirtilen tanımlardan birinde, siber güvenlik: *"siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramaları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımlar, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü*[71]*,* şeklinde tanımlanmıştır. Bir başka tanım ise "*siber uzaydan ya da siber uzaya gelebilecek ataklara/tehditlere, sabotajlara ve terör faaliyetlerine karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan politikalar, oluşturulan güvenlik kavramları, risk yönetimi yaklaşımları gibi faaliyetlerin tamamı* şeklindedir.[72] Türkiye Ulusal Siber Olaylara Müdahale Merkezi (UOMM) tarafından da siber güvenlik kavramı şu şeklinde tanımlanmıştır. *"Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence*

[69]TÜRKER Seyda, **Siber Savaş Hukuku ve Uygulama Sorunsalı**, http://www.arastirmax.com/bilimsel-yayin/istanbul-universitesi-hukuk-fakultesi-mecmuasi/71/1/1177-1227_siber-savas-hukuku-uygulanma-sorunsali, (14.01.2016), s. 117.
[70]Ayrıntılı bilgi için bkz. DEMİRCİOĞLU, op. cit., ss. 41-42.
[71]YILMAZ Seda ve SAĞIROĞLU Şeref, **Siber Güvenlik Risk Analiz, Tehdit ve Hazırlık Seviyeleri**, "6. Uluslararası Siber Güvenlik ve Kriptoloji Konferansı", http://www.iscturkey.org/s/2226/i/2013-paper105.pdf, (14.01.2016), s. 158.
[72]BAKIR Emre, **Siber Savaşlar-Başlangıç**, http://www.siberguvenlik.org.tr/2012/12/siber-savaslar-baslangc.html, (14.02.2016), s. 1.

altına alınmasını, saldırıların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan güvenlik olayı öncesi durumlarına geri döndürülmesini hedefleyen faaliyetler".[73]

Öte tandan siber uzaydaki gelişmeler kapsamında karşımıza çıkan kavramlarla ilgili olarak yapılan tanımlar noktasında bir uzlaşma söz konusu olmasa bile Soğuk Savaş sonrası dönemde, özellikle de 2000'li yılların başı itibarıyla, devletlerin gerek ordularını, istihbarat birimlerini, kurumsal yapılarını gerekse de vatandaşlarını siber uzaydan gelebilecek tehditlere karşı korumak amacıyla siber güvenlik stratejileri geliştirmeye başladıkları ifade edilebilecektir. Devletler, siber güvenlik ile ilgili etkin bir kapasiteden söz edilebilmesi için, siber uzay alanındaki teknolojiye hükmetmeleri, bu alandan gelebilecek saldırılara karşı gerekli ve etkin tedbirleri almaları gerekmekte olduğunun farkındadırlar.

Konu bu açıdan ele alındığında ise teknolojiye ve siber güvenlik araçlarına yatırım yapan devletlerin, kendi güvenliklerini sağlamanın yanı sıra rekabet halinde olduğu devletlere karşı da üstünlük elde edecekleri tartışmasız bir gerçektir. Ayrıca, günümüzde devletlerin güvenliği ile ilgili konuların teknolojik gelişmelerle eşgüdümlü olduğu düşünüldüğünde, siber uzay alanındaki teknolojilere sahip olamama halinin devletler açısından ciddi bir güvenlik zafiyeti yaratacağı da belirtilmelidir. Aynı şekilde devletlerin güvenliklerini sağlama noktasında, geleneksel güvenlik anlayışına göre şekillenmiş tüm kurum ve stratejilerini etkili bir siber güvenlik ve siber savunma kapasitesi yaratmak adına yeniden organize etmesi de gerekmektedir.

Günümüzde devletler konvansiyonel savaş planlamalarının yanı sıra siber güvenlik alanında da yeni bir anlayışla stratejiler geliştirmektedirler. Bu kapsamda, siber savaşlar güvenlik strateji belgelerinde yer almaya başlamış ve devletler siber kuvvetler tesis etme yönünde planlamalara gitmişlerdir. Kuzey Atlantik Paktı (North Atlantic Treaty Organization / NATO)'da görev yapan üst düzey bürokrat Jamie Shea'in deyişiyle yaklaşık 120 devlet siber saldırı kapasiteleri geliştirmek yönünde planlama başlatmıştır.[74] Uluslararası alanda ABD, RF, Çin Halk Cumhuriyeti (ÇHC) gibi güçlü aktörlerin yanı sıra

[73]Ulusal Siber Olaylara Müdahale Merkezi, **Siber Güvenliğe İlişkin Temel Bilgiler**, https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf, (15.02.2016), s. 7.

[74] KLIMBURG Alexander, **NationalCyber Security Framework Manual**, NATO CCD_COE Publication, Talinn, 2012, p. 32.

Avrupa Birliği (AB) ve NATO gibi uluslararası örgütler de siber uzayda yeni bir anlayışla ciddi yatırımlar yapmakta ve siber güvenlik stratejileri ortaya koymaktadırlar.

Gelişmiş ülkelerin ağlanma kapasitelerinin yüksekliği düşünüldüğünde, bu devletlerin ciddi bir siber saldırı tehdidi altında oldukları görülmektedir. Teknolojiyi verimli kullanarak rakiplerine üstünlük sağlayan gelişmiş devletlerin, siber güvenliklerini sağlama kapasitesini elde etme noktasında, gelişmekte olan veya az gelişmiş devletlere nazaran daha ciddi hassasiyetleri bulunmaktadır.

ÇHC, RF ve Kuzey Kore gibi devletler siber savunma alanına önemli yatırımlar yapan aktörlerin başında gelmektedirler. ÇHC şu anda önemli siber saldırı kapasitesine ve gelişmiş istihbarat alt yapısına sahip bir devlet olarak 2050 yılına kadar siber egemenliği hedefleyen ve düşman kuvvetlerinin altyapılarını etkisiz hale getirebilmeyi de içeren bir siber doktrin benimsemiştir.[75] Söz konusu doktrinde ÇHC; *"rakiplerine karşı siber saldırı kapasitesini artırarak sadece fizik dünyada yapılan savaşların üstünlük için yeterli olmadığını kabul etmiştir*."[76] ÇHC'nin özellikle ABD ve RF gibi güçlü rakipleriyle siber alanda başa çıkabilmek için önemli çalışmalar yaptığı ve güçlü virüsler ile kötü amaçlı yazılımlar düzenleyerek düşmanlarının elektronik alt yapılarının çökertmeyi amaçladığı ileri sürülmektedir.[77]

ÇHC gibi RF Ordusu'da bünyesinde bulunan siber alanda uzman profesyoneller ile birlikte dirençli siber saldırı virüsleri ve yazılımlar geliştirmişlerdir. Ayrıca, RF tarafından organize edildiği kabul edilen ve 2007 yılında Estonya'nın bilişim sistemlerini çalışamaz hale getiren siber saldırılar ile konvansiyonel bir savaşın etkilerini propaganda ile desteklediği ve 2008 yılındaki Gürcistan Savaşı esnasındaki siber faaliyetleri, RF'nin siber uzaydaki kapasitesini göstermesi bakımından dikkat çekicidir. Bu kapsamda, Estonya Saldırısı sonrasında, Estonya hükümetinin NATO'dan yardım istemesi üzerine Talinn'de NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence/ CCD COE) 14 Mayıs 2008 tarihinde, özellikle RF'nin olası siber

[75]GÜRKAYNAK Muharrem ve İREN Adem Ali, loc.cit.
[76]Ayrıntılı bilgi için bkz. United States-China Economic and Security Review Commission, **China's Proliferation Practices, And The Development Of Its Cyber and spaceWarfare Capabilities, United States-China Economic and Security Review Commission**, Washington, 2008, http://origin.www.uscc.gov/ites/default/files /transcripts/5.20.08HearingTranscript.pdf (15.02.2016), p. 1-5.
[77]Ayrıntılı bilgi için bkz. GÜRKAYNAK ve İREN, op. cit., ss. 268-269.

saldırılarına karşı koymak amacıyla kurulmuştur.[78] Ayrıca 2014 yılındaki Ukrayna müdahalesi esnasında, RF'nin konvansiyonel silahlar ile birlikte kullandığı siber saldırı silahları *"yeni nesil"* savaşların ilk örneğini teşkil etmesi bakımından ayrıca ele alınmalıdır.

NATO, bünyesinde bir siber mükemmeliyet merkezi tesis etmesi sonrasında da ittifakın topyekûn imkânlarını siber uzay alanı kaynaklı tehditler ile mücadele konusunda planlamalar geliştirmek üzere organize etmeye başlamıştır. Bu kapsamda, 2014 Eylül ayında yapılan Galler Zirvesi'nde NATO'nun siber tehlikelere karşı ortak direnç göstermesi amacıyla genişletilmiş bir eylem planı kabul edilmiştir. 2016 Temmuz ayında yapılan Varşova Zirvesi'nde ise NATO üyelerinin ulusal kritik altyapılarının savunulmasına yönelik tedbirler geliştirmenin NATO'nun öncelikleri arasında olduğu beyan edilerek, bu konudaki planlama ve faaliyetlerin genişletilerek devam etmesine karar verilmiştir. Ayrıca bu zirvede NATO, siber uzay alanını bundan böyle ittifakın savunacağı operasyonel alanlardan biri olarak tanımlayarak, bu alanı diğer operasyonel sahalar arasında yer alan kara, hava ve deniz alanlar ile birlikte müştereken savunma planlarına dahil edeceğini ilan etmiştir.[79]

Sadece yüksek teknolojiye sahip ülkelerin değil, az gelişmiş ülkelerin de siber saldırı kapasite ortaya koymaya yönelik çalışmaları söz konusudur. Bu kapsamda, Kuzey Kore Ordusu da *"Unit 121"* adında siber savaşa odaklanan ve olası bir savaşa karşı kapasitesini geliştirmeye çalışan bir birim kurduğu bilinmektedir.[80]

Siber güvenlik alanında etkinlik tesis etmeye çalışan bir diğer devlet ise Hindistan'dır. Hindistan, Pakistan'la yaşanan Keşmir Sorunu ve nükleer silah denemelerinde maruz kaldığı siber saldırılara önlem almak amacıyla sanal dünyada yaşanan rekabete kayıtsız kalamamış ve 1998'dan itibaren siber savaşı da içine alan yeni güvenlik doktrini doğrultusunda güvenlik stratejisini belirlemiştir.[81] Bu güvenlik stratejisi kapsamında *"Ulusal Savunma Üniversitesi / National Defense University"* ve *"Savunma*

---

[78] Ayrıntılı bilgi için bkz. ÇÖPOĞLU Onur Muhammet, **Muharebe Alanındaki 5.Cephe: Siber Uzay**,http://akademikblog.com/ muharebe-alanindaki-5-cephe-siber-uzay/, (17.02.2016), ss. 1-2.
[79] NATO Resmi İnternet Sayfası, **CyberDefence**, http://www.nato.int/cps/en/natohq/topics_78170.htm, (11.12.2016).
[80] The USA Air Force Law Review, **Cyber War Edtion**, http://www.afjag.af.mil/shared/media/document/ AFD-091026-024.pdf, (17.02.2016), s. 133.
[81] GÜRKAYNAK ve İREN, op. cit., s. 269.

İstihbarat Birimi / Defense Intelligence Agency" şeklinde bir kurumsal örgütlenmeye giden Hindistan siber savaş, psikolojik operasyon, elektro-manyetik ve dalga teknolojilerinde uzman alt birimler kurmuştur.

2010 yılında, nükleer tesisleri, İsrail ve ABD kaynaklı olduğu tahmin edilen Stuxnet[82] isimli gelişmiş bir virüs tarafından fiziksel hasara uğratılan İran'da siber güvenlik kapasitesine sahip olma noktasında analiz edilmesi gereken önemli bir devlettir. İran, silahlı kuvvetleri ve üniversiteleri ile birlikte siber alanda teknoloji ve uzman geliştirebilecek kapasiteye çalışmak amacıyla planlamalar yapmıştır. Ayrıca bu konuda, RF ve Hindistan ile bilgi teknolojileri satın alma, askeri alanda teknik yardım temin etme ve eğitim desteği alma konusunda ciddi işbirliği geliştirmiştir.

Teknoloji lideri ülke olarak bilişim ortamını en etkin kullanan ABD'nin, siber uzay alanında önemli bir etkinliği bulunmaktadır. 1982 yılında, ABD Merkezi Haber Alma Servisi (Central Intelligence Agency / CIA) için bilgisayar teknolojisi giderek önem kazanmaya başlamış ve bir saldırı bir aracı haline gelmiştir. Bu kapsamda, *"mantık bombası"* olarak bilinen yöntemle, ABD bomba gibi her hangi bir savaş ekipmanı kullanmadan, bilgisayar sistemine eklenen bir kod sayesinde ve bilgisayara ait sistem yönetiminin aklını kurcalamasını sağlayarak SSCB'de bulunan Sibirya Gaz Boru hattını patlatmayı başardığı da iddia edilmektedir.[83]

Siber savaş kronolojisinde, ABD Ordusu tarafından ağ teknolojilerinin bugüne kadar tecrübe edilemeyen bir kapasite ile kullanıldığı I. Körfez Savaşı'nın da önemi büyüktür. Bu savaşın ardından, ABD Hava Kuvvetlerinde, Bilgi Savaşı Merkezi (Info War Center) isimli birbirim kurmuş, 1995 yılında ise ABD Ulusal Savunma Üniversitesi siber savaşa komuta edecek olan ilk subaylarını mezun etmeye başlamıştır.[84] Ayrıca, konu kapsamında ABD Hükümeti tarafından, Uzay Komutanlığı (Space Command), Stratejik Komutanlığa (Strategic Command / STRATCOM) dönüştürülmüş ve bu komutanlığa siber savaşa komuta etme yetkisi verilmiştir. Bu gelişmelerin devamında 2009 yılında

[82]BIÇAKCI Salih, "NATO'nun Gelişen …", op.cit., s. 108.
[83]Akademik Portal News, **Bugüne Kadar Gerçekleşmiş Olan Beş Devasa Siber Saldırı**, http://www. akademiportal.com/bugune-kadar-gerceklesmis-olan-5-devasa-siber-saldiri/, (18.02.2016).
[84]YAYLA Mehmet, **Hukuki Bir Terim Olarak Siber Savaş**, http://portal.ubap. org.tr/ App_Themes/Dergi/ 2013-104-1247.pdf, (17.02.2016), s. 186.

STRATCOM'da, bir Siber Komutanlık kurulması emri verilmiş, 2010 yılında ise *"Siber Komutanlık (CYBERCOM)"* tesis edilmiştir.[85]

Diğer yandan 2009 yılında yaptığı bir konuşmada, ABD Başkanı Barack Obama: *"siber tehditleri ABD'nin karşısındaki en ciddi ekonomik ve ulusal güvenlik sorunu olarak göstermiş ve ABD'nin 21. yy.'daki huzur ve refahının siber güvenliğe dayandığını"* söylemiştir.[86]

Yukarıda temel hatları ile özetlenmeye çalışıldığı haliyle, siber uzayda devletlerarasında yaşanmakta olan rekabet, 21. yy.'da ulusal ve uluslararası güvenliğini tehdit eden en yeni sorun olarak karşımıza çıkmıştır. Siber teknolojiler, artık devletler tarafından uluslararası ilişkilerde saldırı amaçlı olarak kullanılmaya başlanmıştır. Bir başka ifadeyle siber uzaydaki yenilikler ve teknolojik gelişmeler günümüzde uluslararası ilişkilerde etkisini süratle hissettirmiştir. Bu nedenle de siber saldırılar, mahiyeti gereği, klasik güvenlik anlayışını da değiştirerek, tehdidin artık asimetrik ve çok boyutlu bir hale gelmesine ve sadece devletten devlete yönelik olma özelliğini kaybetmesine neden olmuştur.

Ayrıca sadece devletlerin değil, aynı zamanda bireylerin, küçük grupların ve terörist örgütlerin de bir saldırı aracı olarak bilgisayar teknolojilerini kullanmaya başlamaları NATO ve AB gibi uluslararası örgütlerin yanında, ABD, ÇHC ve RF gibi ülkeleri de muhtemel bir siber saldırıya karşı tedbirler almaya itmiştir. Uluslararası ilişkilerin temel aktörü olan devletler güvenliklerini tesis etmenin yanı sıra bir saldırı aracı olarak da bilgi teknolojilerini kullanma konusunda yatırımlar yapmaya, kurumsal örgütlemelere gitmeye ve saldırı-savunma stratejileri geliştirmeye önem vermeye başlamışlardır.

Siber alandaki faaliyetlerin kolay ve arkada iz bırakmadan yapılabilir oluşu, uluslararası ilişkilerde tehdit, güvenlik ve caydırıcılık konularında yeni yaklaşımları da gündeme getirmiştir. Hatta kimi devletler, siber saldırı ve siber savaşı önemli bir stratejik savunma ve rakibe zarar verme yöntemi olarak görmeye başlamışlardır.

Bu kapsamda, siber alanda yaşanan gelişmeler yeni güvenlik risklerini beraberinde getirmekte, bu riskleri bertaraf etme noktasında devletlerin önemini arttırmakta, devletleri

[85]Ibid., s. 187.
[86]DEMİRCİOĞLU, op. cit., s. 39.

bu konuda strateji geliştirmeye zorlamakta, küçük grupları, bireylerin kaynaklık ettiği siber saldırılar ile de uluslararası sistemi eskisinden daha belirsiz ve anarşik bir hale getirmektedir.

Diğer yandan siber uzayda yaşanmakta olan gelişmeler ise gücün devletler tarafından kullanımı noktasında uluslararası ilişkiler açısından analiz edilmesi gereken yeni bir alan yaratmıştır.[87] Bu noktada güç konusunda, reelpolitik yaklaşımda, klasik realistler ve neo-realistler arasında bir farklılaşmanın da söz konusu olduğu tekrar belirtilmelidir. Daha önce detayları ile ele alındığı üzere, klasik realistler güç konusunda: "*devletlerin temel amacının güç edinmek olduğunu"* iddia ettikleri, neo-realistlerin ise: *"gücü güvenliği sağlamanın aracı olarak gördükleri"* bilinmektedir. Bununla birlikte, reelpolitik analizlerde ortaya konmak istenen tanım mutlak bir güç değil, göreceli olarak ele alınması gereken bir kavramdır. Yani, bir aktör diğer bir aktör karşısında güçlü iken, bir diğer karşısında güçsüz bir durumda bulunabilir.[88]

Diğer yandan belirtildiği haliyle aktörlerin birbirlerine karşı olan göreceli güç kapasiteleri siber uzay alanında daha da karmaşık bir hale gelmiştir. Bunun en temel sebebi siber uzayın doğasının ortaya çıkardığı çelişkili yapıdır. Söz konusu çelişkili yapı ise bir devletin ağlanma ortanı arttıkça, bir başka ifadeyle siber kabiliyeti geliştikçe, saldırı kapasitesini geliştirmesi, diğer yandan ise bahse konu gelişmeye bağlı olarak savunma kapasitesinin de azalması şeklindeki ters orantı ile açıklanabilecektir.

Ayrıca kritik altyapıların geçmişe ait mekanik sistemlerle kontrol edildiği, ağlanmışlığın sınırlı olduğu bir devlete yapılacak bir siber saldırı yetersiz kalacaktır. Söz konusu durumun bir sonucu olarak ise, ağlanmışlığın gelişmiş ülkelerde oldukça yüksek olduğu, gelişmekte olan ülkelerde ise hızla yükseldiği günümüzde siber uzay, ulus-devlet içinde ve/veya ulus-devletten bağımsız yeni aktörler oluşmasına da neden olduğu açıktır. Bu gelişmeler kapsamda ise siber uzaydaki gelişmelerin uluslararası sistemde devletin rolünü ve bir aktör olarak gücünü ne ölçüde etkilediği, neo-realist yaklaşım dahilinde analiz edilmeli ve yeniden değerlendirilmelidir.

---

[87]NYE Joseph S. Jr.,**Power and National Security in Cyberspace**, America's Cyber Future Security and Prosperity in the Information Age, New York, Public Affairs, 2011, file:///C:/Users/tk44655/ Downloads/Chapt1.pdf,(19.02.2016), p. 8.
[88]Ayrıntılı bilgi için bkz. Ibid. pp. 9-11

Neo-realist yaklaşım, daha önce ele alındığı haliyle, devletleri merkezi ve meşru bir hükümetin yokluğu tarafından tanımlanan anarşik bir dünyada temel aktörler olarak kabul eder ve devletlerin anahtar analiz düzeyini temsil ettiğini belirtir. Neo-realizmde, devlet dışı aktörlerin varlığı yadsınamazsa da, bu aktörleri devletlere göre ikincil olarak analizlerde yer alır. Yani, neo-realizm için devlet bütüncül (unitary) bir aktördür. Neo-realizm, devleti uluslararası ilişkilerin temel aktörü olarak kabul ederek, uluslararası ilişkiler ve uluslararası politikayı devletlerarasındaki mücadele süreci olarak ele alır. Sürekli kapasitesini arttırma güdüsüyle hareket eden devletler, olanakları ölçüsünde diğer devletleri egemenliği altına almaya çalışırlar.

Neo-realist teori, diğer bir devletin ki eğer bu aynı zamana potansiyel bir düşman ise güçlenmesine seyirci kalmaktansa onu önlemek için savaşa başvurmayı meşru saymaktadır. Güç politikası ile eş anlamda olarak da kullanılabilen neo-realizm için, devletlerin sahip oldukları kapasiteler büyük bir önem taşımaktadır. Neo-realist teori devletin kapasitesinin belirlenmesinde askeri gücü temel etkenlerden biri olarak kabul eder.

Askeri güç ve devletlerin kapasiteleri noktasında günümüzde yaşanmakta olan siber uzay merkezli teknolojik gelişmelerin, devletlerin askeri güç yapısını değiştirdiği ve yeni ortaya çıkan yeni şartlar kapsamında devletleri birbirleriyle rekabete zorladığı açıktır. Bu noktada, söz konusu siber uzay merkezli teknolojik gelişmeleri ortaya çıkaran motivasyonun birbirleri ile rekabet halinde olan devletlerin askeri kapasitelerini bugüne kadar artırmış olmalarından kaynaklandığı da hatırlanmalıdır. Bu durum halen devam etmektedir ve bu bağlamda siber uzay merkezli ağ teknolojilerinde yaşanan gelişmelerin devletlerin askeri kapasitelerini, dolayısıyla da uluslararası sistemdeki güçlerini artırma çabalarının bir parçası olarak değerlendirilmelidir.[89] Kısacası, ağ teknolojilerinde devam etmekte olan hızlı değişim ve gelişim, geleneksel devletlerarası rekabet ve çatışmanın ayrılmaz bir parçası olarak süregelmektedir.

Bu kapsamda ise siber uzayın yarattığı imkânların uluslararası sistemde devlet dışında aktörlerin (çok uluslu şirketler, çıkar ve baskı grupları, hükümet dışı aktörler,

[89]Ayrıntılı bilgi için bkz. ERIKSSON Johan ve GIACOMELLO Giampiero, "The Information Revolution, Security, and International Relations: (IR) RelevantTheory?", **International Political Science Review**, Vol.27, No.3, 2006, pp. 221-244.

medya destekli sosyal hareketler, bireyler vb.) çeşitliliğini ve önemini arttırdığı gerçeğine rağmen, neo-realist bakış açısıyla siber uzaydaki gelişmelerin aynı zamanda devletin rolünü daha da pekiştirdiği de ifade edilebilecektir.

Kısacası, devlet uluslararası sistemde teknolojik gelişmelerin boyutu ne olursa olsun hala temel belirleyici ve oyun kurucu temel aktördür. Siber uzay alanındaki genişleme ve gelişmeye bağlı olarak, birçok ülkenin siber güvenlik stratejileri kapsamında siber ordular ve siber güvenlik kurumları tesis ederek, siber uzmanlar ve akademisyenler yetiştirme gayretleri de devletin uluslararası sistemdeki tartışmasız hakim aktör rolünü sağlamlaştırmaktadır.[90] Bu bağlamda, gerek bireylerden, gerekse de hasım devlet destekli olarak, siber uzaydan gelebilecek tehditlere merkezi bir devlet yapılanması ile karşı konulabileceği ve etkili bir siber savunma sistemi gerçekleştirilebileceği tartışmasızdır.[91] Bununla birlikte, ulusal internetin, ulusal interneti denetleyen mekanizmaların, ağ teknolojilerinin ve buna bağlı olarak planlanan güvenlik stratejilerinin devletler tarafından kontrol edildiği dikkate alındığında, uluslararası sistemde devletin başat rolünün hala kesin ve nettir.[92]

Siber uzay alanı doğası gereği, tehdidin kaynağını belirsiz kılması, benzer şekilde tehdidin yeri, zamanı, kökeni hakkında önceden kestirilemeyen şartları mahiyetinde barındırması, uluslararası sistemi neo-realist paradigmaya uygun bir şekilde, Soğuk Savaş dönemine kıyasla, özellikle de 2000'li yıllardan sonrası için çok daha anarşik bir yapıya evrimleştirmiştir.[93] Bu kapsamda, siber uzay alanını düzenleyen evrensel nitelikte kesin ve nihai bir uluslararası hukuk düzenlemesinin hala bulunmaması, siber uzayda devletler arasında işbirliği yerine daha rekabetçi politikaların hakim olması ve bu rekabetin şiddetinin giderek artması hususları dikkate alındığında, uluslararası sistemi eskisinden çok daha fazla belirsiz ve güvensiz bir hal aldığı sonucu da ortaya konabilecektir. Yine benzer şekilde, devletlerin siber güvenlik stratejilerinin temel itibarıyla gizli olması, bu bağlamda bir devletin gerek hasım olduğu gerekse de müttefik olarak kabul ettiği bir devlete yönelik

[90] Ayrıntılı bilgi için bkz. Ibid, pp. 5-10.
[91] LEWIS James Andrew, **The Cyber War Has Not Begun**, Center for Strategic and International StudiesMarch 2010, https://www.google.com.tr/webhp?ie=UTF-8&rct=j#q=james+andrew+ lewis+the+cyber+ war+has+not+begun, (21.02.2016), p. 1.
[92]VENTRE Daniel, **A Constructivist Approach of Cyber security/Cyber defense Concepts: Lessons of Security Studies Theories and Discursive Analysis**, http://www.fvv.um.si/knjigarna /eknjige/pdf/Crime_Social_Control_and_Legitimacy.pdf, (20.02.2016), p. 4.
[93] Ibid., p. 5.

gizli bir siber faaliyet yürütüp yürütmediği kesin olarak bilinememesi, ayrıca siber uzay doğası gereği, siber tehdidin kaynağını belirsiz olması gibi gelişmelerin de uluslararası sisteminin anarşik yapısını derinleşmesine neden olan bir etmenler olarak karşımıza çıktığı da açıktır.

Görüldüğü üzere siber uzay alanında meydana gelen yeni gelişmeler ve şartlar, uluslararası sitemin yapısını daha fazla anarşik hale getirmektedir. Bu durum ise devletler tarafından yeni bir tehdit odağı olarak algılanmakla birlikte, aynı zamanda askeri güçlerini geliştirmeye yönelik bir fırsat olarak da okunmaktadır. Bu kapsamda, devletlerin siber uzay alanındaki yeni gelişmeleri algılayış biçimi, uluslararası ilişkiler ve güvenlik meselelerinde, ayrıca da güç kavramı merkezli analizlerde yeni yaklaşımların ortaya konmasına da neden olmuştur.

Uluslararası ilişkilerde güç: "*bir devletin başka bir devlete karşı uyguladığı ve normal şartlar altında o devletin yapmak istemeyeceği bir şeyi yapmasını sağlamaya yönelik etki*" şeklinde tanımlanabilmektedir. Bu tanımdan hareketle, bir devletin uluslararası ilişkilerde uyguladığı politikanın yegâne vasıtasının güç olduğu da ifade edilebilecektir. Bu vasıtaya sahip olmak devletin amaçlarından biridir ve devletler için güç ancak kullanılabilirse güçtür.[94]

Uluslararası ilişkilerde gücün kullanımı kapsamındaki öncü yaklaşımlar klasik realist teorisyenler Niccolo Machiavelli ve Morgenthau'ye aittir. Özellikle de klasik realist teorisyenler için güce sahip olmak insanlığın ve devletlerin doğal amaçları arasında yer almaktadır. Gücü bir araç olarak ele alarak kavramın gelişmesine yapılan neo-realist katkı ile birlikte reelpolitik yaklaşım için gerek ekonomik ve askeri gelişme, gerekse de kültürel yayılma durumları bir devletin güçlü olma halinin olağan bir sonucudur.

Günümüzde güç kavramı ile ilgili yapılan kimi analizlerde, güç;*"sert güç (hard power)", "yumuşak güç (softpower)"*ve*"akıllı güç (smartpower)"* şeklinde nitelendirilen kategorizasyonlardahilindeele alınabilmektedir. Bu kategorizasyonlarise temelde, Joseph Nye'nin güç kavramı odaklı yaklaşım ve değerlendirmelerini esas almaktadır.

Bu noktada Nye'nin*"siber güç (cyberpower)"* kavramı merkezli analizlerini de içine alacak şekilde, anılanın konu kapsamındaki yaklaşımlarının çalışmamıza yapacağı katkı

[94] TANRIVERDİ Bilal, **Akıllı Güç**, http://akademikperspektif.com/2014/06/11/akilli-guc/, (10.12.2016).

bakımında ayrıca detaylıca irdelenmesinde bizce fayda görülmektedir.

6. Joseph Nye'nin Güç Kavramı Kapsamındaki Analizleri ve Siber Güç

Güç, 20.yy.'da sadece sert/askeri[95] güç olarak kabul edilirken, sert gücün yanında yumuşak gücün varlığı da son yıllardaki uluslararası ilişkiler analizlerinde sıklıkla ele alınmaya başlanmıştır.[96] Yumuşak güç ile ilgili yapılan tanımlamalarda ise Nye'nin analizlerindeki kavramsallaştırmaları birçok düşünür ve akademisyen üzerinde önemli etkisi söz konusu olmuştur. Öte yandan 21.yy.'da siber uzayda meydana gelen teknolojik gelişmeler ve buna bağlı olarak ortaya çıkan ağ teknolojilerindeki yaygınlaşma ile sert güç ve yumuşak güç olarak adlandırılan kavramların yanı sıra akıllı güç şeklinde bir yaklaşım da tartışılmaya başlanmıştır.

Bu noktada konunun daha iyi anlaşılması amacıyla, Nye tarafından güç kavramı kapsamında yapılan analizler daha yakından ele almak önem arz etmektedir. Nye yumuşak gücü, genel itibarıyla : *"bir ülkenin dünya siyasetinde istediği sonuçlara, onun değerlerine hayra olan, onu örnek alan, refah seviyesine ve fırsatlarına öznen ülkelerin kendisini izlemesiyle ulaşması"* şeklinde tanımlanmaktadır.[97] Bu tanımdan da hareketle Nye, yumuşak gücün uygulanması noktasında aşağı yer alan haliyle de üç temel dayanak olduğunu ileri sürülmektedir:[98]

1. Kültür (Hedef bölgenin insanına cazip gelmesi şartıyla).

2. Siyasi Değerler (Gerek içerde, gerekse dışarda sahip olunan değerlere sadık kalınması şartıyla)

3. Dış Politika (Başkalarının bu politikaları meşru görmeleri şartıyla)

Bununla birlikte yumuşak gücün, başlangıçtaki tercihleri aksi yöne çevirme, gündemin çevresini değiştirme ve bu çerçeve içinde gündemi yeniden belirleme, başkaların tercihlerini şekillendirme şeklinde bir işleyişi söz konusudur. Nye, bu noktada yumuşak

[95]Sert /Askeri güç, en genel anlamıyla: askeri ve ekonomik unsurlarının hedef alınan ülkeyi zorla ikna etme, caydırma gibi amaçlarla kullanılmasını ifade etmektedir. Ayıntılı bilgi için bkz. YILMAZ Sait, **Yumuşak Güç ve Evrimi**, http://usam.aydin.edu.tr/YUMUSAKGUCVEEVRIMI(4a4j).pdf, (10.12.2016), p. 1-7.
[96]Ayrıntılı bilgi için bkz. NYE Joseph S. Jr., **Cyber Power**, Harvard Kennedy School, Belfer Center for Science and International Affairs, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, (19.02.2016), pp. 3-7.
[97]NYE Joseph S. Jr., **Yumuşak Güç**, Ankara, Elips Yayınları, 2005, s. 14.
[98]NYE Joseph S. Jr., **The Future of Power**, New York, Public Affairs, 2011, p. 30.

gücün söz konusu işleyiş tarzının doğrudan veya dolaylı gelişim biçimlerinin bulunduğunu düşünmektedir. Örneğin, Obama'nın G-20 toplantısında yaptığı ikna edici bir konuşma, katılımcı ülkelerin, az gelişmiş ülkelere yardım taahhütlerini kimi zaman arttırabilmektedir. Bu örnek, doğrudan bir işleyiştir.

Daha sık görülen bir başka işleyiş tarzı ise iki adımdan oluşur. Önce toplumlar etki altına alınmakta, akabinde ise o toplumlar bilâhare kendi liderine tesir etmektedir. Yumuşak gücün, politika oluşturanlar üzerindeki doğrudan etkilerine anlamlı bir örnek de öğrenci değişim programlarıdır. Hâlihazırda görevde bulunan 46 devlet başkanı ile geçmişte devlet başkanlığı yapmış 165 kişi ABD üniversitelerinde eğitim almışlardır. ABD'ye, bir yılda, üniversite eğitimi için 750 bin öğrenci geldiği düşünülürse, bu gücün etkinliği daha iyi anlaşılır.

Yumuşak gücün aşağıdan yukarıya doğru işlediği durumlarda toplumun yöneticileri etkilemesi, liderlere, istenileni yaptırmak veya caydırmak yönünde olabilir. Örneğin 2003 Irak müdahalesi öncesinde Türk kamuoyu, dönemin hükümetini ABD birliklerinin ülke toprakları üzerinden Irak'a geçmelerine izin vermemeleri yönünde etkileyebilmiştir. Sonuç olarak, ABD birlikler Türk topraklarını kullanamamışlardır. Böylece Bush yönetimi, yumuşak gücünü iyi kullanamayarak kendi sert gücünün zedelenmesine yol açmıştır. Yumuşak gücün hedefi, geniş kitleleri etkileyerek kamuoyu oluşturmak ve tavır değişikliği sağlamaktır. Ayrıca, devletlerin yumuşak güç imkânları ile sadece birbirlerini, dolaylı ve doğrudan yöntemlerle etkilemeye çalışmakla kalmadıkları, diğer ülkelerin çekim gücüne ve meşruiyetine zarar vermek için de uğraştıkları da bilinmelidir. Bu noktada istihbarat servislerinin, diplomasi, değişim ve eğitim programları bu amaca hizmet ettikleri hatırlanmalıdır.[99] Ayrıca ABD'nin sahip olduğu ekonomik, kültürel, teknolojik ve politik gücünden beslenen yumuşak gücü, ABD'nin dış politika stratejilerinin başarıya ulaşmasında büyük etkiye sahiptir. Devasa ekenomik büyüklüğü kapsamında, ABD dünya ekonomisinde büyük rol oynamakta ve bu gücünü kullanarak uluslararası sistemi etkisi altına alabilmektedir.[100]

Öte yandan Nye, akıllı güç kavramını:*"eldeki bütün imkânların uygun zaman ve mekân göz önüne alınarak değerlendirilmesi, hem dostlara, hem de düşmanlara ulaşarak*

[99]Ayrıntılı bilgi için bkz. Ibid., p. 31-35
[100]AKÇADAĞ Emine, **ABD'nin Kamu Diplomasisi Stratejisi: Akıllı Güç...**", http://www.kamudiplomasisi.org/pdf/abdkdstratejisi.pdf, (10.12.2016), p. 1.

ortak payda meydana getirme kabiliyetine sahip olunması ve dış politikada sert ve yumuşak gücün bir arada kullanılması" şeklinde tanımlanmaktadır.[101] Görüldüğü üzere, akıllı güç, dayatma ve ödetmeye odaklı sert güç ile ikna etme ve cezbetmeye dayalı yumuşak gücün bir karışımıdır. Örneğin bu noktada Nye, ABD kurumları içerisinde en iyi eğitilmiş ve en büyük kaynaklara sahip olan kurumun Pentagon olduğunu kabul etmekte, ancak demokrasi, insan hakları ve sivil toplumun gelişmesi gibi meselelerin tek başına silâh zoruyla çözmenin mümkün olamadığını da iddia etmektedir.[102]

Nye göre, gücün imkân/kaynak odaklı olarak tanımlanması halinde bir ülke göreceli olarak büyük nüfusa, toprağa, doğal kaynaklara, ekonomik güce, askeri kuvvete ve sosyal düzlemde istikrara sahip olması halinde güçlü bir devlet olarak kabul edilebilecektir. Ancak böyle bir tanımla ile güç analizi yapanlar, eli kuvvetli olanın oyunu her zaman kazanamadığına da şahit olmuşlardır. Örneğin ABD, kaynak açısından Vietnam'a göre çok daha güçlü olmasına rağmen Vietnam Savaşı'nı kaybetmiştir. Bu noktada Nye'nin güç kaynaklarının önemini küçümsemediği anlamı çıkartılmamalıdır. Nye, ister soyut ister somut olsun gücün, bu kaynaklar/olanaklar sayesinde uygulandığını da açıkça kabul etmektedir. Nye için kaynakları istenen sonuçları elde etmeye yönelik bir alet olarak kullanmak, iyi tasarlanmış stratejiler ve üstün liderlik becerileri gerektirmektedir ve bu durum Nye tarafından akıllı güç şeklinde tanımlanmaktadır. Kısacası sert güç; itmek, yumuşak güç; çekmek ise akıllı güç; itme-çekme eyleminin bir alışımı olarak kabul edilebilecektir. Yani, akıllı güç; yumuşak ve sert güç yöntemlerinin etkin stratejiler oluşturulması amacıyla harmanlanması anlamına gelmektedir.

Nye akıllı gücün, sadece ABD'nin kullanımına özgü bir güç olmadığını, bu gücü küçük devletler, hatta devlet olmayan oyuncuların da kullanabileceğini de ileri sürmektedir. Örneğin, beş milyon nüfuslu Norveç, kalkınma yardımları ve barışçıl politikaları gibi yumuşak güç uygulamaları sayesinde imajını yüceltmiş ama NATO'nun önemli bir askerî ortağı olmaktan da geri durmamıştır. Diğer örnek olarak ise muazzam nüfusuyla ÇHC bulunmaktadır. Askerî ve ekonomik gücünü sürekli olarak yükseltmekte olan ÇHC, bir yandan da yumuşak güç uygulamalarına yatırdığı malî kaynakları artırarak,

[101]Ayrıntılı bilgi için bkz. NYE., "Cyber Power", op. cit., pp. 3-7.
[102]NYE ,"The Future of …", op. cit., p. 4.

gücünü komşuları üzerindeki tehdit algısını hafifletmek suretiyle akıllı stratejiler geliştirmektedir.[103]

Özet olarak, Nye akıllı gücü: "*sert ve yumuşak güçlerin etkin biçimde birleştirilmesi olarak*" tanımlamaktadır. Ayrıca, anılan için akıllı güç ABD'nin hedeflerine ulaşması için hem sert hem de yumuşak güçle oluşturulan entegre bir stratejinin geliştirilmesi anlamına da gelmektedir. Bu kapsamda akıllı güç, güçlü bir askeri yapıya olan ihtiyacın önemini vurgulayan, aynı zamanda ABD nüfuzunu yaymak ve ABD girişimlerine meşruiyet kazandırmak için ittifaklara, ortaklıklara ve kurumlara büyük yatırımlar yapan bir yaklaşım olarak da kabul edilebilecektir.[104] Örneğin,uluslararası arenada dostlar, ortaklar ve müttefikler, politikaların meşruiyeti, kabulü vedesteklenmesi açısından büyük önem taşımaktadır. Ancak 11 Eylül sonrası Bush yönetimininuyguladığı politikalar bu destek ve meşruiyetin azalmasına neden olmuş ve sonuç olarak ABD'nin bahse konu olumlu faktörlerden beslenen akıllı gücünde ciddi bir etki kaybının oluşmasına yol açmıştır. Bu olumsuz durum ilgili olarak Nye: "*ABD, Amerikancılığın iç politikada güdülmesinin intihar anlamına geleceği ölçüde popülarite kaybederse yabancı siyasi liderler istemeyerek de olsa Amerikancılıktan ödün vermek zorunda kalacaktır*" ifadesi ile özetlemeye çalışmıştır.[105]

Bununla birlikte Nye, siber uzay alanındaki gelişmelere bağlı olarak gücün dağılımı noktasında yeniden analiz edilmesi gereken gelişmelerin söz konusu olduğuna da işaret etmektedir. Nye, günümüzde güç kaymalarının iki biçimde tezahür ettiğini iddia etmektedir. Bu durumlar; gücün yayılması ve/veya bir elden diğer ele intikal etmesi şeklindedir.

Gücün, hâkim konumdaki bir ülkeden diğerine kaymasının tarihte birçok örneği bulunmakla birlikte, içinde bulunduğumuz bilgi çağında yaşanmakta olan teknolojik gelişmelerin bir sonucu olarak gücün yayılarak dağılması ise yeni bir olgu olarak karşımıza çıkmaktadır. Kısacası bilgi devrimi ve bu devrimin bir sonucu olarak siber uzayda meydana gelen gelişmeler gücün doğasını değiştirmekte, yayılıp dağılmasını hızlandırmaktadır. Bu gelişmenin bir sonucu olarak ise Nye göre, devletler dünya

[103]Ayrıntılı bilgi için bkz. Ibid., pp. 8-13.
[104]Ayrıntılı bilgi için bkz. NYE Joseph S. Jr., "Get Smart", **Foreign Affairs**, July/August 2009, pp. 1-3.
[105]Ayrıntılı bilgi için bkz. NYE Joseph S. Jr., "The Decline of America's Soft Power", **Foreign Affairs**, No.3, May-June 2004, pp. 16-20.

sahnesindeki eğemenliklerini sürdürmeye devam edecekler ancak sahneyi, sayıları giderek artan farklı oyuncularla paylaşmak zorunda kalacaklar ve uluslararası sistemi tek başlarına kontrol etmekte zorlanacaklardır.[106]

Öte yandan Nye söz konusu güc dağılımı sürecini, *"diffusion of power"* kavramı ile ele almakta ve siber uzayı gücün dağılımına etki eden enformasyon devrimine en uygun örnek olarak tanımlamaktadır. Nye, konu ile ilgili olarak ise*"enformasyon devrimi ile birlikte, seyahat ve iletişim imkânlarının geçmişe göre oldukça kolaylaştığını, bir zamanlar küçük şirketlerin ya da bireylerin erişiminin yüksek maliyetli, hatta imkânsız olduğu bilgisayar teknolojilerinin, artık herkes için ulaşılabilir hale geldiğini, bunun sonucu olarak artık dünya siyasetinde sadece devletlerin değil diğer aktörlerin de (terörst gruplar, bireyler, uluslararası şirket ve örgütler, sivil toplum kuruluşları vs.) etkin olmaya başladığını*" ifade etmektedir.[107] Bu itibarla, siber uzayın doğası gereği devletler tek aktör olarak bu alana hâkim olamayacaklardır. Sonuç olarak, siber uzaydaki gelişmeler kapsamında gücün büyük devletlerden diğer devletlere, daha da önemlisi devlet dışı aktörlere doğru evrildiği de belirtilebilecektir.

Bununla birlikte Nye, siber uzay alanı kaynaklı yeni gelişmelerin ortaya çıkardığı söz konusu güç yayılması durumunun, son noktada, asla devletlerin uluslararası sistemdeki temel aktör rolünü değiştirmeyeceğini de savunmaktadır. Nye açısından bu duruma, bir devletin kritik altyapılarını tamamen çökertmeye yönelik bir saldırının düzenlenmesine hedefleyen sofistike planlamaların ve bu planlamalara ait maliyetlerin günümüzde sadece devletlerin bilgi birikimi, tecrübeleri ve bütçeleri ile karşılanabiliyor olması hali oldukça etkili bir örnek olarak gösterilebilecektir.[108]

Devletin uluslararası sistemdeki rolü sağlamlaştırmasına neden olan bir başka faktör ise siber uzayı oluşturan alanın temel yapı taşlarından olan servis sağlama donanımlarının ve fiber optik kabloların hala devletlerin egemenlik alanları içerisinde kalması ile ilgilidir. Bu kapsamda Nye, bir devletin bu imkânların kullanılmasına engel olarak dış politikada kendisine yeni bir baskı aracı yöntemi geliştirebileceğini savunmaktadır. Örneğin Google, ABD menşeli bir şirket olmasına rağmen Almanya'nın

[106]NYE, Cyber Power, op. cit., p. 35.
[107]New Times Haber Portalı, **Röportaj/Joseph Nye:Bugün bireylerin güç pastasından aldıkları pay, geçmişe göre çok daha büyük**, http://newtimes.az/tr/interview/3042/, (13.04.2016).
[108]NYE, "Cyber Power", op. cit., p. 14

baskısıyla bu ülkeden yapılması olası nefret söylemli arama taleplerini engellemek zorunda kalmış ve Almanya'daki faaliyetlerini Alman yasalarına uygun sürdüreceğini ilan etmiştir.[109] Nye, siber uzayı fiziki ve sanal katman şeklinde ikiye ayırmaktadır. Bu kapsamda Nye, siber uzayın fiziki altyapısını oluşturan parçaların (fiber kablolar, kapalı ağlar, internet altyapısı) klasik egemenlik kurallarına tabi olduğunu belirtmektedir.[110] Bu bağlamda da devletler internetin söz konusu fiziki altyapısına eğitim, ticaret, sanayi, güvenlik, finans odaklı ciddi yatırımlar yapmaktadırlar ve bu yatırımlarının bir sonucu olarak eğemen bir güç olma hakkının da verdiği meşruriyet ile kendi siber uzay alanlarını baskı ve denetimi altında da tutabilmektedirler. Bu değerlendirme kapsamında, ÇHC'nin kendi siber uzay alanı kapsamındaki yatırımları ve bu alanı kontrole yönelik tedbirleri yeterli bir örnek oluşturmaktadır.

Bunlarla birlikte siber uzayın tek bir rejim altında denetlemesi hedefine hala uzak olunması, devletlerin uluslararası bir anlaşma ile bu alanı kontrol etmekten ısrarla kaçınmaları ve gevşek bir işbirliğini tercih etmeleri, siber uzay kaynaklı güvenlik tehditlerine karşı devletlerin giderek daha fazla yatırım yapmaları ve bu alanı denetim altına alma noktasındaki çabaları, siber uzay kaynaklı siber casusluk, saldırı ve terörizm gibi tehditlere etkili karşı koyma mekanizmalarının devletlerin tekelinde olması hususları düşünüldüğünde, siber uzayda meydaa gelen gelişmelerin devletlerin uluslararası sistemdeki rolünü azaltmadığı, aksine arttırmakta olduğu sonucuna da rahatlıkla ulaşılabilecektir.[111]

Konu bağlamında Nye, siber uzayda saldırı savunmaya göre üstün olduğunu, bu durum da siber uzayın yapısından kaynaklandığını kabul etmektedir. Yani, basit bir ağ açığıyla oluşan zafiyetten istifade edilerek, düşük bir maliyet ile bir aktöre önemli ekonomik kayıplar ve fiziki hasarlar verilebilir. Ancak Nye, söz konusu hasarları oluşturabilecek siber suçlar, hacktivist faaliyetler, siber terör eylemleri, devlet kaynaklı siber saldırı/siber savaş tehditleri ve siber casusluk faaliyetlerine karşı koyma

[109]NYE Joseph S. Jr. , **Gücün Geleceği**, http://www.ozetkitap. com/images2/Future%20of%20Power%20-%20Final%20(1).pdf, (10.12.2016), pp. 41-45.
[110]Ayrıntılı bilgi için bkz. NYE Joseph S. Jr., "NuclearLessonsforCyber Security?", **Strategic Studies Quarterly**, Winter 2011, http://www.au.af.mil/au/ssq/2011/winter/nye.pdf, (14.04.2014), pp. 18-20.
[111]NYE, "Gücün Geleceği", loc. cit.

mekanizmalarının oluşturulmasına yönelik planlamalar ise temelde ancak devletlerin etkin katkısıyla işlevsellik kazanabileceğini iddia etmektedir.[112]

Diğer yandan Nye siber güç kavramının artık daha sık bir biçimde analizlerde ele alınmaya başlanması ile birlikte, siber uzaydaki gelişmelere de bağlı olarak bu kavramın uluslararası ilişkiler disiplini için de ciddi değişimlere neden olduğunu da ileri sürmektedir. Siber güç, Nye tarafından: "*insan kaynağı ve yeteneği, yazılım ve donanım teknolojiler, altyapılar ve ağ teknolojileri ile ilgili tüm kaynaklar vasıtasıyla yaratılanbir imkân"*şeklinde tanımlanmaktadır.[113]

Siber güç kavramının neden olduğu değişim ve güç uygulamaları iseNye açısından hem yumuşak güç, hem de sert güç kavramı ile ilgilidir. Enformasyon alanındaki değişim diğer aktörleri etkilemek ve dikkatlerini çekmek için kullanılması halinde bu durum, yumuşak güç kavramı ile açıklanabilir. Ancak değişim başkaları üzerinde kontrol kurmak ve onlara zarar vermek için kullanılması halinde isebu durum, sert güç kavramı kapsamında ele alınmalıdır. Örneğin siber imkânlar kaynaklı olarak elde edilen güç, muhalif bloggerları tutuklayarak mesaj göndermelerini engellemek ise sert güç, ÇHC'de olduğu gibi 1930'lardan kalma bir ihtilâf nedeniyle öğrencileri internet üzerinden örgütleyerek Japonya aleyhine protesto gösterileri yapmaya sağlayabilmek ise yumuşak güc kapsamında değerlendirilmelidir. Ya da internet yasakları ile farklı düşüncelerin yayılmasını engelemek bir sert güç uygulaması olarak kabul edilmeliyken, meşru ve demokratik yöntemlerle bir algı yaratılabilmesi halinde ise bu yumuşak güç uygulması olarak görülmelidir.[114] Konu kapsamındki bir başka somut örnek ise Stuxnet saldırısı kapsamında verilebilecektir. Nye, İran'daki nükleer tesislerin yapılan Stuxnet saldırısını sert güç kullanımına örnek olarak göstermektedir.[115]

Bunlarla birlikte Nye, siber uzaydaki teknolojik imkânların devletler açısında tehdit yaratma potansiyeline sahip yeni aktörlerin saldırı kabiliyetine kavuşmasına yol açtığını belirtmektedir. Bu itibarla sadece devletler değil, aynı zamanda bir terörist grup, hatta gerekli siber kabiliyetlere sahip tek bir kişi bile hasım gördüğü devletin kritik altyapısına saldırı kapasitesine sahip olmuştur. Nye'nin bu yaklaşımlarından da hareketle, artık kara,

[112]Ayrıntılı bilgi için bkz. NYE, "Nuclear Lessons for …"., op. cit., pp. 20-30.
[113]NYE, "Cyber Power", op. cit., p. 7
[114]NYE,"Gücün Geleceği", op. cit. p. 41.
[115]Ayrıntılı bilgi için bkz. NYE, "Nuclear Lessons for …", op. cit., , pp. 11-15.

hava, deniz ve uzay şeklinde tanımlanan dört boyutta, aktörler arasında güçlü-güçsüz ayrımı yapmak kolayken, insan tarafından ortaya konulan teknolojik gelişmeler ile birlikte ortaya çıkan ve beşinci boyut olarak adlandırılan siber uzayda ise aktörler arasında güçlü-güçsüz ayrımı yapmak oldukça zorlaştığı ortadadır. Bu durumun en temel sebebi ise siber uzayın doğasının ortaya çıkardığı çelişkili yapıdır. Belirtilen çelişkili yapı ise bir devletin ağlanma ortanı arttıkça, bir başka ifadeyle siber kabiliyeti geliştikçe, saldırı kapasitesini geliştirmesi, diğer yandan ise bahse konu gelişmeye bağlı olarak savunma kapasitesinin de azalması şeklindeki ters orantı ile açıklanabilecektir.[116]

Tüm bu değerlendirmeler kapsamında Nye, siber güvenlik anlayışan hâkim olan prensiplerin geleneksel güvenlik anlayışına ve güvenlik politikaları açısından bir tezat oluşturduğunu da savunmaktadır. Nye göre, siber güvenlik, geleneksel güvenlik politikalarına ve anlayışına adeta meydan okumaktadır. Bu noktada Nye, geleneksel güvenlik anlayışının hâkim prensibi olan *"sınırda savunma"* kavramına atıfda bulunarak, artık söz konusu olanın siber uzay alanından gelen bir tehdit olduğunda, *"sınırda savunma"* kavramının hiçbir anlam ifade etmediğini belirtmektedir. Nye, *"sınırda güvenlik"* kavramıyla başlayan klasik güvenlik politikalarının doğruluğunu ve geçerliğini günümüzde kısmen korusa bile siber uzay kaynaklı tehditler düşünüldüğündebu yaklaşımın yeterli olmadığını, bundan yaklaşık 50 yıl önce sınır muhafızları ve hava savunma sistemlerine sahip olmak yeterli olmakla birlikte, artık devtlerin güvenliklerini sağlama noktasında siber uzay alanından gelecek olan tehditlere karşı yeni konsept, strateji ve savunma aparatlarına ihtiyacı olduğunu gündeme getirmektedir.[117]

Nye'nin analiz ve değerlendirmelerinde kavramsallaştırdığı üzere, uygulamanın mahiyetine göre hem yumuşak ve hem de sert güç kapsamında değerledirebileceğimiz siber güç imkânları, uluslararası ilişkilerin doğasındaki çatışma olgusu ve bunun beraberinde getirdiği güvenlik kaygılarıyla birlikte, devletlerin bu gücü sahip olma halini askeri kapasiteleri için yeni bir imkan olarak görmelerine yönelik eğilimlerini artırmaktadır.

[116]Ayrıntılı bilgi bkz. NYE, "Cyber Power", op. cit. pp. 10-15.
[117]New Times Haber Portalı, **Röportaj/Joseph Nye: "Bugün bireylerin güç pastasından aldıkları pay, geçmişe göre çok daha büyük**, http://newtimes.az/tr/interview/3042/, (13.04.2016).

Öte yandan devletler arasında siber uzayın sağladığı yeni imkânlar kapsamında ortaya çıkan yeni şartlar, siber uzay kaynaklı tehditleri merkeze alan güvenlik kaygılarını artırmıştır. Gerçekte ise bu durum güvenlik kavramının tarihsel süreç içerisinde teknolojik değişmelere bağlı olarak çeşitli anlamlar kazanmak suretiyle günümüzdeki algılayış biçimine evrimleşmiş olması ile paraleldir. Bilindiği üzere, 20.yy.'da yaşanan büyük savaşlar, toplumsal değişimler ve teknolojik gelişmeler uluslararası ilişkilerde yeni görüşlerin ortaya çıkmasıyla birlikte güvenlik kavramını da değişime uğratmıştır. 20. yy.'ın sonlarına doğru ise Soğuk Savaş döneminin sona ermesiyle güvenliğin farklı sektörleri ortaya çıkmış ve ortaya çıkan bu sektörleşme kavramı güvenlik algılarında da derinleşmeye yol açmıştır. Bu dönemde güvenlik konusu ve kavramı siber uzayda yaşanan gelişmelerin de önemli katkısıyla farklı konular için yeniden değerlendirilmiştir.[118]

Belirtildiği üzere siber uzay alanı merkezli ortaya çıkan yenilikler, teknolojik olarak uluslararası aktörlerin saldırı ve savaş stratejilerini de doğrudan etkilemiştir. Öte yandan siber uzay kaynaklı teknolojiler de son yıllarda tecrübe edilen gelişmeler ve bu alandaki teknolojik ivmenin önümüzdeki yıllarda aratarak devam edeceğine yönelik beklenti dünyadaki büyük güçlerin kendi çıkarlarını birbirlerine karşı koruma adına aldıkları tedbirleri de hızlandırmıştır. Ayrıca siber uzayda yaşanan gelişmelerin uluslararası ilişkilerde devletler tarafından askeri gücün artırılması noktasında yeni bir imkân olarak algılandığı, bu durumunda devletlerarasındaki siber rekabeti körükleyerek uluslararası sistemdeki güvensiz ortamı körüklediği de açıktır. Bu nedenle, özellikle ağlanma oranı yüksek, askeri ve ekonomik açıdan güçlü devletler siber uzayda kendilerini güvensiz hissetmekte ve siber kapasitelerini artırma cihetine gitmektedirler. Bu noktada devletler, güvenlik kavramını adeta *"kazanılan değerlerine yönelik bir tehdidin olmaması hali"* hali olarak algılayarak, rasyonel bir yaklaşımla kazandıkları değerleri koruma adına güçlü olmaları gerektiği sonucuna varmaktadırlar. Bu durumda, devletlerin askeri kapasitelerini artırma noktasında yeni bir imkan olarak gördükleri siber uzaya ilgilerini her geçen gün artırmakta ve bu alana ciddi yatırım yapmalarına neden olmaktadır.

Siber uzayda yaşanmakta olan gelen gelişmelerin uluslararası sistemi yeni tehdit unsurlarını ortaya çıkarması, tehdidin kaynağını anonim hale getirmesi, tehdidin yapısını,

[118] GÜNTAY Vahit, "Uluslararası İlişkiler Bağlamında Güvenlik Algısı ve Siber Güvenlik; Akdeniz, Karadeniz ve Avrupa Bölgeleri Üzerine Bir Değerlendirme", **International Journal of Social Science**, No. 37, Sonbahar, p. 480, 2015.

şeklini ve zamanını belirsizleştirmesi noktasında daha anarşik hale getirdiği çalışmanın önceki bölümlerinde detaylı olarak ele alınmıştır. Bu kapsamda, siber uzay alanındakigelişmelerin daha da kaotik hale getirdiği uluslararası sistemde devletler, güç toplamak ve gücü ulusal çıkarlar çerçevesinde kullanmak amacıyla hareket etmeyi sürdürmektedirler. Bu amaç doğrultusunda da, bu anarşik yapıda devlet kendisini askeri gücüne güvenmek ve onu yeterli düzeyde tutmak zorunda hissetmektedir. Söz konusu durumda, devletlerin askeri gücün artırılması noktasında yeni imkânlar sunan siber uzaya olan ilginin artmasına neden olmaktadır.

Gerek yapılanmanın tehdit algısı üzerine kurulması gerektiğini ileri süren ve sistemi dengede tutan faktörün aktörlerin birbirini ne kadar tehdit olarak algıladıklarına bağlı olduğunu ileri süren defansif (savunucu) reelpolitik yaklaşım ile ele alınsın, gerekse de tehdit algısının yapısını önemsemeyerek, devletler için temel amacın gücünü sürekli artırmalısı gerektiğini iler süren ofansif (saldırgan) reelpolitik yaklaşım ile ele alınsın, devletlerin siber uzayda yaşanmakta olan gelişmelerin ortaya çıkardığı imkânları tehdit olarak algılandığı ve buna göre siber kapasitelerini artırma noktasında stratejiler geliştirdikleri ortadadır. Bu duruma örnek olarak ise dünya genelinde halen 120 ülkenin siber saldırı kapasiteleri geliştirmek yönünde planlama içinde olduğu ve söz konusu devletlerarasında ise ABD ve RF'nin önde geldiği gerçeği hatırlanmalıdır.[119]

Ayrıca siber uzayda yaşanmakta olan gelişmelerin uluslararası ilişkiler disiplini açısından analiz edilmesinin bahse konu disiplinin çalışma konuları bakımından oldukça önemli olduğu kabul edilmelidir. Bu kapsamda da uluslararası sistemi domine etme kapasitesine sahip ülkelerden ikisi olan ve siber uzaydaki gelişmeleri Soğuk Savaş sonrası dönemde ortaya koydukları askeri ve siber güvenlik stratejileri ile yakından takip ettikleri görülen RF ve ABD'nin siber güvenlik stratejilerinin analiz edilmesinin söz konusu kabulü destekleyen bir husus olarak görülmesi gerektiği ortadadır.

Diğer yandan RF Ordusu mensubu General BorisAlekseyev, 2000 yılı Ocak ayında ITAR-TASS ajansına verdiği bir mülakatta:*"iki savaşın mevcut olduğunu, bunlardan*

[119]KLİMBURG, loc.cit.

birinin: güncel çatışmalar, diğerinin ise, bilgi savaşı şeklinde açıklanabileceğini"[120] ifade etmiştir. Yine benzer şekilde, RF Genelkurmay Başkanı Nikolai Makaraov, 28 Ocak 2012 tarihinde verdiği beyanında: *"görüldüğü üzere, savaş merkezi kara ve deniz kaynaklı geleneksel tehditlerden siber güvenliği de kapsayacak şekilde siber uzaya yayıldığını ağ teknolojileri merkezli savaşın ciddi gelişme kaydettiğini, RF olarak bu gelişmleri hesaplamak ve tedbir almak zorunda olduklarını*" belirtmiştir.[121]

Üst düzey Rus güvenlik bürokrasisi mensuplarının da beyanlarıyla onayladığı şekilde, RF Hükümeti'nin siber uzaydaki gelişmeleri yakından takip ettiği ve siber güvenlik alanında başta ABD olmak üzere dünyadaki diğer ülkelerin stratejilerini de etkileyecek şekilde önemli adımlar attığı açıktır. 2016 yılı itibarıyla RF'nun espiyonaj, kontr/espiyonaj, dezenformasyon, elektronik savaş kabiliyetleri, psikolojik savaş ve propaganda, siber saldırı gibi faaliyet ve planlamaları kapsayan geniş bir enformasyon savaşı kabiliyetine sahip olduğu ve bu imkânlar nispetinde RF'nun siber uzaydaki gelişmeleri domine eden en önemli devletlerden biri olduğu görülmektedir.[122]

RF'nin, siber uzayda faaliyet göst eren diğer aktörlere (devletler) göre, siber savaş kapasitesini siyasi çıkarları noktasında kullanma imkan ve kabiliyetine sahip olduğu rahatlıkla ifade edilebilecektir.[123] Bu ifade ile ilgili olarak ise RF'nin 2007 yılında Estonya'ya yönelik siber saldırısı, 2008 yılındaki Rus-Gürcistan savaşı esnasında siber kapasitesini kullanma becerisi, 2014 yılındaki Ukrayna müdahalesi sırasında uygulamaya koyduğu "hibrit savaş" stratejisi ve uçak düşürme krizi sonrasında Türkiye'ye yönelik olarak 2015 Aralık ayında başlayan siber saldırıları örnek gösterilebilecektir.

Bu açıdan bakıldığında, RF'nin siber saldırı kapasitesi ABD ve diğer NATO üyesi ülkeler için endişe edilmesi ve tedbir alınması gereken bir tehdit kaynağıdır.[124] Bu

---

[120]HAGESTAD II William, **Comparative Study: Iran, Russia and PRC Cyber War**, RSA Conference, 2013 Europe, http://www.rsaconference.com/writable/presentations/file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf, (05.03.2016), p. 17.
[121]Ibid, p. 20.
[122]WIRTZ James J., **CyberWarand Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy**, NATO CCD COE Publications, Tallinn 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf (05.03.2016), p. 30.
[123]Ibid., p. 31.
[124]GILES Keir, "**Russian Cyber Security: Concepts and Current Activity**, Chatham House ConflictStudiesResearchCentre,https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Russia%20and%20Eurasia/060912summary.pdf (05.03.2016), p. 2.

kapsamda, ABD Kongresi tarafından hazırlanan bazı raporlarda, ABD güvenlik bürokrasi mensuplarınca yapılan beyanlarda ve ABD'nin savunma stratejilerinin açıklandığı belgelerde, temeli itibarıyla özetle:[125]

-RF'nin siber uzaydaki en önemli aktörlerden biri olduğu, bu haliyle ABD'nin ulusal ve uluslararası çıkarları için potansiyel bir tehdit kabul edilmesi gerektiği,

-RF'nin siber kapasitesini, espiyonaj, propaganda ve siber saldırı amacıyla kullanmaktan çekinmediği,

-RF için siber saldırı yöntemlerini uluslararası ilişkilerde bir zor kullanma/baskı aracı olarak kullanmaktan çekinmediği ve bu kapsamda ciddi mesafe aldığı,

-Söz konusu nedenler ile ABD'nin siber uzaydaki gelişmeleri yakından takip etmesinin şart olduğu ve bu çerçevede ulusal ve uluslararası çıkarlarına yönelik tehditleri bertaraf etme noktasında kapsamlı, caydırıcı ve etkili tedbirler alması gerektiği sıklıkla gündeme getirilmektedir.

Söz konusu gelişmeler ve değerlendirmeler ışığında, çalışmanın bundan sonraki aşamasında öncelikle ABD'nin akabinde ise RF'nin siber savunma ve saldırı stratejileri karşılaştırmalı olarak ve örnek olayların detayları irdelenmek suretiyle analiz edilecektir. Bahse konu analizler neticesinde ise siber uzayda yaşanmakta olan gelişmelerin, uluslararası ilişkiler disiplini açısından yeni bir güvenlik olgusu olarak görülmesinin ve tüm detayları ile analiz edilmesinin gerekliliği ortaya konmaya çalışılacaktır.

[125]MEDVEDEV A. Sergei, **Offence-Defence Theory Analysis of Russian Cyber Capability**, Naval Post-GraduateSchool,Monterey,California,https://www.google.com.tr/?gfe_rd=cr&ei=qzHZVrreN7Go8wf MuYegDw#q=this+thesis+represent+mikhail+tsypkin, (05.03.2016), p. 2.

İKİNCİ BÖLÜM

AMERİKA BİRLEŞİK DEVLETLERİ'NİN SİBER GÜVENLİK STRATEJİSİNİN ANALİZİ

ABD, 1900'lerin ilk yıllarından bu yana tecrübe etmekte olduğu siyasi, askeri, ekonomik ve kültürel gelişim ivmesinin bir sonucu olarak, günümüzde teknolojide dünyanın lider ülkesi konumuna kavuşmuştur. Bu teknolojik gelişmişlik düzeyi, aynı zamanda insan eliyle yapılmış dijital bir alan olan siber uzayda, ABD'nin tartışmasız bir biçimde öncü devletlerden biri konumuna gelmesine de neden olmuştur.

Soğuk Savaş döneminde, ağ teknolojileri kaynaklı ilk nesil teknolojileri SSCB ile yaşadığı asker rekabet ve uzay yarışı kapsamında kendisine yeni bir fırsat olarak okuyan ABD, 1960'lar ile birlikte bu teknolojilerin gelişmesi noktasında ciddi gayret göstermiştir. Soğuk Savaş sonrası dönemde ise ağ teknolojilerini yeni bir ticari alan gören ABD, internetin ticarileşmesi ve sivilleşmesi noktasında gerekli teşvikleri sağlamış ve bu alana önemli yatırımlar yapmaya başlamıştır.

Söz konusu yatırım ve teşviklerinde etkisiyle hızla gelişen internet temelli teknolojiler, özellikle 1990'lar ile birlikte tüm dünya genelinde gerek askeri gerekse de ticari ve toplumsal alanlarda günümüz dünyasını temelden sarsan gelişmelere yol açmaya başlamıştır.

1. ve 2. Körfez Savaşları esnasında ağ teknolojileri merkezli kitle iletişim araçlarını ve askeri teknolojileri aktif bir şekilde kullanan ABD, uluslararası sistemin yanı sıra siber uzay olarak adlandırılan alanda da etkili bir hegemon güç olduğunu ve bu alanı domine edeceğini net bir şekilde ortaya koymuştur.

2000'li yıllar ile birlikte RF'nin de siber uzayı askeri kapasitesini artırmak amacıyla yeni bir imkan olarak kabul eden stratejik hamleler yapması birlikte ABD, siber kapasitesini savunma ve saldırı yönünde geliştirmek amacıyla siber güvenlik stratejilerini revize etmeye başlamıştır. Diğer bir değişle ABD, siber uzayı RF gibi askeri gücünü artırmak ve bu ülkenin siber faaliyetlerine karşı koymak amacıyla daha aktif bir şekilde kullanmaya başlamıştır. Bu bağlamda ABD ve RF arasında belirtilen şekilde vuku bulmaya başlayan siber rekabetin de etkisiyle siber uzayın hızla gelişmeye başlayan yeni bir güç mücadelesi alanı olarak karşımıza çıktığı açıktır. Bu itibarla siber uzayın doğası gereği tehdit kaynaklarını çeşitlendirmesi, bu tehditlerin de anonim yapıda oluşu, ayrıca RF ve

ABD gibi iki küresel gücün bu mecrayı askeri kapasiteleri için yeni bir fırsat olarak gören stratejileri ile birlikte uluslararası sistemin anarşik yapısının daha da karmaşıklaştığı ileri sürülebilir.

Bu kapsamda çalışmamızın ABD'nin hegemon siber güç haline geliş süreci; ağ teknolojilerinin tarihsel gelişimi ve askeri imkânlar için kullanılması; ABD'nin siber güvenlik alanındaki resmi strateji belgeleri; bu alandaki resmi kurum ve kuruluşlarının faaliyetleri; maruz kaldığı ve planladığı iddia edilen siber saldırı vakaları irdelenmek suretiyle analiz edilecektir.

1. ABD'nin Siber Güvenlik Stratejisinin Temelleri

ABD'nin siber gücünün evriminin başlangıcı tarihsel olarak 1930'lara dayandırılabilir. Bu kapsamda, ilk işlevsel bilgisayar örneklerinden biri olarak da görülebilecek olan ve Alman Donanması'nın 1920'lerde ilk örneğini ortaya koyduğu "ENİGMA" kripto cihazının muadili, ABD Donanması tarafından 1930'ların son yarısında "SIGIBA" adı altında üretilmiştir. Öte yandan İngiliz ve ABD'leri kökenli bilim insanlarının 2. Dünya Savaşı esnasında, "ENİGMA"cihazının gelişmiş bir versiyonunun şifresini çözmeye yönelik çabaları da ABD'nin bilgisayar yazılımı alanındaki ilk teknolojik tecrübeleri arasında önemli bir yere sahip olmuştur. 1940'ların sonu itibarıyla ise ABD'de Atanasoff-Berry Computer Şirketi, ilk elektronik dijital bilgisayarı, ardından da AT&T2s Bell Labs Şirketi bilgisayarların gelişimi açısından büyük öneme sahip ilk transistörü icat etmişlerdir.[126] 1950'ler ile birlikte International Business Machines (IBM) ilk yüksek seviye bilgisayar dili olan FORTRAN'ı geliştirmeyi başarmış, ayrıca söz konusu yıllarda ilk bilgisayar cipleri ABD'de kullanılmaya başlanmıştır.[127]

Bununla birlikte, ABD yönetimi SSCB ile bilimsel alanda rekabet edebilmek amacıyla Şubat 1958'de İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency / ARPA)'nıkurmuştur. ARPA'daki projelerin kapsamı ise uzay araştırmalarının yanı sıra balistik füze savunması, dünya üzerinde nükleer test yapılan coğrafi noktaların

[126]AFCEA Organization, **The Evolution of US Cyberpower**,http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf, (23.05.2016), p. 7.
[127]CHIVERS Ian ve SLEIGHTHOLME Jane, **Fortran History and Development**, http://www.fortranplus.co.uk/resources/Fortran_history_and_development.pdf, (23.05.2016), p. 5

saptanması gibi konuları da kapsayacak biçimde düzenlenmiştir.[128] ARPA bünyesinde, proje kapsamında çalışma yürüten bilim insanlarını tek bir ağ altında toplanmasını sağlayabilecek bir teknolojinin geliştirilmesi ile birlikte, söz konusu proje internet tarihinin başlangıcını teşkil etmiştir. Bu kapsamda da ARPA projesi, ARPANET şeklinde isimlendirilmiştir.

Küba Krizi ile birlikte olası bir nükleer savaş halinde ARPANET'in bu saldırılardan etkilenmesi için ne tür önlemler alınması gerektiği şeklinde tartışmalar da yaşanmaya başlamıştır. Bu tartışmalar ise Paul Baran isimli bir bilim adamının fiziksel saldırı sonrasında kalan en büyük grupla elektrik bağlantısı sağlayarak iletişimi sürdürebilecek bir ağ yapının yaratılabileceğini ortaya koyması ile nihayetlenmiş ve farklı merkezlerde çalışan ağlar belirtilen yaklaşıma göre düzenlenmiştir. Akabinde söz konusu teknik altyapı ile birbirine bağlı olan ARPANET, ilk olarak İngiltere'deki Ulusal Fizik Laboratuarı (NationalPhysical Laboratory)'ndaki ticari ağ ve Fransa'daki araştırma ağı olan Cyclades ile birleştirilmiştir.[129] Böylelikle de internetin uluslararası boyutta ulaşan ilk çekirdek altyapısı oluşturulmuştur. İnternetin temelinin atılması sonrasında ise 1971 yılında *"creeper"* isimli ilk bilgisayar solucanı yazılımı tarafından ARPANET'in olumsuz bir şekilde etkilenmesi söz konusu olmuştur. Bu çerçevede anılan yazılım siber alandaki ilk olası tehdit emaresi olarak değerlendirilmiştir. Bahse konu gelişmelere rağmen sınırlı sayıda kullanıcı tarafından erişilebilen bilgisayar teknolojisi, 1970 yılında elektronik parçaları kendin yap projesi (DIY-Do it yourself), 1975 yılında kişisel bilgisayar olarak tanımlayabileceğimiz "Altair 8800"isimli bilgisayarların üretilmesi ve 1975 yılında piyasaya çıkan "IBM 5100"ler" ile birlikte, bir iletişim ve ağ kültürü olarak günlük hayatımızda yer edinmeye başlamıştır.[130]

Öte yandan ABD ve SSCB arasında söz konusu dönemde yaşanan askeri ve bilimsel rekabet ile uzay yarışının bir benzeri kültür ve sanat alanında da gözlemlenmiştir. Bu kapsamda Staney Kubrik tarafından 1968 yılında yönetilen "*2001: A Space Odyssey*" filmi ile Andrei Tarkovsky'in 1972 tarihli "Solaris" filmi arasında yapılan kıyaslamalarda bu bağlamda değerlendirilebilir. Sanatsal kıyaslamalar haricinde, bu iki filmin çalışmamız açısından önemi her iki yönetmenin bahse konu filmlerinde yarattıkları kurgu ve gelecek

[128]BIÇAKCI, "NATO'nun Gelişen Tehdit …", op. cit., ,s.103.
[129]Ayrıntılı bilgi için bkz. BIÇAKCI,"21. Yüzyılda Siber…, op. cit.", s. 6.
[130] Ibid., s. 7.

dönem tasvirlerinin aslında günümüz siber uzay alanı merkezli ağ teknolojilerinin de temel örnekleri arasında gösterilebilecek olmasıdır. Bu noktada içinde bulundukları rekabet motivasyonu ile birlikte, dönemin ABD ve SSCB bilim ve kültür insanlarının siber uzay temelli teknolojilerin önemini kavramada ne kadar başarılı oldukları görülmektedir.

Bu gelişmeler ile birlikte internetin temel alt yapısı olarak kabul edebileceğimiz, TELENET kamusal alanda servis vermeye başlamıştır. 1980'ler ile birlikte kişisel bilgisayar kullanımın artması ile birlikte ağlara katılımlar da artmaya başlamış ve sonuç olarak 1980 yılında ARPANET'e sızan bir virüs ile birlikte ARPANET'te ki iletişim 72 saatliğine kesintiye uğramıştır.[131] Bu bağlamda ABD'de internet teknoloji ile birlikte gelişmekte olan ağ sistemlerinin güvenliği kavramı ilk defa tartışılmaya başlanmıştır. 1982 yılına gelindiğinde ise ARPANET'te ki tehditlerin artması üzerine, ABD Savunma Bakanlığı gizli askeri verilerin iletişimin sağlanacağı yeni bir altyapı oluşturulmasına karar vermiş ve ARPANET'e ilave olarak, Militarynet (MILNET) isimli bir altyapının oluşturulmasını tesis etmiştir.[132] Diğer yandan sanal dünyanın temelini atmış olan ARPANET, teknolojik yetersizlik nedeniyle yavaşlaması, ayrıca daha nitelikli bir altyapıya sahip Ulusal Bilim Vakfı Ağı (National Science Foundation Network / NSFNET) gibi ağların kurulması kapsamında, 1990 yılında kapatılmıştır.[133]

Tim Berners-Lee isimli bir fizikçi tarafından Avrupa Nükleer Araştırma Örgütü (European Organization for Nuclear Research / CERN)'nde çalışan bilim insanlarının farklı bilgisayarlardaki bilgiye kolayca erişebilmesi için geliştirdiği "world wide web (www)" formatı ile birlikte, internet üzerinden bilgisayarlar tarafından sunulan web sayfalarının oluşturulmasına ve ziyaret edilmesine imkân sağlanarak, internetin başta ABD olmak üzere, tüm dünya genelinde hızla gelişmesi mümkün olmuştur.[134] Bu gelişmenin bir uzantısı olarak da 15 Eylül 1997 tarihinde ise iki Stanford Üniversitesi öğrenci olan Larry Page ve Sergey Brin, ilk internet arama motoru olan "google.com"un tescilini yapmıştır.[135]

Bu noktada çalışmamızın ilk bölümünde ele alındığı üzere neo-realist teorinin siyasetin köklerini insan tabiatında arayan, uluslararası politikayı temel itibarıyla "güç" ve

[131]ABBATE Janet, "Government, Business, and the Making of the Internet", **Business History Review**,Vol. 75, No. 1, Spring 2001, p. 164
[132]BIÇAKCI, "NATO'nun Gelişen Tehdit …", op. cit., s. 107.
[133]BIÇAKCI, "21. Yüzyılda Siber…", op. cit. s.25.
[134]Ibid., s. 26.
[135]AFCEA Organization, op. cit, p. 10.

bu terim ile etkileşim içinde olan "*çıkar*" kavramını merkeze alarak açıklayan düşünce biçimi olduğu unutulmamalıdır.[136] Bu bağlamda Waltz'a göre uluslararası sistemin yapısının anarşik bir süreçle şekillendiğini ve bu sistemde her bir devletin egemenliğini ve güvenliğini koruma amaçlarına odaklandığını, anarşik yapıdaki uluslararası sistemin devletlerarasındaki güvensizlik ortamını teşvik ettiğini, bu durumun da devletlerin uzun süreli işbirliği yapmasını engellemekte olduğunu hatırlamak gerekecektir.[137] Zira ABD'nin Soğuk Savaş döneminde SSCB ile giriştiği askeri, bilimsel ve uzay alanlarındaki sert rekabetin bir sonucu olarak, neo-realist paradigmalara uygun şekilde, iki devletin işbirliği imkânları kısıtlanmış, askeri kapasitelerine ciddi yatırımlar yapmalarının önü açılmış ve sonuç olarak uluslararası sistem çok daha güvensiz hale gelmiştir. Yukarıda özetlendiği şekliyle ABD, SSCB ile yaşadığı rekabette avantaj sağlamak adına modern ağ teknolojilerinin temelini oluşturan bilimsel ve teknik gelişmeleri Soğuk Savaş döneminde teşvik etmek suretiyle, günümüzde siber uzay olarak adlandırılan dijital alanın insan eliyle oluşturulmasına da ciddi katkı sağlamıştır. Bununla birlikte Soğuk Savaş sonrası dönemde ağ teknolojilerini askeri kapasitesini geliştirme noktasında yeni bir fırsat olarak görmeye devam eden ABD, 1990'lar sonrasında da bu alanlara yatırımlara devam etmiştir.

Bu yatırımların bir sonucu olarak da siber uzay teknolojilerinde meydana gelen yeni nesil gelişmeler ile birlikte ABD Ordusu tarafından ağ teknolojileri ilk kez bugüne kadar tecrübe edilemeyen bir kapasite ile 1990–1991 yılındaki 1. Körfez Savaşı esnasında kullanılmıştır. 1. Körfez Savaşı esnasında, ABD güçlerinin kullandığı iletişim ve enformasyon tekniklerinin, Irak Silahlı Kuvvetleri'nin harekât kabiliyetine verdiği zararın yanı sıra ABD Ordusu'na kazandırdığı hız, başta Rus askeri ve güvenlik uzmanları olmak üzere, tüm dünya genelinde yakından takip edilmiştir. Bununla birlikte 1. Körfez Savaşı'ndaki sıcak çatışmaların dünya kamuoyuna adeta canlı olarak aktarılmasında, kitle iletişim araçlarının ortaya koyduğu imkân ve kabiliyetin anlaşılması noktasında büyük öneme sahip olmuştur. Bu kapsamda da ABD Hava Kuvvetleri bünyesinde Bilgi Savaşı Merkezi (Info War Center) isimli bir birim kurulmuş, 1995 yılında ise ABD Ulusal Savunma Üniversitesi siber savaşa komuta edecek olan ilk subaylarını mezun etmeye başlamıştır. Ayrıca konu kapsamında ABD Hükümeti tarafından, Uzay Komutanlığı (Space Command), "Stratejik Komutanlık (Strategic Command / STRATCOM)'a

[136]Ayrıntılı bilgi için bkz. MORGENTHAU J. Hans, **Politics Among Nations**, Mc Graw Hill Press, New York, 7th Edition, pp. 3-5, 2006.
[137]WALTZ ve QUESTER, "Uluslararası İlişkiler Kuramı…", loc.cit.

dönüştürülmüş ve bu komutanlığa siber savaşa komuta etme yetkisi verilmiştir. Bu gelişmelerin devamında 2009 yılında STRATCOM'da, bir siber komutanlık kurulması emri verilmiş, 2010 yılında ise müstakil bir Siber Komutanlık (Cyber Command / CYBERCOM) tesis edilmiştir.[138]

Belirtildiği şekliyle 1990'lı yıllar ile birlikte, ABD yönetimlerinin kendi ülkesinde yaşanmakta olan siber uzay teknolojileri alanındaki gelişmeleri, askeri kapasitesini geliştirme yönünde bir fırsat olarak okuduğu ve bu konuda kurumsal altyapılar oluşturma sürecine bu yıllarda ciddi hız verdiği görülmektedir. Ayrıca 1990'lar ile birlikte, ABD'nin günümüzdeki siber güvenlik stratejisin temelini oluşturan belge, doktrin ve planlamaları da dünya kamuoyuna ilan etmeye başlamıştır.

Bu noktada ABD'nin siber güvenlik stratejisini belirleyen temel belgelerin, RF'de analiz edilen süreçlerin aksine, sadece ilgili ABD kurumlar tarafından yayımlanmış olan strateji belgeleri, askeri ve güvenlik doktrinlerinden ibaret olmadığı da ifade edilmelidir. Zira federal sisteminin bir sonucu olarak, ABD'nin siber güvenlik stratejisinin şekillenmesinde, ABD başkanlık direktifleri; ilgi kurumların kendi güvenlik alanlarına yönelik olarak ortaya koydukları stratejiler ve eyalet bazında yapılan siber stratejik planlamalar da ciddi önem sahiptir.

1.1. Temmuz 1995 ve Mayıs 1997 Tarihlerinde Başkan Bill Clinton Tarafından İlan Edilen Başkanlık Direktifleri

Söz konusu direktiflerden ilki olan ve Temmuz 1995'de yayımlanan *"13010 No'lu Başkanlık Direktifi (Presidential Directive-13010)*'nin, ABD'nin siber güvenlik alanındaki gelişmelere doğrudan vurgu yapan ilk resmi belge olması bakımından önemi büyüktür.[139]

Bu belgenin önemli bir bölümü gizli niteliği haiz olmakla birlikte, anılan belgede dönemin ABD Başkanı Bill Clinton, başsavcılık makamını ülkenin kritik altyapılarına yönelik olası bir siber saldırıya karşı hazırlık durumunu araştıran bir çalışma yapması

[138]Ayrıntılı bilgi için bkz. YAYLA, op. cit., ss. 186-187.
[139]TIRRELL K. William, **United States Cybwer Security Strategy,Policy and Organization: Poorly Postured to Cope With a Post-9/11 Security Environment**, Master Thesis, Washington University, 2012, https://www.hsdl.org/?view&did=729810, (10.01.2016), p. 20. Ayrıntılı bilgi için bkz. https://www.federalregister.gov/executive-orders/william-j-clinton/1997, (15.01.2017).

konusunda görevlendirmiştir.[140] Bu görevlendirme ile oluşturulan "Kritik Altyapıları Koruma Komisyonu" tarafından yapılan çalışma neticesinde hazırlanan raporda:[141]

—Kritik altyapıların korunması için, ABD kamu ve özel sektörünün birlikte hareket etmesi gerektiği,

—Bugüne kadar tecrübe edilen siber saldırıların henüz ABD kritik altyapılarını tamamen çökertecek bir seviyeye sahip olmadığı, bununla birlikte söz konusu saldırıların sisteme zarar verebileceği,

—Bu nedenle de ABD yönetiminin konu kapsamında tedbirler almasının şart olduğu, hususları yer almıştır.

Mayıs 1997 tarihinde yayımlanan "*63 No'lu Başkanlık Direktifi (Presidential Directive - 63)"* ise ABD'nin kritik altyapılarını tanımlayan ilk resmi dokümandır. Bu belgeye göre ABD kritik altyapıları; *"enformasyon, iletişim, enerji, bankacılık ve finans, ulaşım sektörleri ile içme suyu ve acil müdahale altyapısı (911) ve kamu sağlığı alanı"* şeklindedir.[142] Ayrıca bu direktif, gelecek dönemde ABD resmi kurumları tarafından hazırlanacak olan stratejik belge, planlama ve doktrinlere kaynaklık teşkil etmiş olması bakımından da öneme sahiptir.[143]

Öte yandan ABD kritik altyapılarını tanımlamayı amaçlayan söz konusu iki belgenin hazırlanması sonrasında günümüze kadar ülkenin kritik altyapılarına dair rejimi tanımlayan, denetleyen ve kontrol eden çok sayıda düzenleme yapılmıştır. Bu düzenleyici kuralların yetki alanı ise ortaya konan her doküman ile birlikte, daha geniş yetkileri kamu otoritesine veren ve daha sıkı bir denetim rejimini gündeme getiren nitelikte olmuştur.

1.2. "Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji" İsimli Belge

"The National Strategy to Secure Cyberspace / Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji" belgesi, Şubat 2003'de yayımlanmıştır. Bu belge, ABD'nin siber uzay alanını tanımlayan, bu alandaki hedef ve planlamalarını ortaya koyan, ulusal siber uzayın

[140]Ayrıntılı bilgi için bkz. Presidency Of USA, **Executive Order 13010—Critical InfrastructureProtection,**http://www.presidency.ucsb.edu/ws/?pid=53066, (17.02.2017).
[141]Chairman, President's Commission on Critical Infrastructure Protection, **Critical Foundations: Protecting America's Infrastructure-The Report of the President's Commission on Critical Infrastructure Protection**,https://www.fas.org/sgp/library/pccip. pdf, (24.05.2016).
[142]White House, **Presidential Decision Directive (PDD)-63, Critical Infrastructure Protection**, http://fas.org/irp/offdocs/pdd/pdd-63.htm, (24.05.2016).
[143]TIRRELL, op. cit., p. 24.

nasıl korunacağına dair planlanan sistemi belirleyen, siber uzay kaynaklı tehditleri tarif eden ilk geniş kapsamlı dokümandır.

Bu belgede, 2003 stratejisinin amaçları: *"ABD kritik altyapısını siber ataklara karşı korumak, ABD siber savunma sistemindeki açıkları tespit etmek ve gidermek, olası saldırılar karşısında uğranılabilecek zararı minimize etmek"* şeklinde ifade edilmiştir.[144] Belgede, ulusal siber uzayın korunması amacıyla beş yapının tesis edileceği belirtilerek, bu yapılar aşağıda belirtildiği şekilde isimlendirilmiştir:[145]

-Ulusal Siber Uzay Cevap Sistemi

-Ulusal Siber Uzay Savunma Açıklarını Giderme Programı

-Ulusal Siber Uzay Farkındalık ve Eğitim Programı

-Resmi Kurumların Siber Saldırılara Karşı Korunması Yapılanması

-Ulusal ve Uluslararası Siber Uzay İşbirliği

"*Ulusal Siber Uzay Cevap Sistemi"* ile siber uzay alanından gelebilecek saldırılara karşı kamu ve özel sektörün birlikte hareket etmesi, bu ortak hareket kabiliyetinin geliştirilmesi noktasında taktik ve planlamalar ortaya konması, özel sektörün siber uzay alanındaki görevlerini yerine getirme noktasında teşvik edilerek, desteklenmesi ve tüm bu amaçlar kapsamında federal bir sistemin geliştirilmesi hedeflenmektedir.

"Ulusal Siber Uzay Savunma Açıklarını Giderme Programı" ile ulusal siber uzay alanının korunması noktasında gerekli yasal düzenlemelerin yapılması, internet güvenliğinin tesis edilmesi, güvenilir bir dijital kontrol sisteminin oluşturulması, yazılım güvenliğinin sağlanması, siber sistemin ve altyapıların fiziki güvenliğine yönelik tedbirlerin geliştirilmesi ve federal siber güvenlik araştırmaları ile kalkınma ajandasına öncelik verilerek, siber güvenliğe yönelik tehditlerin belirlenmesi amacıyla bir uyarı sisteminin geliştirilmesine gayret edilmesi amaçlanmıştır.

"Ulusal Siber Uzay Farkındalık ve Eğitim Programı" ile başta ABD iş ve işveren kesimi ile tüm toplumun siber saldırılar karşısındaki farkındalığının artırılması, bu konudaki eğitim ve oryantasyon faaliyetlerine federal düzeyde önem verilmesi, özel-kamu

[144]Ayrıntılı bilgi için bkz. https://www.us cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (16.01.2017).
[145]Ayrıntılı bilgi için bkz. TIRRELL, op. cit., pp. 35-40.

sektör siber işbirliğinin hızlandırılması ve siber güvenlik sertifika eğitim programlarının teşvik edilmesi hedeflenmiştir.

"Resmi Kurumların Siber Saldırılara Karşı Korunması Yapılanması" ile öncelikle ABD'nin resmi kritik altyapıları yeniden tanımlanmıştır. Bu tanımlamaya göre: *"tarım ve gıda sektörlerindeki, içme suyu ve kamu sağlığı ve acil müdahale sistemlerindeki, sosyal güvenlik, bilgi ve telekomünikasyon altyapılarındaki, enerji, ulaşım, bankacılık ve finans ve kimya sektörlerindeki, posta ve gemicilik sistemlerindeki tüm resmi bilgisayar, yazılım ve ağ teknolojileri"*, ABD'nin kritik altyapıları olarak belirlenmiştir. Bu yapılanmayla da söz konusu altyapılardaki federal güvenliğin sağlanması, federal kablosuz yerel ağ sistemlerinin korunması, merkezi yapılanma ile eyalet hükümetlerinin konu kapsamındaki koordinasyonun tesis edilmesi, bu kapsamda federal düzeyde eğitim, bilgi paylaşımı ve analiz yeteneklerinin geliştirilmesi amaçlanmıştır.

"Ulusal ve Uluslararası Siber Uzay İşbirliği" başlığı altında ise ilk olarak ABD siber uzay alanının, küresel siber uzayın bir parçası olduğu, siber saldırıların sınır aşan bir boyuta ve kapasiteye ulaştığı vurgusu yapılarak, bu alandaki işbirliğinin önemi gündeme getirilmiştir. Bu kapsamda ABD'nin, ulusal ve uluslararası siber kontr/espiyonaj faaliyetleri ile ilgili olarak işbirliği imkânlarını geliştirmesi gerektiği, küresel bir siber güvenlik kültürün tesis edilmesi noktasında uluslararası kurum ve kuruluşlar nezdinde girişimlerde bulunulmasının şart olduğu, ulusal ve uluslararası düzeyde siber saldırıları tespit eden ve bunlara hızla cevap verebilen bir sistemin geliştirilmesinin önem arz ettiği, Avrupa Konseyi Sanal Suçlar Sözleşmesi (Council of Europe Convention on Cybercrime)'ni[146] henüz imzalamayan devletlerin teşvik edilmesi gerektiği, hususları vurgulanmıştır.

[146]"Sanal Suçlar Sözleşmesi/ Sanal Ortamda İşlenen Suçlar Sözleşmesi (Council of Europe Convention on Cybercrime)" bilgisayar suçlarını ve internet suçlarını gözeten ilk uluslararası sözleşmedir. Ulusal kanunların harmonisini sağlayarak, araştırma tekniklerini geliştirerek ve ülkeler arası işbirliğini arttırarak bunu sağlamayı hedeflemektedir. Avrupa Konseyitarafından Strazburg'da tasarlanmış ve Avrupa Konseyi izleyicisi statüsündeki Kanada, Japonya, ÇHC gibi ülkelerin de aktif katılımı sağlanmıştır. Sözleşme ve açıklayıcı raporu Avrupa Konseyibakanları tarafından 109. oturumda 8 Kasım 2001 tarihinde kabul edilmiştir. 23 Kasım 2001 tarihinde imzaya açılıp 1 Temmuz 2004 tarihinde yürürlülüğe girmiştir. Kasım 2015 itibariyle 47 ülke ilgili sözleşmeyi onaylamıştır. 7 ülke ilgili sözleşmeyi imzalamış fakat onaylamamıştır. Söz konusu sözleşme ile birlikte, internet ve ağ teknolojileri kaynaklı olarak işlenen çeşitli suç kategorileri detaylı olarak ele alınmıştır. Ayrıntılı bilgi için bkz. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, (02.04.2017).

Diğer yandan bu belgenin bir sonucu olarak, ABD Kongresi kamu ve özel sektörün siber güvenlik alanındaki faaliyetlerinin teşvik edilmesi ve desteklenmesi amacıyla, 2004 yılında 4,7 Milyar ABD Doları tutarındaki bir bütçeyi de onaylamıştır.[147]

1.3. Siber Uzay Politika Revizyonu

"Cyberspace Policy Review / Siber Uzay Politika Revizyonu", Başkan Obama'nın talimatıyla 2009 yılında hazırlanmış olan bir belge niteliğindedir. Bu belgede temel olarak, ABD siber savunma sisteminde görev alan resmi kurum ve kuruluşların, federal ve yerel düzeyde çok başlı yapısına eleştiride bulunularak, bu durumun giderilmesi için bazı tedbirlerin alınması gerektiği ve ulusal siber güvenlik sistematiğinin ancak bu kuruluşların birlikte ve eşgüdüm halinde hareket etmesi ile etkili olabileceği belirtilmektedir. Bu kapsamda, söz konusu çok başlı yapının giderilmesi amacıyla özetle:[148]

-Ulusal siber güvenlik politika ve faaliyetlerini koordine edecek olan bir görevlinin (Ulusal Siber Güvenlik Koordinatörü) atanması,

-Ulusal Siber Güvenlik Koordinatörü'nün kendi müstakil bir siber güvenlik direktörlüğüne sahip olması,

-Bu direktörlüğün siber güvenlik ile ilgili güncel gelişmeleri Başkan'a rapor halinde düzenli olarak sunması, kararlaştırılmıştır.

1.4. "Siber Uzay İçin Uluslararası Strateji: Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık" İsimli Doküman

"*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World / Siber Uzay İçin Uluslararası Strateji: Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık"* isimli doküman, dönemin ABD Başkan Obama'nın talimatıyla Mayıs 2011'de ABD ve dünya kamuoyuna ilan edilmiş olan ve ABD'nin uluslararası düzeyde ülkenin siber uzay alanındaki amaç ve hedeflerini ortaya koyan bir siber güvenlik strateji belgesidir.

---

[147]Ayrıntılı bilgi için bkz. https://www.us cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (16.01.2017).

[148]Ayrıntılı bilgi için bkz. NATO Cooperative Cyber Defense Centre of Excellence, **Cyberspace Policy Review**, https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf, (24.05.2016). Ayrıca bkz. https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_ Review_ final_0.pdf, (17.01.2017).

Bu belge ile ABD, enformasyon teknolojilerinin küresel düzeyde daha fazla ekonomik refah için teşvik edilmesi için çaba harcayacağını ve bu alanlarda uluslararası normların oluşturularak siber güvenliğin sağlanması gerektiğini bir dış politika hedefi olarak tespit ettiğini ilan etmektedir. Bu kapsamda ABD yönetimi gelecek dönemlerde; *"uluslararası düzeyde siber suçlarla mücadele için gerekli çabayı harcayacağını, internetin yaygınlaşmasını ve uluslararası işbirliği ile yönetilmesini destekleyeceğini, internet özgürlüğünün temel önceliği olduğunu ve ekonomik refah için enformasyon teknolojilerinin geliştirilmesin büyük önem arz ettiğini"* dünya kamuoyuna duyurmaktadır.[149]

Bu belgenin dış politika ve siber uzay ilişkisi kapsamında ele alınması halinde ise belgede ortaya konan hedeflerin Obama yönetiminin uluslararası ilişkilerde müzakere süreçlerine önem veren stratejisinin bir yansıması olduğu belirtilebilecektir. Söz konusu belgenin analizi bağlamında, Obama yönetiminin siber güvenlik alanında sert ve tekilci politikalar sürdürmeyi tercih eden George W. Bush'un yönetiminden farklı bir yaklaşımı benimsemiş olduğu da görülmektedir.

Öte yandan RF'nin 2007 Estonya'ya, 2008 yılında Gürcistan'a ve Litvanya'ya, 2009 yılında ise Kırgızistan'a yönelik siber saldırıları karşısında, ABD'nin bir caydırıcılık unsuru olarak ABD ordusu bünyesindeki Uzay Komutanlığı'nı, STRATCOM'a dönüştürdüğü ve bu komutanlığa siber savaşa komuta etme yetkisi verdiği, bu gelişmelerin devamında ise 2009 yılında STRATCOM'da, bir siber komutanlık kurulmasını kararlaştırdığı ve nihai olarak 2010 yılında da müstakil bir CYBERCOM'u tesis ettiği belirtilmelidir. Bu itibarla Obama yönetimi ılımlı bir üslupla hazırlanmış olan söz konusu strateji belgesi ile CYBERCOM'un aktiviteleri çerçevesinde siber uzayı domine etmeyi amaçlamadığını dünya kamuoyuna ilan etmek istemektedir. Diğer bir deyişle ABD, bu belge ile CYBERCOM'un olası faaliyetleri kapsamında uluslararası kamuoyunda duyulan rahatsızlığı dengelemeyi hedeflemektedir.[150]

[149]Ayrıntılı bilgi için bkz. NATO Cooperative Cyber Defense Centre of Excellence,**International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World**, https://ccdcoe.org/cyber-security-strategy-documents.html, (25.05.2016).

[150]NAKASHİMA Ellen, **Obama Administration Outlines International Strategy for Cyber Space**, https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html, (24.05.2016).

1.5. Kritik Altyapıların Geliştirilmesi İçin Taslak Plan

ABD'nin kritik altyapılarına yönelik artan siber tehditler karşısında, Obama yönetimi tarafından 12 Şubat 2013 tarihinde "*President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity / Kritik Altyapıların Geliştirilmesi)* başlıklı bir başkanlık direktifi yürürlüğe konmuştur.[151] Bu direktif doğrultusunda ise 12 Şubat 2014 tarihde *Draft Strategy for Improving Critical Infrastructure Cybersecurity / Kritik Altyapıların Geliştirilmesi İçin Taslak Plan)* isimli plan hazırlanmıştır. Bu planda özel sektör ile resmi kurumların işbirliği yaparak kritik altyapıların korunması noktasında ortak standart ve metodoloji geliştirilmeleri hedeflenmiştir.[152] Bu kapsamda da kritik altyapıları kontrol eden sanayi kuruluşları ile kamu otoritesinin aynı dili kullanması hedefi noktasında, bir çerçeve planlama hazırlanmıştır. Belirtilen çerçeve planlamaya göre olası siber saldırıların ortak standartlar dâhilinde, ilk olarak tanımlanması, daha sonra bu saldırılara karşı koruma sağlanması, yapılan tespit ile birlikte gerekli karşı reaksiyonun (cevabın) verilmesi ve olası zarar giderilerek, oluşan hasarın geri döndürülmesi aşamalandırılmıştır. Bu aşamaların ise oluşturulan bir çerçeve profil dahilinde pratiği sağlanmış metotlar ile uygulanması tesis edilmiştir.

Söz konusu planda da görüldüğü üzere, ABD'nin ekonomik refahı ve ülkesinin güvenliği açısından büyük öneme sahip olan ve temel olarak özel sanayi kuruluşları tarafından kontrol edilen kritik altyapılarını korumayı amaçlayan geniş kapsamlı bir planlamayı ihtiva etmektedir. Bu planlama ile birlikte, ABD'nde özel sektörün ve kamu otoritesinin ilk kez siber güvenlik alanında ortak bir standarda kavuşması ve bu alanda sanayi, akademi ve kamunun ortak bir platformda birlikte hareket etmesi hedeflenmiştir.[153]

1.6. Ulusal Güvenlik Stratejisi

Şubat 2015 tarihli *"National Security Strategy / Ulusal Güvenlik Stratejisi"* genel olarak ABD'nin gelecek dönem tehdit algılamaları ile güvenlik stratejisi kapsamında

---

[151]Ayrıntılı bilgi için bkz. NATO Cooperative Cyber Defense Centre of Excellence, **President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity**, https://ccdcoe.org/cyber-security-strategy-documents.html, (24.05.2016). Ayrıca bkz. https://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, (17.01.2017).
[152]Ayrıntılı bilgi için bkz. NATO Cooperative Cyber Defense Centre of Excellence, **Draft Strategy for Improving Critical Infrastructure Cyber Security**, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, (24.05.2016).
[153]Ibid.

alacağı tedbirler hakkında bilgiler sunmakla birlikte, belgenin birçok bölümünde siber güvenlik kavramına ilişkin değerlendirme ve öneriler de mevcuttur. Bu değerlendirme ve öneriler ise özetle:[154]

-RF'nin artan siber gücünün ve siber meydan okumalarının ABD'nin güvenliği için ciddi tehdit oluşturduğu,

-ÇHC'nin özellikle siber casusluk faaliyetleri noktasında ABD için tehdit yarattığı, bu nedenle de ABD'nin teknolojik yeniliklerini ve özel sektörünün ticari çıkarlarını korumak için gerekli tedbirleri alacağı,

-ABD'nin ortaya koyduğu girişimler ile birlikte, küresel düzeyde siber güvenlik standartlarının belirlenmesine yönelik çabalarını artırarak sürdüreceği,

-ABD için, çeşitli aktörlerden kaynaklanan siber casusluk faaliyetlerinin artan bir tehlike olduğu, bu kapsamda da ilgili ABD kurumlarının tedbirler geliştirmeye devam edeceği,

-İklim değişikliği, salgın hastalıklar, kıtalararası suç ve terör faaliyetleri ile birlikte, siber suçların da ABD'nin yeni dönemde karşılaşacağı tehditler arasında yer aldığı, Bu çerçevede, ABD Silahlı Kuvvetleri'nin, ilgili güvenlik ve istihbarat kurumlarının tedbirlerini sıkılaştırmasının şart olduğu,

-Siber uzayın ve okyanusların küresel düzeyde ortak kullanım alanları olduğu, bu alanların mal ve hizmetlerin, fikirlerin, girişimcilerin ve sermayenin serbest dolaşımının sağlanması noktasında güvenli ve özgür olması gerektiği, Bu kapsamda da ABD'nin söz konusu serbestlik imkânlarını sağlamak için her türlü tedbiri alacağı,

-ABD'nin müttefik ülkelerin istikrarını bozmayı hedefleyen siber saldırlara karşı, ilgili ülkelere tam destek vereceği, hususları belirtilmektedir.

Bahse konu değerlendirme ve öneriler arasında, ABD'nin RF'nin ve ÇHC'nin siber tehdit yaratma kapasitesine yaptığı vurgu, ABD'nin gelecek dönem siber güvenlik stratejisinin şekillenmesi bakımından oldukça önemli görülmelidir. Bu noktada ilgili belgede, ABD, ÇHC'yi dar bir kapsamda siber casusluk açısından hedef göstermekte, RF'yi ise çok daha geniş bir değerlendirme ile birlikte ülkesi için açık bir siber tehdit

[154]Ayrıntılı bilgi için bkz. NATO Cooperative Cyber Defense Centre of Excellence, **National Security Strategy**, https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf, (25.05.2016).

olarak kabul etmektedir. Bu itibarla da söz konusu belgede yer alan *"Rusya'nın artan siber gücünün ve siber meydan okumalarının ABD'nin güvenliği karşısında ciddi tehdit oluşturduğu*" ve Rusya'nın komşusu ülkelere yönelik olarak yaptığı siber saldırıları da işaret edecek şekilde, *"ABD'nin müttefik ülkelerin istikrarını bozmayı hedefleyen siber saldırlara karşı, ilgili ülkelere her türlü desteği vereceği*", ifadelerinin dikkat çekici olduğu belirtilmelidir.[155]

1.7. "ABD Savunma Bakanlığı Siber Stratejisi" İsimli Belge

"The Department of Defence Cyber Strategy / ABD Savunma Bakanlığı Siber Strateji" isimli belge, 23 Nisan 2015 tarihinde kabul edilmiştir. Bu belge ABD'nin ilan ettiği son resmi siber güvenlik stratejisi dokümanı niteliğindedir. ABD Savunma Bakanlığı bu belgenin kabul edilmesi amacını, ABD siber savunma ve ulusal siber güçlerinin faaliyetlerine rehberlik etmek olarak açıklamıştır. Söz konusu belge ile ABD Silahlı Kuvvetleri'ne:

-ABD ağ teknoloji ve sistemleri ile gizli siber bilgilerini savunma,

-Siber ataklara karşı ABD çıkarlarını koruma,

-Askeri ve gizli siber operasyonları planlama ve bu tür operasyonlara rehberlik etme, görevleri verilmiştir.[156]

Bu belgenin kabul edilmiş olması, ABD'nin operasyonel bir siber güç olma yönündeki iradesini dünya kamuoyuna ilan etmesi bakımından oldukça önemlidir. Bu nedenle de bahse konu stratejinin geniş bir persfektik ile hazırlandığı ileri sürülebilir.

Zira söz konusu strateji belgesinde, RF ve ÇHC'nin oldukça ileri bir siber kapasite ve strateji geliştirmiş oldukları vurgulanmaktadır. Bu kapsamda, RF'nin siber gücü: *"tespiti ve deşifresi oldukça zor"* şeklinde bir ifade ile tanımlanmaktadır. ÇHC ise ulusal şirketlerinin ticari çıkarları kapsamında ABD'nin entelektüel varlığını çalmaya yönelik siber casusluk operasyonları planlamakla suçlanmaktadır. Bu belge, ÇHC ve RF'nin yanı

[155] Ibid.
[156]NATO Cooperative Cyber Defense Centre of Excellence, **The Department of Defence Cyber Strategy**,http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, (25.05.2016). Ayrıntılı bilgi için bkz.http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_ 2015.pdf, (15.04.2017).

sıra İran ve Kuzey Kore'de sınırlı siber kapasiteye sahip ülkeler olmakla birlikte, ABD siber savunması için tedbir alınması gereken aktörler olarak ifadelendirilmektedir.[157]

Görüldüğü üzere Şubat 2015'de yürürlüğe giren *"Ulusal Güvenlik Stratejisi"* ile Nisan 2015'te kabul edilen "*Savunma Bakanlığı Siber Stratejisi*" isimli dokümanlarda ABD, açıkça RF ve ÇHC'nin siber kapasitelerini ülkesine yönelik bir tehdit odağı olarak değerlendirmiştir. Bu gelişmeye tepki olarak ise 2015 Mayıs ayında ÇHC ve RF arasında siber güvenlik alanın siber işbirliği yapılması noktasında ortak niyet beyanın da bulunulmuştur. Bu ortak niyet beyanı ile birlikte RF ve ÇHC, birbirlerine karşı siber saldırılar gerçekleştirmeme, siber uzay teknolojileri konusunda eğitim ve teknoloji transferi konusunda işbirliği geliştirme, iki ülkenin iç politik yapısını ve sosyo-ekonomik atmosferini bozmayı hedefleyen siber saldırılara karşı ortak tedbir alma, siber uzayın denetleyen uluslararası bir rejim tesis etme yönünde uluslararası örgütler nezdinde ortak hareket etme hususlarında iyi niyetli politikalar izleyeceklerini ilan etmişlerdir.[158] Bu kapsamda, bahse konu gelişmeler ile RF ve ÇHC'nin, siber uzayda temel aktör konumuna gelmek istediğini iddia ettikleri ABD'ye karşı ortak bir duruş sergilemeyi ve siber uzayda ABD'nin başat devlet olmasını engellemeyi amaçladıkları da ileri sürülebilecektir.

Ayrıca bu belgede ABD'nin Ortadoğu ve Asya-Pasifik bölgesinde yer alan müttefikleri ile NATO üyelerine yönelik siber tehditler karşısında, müttefiklerine yardım edeceği açıkça ilan edilmektedir. Bahse konu vurgunun ise ABD'nin RF'nin sorun yaşadığı komşu ülkelere yönelik olarak gerçekleştirdiği siber saldırılarına yönelik bir mesaj olarak değerlendirilebileceği de belirtilmelidir.[159]

Aktardığımız bu bilgilerden de anlaşılacağı üzere siber uzayın uluslararası sistemde ki hegemon devletlerce yeni bir mücadele alanı olarak okunduğu açıktır. Bu alan özellikle ABD ve RF tarafından askeri güçlerini geliştirme noktasında yeni fırsatlar yaratan bir mecra olarak görülmektedir. Bahse konu ABD resmi belgeleri dâhilindeki tespitlerimizde de yer aldığı haliyle ABD'nin veya RF'nin siber kapasitesini geliştirme adına aldığı her tedbir veya plan bir etki-tepki ilişkisi içerisinde karşı bir hamle ile cevap bulabilmektedir. Bu durum neo-realist teorinin devletlerarasındaki rekabete ilişkin paradigmaları ile de

[157]Ibid.
[158]RAZUMOVSKAYA, loc.cit.
[159]ZHENG E. Denise, **2015 DOD Cyber Strategy-Center for Strategic&International Studies**, https://www.csis.org/people/denise-e-zheng, (25.05.2016).

paralellik arz etmektedir. Zira siber uzay merkezli teknolojik gelişmelerin, devletlerin askeri güç yapısını değiştirdiği ve ortaya çıkan yeni koşullar kapsamında RF ve ABD arasındaki siber mücadele de müşahede edildiği üzere devletleri birbirleriyle rekabete zorladığı açıktır.

Bu noktada günümüz ağ teknolojileri merkezli gelişmeleri ortaya çıkaran motivasyonun, Soğuk Savaş döneminden bu yana süregelen ABD ve RF arasındaki askeri rekabetten kaynaklandığı da hatırlanmalıdır. Bu rekabet hali halen devam etmektedir ve ağ teknolojilerinde yaşanan sofistike gelişmeleri teşvik etmektedir. Bu kapsamda ABD ve RF'nin siber güçlerini arttırma yönündeki her girişimi, askeri kapasitelerini dolayısıyla da uluslararası sistemdeki güçlerini artırma çabalarının bir parçası olarak değerlendirilmelidir.[160] Kısacası ağ teknolojilerinde devam etmekte olan hızlı değişim ve gelişim, uluslararası sistemdeki devletlerarasındaki geleneksel rekabet ve çatışmanın ayrılmaz bir parçası olarak süregelmektedir.

1.8. ABD'nin Siber Güvenlik Kapsamındaki Resmi Plan, Belge, Strateji, Doktrin ve Başkanlık Emirlerine İlişkin Genel Değerlendirmeler

ABD'nin federal sistemi, bu sistemden kaynaklanan birbirinden bağımsız karar mekanizmalarının varlığı, siber güvenlik alanında faaliyet gösteren kurum ve kuruluş sayısının fazlalığı, iktidara gelen yönetimlerin yıllar içinde değişen politika öncelikleri, görece olarak daha açık yönetim yapısı nedenleriyle, ABD'nin RF'ye kıyasla 1990'ların ikinci yarısından itibaren siber güvenlik alanı ile ilgili olarak çok sayıda resmi plan, belge, strateji, doktrin ve başkanlık emri ortaya koyduğu görülmektedir. Bu itibarla da söz konusu resmi belgelerin önemli ve süreçleri belirleyici olanları bu çalışmada analize tabi tutulmuştur.

Bu belgeler ile ilgili olarak ABD başkanlarını da dikkate alarak; Bill Clinton'un başkanlık dönemine denk gelen 1993-2001 yılları arasında yayımlanan dokümanlarda, kritik altyapıların korunması, uluslararası siber suç ile mücadele ve bu konuda devletler arasında işbirliği hususlarına vurgu yapıldığı açıkça görülebilecektir.

[160]Ayrıntılı bilgi için bkz. ERIKSSON Johan ve GIACOMELLO Giampiero, "The Information Revolution, Security, and International Relations: (IR) RelevantTheory?", **International PoliticalScienceReview**, Vol.27, No.3, 2006, pp. 221-244.

Başkan George W. Bush'un iktidarda olduğu 2001–2009 yılları için ise ilk olarak 2000-2001 arasında ABD'nin özellikle Asya-Pasifik alanında ÇHC ve Tayvan arasındaki siber mücadelenin de etkisiyle siber güvenlik alanına ilişkin olarak, bu alanı militarize eden ve daha fazla askeri anlam yükleyen belgeler ortaya koyduğu tespit edilebilir. 11 Eylül sonrasında ise ABD'nin kendisini küresel terör ile bir savaş ortamında kabul etmesinden ötürü, siber güvenlik strateji belgelerinde de siber uzayın ABD askeri gücüne destek sağlayan ve bu gücü pekiştiren bir alan olduğu hususu gündeme getirilmiştir.

2009 sonrasında Obama iktidarında yayımlanan dokümanlarda ise siber güvenlik alanı görece olarak daha ılımlı bir üslupla ve kritik altyapıların korunması, ABD siber savunma sisteminin merkezileştirilmesi, siber casusluk faaliyetlerine karşı konulması, siber uzayda küresel işbirliğinin sağlanması, siber suçlarla mücadele edilmesi, siber farkındalığın ulusal ve uluslararası düzeyde sağlanması gibi önceliklerle hazırlandığı görülmektedir.[161]

Siber güvenliğin arttırılması konusunda hassas olan Obama yönetiminin talimatlarıyla; ağ güvenliğinin sağlanması, tehditlerin engellenmesi konusunda devlet, hükümet ve özel sektör ortaklarının, ortak bir durumsal farkındalık yaratması ve tehditlere karşı acil savunma cephesi kurulması için mevcut güvenlik açıklarının azaltılması, izinsiz erişimin engellenmesi için hızlı hareket edilmesi hususlarında önemli ilerlemeler kaydedilmiştir.[162]

ABD'nin siber güvenlik stratejisinin tüm detayları ile anlaşılabilmesi için, belirtilen plan ve stratejileri uygulamakla görevli ABD'nin resmi kurum ve kuruluşlarının görev, yetki ve sorumluluklarının analiz edilmesinin de çalışmamıza katkı sağlayacağı düşünülmektedir.

2. ABD'nin Siber Güvenlik Alanında Faaliyet Gösteren Resmi Kurum ve Kuruluşları

ABD'nin resmi siber organizasyonu oldukça karmaşık bir yapıya sahiptir. Daha önce belirtildiği üzere bu karmaşık yapı ABD'nin federatif yönetim anlayışı ile şekillenen adem-i merkeziyetçi idare şekliyle doğrudan ilintilidir. ABD'nin resmi siber organizasyonu

[161]BISSON David, **A Cyber Study of the U.S. National Security Strategy Reports**, http://www.Tripwire .com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports/, (25.05.2016).
[162] KARA, op. cit., s. 60.

temelde: "ABD Savunma Bakanlığı (United States Department of Defense), ABD İç Güvenlik Bakanlığı (The Department of Homeland Security) ve ABD Gizli Servisleri (FBI / CIA)" şeklinde üçlü bir yapıya sahiptir.

Bunun dışında, bazı resmi kurumların kendi görev sahalarına yönelik olarak yetki ve sorumlulukları da bulunmaktadır. Ayrıca, eyalet yönetimleri, ulusal siber güvenlik ağı haricinde, kendi siber güvenliklerini sağlamak amacıyla çeşitli yapılanmalar da kurarak, bu yapılardan aktif olarak istifade etmeyi de tercih etmektedirler.[163]

2.1. ABD Savunma Bakanlığı (United States Department of Defense)

ABD Savunma Bakanlığı, ABD Silahlı Kuvvetleri'nden sorumlu olan bakanlıktır. 18 Eylül 1947 tarihinde oluşturulmuştur ve karargâhı ABD'nin başkenti Washington DC'de bulunan Pentagon'dur. Pentagon, ABD'nin Savunma Bakanlığı ve Genelkurmay Başkanlığı'nın genel adıdır. Savunma Bakanlığı'ndan sorumlu kişilere "Savunma Bakanı (Secretary of Defense)"denmektedir. Savunma Bakanı, Başkan'a karşı doğrudan sorumludur. Savunma Bakanlığı, Kara Kuvvetleri Dairesi'nden (The Department of the Army), Deniz Kuvvetleri Dairesi'nden (The Department of the Navy), ABD Hava Kuvvetleri Dairesi'nden (The Department of the Air Force), Ulusal Güvenlik Teşkilatı'ndan (The National Security Agency) ve ABD Savunma İstihbarat Teşkilatı'ndan (The Defense Intelligence Agency) oluşmaktadır.[164]

Savunma Bakanlığı, ABD'nin siber güvenlik stratejisinin uygulanmasında etkin bir role sahiptir. Savunma Bakanlığı bünyesinde siber güvenlik alanında en etkili rolü, STRATCOM bünyesinde faaliyet gösteren ve 2010 yılında kurulan CYBERCOM üstlenmektedir.[165] CYBERCOM mevcut siber kaynaklarını düzenler ve ABD askeri bilgisayar ağları müdafaasını eşzamanlı bir hale getirir. Bünyesinde: *"24. Hava Kuvvetleri, Ordu Siber Savaş Birimi, Donanma Siber Savaş Birimi, Deniz Kuvvetleri Siber Savaş Birimi*"[166] şeklinde yapılanmalar mevcuttur.

CYBERCOM aktif olarak faaliyete geçmeden çok daha önce, 1990'ların başı itibarıyla de ABD Ordusu kısmi siber saldırı kapasitene sahip olmuştur. Bu kısmi saldırı

[163]TIRRELL, op. cit., p. 55.
[164] United States Department of Defense, **About the Department of Defense (DoD)**", http://www.defense.gov/About-DoD, (30.05.2016).
[165] YAYLA, op. cit., s. 186.
[166] TIRRELL, op. cit., p. 57.

kapasitesi ise ilk defa bir savaş ortamında, başarılı bir şekilde ve geniş bir askeri planlamanın etkili bir elementi olarak 1990 yılındaki 1. Körfez Savaşı esnasında kullanılmıştır. Savaş başlamadan önce dünyanın 5. en büyük kara ordusuna sahip Irak Silahlı Kuvvetleri'nin, kara, deniz ve hava unsurları arasındaki koordinasyon ABD Ordusu'nun siber saldırıları ile engellenmiştir. Bu kapsamda ABD Ordusu telsiz frekansı tespit donanımlarıyla yüklü helikopterleri Irak sınırı boyunca güvenli alanlarda mobilize ederek, Irak Ordusu'nun telsiz frekanslarını karıştırmış, karıştırmakla da kalmayarak kriptolu bu frekanslara sızmak suretiyle Irak Ordusu unsurlarını yanlış yönlendirmiştir.[167] Söz konusu başarılı siber saldırı faaliyeti ile kazanılan tecrübe, günümüzdeki CYBERCOM operasyonlarının da temelini teşkil etmiştir.

Daha sonra 1990 yılında NATO'nun Kosova müdahalesi ile başlayan süreç dahilinde Rus ve Çinli hackerların destek verdiği Sırp hackerların NATO ve NATO üyesi devletlerin internet erişimlerine ve e-posta trafiğini hedef alan saldırıları, ABD Ordusu'nun siber savunma kapasitesini geliştirme konusundaki çalışmalarına hız vermesine neden olmuştur.[168]

2003 yılındaki 2. Körfez Savaşı esnasında da 1. Körfez Savaşı döneminde olduğu gibi ABD Silahlı Kuvvetleri mevcut siber saldırı kapasitesi imkânlarından istifade etmeye çalışmıştır. Söz konusu siber saldırı kapasitesi Irak Ordusu'nun haberleşme sistemlerinin etkisizleştirilmesinin yanı siber propaganda faaliyetlerini de içermiştir. Irak Ordusu'nun kriptolu haberleşme sistemlerine sızılarak Iraklı subayları hedefleyen moral bozucu ve teslim olmaya davet edici mesajlar oldukça etkili olmuştur.[169]

2013 yılında ise internet üzerinden gelen tehdit boyutunun artmasıyla birlikte, CYBERCOM tarafından siber savaşçılarının sayısını artırma yoluna gidilmiştir. Bu kapsamda, CYBERCOM tarafından 5.000'e çıkarılan siber savaşçı kadrosuyla adeta yeni bir yapılanma oluşturmuştur. Küresel avantaj sağlamak için profesyonel bir ekip oluşturmayı hedefleyen CYBERCOM'un, ABD Ordu ağını savunmak ve siber savaş

[167] CLARKE A. Richard ve KANKE K. Robert, **Siber Savaş**, çeviren Murat ERDURAN, İstanbul Kültür Üniversitesi Yayınları, İstanbul, s.8, 2011.
[168]KARA Mahruze, **Siber Saldırılar- Siber Savaşlar ve Etkileri**, Yüksek Lisans Tezi, İstanbul BilgiÜniversitesi SBE Bilişim ve Teknolojis Hukuku Yüksek Lisans Programı, 2013,http://openaccess.bilgi.edu.tr:8080/xmlui/bitstream/handle/11411/346/Siber%20Sald%C4%B1r%C4%B1lar%20Siber%20Sava%C5%9Flar%20ve%20Etkileri.pdf?sequence=2&isAllowed=y, (17.02.2017), s. 44
[169]CLARKE ve KANKE, loc.cit.

mücadele etkisini artırmak için personel sayısını sayıyı 21.000kişiyi çıkarmayı planladığı ileri sürülmektedir.[170]

Tahmin edileceği üzer CYBERCOM'un güncel olarak sürdürmekte olduğu görevler ve operasyonlar ile ilgili olarak ise sınırlı açık kaynak bilgisi bulunmaktadır. Bu bilgilerden en önemlisi olan ve CYBERCOM'un sahip olduğu operasyonel kapasite hakkında bilgi veren gelişme ise 29 Nisan 2016 tarihi itibarıyla IŞİD'ın Irak ve Suriye'deki unsurlarına yönelik olarak başlattığı gündeme gelen siber savaş harekâtı ile ilgilidir. Söz konusu operasyon ile ilgili olarak Pentagon: *"hedefin terör örgütünün internet ve iletişim bağlantılarını çökertmek ve IŞİD'i sanal izolasyona sürüklemek olduğunu"* açıklamıştır. ABD Savunma Bakanı Ashton Carter gelişmeyi: *"CYBERCOM'un Irak ve Suriye'de ABD öncülüğünde yürütülen operasyonlarda önemli rol oynadığını"* belirterek, *"internet harekâtını CYBERCOM'un ilk büyük muharip operasyonu"* olarak nitelendirmiştir. Ayrıca Carter operasyonun hedefini: *"IŞİD'in komuta ve kontrol zincirini kesintiye uğratmak, para dolaşımını engellemek, nüfus üzerindeki kontrol gücünü sekteye uğratmak ve dışarıdan savaşçı edinme becerisini yok etmek"* olarak açıklamıştır. Amerikan Savunma Bakanı, konuyla ilgili olarak: *"Onları bombalıyoruz ve interneti de ellerinden alacağız"* şeklinde bir beyanda da bulunmuştur.[171]

ABD Savunma Bakanlığı bünyesinde siber güvenlik alanında faaliyet gösteren bir diğer kuruluş ise adı "Edward Snowden Olayı" kapsamında dünya kamuoyunda oldukça sık gündeme gelen Ulusal Güvenlik Ajansı (National Security Agency / NSA)'dır. NSA, 04 Kasım 1952 tarihinde kurulmuştur. NSA, ABD'nin küresel izleme, şifre çözme, veri toplama, veri analizi, sinyal toplama, çeviri ve yabancı istihbaratlara karşı istihbarat yapma amaçları için tesis ettiği istihbarat kuruluşu ve örgütüdür. NSA, ABD'nin ağ savaşları kapsamındaki haberleşme ve bilgi veri sistemlerinin korunmasından da sorumludur.[172] NSA'nın elektronik sistemleri dinlemek için edindiği misyonunu, gizli yöntemler ve subversif yazılım araçları ile sistemleri sabote edecek şekilde kullandığı da iddia edilmektedir.

---

[170] Reuters, **Obama Budget Makes Cybersecurity Growing U.S. Priarity**, http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411, (17.02.2017).

[171] National Public Radio (NPR), **In Fight Against ISIS, U.S. Adds Cyber Tools**http://www.npr.org/2016/02/28/468446138/in-fight-against-isis-u-s-adds-cyber-tools, (19.04.2017).

[172] National Security Agency, **60 Years of Defending Our Nation**, http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf, (30.05.2016).

NSA'nın personel sayısının 30–40 bin kadar olduğu ileri sürülmektedir. Bütçesi de çalışan sayısı gibi gizli tutulmaktadır. Ancak 2013 yılındaki bütçesinin 10,8 milyar dolar olduğu tahmin edilmektedir.[173] NSA, ABD Ordusu ve diğer istihbarat servisleri için kriptanaliz desteği de sağlamaktadır. Söz konusu destek verilmeden, ABD gizli servislerinin operasyonel çalışma planlamaları yasa ile önlenmiştir. 1972 yılında, NSA'nın diğer istihbarat servisleri ile arasındaki işbirliğinin kolaylaştırmak amacıyla Merkezi Güvenlik Servisi (National Security Servise / CSS) isimli organizasyon kurulmuştur.[174] NSA'nın başkanlığını yürüten NSA Direktörü, ayrıca CYBERCOM komutanı ve CSS'nin şefi olarak da görev yapmaktadır.

NSA'nın bilgi toplamak için internet, telefon görüşmeleri ve e-postaları da izlemektedir. "Edward Snowden Olayı" kapsamında, yeryüzündeki en büyük telefon ve e-posta iletişim arşivinin bu ajansa ait olduğu iddia edilmiştir. Bu olay ile ayrıca NSA'nın elindeki güç ve yetkiyi, yasal dayanak olmaksızın ABD'de mukim sivillerin telefon görüşmelerini takip etmek, bununla birlikte dünya genelinde siber casusluk operasyonları planlamak amacıyla kullandığı da gündeme gelmiştir.[175] Bu iddialar, çalışmamızda Edward Snowden Olayı'nın ele alınacağı ayrı bir başlık altında detaylıca analiz edilecektir.

Söz konusu kuruluşların yanı sıra Savunma Bakanlığı bünyesindeki Kara, Deniz ve Hava Kuvvetleri Daireleri'nde her biri kendi görev ve sorumluluk alanı ile ilgili olarak faaliyet ve eşgüdüm görevi ifa eden birer Birleşik Siber Merkezi (Joint Cyber Center/ JCC) isimli organizasyonları da mevcuttur.[176]

ABD'nin siber güvenlik alanında çeşitli iç yasalar düzenlemeler ile daha geniş kapsamlı askeri strateji belgeleri bulunmaktadır. Bahse konu geniş kapsamlı belgelerden ilki, 2006 yılında kabul edilen "*The National Military Strategy for Cyberspace Operations / Siber Operasyonlar İçin Ulusal Askeri Strateji*" isimli dokümandır. Bu dokümanda ABD Ordusu'nun ulusal çıkarları korumak amacıyla siber uzayda faaliyet yürütmesi gerektiği

[173]BARTON Gellman ve MILLER Greg, **U.S. Spy Network's Successes, Failures and Objectives Detailed in 'Black Budget' Summary**". The Washington Post, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html, (30.05.2016).
[174]National Security Agency, **The Creation of NSA**, https://archive.org/stream/The_Creation_of_NSA _Part_3-nsa/The_Creation_of_NSA_Part_3_djvu.txt, (30.05.2016).
[175]Ayrıntılı bilgi için bkz. SEZGİN Fatih, Edward Snowden Olayı'nın ABD-Rusya İlişkileri Üzerindeki Etkileri, **Journal of International Management and Social Researches Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi**, http://dergipark.ulakbim.gov.tr/uysad/article/view/5000108153/5000100862, (30.05.2016), ss. 1-8.
[176]TIRRELL, op. cit., p. 57.

açıkça belirtilmekte ve siber uzay ulusal çıkarların sağlanması noktasında askeri ve istihbarat operasyonlarının yapılabileceği bir alan olarak tanımlanmaktadır.[177] Diğer belge ise "*The National Military Strategy of the United States of America / ABD Ulusal Askeri Stratejisi"* isimli dokümandır. Bu dokümanda siber uzay kendi özel şartlarına sahip bir çatışma alanı olarak tanımlanmaktadır. Söz konusu belge de ayrıca, ABD Ordusu'nun siber uzayda caydırıcı bir güce sahip olması gerektiği, bu alan kaynaklı tehditlerin engellenmesini hedefleyen ve ülkenin kritik altyapılarını korumayı amaçlayan planlamalar geliştirmesinin şart olduğu ifade edilmektedir.[178]

2.2. ABD İç Güvenlik Bakanlığı (The Department of Homeland Security)

ABD İç Güvenlik Bakanlığı (United States Department of Homeland Security / DHS), 11 Eylül 2001 saldırılarından sonra kurulan ve ülkede terörle mücadele konusunda asıl görevli olan devlet kurumudur. ABD Kongresi tarafından 2002 yılında çıkartılan "Kamu Güvenlik Yasası" ile kurulmuştur. Bu kanun, ABD İç Güvenlik Bakanlığı'nın da kurucu belgesidir.[179] ABD İç Güvenlik Bakanı (The Secretary), Bakanlığın başı olup (Head Of Department), Bakanlık üzerinde yönetim, yetki ve denetim gücünü elinde bulundurmaktadır. Bakanlığın bütün örgütsel birimlerinin, yöneticilerinin ve çalışanlarının, bütün işlevleri Bakan'ın himayesindedir.

Diğer yandan söz konusu kanuna göre İç Güvenlik (Homeland Security); *"ABD içinde gerçekleşmesi muhtemel terörist saldırıları önlemek, Amerika'nın terörizm konusundaki güvenlik açıklarını (kırılganlıklarını) azaltmak, saldırı olduğunda ise bu saldırıdan dolayı meydana gelen zararları azaltmak ve en kısa sürede onarmak için ulusal imkân ve çabaları bir araya getirmek*" şeklinde tanımlanmaktadır. ABD İç Güvenlik Bakanlığı'nın siber güvenlik alanındaki amaçları ise: *"kritik altyapıları korumak, kritik öneme haiz altyapı yatırımlarını ve hayati öneme haiz kaynaklarının direncini*

[177]Ayrıntılı bilgi için bkz. The Joint Chiefs of Staff (JCS), **The National Military Strategy for Cyberspace Operations**, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, (20.02.2017).
[178]Ayrıntılı bilgi için bkz. United States Department of Defense, **Sustaining U.S. Global Leadership: Priorities for 21st Century Defense**, http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf>, (20.02.2017).
[179]BAŞA Şafak, **ABD İç Güvenlik Bakanlığı**, http://www.academia.edu/9830086/ABD_%C4%B0%C3%87_G%C3%9CVENL%C4%B0K_BAKANLI%C4%9EI_SUNUM_, (31.05.2016).

güçlendirmek, hükümetin iletişimini ve operasyonel gücünün devamlılığının sağlamak, ulusal siber güvenlik şartlarını ilerletmek" olarak belirlenmiştir.[180]

ABD İç Güvenlik Bakanlığı organizasyon şeması ele alındığında, ülke genelinde 7/24 esasına göre bir füzyon merkezi olarak görev ifa eden Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (National Cybersecurity and Communications Integration Center / NICIC)'nin siber güvenlik alanındaki temel sorumlu birim olduğu görülmektedir. Bu merkez federal, eyalet ve diğer yerel birimler nezdinde ülke genelinde meydana gelen siber olayları izleyerek, bu olaylara anında cevap vermekten sorumludur. Ayrıca NICIC görevi kapsamında, ilgili güvenlik ve istihbarat birimleri ile özel sektör arasında eşgüdüm ve uyumu tesis eder.[181]

Bu noktada ABD'de kamu-güvenlik-istihbarat örgütleri ve özel sektör arasında siber güvenlik alanındaki işbirliği yapısından da bahsetmek gerekmektedir. ABD'de kamu ve özel sektör arasındaki işbirliği, Kıta Avrupa'sı sisteminin tersine özel sektör için zorunluluk ihtiva eden bir durum değildir ve gönüllülük esasına göre işleyen bir sistem olarak tesis edilmiştir. [182]

ABD İç Güvenlik Bakanlığı bünyesinde siber güvenlik alanında görev yürüten diğer birimler ise Bilgisayar Acil Müdahale Hazır Ekibi (Computer Emergency Readiness Team / US-CERT) ve Sanayi Kontrol Sistemleri Bilgisayar Acil Müdahale Hazır Ekibi (Industrial Control System Computer Readiness Team / ICS-CERT)'dir. Bu takımlar ve servisler 7/24 esasına göre, ülke genelindeki siber saldırıları takip eden operasyonel birimler şeklinde organize edilmiştir ve görevleri ile ilgili olarak "Ulusal Siber Güvenlik Birimi (National Cyber Security Division/ NCSD)'ne karşı sorumludur. Ayrıca ABD İç Güvenlik Bakanlığı bünyesinde "Gelişmiş Siber Güvenlik Servisleri (Enhanced Cybersecurity Services / ECS) şeklinde örgütlenmiş birimler de bulunmaktadır ve bu birimler siber güvenlik alanında özel sektör ile bilgi paylaşımı süreçlerini koordine etmekten sorumlu olacak şekilde planlanmışlardır. Diğer yandan NICIC ve NCSD görevleri ile ilgili olarak, ABD İç Güvenlik Bakanlığı Ulusal Koruma ve Programlar

[180]Ibid.
[181]TIRRELL, op. cit., p. 58.
[182]Ayrıntılı bilgiiçin bkz. NATO Cooperative Cyber Defense Centre of Excellence, **National Cyber Security Organisation in United States**, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf, (20.02.2017), pp. 24-25.

Direktörü'ne bağlıdırlar ve bu iki birimin birlikte hareket etmeleri ve koordinasyonda bulunmaları da ilgili direktörün sorumluluğundadır.[183]

ABD İç Güvenlik Bakanlığı, ABD siber savunma planlamasının şekillenmesinde, önemli bir eşgüdüm merkezi olarak da görev yapar. Bu itibarla ABD İç Güvenlik Bakanlığı, istihbarat ve güvenlik servisleri ile gelecek dönemde meydana gelmesi muhtemel siber saldırıların mahiyeti, kaynağı ve organizasyonu ile ilgili duyumlarını paylaşmak, ABD Savunma Bakanlığı ile ülkenin ulusal siber güvenlik savunma sistematiğini geliştirmek, ABD Adalet Bakanlığı (United States Department of Justice) ile ABD'ye yönelik siber saldırıların faillerinin tespiti ve yargılanması sürecinde hukuki destek sağlamak ile sorumludur.[184]

ABD İç Güvenlik Bakanlığı'nın ülke genelinde siber güvenliğin sağlanması amacına yönelik olarak etkin bir şekilde kullandığı sistemin adı ise Ulusal Siber Güvenlik Koruma Sistemi (National Cybersecurity Protection System / NCPS)'dir.[185] NCPS, bir zorlama uygulama olarak, federal ağ sistemindeki siber saldırıları tespit ederek, etkisizleştirmek amacıyla sistemin partnerlerine NICIC ve NCSD uzmanları ile bilgi paylaşımı ve koordinasyon noktasında kanuni sorumluluklar yüklemektedir. NCPS'nin etkinleştirilmesini sağlamak amacıyla da "EINSTEIN" adı verilen bir yazılım kullanılmaktadır ve bu yazılım eksikleri ortaya çıkan yeni durumlar kapsamında sürekli olarak teste tabi tutulmaktadır. Böylelikle de bu yazılımın her seferinde daha sıkı kontrol unsurları getiren ve yenilenen üç yeni versiyonu bugüne kadar geliştirilmiştir.[186]

ABD İç Güvenlik Bakanlığı'nın faaliyetleri sıklıkla ABD kamuoyunda tartışma konusu olabilmektedir. Bu tartışmaların temel odak noktası ise ABD İç Güvenlik Bakanlığı'nın George W. Bush yönetimi tarafından 11 Eylül sonrasında oluşan gergin güvenlik ikliminden de istifade edilerek kurulmuş olması ve bu bakanlığın görev ve yetkilerinin oldukça geniş bir şekilde düzenlenmesidir. ABD İç Güvenlik Bakanlığı'nın siber güvenlik alanındaki çalışmaları ile görev ve sorumlulukları da söz konusu tartışma

[183]Ibid., p. 60.
[184]Department of Homeland Security, **National Cybersecurity and Communications Integration Center**, https://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2012-04-30%20Spring%20Conference-Meeting/2%20Lichtenfels%20DHS%20NCCIC%202.pdf, (31.05.2016).
[185]Ayrıntılı bilgi için bkz. Committee on Homeland Security and Governmental Affairs, **A Review of the Department of Homeland Security's Missions and Performance**, https://www.google.com.tr/?gfe_rd=cr&ei=v9RlWb4NNGv8wev6rvQBg#q=A+Review+of+the+Department+of+Homeland+Security%E2%80%99s+Missions +and+Performance, (31.05.2016), pp. 82-85.
[186]Ayrıntılı bilgi için bkz. Ibid., pp. 85-87.

sürecinin en önemli konusudur. Bu itibarla, ABD'de bulunan kimi siber güvenlik uzmanları ve siyasetçiler, ABD İç Güvenlik Bakanlığı'nın siber güvenlik alanındaki çalışmalarını; sadece siber saldırıların etkisini azaltmaya odaklanmış olması, caydırıcılık faktörünü göz ardı etmesi, ayrıca bu faaliyetlerin bugüne kadar önemli hasar yaratan kimi siber saldırıları engelleyememiş olması kapsamında eleştirmektedirler. Ayrıca bu çevreler, ABD İç Güvenlik Bakanlığı'nın bireylerin ve özel ticari şirketlerin iletişim bilgileri üzerindeki geniş denetim ve yetkisi ile Bakanlığın siber savunma bütçesinin yıllık 750 milyon ABD Doları tutarına ulaşmış olmasını da bir başka eleştiri konusu olarak gündeme getirmektedirler.[187]

2.3. ABD İstihbarat Servisleri (FBI ve CIA)'nin Siber Uzaydaki Faaliyetleri

ABD istihbarat topluluğu, bünyesinde çeşitli örgütlenmeleri barındıran bir yapı olup, bu örgütlenmeler arasındaki koordinasyon ise Ulusal İstihbarat Direktörü / Director of National Intelligence (DNI) tarafından sağlanmaktadır. Bu kapsamda DNI'ya bağlı 17 ajans ve örgüt bulunmaktadır.[188] Söz konusu örgütlerin siber güvenlik alanına ilişkin faaliyetleri ile ilgili koordinasyonu da DNI'nın görevleri arasında yer almaktadır.

Bu örgütlenmelerin en önemlileri arasında yer alan Federal Araştırma Bürosu (The Federal Bureau of Investigation / FBI), ABD'nin iç istihbarat ihtiyaçlarını karşılayan ve diğer devletlerin ABD'ye yönelik casusluk operasyonları ile subversif faaliyetlerine karşı koyan istihbarat organizasyonudur. Bu görevleri kapsamında FBI, RF'nin FSB (Rus Federal Güvenlik Servisi / Federalnaya Slujba Bezopasnosti)'si ile aynı işlevi gördüğü de ifade edilebilir. Bu itibarla örneğin RF'nin ABD'ye yönelik siber casusluk operasyonlarına karşı koymak, ÇHC'nin ABD'nin teknolojik sırlarına ulaşmaya yönelik faaliyetini engellemek, IŞİD destekli bir terör eylemini açığa çıkarmak veya ABD'de faaliyet gösteren aşırı sağcı bir grubun, tarikatın ya da örgütlenmenin aktivitelerini izlemek, FBI'ın görev ve sorumluluğundadır.

FBI'ın ABD'nin siber güvenlik stratejisinin uygulanmasında, siber suçlulardan, devlet destekli unsurlardan ve terörist gruplardan kaynaklanan siber ataklara karşı koyma görev ve yetkisi kapsamında önemli rolü bulunmaktadır. Bu çerçevede FBI siber güvenlik

[187]Ayrıntılı bilgi için bkz. Ibid., pp. 93-95
[188]NATO Cooperative Cyber Defense Centre of Excellence, **National Cyber Security Organisation in United States**, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_ organisation_USA_122015.pdf, (01.06.2016), p. 23.

ile ilgili yetki ve sorumluluklarını sürdürmek amacıyla, Siber Ulusal Güvenlik Bölümü (Cyber National Security Section / CNSS) ve Siber Suç Bölümü (Cyber Criminal Section / CCS) şeklinde örgütlenmeler tesis etmiştir. Bu örgütlemelerden CNSS, terörist gruplardan ve hasım devletlerden kaynaklanan siber saldırıları takip etmek, izlemek ve deşifre etmekten sorumluyken, CCS ise adı suç kapsamında olan, ancak federal güvenliği tehlikeye düşüren siber suçlar ile mücadele etmektedir.[189] CCS ve CNSS'nin, söz konusu görevleri kapsamında diğer hükümet kurumları ile olan koordinasyonu ise Ulusal Siber Araştırma Birleşik Görev Gücü (National Cyber Investigative Joint Task Force / NCIJTF)" aracılığıyla sağlanır. CNSS direktörü ise aynı zamanda NCIJTF'nin de başkanıdır ve siber güvenlik faaliyetlerinden sorumlu FBI direktör Yardımcısı'nın emrinde çalışır.[190]

FBI'ın faaliyetleri de her istihbarat servisinin operasyonları gibi gizli bilgi niteliğinde olup, bu operasyonlardan ancak belli bir amaç kapsamında medyaya sızdırılanları kadar kamuoyunun bilgisi olabilmektedir. Bu çerçevede, 2016 Haziran ayı için FBI'ın resmi internet sayfası incelendiğinde, ABD'ye yönelik siber saldırılar ve casusluk operasyonları ile ilgili olarak, FBI tarafından:[191]

-Yedi İran vatandaşının fotoğrafları ve açık isimleri yayımlanarak, anılanların 2011-2013 yılları arasında, "İran Devrim Muhafızları" adına, ABD'nin finans ve bankacılık sektörüne zarar vermek amacıyla "DDoS" saldırıları gerçekleştirdikleri,

-Firas Dardar ve Ahmed Al Agha isimli bir şahısların, 2014 yılı içinde, "Suriye Elektronik Ordusu" isimli bir örgüt adına, Esad rejimine destek vermek amacıyla, aralarında ABD orjinli şirketlerinde olduğu çeşitli uluslararası iş çevrelerine siber saldırı düzenlediği,

-Mikhailovich Bagachov, Farhan Ul Arshad, Noor Aziz Uddin, Jashua Samuel Aron ve Bjorn Daniel Sundin isimli şahısların, ABD bankacılık ve sosyal güvenlik sistemini de kullanacak şekilde, 100-300 Milyon-ABD Doları tutarında siber dolandırıcılık faaliyeti gerçekleştirdiği,

[189]Ayrıntılı bilgi için bkz. TIRRELL, op. cit., pp. 60-62.
[190]Ayrıntılı bilgi için bkz. Federal Bureau of Investigation, **Cyber Crime**, https://www.fbi.gov/about-us/investigate/cyber/ncijtf, (01.06.2016).
[191]Ayrıntılı bilgi için bkz. Federal Bureau of Investigation, **Wanted by FBI**, https://www.fbi.gov/wanted/cyber, (01.06.2016).

-Çin uyruklu Wong Dong, Gu Chunhui, Jun Kailiong, Huang Zhenyu ve Wan Xinyu isimli şahısların, 2013-2014 yılları arasında, "Halkların Özgürlüğü Ordusu" adına ABD orijinli bazı uluslararası şirketlerin gizli niteliğe sahip olan teknolojik ve ticari sırlarını siber casusluk faaliyeti kapsamında çaldıkları, gerekçeleriyle para ödülü karşılığında uluslararası düzeyde arandıkları görülmektedir.

Deşifre edilen söz konusu güncel siber saldırı faaliyetlerinin yanı sıra FBI tarafından 1998 yılında ve ABD Savunma Bakanlığı, Enerji Bakanlığı, bazı kuruluş ve üniversitelerin özellikle de uzay araştırmalarını hedefleyen bir siber espiyonaj operasyonu da tespit edilmiştir. Kamuoyunda "Moonlight Moze / Ay Işığı Labirenti" adıyla bilinen söz konusu operasyonun planlayıcılarının ise RİS ile irtibatlı Rus hackerlar olduğu da yapılan araştırmalar kapsamında iddia edilmiştir. Bu operasyon ile ABD'nin gizli araştırma faaliyetleri ve askeri çalışmaları dahilindeki çok önemli bilgiler çalınabilmiştir. Bahse konu iddiaları ise Rus tarafı kabul etmemiştir. Bu olay ABD güvenlik ve istihbarat bürokrasi ile kamuoyunda siber saldırıların yaratabileceği olumsuz etkiler ile ilgili olarak ciddi bir farkındalığın oluşmasına vesile olmuştur.[192]

Öte yandan Merkezi Haber Alma Örgütü (Central Intelligence Agency/ CIA), ABD'nin ülke dışındaki istihbarat ihtiyaçlarını karşılayan ve belirlenen stratejiler kapsamında gizli faaliyetlerini planlayan gizli servisi konumundadır. Bu itibarla CIA'ni, RF'nin SVR (Rus İstihbarat Servisi / Sluzhba Vneshney Razvedki)'si ile aynı işlevi gördüğü de ifade edilebilir. Bu kapsamda örneğin RF'nin Ukrayna'ya yönelik sürdürdüğü hibrit savaş konsepti kapsamındaki gelişmeleri istihbar etmek, Fransa'da 2016 Mayıs ayında başlayan sokak olaylarının seyrini izlemek, bir Latin Amerika ülkesinde ABD karşıtı bir sosyalist hükümeti devirmek, IŞİD'ın Irak ve Suriye'deki, El-Kaide'nin Afganistan'daki faaliyetlerini takip etmek ya da Türkiye'nin terörle mücadelesinin seyri ile ilgili olası gelişmeleri raporlamak CIA'in görev ve sorumluluğundadır.

CIA'in siber operasyonları da FBI'ın operasyonları gibi gizli bilgi niteliğindedir ve bu operasyonların mahiyeti ile ilgili olarak açık kaynaklarda sınırlı ve manipülatif bilgiler bulunmaktadır. Bununla birlikte tarihte organize edilen ve büyük hasara yol açan ilk siber atak olma niteliğine sahip SSCB'de bulunan Sibirya Gaz Boru hattına yönelik 1982 yılındaki "mantık bombası" saldırısı, CIA tarafından düzenlendiği iddia edilmiştir. Bu

[192]INC Comittee on Govermental Affairs US Senate, **Testımony of James Adams Chief Executıve Offıicer**,https://fas.org/irp/congress/2000_hr/030200_adams.htm,(16.02.2017).

saldırı ile teknoloji lideri ülke olarak bilişim ortamını en etkin kullanan ABD'nin, siber uzay alanındaki illegal istihbarat operasyonlarının altyapısını, saldırının düzenlendiği 1980'ler itibarıyla kurmaya başladığı görülmektedir. Bu kapsamda 1982 yılında CIA, "mantık bombası" olarak bilinen yöntemle, her hangi bir savaş ekipmanı kullanmadan, bilgisayar sistemine eklenen bir kod sayesinde ve bilgisayara ait işletim sistemi yönetiminin aklının kurcalamasını sağlayarak SSCB'de bulunan Sibirya Gaz Boru hattını patlatmayı başarmıştır.[193]

Bu saldırının detayları ise 2004 Şubat ayında İngiliz Telegraph Gazetesi'nde yer almıştır. Bu habere göre CIA ilk olarak SSCB'nin Paris Büyükelçiliği'nde görev yapan Albay Vladimir Vetrov'u angaje etmeyi başararak, anılana "*farewell*" takma adını vermiştir. Daha sonra Vetrov vasıtasıyla SSCB'nin ABD ve Kanada'nın doğalgaz hatlarında kullanmakta olduğunu yazılım programlarını teknoloji casusluğu kapsamında elde etmeye gayret ettiğini istihbar eden CIA, Vetrov'u kullanarak "mantık bombası" işlevi görecek olan virüslü bir yazılım programını SSCB'ye intikal ettirmiş, böylelikle de bu hatalı yazılımın Sibirya Gaz Boru hattında kullanılmasını sağlamıştır. Sonuç olarak CIA tarafından söz konusu gizli faaliyet ve sabotaj eylemi başarılı bir şekilde nihayetlendirilmiştir. Vetrov ise casusluk suçuyla 1983 yılında SSCB'de idam edilmiştir.[194]

CIA tarafından organize edilen bir diğer siber saldırı ise 2010 yılında İran nükleer tesislerine yönelik olarak, İsrail ile işbirliği yapılarak planlandığı iddia edilen "Stuxnet"[195]atağıdır. "Stuxnet" isimli gelişmiş virüs tarafından İran'ın nükleer tesisleri fiziksel hasara uğratılarak, İran'ın nükleer programını sürdürme süreci geciktirilmiştir. Görüldüğü üzere "Stuxnet", 2010 Haziran ayında fark edilen ve İran'ın Natanz nükleer geliştirme tesisine saldırmak için geliştirilmiş olan bir siber yazılımdır. Bu saldırı, resmi olarak hiçbir devlet tarafından üstlenmemiş olsa da saldırı çok büyük ihtimalle ABD-İsrail ortak yapımı bir subversif gizli faaliyet olarak değerlendirilmelidir. Zaten bu iddia ile ilgili olarak bugüne kadar her iki ülkeden de herhangi bir yalanlama gelmemiştir.

---

[193]Akademik Portal News, **Bugüne Kadar Gerçekleşmiş Olan Beş Devasa Siber Saldırı**, http://www.akademiportal.com/bugune-kadar-gerceklesmis-olan-5-devasa-siber-saldiri/, (18.02.2016).
[194]The Telegraph OnlineNews, **CIA plot led to huge blast in Siberian gas pipeline**,http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html, (02.06.2016).
[195]BIÇAKCI, "NATO'nun Gelişen Tehdit…", op. cit.,,s.108.

Konu ile ilgili olarak, David Sanger isimli bir gazeteci tarafından 2011 yılında yazılan bir makalede *"Stuxnet"in Obama'nın emriyle CIA'in koordinasyonun da NSA'in Maryland'deki merkezinde geliştirildiği ve İsrail'de kurulan bir model nükleer tesiste denendiğini"* iddia edilmiştir.[196] Diğer yandan Natanz Nükleer Tesisleri'nde görev yapan ve kuvvetle muhtemelen önceden İsrail Gizli Servisi (MOSSAD) tarafından angaje edilen bir İranlı görevli vasıtasıyla, bir taşınabilir bellek ile sisteme bulaştırılan "Stuxnet", aktif olduğu süre boyunca, nükleer tesiste içinde uranyum zenginleştirilen santrifüjlerin dönüş hızlarını etkileyerek ve böylelikle de kullanım ömürlerini azaltmak suretiyle zenginleştirme sürecine zarar vermeyi hedeflemiştir. Bunu yapmaya başlamadan önce de sistem ekranlarında, daha önceden almış olduğu 21 saniyelik ekran görüntüsünü defalarca döndürerek kontrol mühendislerini yanıltmayı başarmıştır. Arka planda santrifüjlerin dönüş hızlarını artırıp azaltarak ömürlerini azaltmıştır. Kırılan veya parçalanan santrifüjlerin yerine yenilerinin takılmadığı içinde söz konusu sabotaj hedeflenen şekilde patlamaya yol açmıştır. Sonuç olarak, İran'ın nükleer zenginleştirme süreci tamamen sekteye uğramasa da en azından iki yıllık bir üretim aksaması olduğu değerlendirilmiştir.[197]

3. ABD Ulusal Siber Güvenlik Rejimi

ABD'nin ulusal siber uzay alanını düzenleyen kanun, direktif ve diğer yasal düzenlemeleri karmaşık, iç içe geçmiş ve farklı amaçlara göre hazırlanmıştır. Bu alanda, federal düzeyde geçerli olan çok sayıda ulusal kanunun yanı sıra eyaletlerin kendi siber güvenliklerini sağlamayı hedefleyen yasal düzenlemeler de söz konusudur.

ABD siber güvenlik düzenlemeleri temelde, finans kesimini de kapsayacak bir şekilde ABD kritik altyapısı kapsamında tanımlanmış sektörlerde faaliyet göstermekte olan özel sektör kuruluşlarının ve diğer örgütlenmelerin kamu otoritesi ile uyumlu bir şekilde kendi ağ teknolojilerini siber saldırılardan ve siber casusluk amacı ile hazırlanmış olan yazılımlardan korunması hedefine odaklanmaktadır.[198] Bu kapsamda ABD hükümetleri, her yıl artış eğilimi içinde olan sofistike siber saldırılar karşısında, siber güvenlik düzenlemelerini ABD'nin ekonomik refahının sürdürülmesi ve ülke güvenliğin sağlanması noktasında hayati öneme sahip kabul ederek, bu alanda bugüne kadar çok sayıda federal ve

[196]SANGER David, **Israeli Test on Worm Called Crucial in Iran Nuclear Delay**, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0, (02.06.2016).
[197]Siber Bülten, **Stuxnet ve Uluslararası Hukuk: Bir Siber Saldırının Anatomisi**, https://siberbulten.com/makale-analiz/stuxnet-ve-uluslararasi-hukuk-bir-siber-saldirinin-anatomisi/, (02.06.2016).
[198]TIRRELL, op. cit., p. 57.

eyalet düzeyinde kanunlar ve yönetmelikler tanzim etmişlerdir. Bu önemin vurgulanması bakımından ABD İç Güvenlik Bakanı Janet Napolitan'ın 2012 yılında ABD Senatosu'ndaki bir toplantıda: *"ABD'de ulusal düzeyde 2011 yılı içinde 10.000'in üzerinde siber saldırı olayının rapor edildiğini, bu nedenle de ABD'nin siber güvenliğini sağlama noktasında sıkı tedbirler alması gerektiğini"* belirtmesi oldukça dikkat çekici olarak kabul edilebilecektir.[199]

Öte yandan 1996 yılında Clinton yönetimi tarafından kabul edilen Sağlık Sigortası Sürdürülebilirlik ve Hesaplanabilirlik Yasası (Health Insurance Portability and Accountability Act/ HIPAA)"[200] ve 1999 yılında kabul edilen Finansal Hizmetler Modernizasyon Yasası (Gramm-Leach-Bliley Act)[201], ABD'de siber güvenlik alanındaki dikkate değer ilk hukuki düzenlemeler arasında sayılabilecektir. Kısaca HIPAA olarak adlandırılan yasa ile Clinton yönetimi genel olarak sağlık sistemi ile ilgili yasal yükümlülükleri yürürlüğe koyarken, elektronik ortamda sürdürülmekte olan sağlık sigortası işlemlerinin güvenliğinin standardizasyonuna ilişkin bazı düzenlemeleri de yasalaştırmıştır. Finansal Hizmetler Modernizasyon Yasası ile güvenlik, finans ve bankacılık şirketlerinin güvenlik standartları konusunda birlikte hareket etme ve uyumu sağlamasına yönelik düzenlemeler de kabul edilmiştir.

11 Eylül 2001 saldırıları sonrası siyasi atmosferinde 2002 yılında kabul edilen, İç Güvenlik Yasası (Homeland Security Act) ise ABD'nin siber güvenlik alanındaki yasal düzenlemeleri arasında önemli bir yere sahiptir. Bu yasa ile birlikte ABD İç Güvenlik Bakanlığı tesis edilmiştir ve bu bakanlığın terörle mücadele kapsamındaki görevleri noktasında, ABD ulusal siber savunma sistematiğinin uygulanmasında önemli bir rolü mevcuttur. Bu kanun ile birlikte ABD İç Güvenlik Bakanlığı'nın yanı sıra siber güvenlik alanında faaliyet göstermek üzere, ABD Adalet Bakanlığı bünyesinde: "*Altyapıların Korunması ve Bilgi Analizi Müsteşar Yardımcılığı, Acil Durum ve Hazırlık Müsteşar Yardımcılığı ile Teknoloji ve Bilim Geliştirme Ofisi*" isimli yeni kurumsal yapılar da tesis

[199]Department of Homeland Security,**Written testimony of Secretary Napolitano for a Senate Committee on Homeland Security and Governmental Affairs hearing titled Homeland Threats and Agency Responses**, https://www.dhs.gov/news/2012/09/19/written-testimony-secretary-napolitano-senate-committee-homeland-security-and, (13.06.2016).

[200]ATCHINSON Brian ve FOX Daniel, **The Politics Of The Health Insurance Portability And Accountability Act**, http://www.library.armstrong.edu/eres/docs/eres/MHSA8635-1_CROSBY/8635_ week2_ HIPAA_politics.pdf, (13.06.2016).

[201]Federal Trade Comission, **Gramm Leach Bliley Act**, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, (13.06.2016).

edilmiştir. Ayrıca kritik sektörler tarafından ortaklaşa kullanılacak olan bir Ulusal Altyapı Koruma Planı (National Infrasture Protection Plan / NIPP) da kabul edilmiştir.[202]

Vatanseverlik Yasası (Patriot Act) şeklinde de ifade edilen bu Kanunla, siber güvenlik alanında genel olarak federal istihbarat ve güvenlik servislerinin, internet şirketleri, internet bağlantı sağlayıcıları ve telekomünikasyon şirketleriyle yaptıkları yasal iş birliği kapsamında terörist faaliyet içinde bulunması olası şahısları izlemeleri ve takip edebilmeleri kolaylaştırılmıştır. Bu yasa ile dinleme ve takip cihazlarının yetkileri ve tanımları genişletilerek, artık internet üzerinden yapılan aktivitenin gözlemlenmesi ve izlenmesi oldukça basit yasal düzenlemeler ile gerçekleştirilebilir hale getirilmiştir.[203]

Vatanseverlik Yasası, uzun yıllar terörle mücadele adına uygulanmış, "Edward Snowden Olayı" olarak adlandırılan skandalın ortaya çıkması akabinde, bu yasa ABD kamuoyunda daha sık tartışılır hale gelmiştir. Öte yandan ABD Özgürlük Kanunu (The USA Freedom Act) şeklinde isimlendirilen ve Obama yönetimi tarafından 2 Haziran 2015 tarihinde kabul edilen yasa ile birlikte, Vatanseverlik Yasası'nın getirdiği düzenlemeler revize edilerek, ABD siber güvenlik ortamı görece olarak daha demokratik bir hale getirilmeye çalışılmıştır. Bu yeni yasal düzenlemeler ile ABD vatandaşlarının ve kurumsal kişiliklerinin ağ teknolojileri kullanmak suretiyle yaptıkları haberleşmenin ilgili güvenlik ve istihbarat servislerince takip edilmesi, izlenmesi ve delil olarak muhafaza edilmesi zorlaştırılmıştır.[204]

2002 yılında kabul edilen Federal Bilgi Güvenliği Yönetimi Yasası da (Federal Information Security Management Act of 2002/FISMA), ABD siber güvenlik alanını düzenleyen önemli kanunlardan biri olarak kabul edilmelidir.[205] Bu yasa ile ABD'nin ekonomik ve ulusal çıkarları kapsamında bilgi güvenliğini sağlaması gerektiği vurgulanmak suretiyle, her federal kurumun kendi enformasyon güvenliğini sağlaması ve diğer resmi kurumlar ile bu alanda eşgüdümü gerçekleştirmesi noktasında iç düzenlemeler yapması zorunlu hale getirilmiştir. Yasa ile ayrıca, her federal kuruluşun konu kapsamında

[202]TIRRELL, op. cit., p. 63.
[203]Department of Homeland Security, **Homeland Security Act**, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf, (13.06.2016).
[204]Judiciry Committee, **The USA Freedom Act**, https://judiciary.house.gov/issue/usa-freedom-act/,(13.06.2016).
[205]Ayrıntılı bilgi için bkz. NATO Cooperative Cyber Defense Centre of Excellence, **National Cyber Security Organisation in United States**, op. cit., p. 14

yaptığı yıllık faaliyetleri ve harcamaları Bütçe Yönetimi Ofisi (Office of Management and Budget / OMB)'ne rapor etmesi zorunlu hale getirilmiştir.[206]

Bunlarla birlikte federal ve eyalet resmi güvenlik birimleri ile özel sektör arasında internet trafiği, ABD vatandaşlarının internet iletişim bilgileri ve teknoloji geliştirme konusunda işbirliğini geliştirmeyi hedefleyen Siber Güvenlik Bilgi Paylaşımı Yasası (Cyber Security Information Sharing Act/CISA)[207] 2015 yılında kabul edilmiştir.

ABD'nin siber suç alanındaki güvenlik rejimini belirleyen temel yasa ise 1986 yılında ilk versiyonu kabul edilen Bilgisayar Dolandırıcılığı ve Suiistimali Yasası (Computer Fraud and Abuse Act / CFAA)'dır. Yasa ile bilgisayar teknolojileri ve internet üzerinden işlenen adi nitelikli siber suçlara yönelik sert tedbirler getirilmektedir. Söz konusu yasa, günün şartlarına göre 1989, 1994, 1996, 2001 (Vatanseverlik Kanunu kapsamında) 2002, 2008 ve 2015 tarihlerinde revize edilmiştir.[208]

ABD'de yönetim rejiminin bir sonucu olarak, teknolojik ve ekonomik büyüklük bakımından ön plana çıkmış olan eyaletlerin de ABD siber güvenlik stratejisinin şekillenmesinde, çıkardıkları yasalar kapsamında önemli rolü bulunmaktadır. Bu kapsamda, Koliforniya Eyaleti'nin 2003 yılında kabul ettiği Güvenlik İhlal Genelgesi/Kanunu (Notice of Security Breach Act) diğer eyaletlerin de benzer kanunlar çıkarmasına vesile olması bakımdan önemlidir.[209] Bu yasayla, Kaliforniya'da mukim vatandaşların dijital ortamda muhafaza edilen ad-soyad, sosyal güvenlik numarası, ehliyet numarası, kredi kartı ve diğer finansal bilgilerinin gizliliği güvence altına alınmıştır. Bu yasanın kabulü sonrasında çok sayıda eyalet yönetimi de benzer yasaları kabul ederek yürürlüğe koymuştur.

2004 yılında ise Kaliforniya Eyalet Meclisi, 1950 sayılı Kaliforniya Asamble Yasası (California Assembly Bill-1950)'nı kabul etmiştir. Bu yasayla Kaliforniya'da mukim iş çevrelerinin ticari ortaklarının özel bilgilerini korumaya yönelik siber güvenlik

---

[206]Department of Homeland Security,**Federal Information Security Management Act of 2002-FISMA**, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, (13.06.2016).
[207]ISACA Cyber Security Nexus, **Cybersecurity Information Sharing Act**, http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx, (13.06.2016).
[208]DOYLE Charles, **Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws-Computer Fraud and Abuse Act**, https://www.fas.org/sgp/crs/misc/97-1025.pdf, (13.06.2016).
[209]State of California Department of Justice, **Notice of Security Breach Act**, https://oag.ca.gov/ecrime/databreach/reporting, (13.06.2016).

tedbirleri almaları zorunlu kılınmıştır.[210] Ayrıca bu yasanın uygulanması ile birlikte, Kaliforniya yönetimi federal siber güvenlik standartlarını sağlama noktasında, harekete geçen ve bu alanda ilk yasal düzenlemeleri hazırlayan eyalet olması bakımında öncü rol oynadığını da göstermiştir.

Diğer yandan ABD'nde siber güvenlik rejimini düzenleyen federal ve eyalet yasaları ile ilgili olarak ciddi bir tartışmada söz konusudur. Bu tartışmaların ise üç tarafı bulunmaktadır. Taraflardan ilki, siber güvenlik düzenlemelerinin ABD'nin ekonomik refahı ve güvenliği için şart olduğunu belirterek, bu düzenlemeleri desteklemektedirler. Diğer bir görüş kapsamında ise siber güvenlik yasaları desteklenmekte, ancak bu noktada inisiyatifin kamudan çok, kritik altyapıların önemli bir bölümünü kontrol eden özel sektörde olması gerektiği görüşünü savunulmaktadır. Tarafların sonuncusu da siber güvenlik düzenlemelerinin yaratıcılığı öldürdüğünü, bilimsel gelişmelerin önünü tıkadığını ve maliyetlerin artmasına neden olarak özel sektörün rekabet gücünü azalttığını iddia etmektedirler.[211]

Ayrıca ABD'nin teknolojik imkânlarına bağlı olarak e-devlet alanında ciddi bir gelişmişlik düzeyi söz konusudur. Bu kapsamda ABD, 2002 yılında e-yönetim yasasını kabul etmiştir. Bu yasa, ABD'nin e-yönetim sistemindeki federal yapı ile eyalet arasındaki eşgüdümü sağlaması ve e-yönetim sisteminin güvenliğini tesis etmesi bakımından önemlidir.[212] 2012 yılında ise "*Digital Goverment Strategy / Dijital Hükümet Stratejisi*" yenilenmiştir. Bu yenilenme kapsamında da ABD hükümetlerinin en uygun ve verimli teknolojiye sahip olmayı amaç edinmesi ile özel sektörün yeni teknolojik gelişmeleri sağlaması noktasında teşvik edilmesi temel hedefler olarak belirlenmiştir.[213]

Görüldüğü üzere 11 Eylül 2001 sonrası oluşan siyasi atmosferin ve akabinde devam eden uluslararası terör tehdidinin de etkisiyle ABD ulusal siber güvenlik alanı düzenleyen yasalar, 2010 yılına kadar oldukça sıkı bir denetim rejimini ihtiva etmiştir. 2010 yılı

---

[210]StateofCalifornia Department of Justice, **California Assembly Bill-1950**, http://www.steptoe.com/assets/attachments/1477.pdf,(13.06.2016).
[211]SFGATE News Portal, **Former White House aide backs some Net regulation/Clarke says government, industry deserve 'F' in cybersecurity**,http://www.sfgate.com/business/article/Former-White-House-aide-backs-some-Net-regulation-2729985.php, (13.06.2016).
[212]FISCHER A.Eric, **Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions**, Congressional Research Service, 2013 https://fas.org/sgp/crs/natsec/R42114.pdf, (20.02.2017).
[213]Department of Homeland Security, **Digital Government. Building a 21st Century Platform to Better Serve the American People**, https://www.dhs.gov/sites/default/files/publications/digital-strategy/digital-government-strategy.pdf, (20.02.2017).

sonrasında ise Obama yönetimi ile birlikte, ABD'nin siber güvenlik rejimini düzenleyen yasalarda da daha liberal bir eğilim söz konusu olmuş ve daha çok internet yönetimini düzenleyen, özel sektör ile kamu arasında uyumu artırmayı hedefleyen, siber güvenlik alanında faaliyet gösteren resmi güvenlik ve istihbarat örgütleri arasındaki işbirliğini arttıran yasalar gündeme gelmiştir. Söz konusu sıkı denetim rejiminden daha liberal bir sisteme geçiş ile ilgili tartışmalar kapsamında ise "Edward Snowden Olayı" olarak adlandırılan gelişmelerin ABD ulusal siber güvenlik rejiminin yanı sıra ABD dış politikası ve RF ile ilişkilerindeki etkisinden de bahsetmek gerekmektedir.

Zira Haziran 2013 ayında patlak veren "Edward Snowden Olayı" ile birlikte, ABD'nde siber güvenlik alanını denetleyen ve anti-demokratik uygulamaları da bünyesinde barındırması nedeniyle sert bir şekilde eleştirilmekte olan federal yasaların, özellikle de Vatanseverlik Kanunu'nun, revize edilmesini destekleyen eğilimler artmıştır. Bunun bir sonucu olarak da, Obama yönetimi tarafından, göreli olarak daha demokratik olduğu iddia edilebilecek olan ABD Özgürlük Kanunu 2015 yılında kabul edilmiştir. Bu yasa ile birlikte, internet üzerinden yapılan haberleşmenin izlenmesi, takip edilmesi ve delil olarak arşivlenmesi daha sıkı bir rejim ile denetim altına alınmıştır.

Bu noktada, "Edward Snowden Olayı"nın ABD hukuk sisteminin yanı sıra özellikle ABD'nin RF ile ilişkileri temelinde ABD dış politikası üzerinde de önemli etkisi olduğu ifade edilmelidir. Bu skandalın açığa çıkması ile birlikte, ABD'nin kendi vatandaşlarının yanı sıra müttefiklerinin ve hasım kabul ettiği ülkelerin vatandaşları, politikacıları, kamu ve ticari kurumları tarafından gerçekleştirilen iletişimi illegal bir şekilde, sofistike yazılımlar, programlar ve teknolojik imkânlar kullanmak suretiyle uzun yıllardan bu yana izlediği deşifre edilmiştir. Bu kapsamda çalışmamız açısından "Edward Snowden Olayı"nın detaylı bir şekilde ele alınmasının ABD'nin siber güvenlik stratejilerin analiz edilmesine önemli katkı sağlayacağı düşünülmektedir.

4. Edward Snowden Olayı

Dünya kamuoyu, 20 Mayıs 2013 tarihi sonrasında yoğun bir şekilde Edward Snowden adlı otuz yaşındaki Amerikalı genci konuşmaya başlamıştır. Snowden'ı bir anda dünya gündemine taşıyan olay ise NSA'daki görevi kapsamında elde ettiği gizli bilgileri

The Guardian Gazetesi yetkililerine vermesi ve bu belgelerin bir kısmını yayınlanmasıdır.[214]

Snowden, 21 Haziran 1983 yılında Kuzey Carolina'da doğmuş ve Elizabeth City'de büyümüştür. Annesi Baltimore Federal Mahkemesi'nde çalışan bir kâtip, babası ise Pennsylvania'da yaşayan emekli bir sahil güvenlik memurudur. Snowden, orta öğretimini yarıda bırakarak Arundel Community College'a bilgisayar öğrenimi için müracaat etmiştir. Daha sonra askere giden Snowden burada dört ay kadar özel kuvvetlerde eğitim almış ve ayağının kırılmasından sonra bu eğitimini de yarıda bırakmıştır.[215] Snowden NSA'da ilk kez güvenlik uzmanı olarak 2004 yılında görev yapmaya başlamıştır. Daha sonra, bileşim uzmanı olarak CIA'de çalışmaya başlamış anılan, 2007 yılında kapalı bir görev için Cenova'ya diplomatik bir kimlikle gönderilmiş ve burada 2009 yılına kadar görev yapmıştır. 2009 yılında CIA'den ayrılan Snowden, NSA'e bağlı olarak iş yapan özel firmalarda çalışmaya başlamış ve bu şirketlerden biri olan Booz Allen adlı bir şirketin Hawaii ofisinde görev yaparken The Guardian muhabiri Glenn Greenwald'a ABD'nin istihbarat yöntemleri hakkında bilgi sızdırmaya başlamıştır.

Snowden tarafından sızdırılan bilgiler tüm dünyada adeta bir deprem etkisi yaratmıştır. Bunun üzerine ABD, ÇHC'den Snowden'ın iadesini talep etmiştir. ÇHC ilk etapta ABD'nin iade talebine direnmiştir. Daha sonra ABD tarafından gelen yoğun baskılara dayanamayan ÇHC yönetimi Snowden'ın da Hong Kong'tan ayrılmasını sağlayarak, anılanı RF'ye göndermiştir. Uzun bir süre RF'de Sheremetyevo Uluslararası Havalimanı'nın transit yolcu bölümünde kalan Snowden, daha sonra RF'den sığınma talebinde bulunmuş ve bu talebi kabul edilmiştir. Bu gelişme ise ABD ve RF arasındaki ilişkilerin ciddi bir şekilde gerilmesine neden olmuştur.

Sızdırdığı bilgilerin dünya kamuoyunu yoğun bir şekilde meşgul etmesinin ve Snowden'ın susturulmasının veya ABD'ye iade edilmesinin sağlanması kapsamında, ABD'nin bu denli ısrarcı olmasının nedenleri ise Snowden'ın ABD'nin yıllardan bu yana teknolojik imkânlardan azami istifade etmek suretiyle sürdürmekte olduğu siber espiyonaj kapasitesini ifşa etmesi bağlamında değerlendirilmelidir. Bu itibarla Snowden tarafından

[214]SEZGİN,op. cit.,s.24.
[215]Biography Web Page, **Edward Snowden**,http://www.biography.com/people/edward-snowden-21262897, 15.06.2016.

sızdırılan bilgilerin ABD açısından önemi, aşağıdaki başlıklar dahilinde kategorize edilerek daha iyi anlaşılabilecektir.[216]

1. ABD, NSA'nın geliştirdiği siber kapasiteyi kullanmak suretiyle küresel düzeyde kendi vatandaşlarının yanı sıra müttefiklerinin ve hasım kabul ettiği ülkelerin vatandaşlarının, politikacılarının ve önemli şahsiyetlerinin internet, cep telefonu ve diğer özel yazılım programları üzerinden gerçekleşen iletişim bilgilerini, her hangi bir yasal dayanak bulunmadan, izleyebilmekte ve kayıt altına alabilmektedir.

2. NSA, bu siber kapasiteyi kullanabilmek amacıyla "PRISM" ve "Tempora" adlı iki özel program geliştirmiştir. Tempora Programı, İngiltere'nin ABD ile işbirliği halinde dünya genelinde telefon ve internet haberleşmesini takip etmek amacıyla geliştirdiği gizli faaliyetin adıdır. Tempora Programı, muadili NSA tarafından kullanılmakta olan PRISM programına göre daha geniş kapsamlı, etkin ve yaygın bir gizli siber casusluk faaliyettir. PRISM Programı ise NSA tarafından 2007 yılında faaliyete geçirilen ve Microsoft, Yahoo, Apple, Google, Facebook, Skype vb. kaynaklardaki bilgilere doğrudan ulaşabilme amacını güden, ABD hükümetinin gizli bir faaliyeti olarak tanımlanabilecektir. Diğer yandan ABD'nin Tempora, İngiltere'nin de PRISM programına giriş izninin olduğu da iddia edilmiştir.[217]

3. ABD ve İngiltere arasında süre gelmekte olan söz konusu siber casusluk alanındaki işbirliği ise UKUSA Anlaşması (United Kingdom - United States of America Agreement)'nın bir gereği olarak sürdürülmektedir. UKUSA Anlaşması, "Beş Göz" olarak da bilinmektedir. Bu anlaşmaya Kanada, Avustralya ve Yeni Zelanda'da dâhildir. Bu anlaşma, ilk olarak İngiltere ve ABD tarafından Mart 1946'da imzalanmıştır. Daha sonra Kanada, Avustralya ve Yeni Zelanda'yı kapsayacak şekilde genişletilmiştir.[218] Günümüzde bu anlaşmanın güncel işlevi hakkında sınırlı bilgi mevcuttur. Bununla birlikte Snowden tarafından sızdırılan bilgiler kapsamında örneğin Avustralya'nın Asya-Pasifik bölgesi ile ilgili sinyal ve elektronik istihbarat toplama vasıtaları konusunda ABD ile işbirliği halinde olduğu bilinmektedir. Öte yandan orijinal UKASA Anlaşması'nın taraf devletlere sadece

[216]SEZGİN, op. cit.,s.25.
[217]HUHNE Chris, **Prism and Tempora: The Cabinet was told nothing of the surveillance state's excesses**, http://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state, (15.06.2016).
[218]FARRELL Paul, **History of 5-Eyes**, https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer, (15.06.2016).

ülke dışındaki hedeflere yönelik istihbarat paylaşımı yetkisi verdiği bilinmekle birlikte, Snowden Olayı dahilinde NSA'nın UKASA üyesi diğer devletlerin bazı ulusal verilerine de erişebildiği deşifre edilmiştir.[219]

Öte yandan Snowden'ın bahse konu bilgileri ani bir şekilde ifşa etmeye karar vermesinin, istihbarat tekniği açısından en makul açıklaması ise Snowden'ın Hong Kong'ta görev yaptığı dönemde yabancı istihbarat servisleri (ÇHC ve RF) tarafından bağımsız bir şekilde ve/veya müştereken sürdürülen bir angaje operasyonu neticesinde ele alınmış olması kapsamında analiz edilebilecektir. Snowden her ne kadar, söz konusu itiraflarını, demokratik-insancıl düşünceleri kapsamında gerçekleştirdiğini iddia etse bile bu durum yıllardır bu bilgilere sahip olan Snowden'ın neden Hong Kong'ta görev yapıncaya kadar beklediği gerçeğini yeterince açıklayamamaktadır.[220] Bu itibarla Snowden'ın Hong Kong'ta görev yaptığı dönemde ÇHC veya RF istihbaratı tarafından birbirinden bağımsız veya müştereken sürdürülen bir taraf değiştirme operasyonu kapsamında ele alındığı, bu ele alınma sürecinin angaje ile tamamlanmasına yakın bir dönemde, söz konusu gizli faaliyetin ABD kontr/espiyonajı tarafından deşifre edildiği, bunun üzerine de yasal takibattan kurtulmak adına Snowden'ın kasıtlı olarak bahse konu ifşa sürecini, kendisini ele alan servislerin de bilgisi dahilinde başlattığı, istihbarat tekniği açısından Snowden olayının baştan sona en makul açıklaması olarak değerlendirilebilecektir. Snowden olayının diğer casusluk veya bilgi sızdırma olaylarından temel farkı ise günümüzde daha çok siber casusluk faaliyetleri üzerinden yürütüldüğü bilinen RF ve ABD istihbarat servisleri arasındaki mücadeleyi açıkça betimleyen önemli bir vaka olmasıdır.[221]

Snowden olayının patlak vermesi ile birlikte, ABD yönetimi ilk etapta olayı yatıştırma politikası gütmüştür. Bu kapsamda, ÇHC'ye yapılan diplomatik baskılar ile birlikte, ABD ile ilişkilerinde gerginlik istemeyen ÇHC yönetimi, bir orta yol bularak, Snowden'ın RF'ye geçmesine izin vermiştir.[222] Diğer yandan ABD yönetimi için,

[219]Guardian, **History of 5-Eyes–explainer**, https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer, (18.04.2017).
[220]Uluslararası Politika Akademisi, **Edward Snowden Olayı**, http://politikaakademisi.org/2013/06/28/edward-snowden-olayi/, (15.06.2016), s. 1.
[221]SEZGİN, op. cit.,s.26
[222]KSHETRI Nir, **Cybersecurity and International Relations: The U.S. Engagement with China and Russia**,http://docplayer.net/2657945-Cybersecurity-and-international-relations-the-u-s-engagement-with-china-and-russia.html, (15.06.2016)., p. 2.

Snowden olayının RF ile ilgili kısmı ise çok daha sancılı ve sıkıntılı bir süreci ihtiva etmiştir.

Bu kapsamda RF, ABD'nin sert tepkilerine rağmen ilk etapta, Snowden'e bir yıllık geçici sığınma, sürenin dolmasından sonrasın da ise 1 Ağustos 2014 tarihinden itibaren ise üç yıllık geçici oturum hakkı vermiştir.[223] Krizin ilk aylarında ise RF, Snowden'ın Sheremetyevo Uluslararası Havalimanı'nın da uluslararası medya temsilcileri, sivil toplum görevlileri ve tanınmış aktivistlerle temas etmesini sağlayarak, Snowden olayının ABD aleyhine dünya kamuoyunda tartışılmasını ve gündemde tutulmasını sağlamıştır.[224] Tüm baskılara rağmen, Snowden'i ABD'ye iade etmeyen ve anılanın oturma süresini uzatan RF'nin bu tavrı Cumhuriyetçi Senatör John McCain tarafından: *"her Amerikalının yüzüne atılan şamar"* şeklinde tanımlanmıştır. Aynı konuda The New York Times ise 2 Ağustos 2013 tarihinde yayımlanan bir makaleye, *"Meydan Okuyan Rusya"* başlığını atmıştır.[225] Bu tepkiler karşısında ise RF geri adım atmayarak, Snowden'i adeta ABD'nin kirli yüzünü ifşa eden bir demokrasi kahramanı şeklinde dünya kamuoyuna lanse etmeye gayret etmiştir. Bu kapsamda, Putin'in konuyla ilgili olarak, alaycı bir ifadeyle: *"Snowden'ın kendisini bir demokrasi kahramanı olarak gördüğünü, gizli ve karanlık bilgilerin deşifresi için çalıştığını ilan ettiğini, bu durum da herkesin -böyle bir şahsı karşı tarafa verebilir miyim?- şeklindeki soruyu kendisine sorması gerektiğini"* beyan etmiştir. Tüm bu gelişmelerin bir sonucu olarak, RF ve ABD ilişkileri ciddi bir şekilde gerilmiş ve ABD yönetimi RF ilişkilerini dondurma kararı almıştır.[226]

Snowden olayının ABD dış politikası açısından olumsuz yönde ciddi sonuçları olmuştur. Her şeyden önce, yoğun baskılara rağmen ÇHC ve RF'nin Snowden'i ABD'ye iade etmemesi, ABD'nin caydırıcı gücünün değerlendirilmesi noktasında ciddi bir prestij kaybı olarak görülmelidir.[227] Örneğin ABD'nin Snowden olayı kapsamında, 2009 yılında yapılan G–20 zirvesine katılan dünya liderlerinin iletişim bilgilerini dinlediğinin deşifre edilmesi, ABD'ni söz konusu ülkeler nezdinde izahı oldukça zor olan bir duruma düşürmüştür. Snowden'ın yaptığı açıklamalar, başta Fransa ve Almanya yönetimleri olmak üzere, ABD'nin müttefiki ülkelerde dahi büyük bir endişe ve tepkiyle karşılanmıştır. Bu

[223]Haberus İnternet Haber Portalı, **Snowden Rusya'dan Ayrılmayı Düşünmüyor**,http://haberrus.com/politics/2015/08/15/snowden-rusyadan-ayrilmayi-dusunmuyor.html, (15.06.2016).
[224]Uluslararası Politika Akademisi, op. cit.,s.2.
[225]SEZGİN, op. cit.,s.29
[226]KSHETRİ, op. cit., p. 3
[227]Ibid.,s.24

dönemde Guardian Gazetesi'nde Snowden'ın itirafları başlığı altında çıkan haberler, ABD'nin birçok müttefiki ile ilişkisini olumsuz yönde etkilemiş ve yaşanan iltica krizi, ÇHC ve RF başta olmak üzere bu süreç çerçevesinde rol oynayan ABD'nin sistemsel rakiplerine kendisine karşı ileri sürebilecekleri bir koz vermiştir.[228]

Siber güvenlik açısından ise Snowden Olayı dijital ortamda ve ağ teknolojileri kullanılmak suretiyle toplanan, arşivlenen ve istihbari bilgi olarak analiz edilen her türlü bilginin 21. yy. dünyasında gizli kalmasının oldukça zor olduğunu göstermiştir. Bu nedenle de söz konusu tarzda skandalların ortaya çıkmasının engellenmesi amacıyla, devletlerin mümkün olduğunca şeffaf ve demokratik yöntemler ile siber istihbarat çalışmalarını sürdürmesi gerektiği gerçeği, Snowden Olayı ile bir kez daha açıkça kanıtlanmıştır.

Snowden olayı kadar, ABD'ni dünya kamuoyunda tartışılır kılan siber güvenlik temelli bir başka skandal olay ise WikiLeaks sitesinin kurucusu ve yayın yönetmeni Julian Assange tarafından dünya kamuoyuna ifşa edilen ve "WikiLeaks Belgeleri" şeklinde adlandırılan dokümanlardır. "WikiLeaks Belgeleri" kapsamındaki tartışmaların da ABD'nin siber güvenlik sistemindeki zafiyetleri göstermesi bakımından yakından irdelenmesin de bizce fayda görülmektedir.

5. WikiLeaks Belgeleri

WikiLeaks, Çinli muhaliflerin yanı sıra ABD, Tayvan, Avrupa, Avustralya ve Güney Afrikalı gazeteciler, matematikçiler ve şirket teknologları tarafından kurulmuş, internet temelli olarak "sızıntı gazeteciliği" şeklinde tanımlayabileceğimiz bir haber anlayışına sahip internet haber portalı organizasyonudur. Avustralyalı gazeteci ve internet aktivisti Julian Assange, organizasyonun görünen yüzüdür. WikiLeaks internet sitesi, 4 Ekim 2006 tarihinde yayına girmiştir.[229]

Julian Assange ise 3 Temmuz 1971 tarihinde Avustralya'da doğmuştur. Çalışma hayatı boyunca bilgisayar programcılığı, internet aktivistliği, WikiLeaks internet sitesinin editörlüğü ve basın sözcülüğü görevlerinde bulunmuştur.[230] 1987 yılında "Mendax" kullanıcı adıyla hackerlık işine girmiştir. Daha sonra arkadaşlarıyla birlikte, "Mendax, Trax ve Prime Suspect; International Subversives" isimli hacker grubunu oluşturmuşlardır.

[228]Ayrıntılı bilgi için bkz. Ibid.,ss.25-28
[229]BBC News, **What is Wikileaks?**, http://www.bbc.co.uk/news/technology-10757263, (16.06.2016).
[230]Biography Web Page, **Julian Assange**,http://www.biography.com/people/julian-assange-20688499, (16.06.2016).

Bu dönemde siber saldırı gerçekleştirdikleri siteler arasında, Pentagon, ABD Deniz Kuvvetleri, NASA, Overseas Telecommunications Commission, Citibank, Lockheed Martin, Motorola, Panasonic gibi resmi kurumlar ve uluslararası şirketler bulunmaktadır.[231]

Assange, WikiLeaks'in 2006 yılında kurulmasına öncülük etmiştir. Dokuz kişiden oluşan WikiLeaks yönetim kurulu üyelerinden olup ayrıca basın sözcüsüdür. Gazeteler onu WikiLeaks'in "yöneticisi" veya "kurucusu" olarak tanımlasa da Assange: *"Ben kendimi kurucu olarak görmüyorum, sadece editörüm"* demiştir. Bununla birlikte siteye yüklenecek belgelerde en son söz ve onay daima Assange'da olmuştur. Diğer bütün site çalışanları gibi Assange da site için ücretsiz ve gönüllü olarak çalışmaktadır. Kurucusu olduğu WikiLeaks, ilk dönemlerinde Küba'daki Amerikan üssü Guantanamo'da esirlere yapılan muameleye dair kurallar, Kenya'daki yargısız infazlar, Afganistan ve Irak Savaşı'ndaki sivil ölümlerine dair belgeler yayınlamıştır.[232]

WikiLeaks ile dünya kamuoyunun tanışması ise ABD Dışişleri Bakanlığı ve dünya genelindeki ABD Büyükelçilikleri arasındaki ayrıntılı yazışmalardan oluşan 251.857 adet gizli belgeyi, Kuveyt'teki Camp Arfijan üssünde görev yapan ABD ordusunda görevli asker Bradley Manning'den illegal bir şekilde temin ederek, bunları internet sayfası üzerinden dünya kamuoyuna sızdırmasıyla söz konusu olmuştur. Bu sızdırma sürecinde, WikiLeaks organizasyonuna El Pais, Le Monde, Der Spiegel, The Guardian ile The New York Times gazeteleri de hatırı sayılır bir destek sağlamıştır.[233]

28 Kasım 2010 tarihi itibarıyla kamuoyuyla paylaşılmaya başlanan ABD'nin diplomatik gizli yazışmaları, bugüne kadar kamuoyuna sızdırılan en fazla miktardaki gizli belge olması bakımından önemlidir. Belgeler, 274 elçilik, konsolosluk ve diplomatik temsilcilikten sızdırılmıştır. 28 Aralık 1966 tarihinden 28 Şubat 2010 tarihine kadar olan diplomatik yazışmaları içeren belgeler arasında ABD'ye ait 15.652 belge "gizli" olarak nitelenmektedir. 15.365 belge ile Irak, belgelerde en çok adı geçen ülkedir. Irak kaynaklı belgelerin sayısı 6.677'dir. ABD Dışişleri Bakanlığı'ndan 8.017 belge gelmiştir. Türkiye'nin ise 7.918 belgeye kaynaklık ettiği bilinmektedir. ABD Dışişleri Bakanlığı'nın

[231]Sydney Morning Herald, **International Man of Mystery**, http://www.smh.com.au/technology/technology-news/international-man-of-mystery-20100409-ryvf.html, (16.06.2016).
[232]NTV Internet Haber Portalı, **Kim Bu Assange?**, http://www.ntv.com.tr/dunya/kim-bu-assange, xZtbkT2VJku5p4lk_WHjAA, (16.06.2016).
[233]The New York Times, **Leaked Cables Offer Raw Look at U.S. Diplomacy**, http://www.nytimes.com/2010/11/29/world/29cables.html, (16.06.2016).

etiketleme sistemine göre belgelerin 145.451'i dış siyasi ilişkilerle, 122.896'sı hükümetlerin kendi iç meseleleriyle, 55.211'i insan haklarıyla, 49.044'ü ekonomik koşullarla, 28.801'i teröristler ve terörizmle ve 6.532'si BM Güvenlik Konseyi ile ilgilidir.[234] Belgelerin yaklaşık 100 bini *"hizmete özel (confidential)"*, 15 bini *"gizli (secret)"* olarak sınıflandırılırken, *"çok gizli (top secret)"* sıfatını taşıyan hiçbir belge yayınlanmamıştır.[235]

Bu gizli belgelerin açıklanmasıyla birlikte WikiLeaks ve en yetkili ismi Assange üzerindeki maddi ve manevi baskılar artmıştır. İlk etapta, WikiLeaks sitesi sürekli olarak siber saldırılara maruz kalmış ve site alan adı ve sunucusuyla ilgili sorunlar yaşamıştır.[236] Daha sonra, Assange hakkında tecavüz suçlamasıyla Interpol tarafından kırmızı bülten çıkarılmış ve anılan Londra'da gözaltına alınmıştır. Dokuz gün tutuklu kalan Assange, kefaletle serbest bırakılmış, ancak baskılar devam etmiştir. Bu kapsamda, İsveç'teki savcılık 18 Kasım 2010 tarihinde Assange için uluslararası yakalama kararı çıkarmıştır. Bunun üzerine Assange 19 Haziran 2012 tarihinden itibaren bulunduğu Ekvador'un Londra Büyükelçiliği'ndeyken, 16 Ağustos 2012 tarihi itibarıyla bu ülkeden siyasi sığınma hakkı talep etmiştir. Bu talep Ekvator hükümeti tarafından onaylanmıştır.

Söz konusu bilgiler doğrultusunda *"WikiLeaks belgeleri orijinal ve güvenilir kaynaklar mıdır?"* sorusu da sorulmalıdır. Bu belgelerinin orijinal olduğu bizzat ABD tarafından doğrulanmıştır. Bununla beraber belgelerin orijinal olması, aynı zamanda da güvenilir oldukları anlamına gelmemektedir.[237] Bu kapsamda, konuyla ilgili olarak, Çağrı Erhan: "Wi*kiLeaks belgeleri üç kategoriden oluşuyor. Birinci grupta, ABD büyükelçiliklerinden yollanan ve çeşitli ülkelerin liderleri ve devlet adamları hakkında, hiçbir somut delile dayanmayan, 'dedikodu' mahiyetinde ifadelere yer verilen belgeler bulunuyor. Bunların sayısı nispeten az. İkinci grup, ABD büyükelçilerinin, görev yaptıkları ülkelerde meydana gelen siyasi, ekonomik, askerî, sosyal gelişmelerle ilgili analizlerini içeriyor. Bunlar arasında çok yüksek bir gözlem ve analiz kabiliyetinin sonucu ortaya çıkarılmış kaliteli belgeler kadar, sübjektif yönü ağır basanlar da var. Üçüncü ve son grup*

[234]Uluslararası Stratejik Araştırmalar Kurulu (USAK), **WikiLeaks Belgelerinde Türkiye ve Yakın Çevresi-Türkiye, Rusya, Güney Kafkasya ve Ortadoğu ile İlgili Belgeler**, USAK Raporları No:11-03,Nisan 2011, http://www.usak.org.tr/_files/2942016144245-TYMHBSBGOI.pdf, (17.06.2016), s. 9.
[235]ABS-CBS News, **1,796 memos from US embassy in Manila in WikiLeaks Cablegate**, http://news.abs-cbn.com/nation/11/29/10/1796-memos-us-embassy-manila-wikileaks-cablegate,(16.06.2016).
[236]The Guardian, "**Assange Walks Free after Nine Days in Jail**", http://www.theguardian.com/media/2010/dec/16/julian-assange-walks-free-nine-days-jail?intcmp=239, (16.06.2016).
[237] "Uluslararası Stratejik Araştırmalar ….", op. cit, s. 5.

ise ABD'li yetkililer ile çeşitli ülkelerin yetkilileri arasında yapılan görüşmelerin tutanaklarından oluşuyor. WikiLeaks belgelerinin en önemlileri bu üçüncü kategoride yer alıyor. Tarafların birbirlerine söyledikleri cümleler, virgülüne dokunulmadan, tırnak içinde sunuluyor. Bu zabıtların inkârı mümkün değil. Zira ABD Dışişleri Bakanlığı belgelerin otantik ve orijinal olduğunu çoktan kabul etti", yorumunda bulunmuştur.[238]

WikiLeaks belgelerinin yayımlanma süreci ve içeriği ile ilgili olarak istihbarat tekniği ve siber güvenlik ilişkisi kapsamında bir analiz yapılması halinde, konuyla ilgili olarak aşağıdaki yorumlarda bulunabiliriz.

1. WikiLeaks belgelerinin yayımlanması, hızla gelişen iletişim teknolojisinin, kişilerin ve devletlerin (ABD) gizli hayatlarını açığa çıkarmak amacıyla kullanılabileceğini, bu kapsamda ortaya çıkan bilgilerin ise uluslararası ilişkiler ve devlet-toplum ilişkileri açısından çok ciddi sonuçlar meydana getirebileceğini ortaya koymuştur.

2. Ortaya çıkan belgelerdeki iddiaların belli coğrafyalarda yoğunlaşması belgelerin seçilerek ve belli bir amaç doğrultusunda ayıklanarak yayınlandığı izlenimini doğurmaktadır. Gerçekten de yayınlanan belgelerde Irak Savaşı, Türkiye ve Ortadoğu ile ilgili ciddi iddialar yer alırken, örneğin İsrail'i zor durumda bırakacak ifadelere rastlanmamaktadır. Ayrıca bu belgeler arasında sadece *"gizli"* olanlar yer alırken, *"çok gizli"* belgelerin bulunmaması da kuşku uyandırmaktadır.[239]

3. WikiLeaks Olayı'nın siber güvenlik literatürüne yeni tartışmalar kazandırdığı açıktır. Bu itibarla bu skandal, alınan tüm tedbirlere rağmen, dijital ortamda saklanan hiçbir bilginin gizliliğinin garanti edilemeyeceğini ve sistemdeki insan unsurunun her zaman sızıntılara neden olabileceği gerçeğini ortaya koymuştur. Bu kapsamda, WikiLeaks *"iletişim teknolojilerinin gelişiminin devlet-toplum ilişkileri üzerindeki etkisi"* ile "*devletlerin gizliliği ilkesi"* arasındaki etkileşimi tartışmaya açması bakımından önem kazanmıştır.

4. WikiLeaks, internet bazlı gazetecilik anlamında yeni bir model ortaya koymuştur. Bu çerçevede, WikiLeaks, günümüz dünyasında artık, internet teknolojileri kaynaklı olarak: *"savaş, cinayetler ve tutukluluk, ticaret, şeffaflık, ifade ve basın özgürlüğüne baskı,*

[238] ÇAĞRI Erhan, **Diplomaside Wiki-Tsunami**, http://www.turkiyegazetesi.com.tr/yazarlar/prof-dr-cagri-erhan/473614.aspx, (17.06.2016).
[239] "Uluslararası Stratejik Araştırmalar …", op. cit., s. 6.

diplomasi, espiyonaj, kontr-espiyonaj, ekoloji, iklim, doğa ve bilim, yolsuzluk, finans, vergiler, sansürleme teknolojisi, internet filtrelemesi, tarikatlar ve diğer dini örgütler, şiddet, ihlal ve suiistimal" gibi konulara odaklanan "*sızıntı gazeteciliğinin"* en etkili örneğini oluşturmuştur. Bu modeli savunan yeni nesil gazeteciler, konu kapsamında kar amacı gütmedikleri için diğer basın yayın kuruluşları ile işbirliği içerisinde çalıştıklarını, yani geleneksel yöntemlerden farklı olarak diğer medya kuruluşları ile yarışa girmediklerini iddia etseler bile, bu tür gazeteciliğin istihbarat servislerinin bilgi akışı desteği ve manipülasyonu olmadan beslenemeyeceği ve varlığını idame ettiremeyeceği de açıktır. Ayrıca, Türkiye'de Taraf Gazetesi'nin 2014 yılına kadar sürdürdüğü yayın politikası ile kamuoyunda *"Panama Belgeleri"* olarak tanımlanan skandalın da, bu tür *"sızıntı gazeteciliğinin"* birer örneğini oluşturduğu ileri sürülebilir.

5. WikiLeaks, bilginin bir güç olduğunu, bir devletin sahip olduğu bilginin herkes tarafından bilinmesinin, o devletin gücünü azaltacağını ortaya koymuştur.[240] Bu itibarla, ABD gibi dev bir teknolojik gücün, küresel gücünü sürdürmesi noktasında ihtiyaç duyduğu bilgiyi muhafaza ederken bile zorlanmasının, günümüz dünyasında siber güvenliğin sağlanmasının devletlerin bekası için nedenli önemli olduğunu göstermesi bakımından oldukça önemlidir. Bu itibarla WikiLeaks Olayı süresince, ABD'nin dijital ortamda muhafaza ettiği sırlarına hakim olmakta zorlanan bir ülke görüntüsü vermesi, ABD'nin küresel hegemonyasına bir darbe olarak da okunabilecektir.

WikiLeaks ve Snowden olayları ile ilgili tespitlerimizde de açıkça görüldüğü üzere uluslararası sistemde ABD, RF ve ÇHC gibi küresel güç olan devletler, siber saldırıları ve yeni nesil enformasyon savaşı tekniklerini önemli bir stratejik savunma ve rakibe zarar verme yöntemi olarak görmeye başlamışlardır. Siber alandaki faaliyetlerin kolay ve arkada iz bırakmadan yapılabilir oluşu da bu yöntemi teşvik eden en temel faktörlerden birisidir.

Bu kapsamda siber alanda yaşanan gelişmeler yeni güvenlik risklerini beraberinde getirmiştir. Bu riskleri bertaraf etme noktasında ise devletlerin önemi daha da artarken, devletler bu konuda strateji geliştirmekte zorlanmıştır. Zira küçük gruplar ve bireylerin kaynaklık ettiği siber saldırılar ile uluslararası sistemin yapısının, neo-realist paradigmalara uygun şekilde eskisinden daha belirsiz ve anarşik bir hale dönüşmeye başladığı ileri sürülebilir.

[240]KOÇ Şanlı Bahadır, **Wikileaks Üzerine Notlar ve Yorumlar**, http://www.21yuzyildergisi.com/assets/uploads/files/16.pdf,(17.06.2016)

Bu itibarla siber uzay alanının doğası gereği, tehdidin kaynağını belirsiz kılmasının, benzer şekilde tehdidin yeri, zamanı, kökeni hakkında önceden kestirilemeyen şartları mahiyetinde barındırmasının, uluslararası sistemi Soğuk Savaş dönemine kıyasla çok daha anarşik bir yapıya dönüştürdüğü değerlendirilebilir. Ayrıca siber uzay alanını düzenleyen evrensel nitelikte kesin ve nihai bir uluslararası hukuk düzenlemesinin hala yapılmaması, siber uzayda devletler arasında işbirliği yerine daha rekabetçi politikaların hakim olması ve bu rekabetin şiddetinin giderek artması hususları dikkate alındığında, uluslararası sistemin eskisinden çok daha fazla belirsiz ve güvensiz bir hal aldığı da ileri sürülebilir.

Benzer bir şekilde devletlerin siber güvenlik stratejilerinin temel itibarıyla gizli olması, bu bağlamda bir devletin gerek hasım olduğu gerekse müttefik olarak kabul ettiği bir devlete yönelik gizli bir siber faaliyet yürütüp yürütmediğinin kesin olarak bilinememesi de uluslararası sisteminin anarşik yapısının derinleşmesine neden olan etmenler olarak karşımıza çıkmaktadır.

Siber uzayın yarattığı imkânların uluslararası sistemde devlet dışında aktörlerin (çok uluslu şirketler, çıkar ve baskı grupları, hükümet dışı aktörler, medya destekli sosyal hareketler, bireyler vb.) çeşitliliğini ve önemini arttırdığı gerçeğine rağmen, neo-realist bir bakış açısıyla siber uzaydaki gelişmelerin aynı zamanda devletin rolünü daha da pekiştirdiği de ifade edilebilecektir. Zira bağımsız kabul edilseler bile devlet dışı aktörlerin uluslararası sistemde kalıcı bir tesir yaratabilmeleri, büyük ölçüde devlet destekli bir planlamaya dahil edilebilmeleriyle mümkün olabilmektedir. Bu itibarla çalışmamızda da irdelendiği haliyle Snowden ve Assange'ın faaliyetlerinin arka planında yer aldığı iddia edilen RF ve ÇHC kaynaklı teşvik ve yönlendirmeler hatırlanmalıdır.

Kısacası, teknolojik gelişmelerin boyutu ne olursa olsun uluslararası sistemde hala temel belirleyici ve oyun kurucu temel aktör devletlerdir. Zira siber uzay alanındaki genişlemeye bağlı olarak, devletler düşman devletlerden veya devlet dışı aktörlerden gelecek olan tehditlere siber güvenlik stratejileri kapsamında siber ordular ve siber güvenlik kurumları tesis ederek, ayrıca siber uzmanlar ve akademisyenler yetiştirerek reaksiyon göstermektedirler. Bu bağlamda gerek bireylerden gerekse de hasım devlet destekli olarak siber uzaydan gelebilecek tehditlere ancak merkezi bir devlet yapılanması ile karşı konulabileceği ve etkili bir siber savunma sistemi gerçekleştirilebileceği

tartışmasızdır.[241] Bununla birlikte, ulusal internetin, ulusal interneti denetleyen mekanizmaların, ağ teknolojilerinin ve buna bağlı olarak planlanan güvenlik stratejilerinin devletler tarafından kontrol edildiği dikkate alındığında, uluslararası sistemde reelpolitik paradigmalara uygun bir şekilde devletin başat rolü hala kesin ve nettir.[242] Tüm bu gelişmelerin de devletlerin uluslararası sistemdeki hâkim aktör rolünü pekiştiren faktörler olarak değerlendirilmesi gerekmektedir.[243]

WikiLeaks ve Snowden olayları kapsamında irdelenmesi gereken diğer bir husus ise çalışmamızın ilk bölümünde ele aldığımız ve Nye tarafından da güç dağılımı (diffusion of power) kavramı ile analiz edilen tespitlerdir. Bu kapsamda Nye siber uzayı, gücün dağılımına etki eden enformasyon devrimine en uygun örnek olarak tanımlamaktadır. Nye, konu ile ilgili olarak ise *"enformasyon devrimi ile birlikte, seyahat ve iletişim imkânlarının geçmişe göre oldukça kolaylaştığını, bir zamanlar küçük şirketlerin ya da bireylerin erişiminin yüksek maliyetli, hatta imkânsız olduğu bilgisayar teknolojilerinin, artık herkes için ulaşılabilir hale geldiğini, bunun sonucu olarak artık dünya siyasetinde sadece devletlerin değil diğer aktörlerin de (terörst gruplar, bireyler, uluslararası şirket ve örgütler, sivil toplum kuruluşları vs.) etkin olmaya başladığını*" ifade etmektedir. [244]

Bununla birlikte Nye, siber uzay alanı kaynaklı yeni gelişmelerin ortaya çıkardığı söz konusu güç yayılması durumunun son noktada asla devletlerin uluslararası sistemdeki temel aktör rolünü değiştirmeyeceğini de savunmaktadır. Nye savunduğu bu duruma, bir devletin kritik altyapılarını tamamen çökertmeye yönelik bir saldırının düzenlenmesine hedefleyen sofistike planlamaların ve bu planlamalara ait maliyetlerin günümüzde sadece devletlerin bilgi birikimi, tecrübeleri ve bütçeleri ile karşılanabiliyor olması, örnek olarak gösterilebilir.[245] Bu noktada Snowden ve Assange'ın faaliyetlerinin en başından bu yana özellikle RF, kısmen ise ÇHC tarafından nasıl himaye edildiği de çalışmamızda ana hatlarıyla özetlendiği haliyle tekrar irdelenmelidir.

ABD'nin küresel gücünü sarsan bir diğer gelişme ise RF hükümeti ve Rus istihbarat örgütleri ile bağlantılı hacker gruplarının ABD'nin başkanlık seçim sürecini etkilemeye

[241] LEWIS, loc.cit.
[242] VENTRE, loc.cit.
[243] ERIKSSON and GIACOMELLO, loc.cit.
[244] New Times Haber Portalı, **Röportaj/Joseph Nye:Bugün Bireylerin Güç Pastasından Aldıkları Pay, Geçmişe Göre Çok Daha Büyük**, http://newtimes.az/tr/interview/3042/, (13.04.2016).
[245] NYE, "Cyber Power", op. cit., p. 14

yönelik olduğu iddia edilen geniş kapsamlı siber saldırı operasyonlarıdır. ABD medyasında yer alan ve ABD devlet kurumlarından sızan bilgilere dayanılarak hazırlanan haberlerde, söz konusu siber saldırıların RF hükümeti ve Rus istihbarat örgütleri ile bağlantılı gruplar tarafından gerçekleştirildiği, bu saldırıların amacının ise başkan adayı Hillary Clinton'ın seçim çalışmaları süreçlerine sızdırılan bazı e-postalar ile müdahale edilmek suretiyle diğer başkan adayı Donald TRUMP'ın desteklenmesi olduğu hususları yer almıştır.

6. RF'nin Siber Saldırı Yöntemleri ile ABD Başkanlık Seçimlerine Müdahale Ettiğine Yönelik İddialar

İlk olarak Demokrat Parti yönetimi, sonrasında ise ABD'nin siber güvenlik alanında faaliyet gösteren kuruluşları tarafından, RF'nin 2016 yılı içerisinde Demokrat Parti Ulusal Komitesi (DUK)'nin, Clinton'ın seçim kampanyası direktörü olan John Podesta ile ABD eski Dışişleri Bakanı ve aynı zamanda Demokrat Parti'nin seçim çalışmalarına aktif olarak destek veren Colin Powell'ın e-postalarını siber saldırı yöntemleri ile temin ettiği ve bu e-postalardan bazılarını kamuoyuna sızdırdığı, böylelikle de RF'nin aktif bir şekilde ABD seçim sürecini kendi ulusal çıkarları kapsamında manipüle ettiği iddia edilmiştir.[246]

Söz konusu siber saldırılar ile ilgili olarak ise açık kaynaklarda yer alan haberlerde, RF istihbarat örgütlerinin bizzat V. Putin'in talimatıyla bu saldırıları organize ettiği, bahse konu saldırıların nedeninin ise 2012 yılında RF başkanlık seçimlerine yönelik olarak Clinton'ın da dışişleri bakanı olarak yer aldığı ABD yönetiminin Putin karşıtı açık ve örtülü faaliyetleri olduğu hususları da gündeme getirilmiştir.[247]

RF tarafından gerçekleştirildiği iddia edilen siber saldırılar, 2015 yaz ayları içinde başlayacak şekilde RF iç istihbarat örgütü FSB, RF askeri istihbarat örgütü GRU (Glavnoye Razvedyvatel'noye Upravleniye) tarafından bizzat veya bu örgütler tarafından desteklenen hacker grupları vasıtasıyla gerçekleşmiştir. Söz konusu hacker grupları arasında yer alan ve FSB tarafından desteklendiği iddia edilen yapılanmaların adları, Cozy Bear, the Dukes ve APT 29'dur. GRU tarafından desteklendiği iddia edilen grup ise Fancy

[246] Türk İnternet Haber Sitesi, **Clinton'a 4 ay Boyunca Yapılan Siber Saldırılar, Seçimleri Manipule Etti**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=55005, (20.02.2017).
[247] NY Times, **Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says**, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html, (20.02.2017).

Bear veya APT 28 olarak isimlendirilmektedir. Ayrıca "Guccifer 2.0" adıyla bireysel olarak faaliyet gösteren bir hacker yapılanması da bahse konu saldırılarda rol oynamıştır. Saldırılar, "spread phishing" şeklinde ifade edilen hedef odaklı ve yemleme yöntemleri ile gerçekleştirilmiştir. Bu yöntemle, hedef kurum ve şahısların e-postaları (50-60 bin civarı) siber casusluk amaçlı kötü yazılımlar ile temin edilerek, manipülasyonun amacına uygun olanları çeşitli internet sayfaları ve medya kuruluşları (WikiLeaks, The New York Times, DC Leaks, The Washington Post, The Wall Street Journal) tarafından kamuoyuna ifşa ettirilmiştir.[248]

Söz konusu ifşalar neticesinde ise ABD Demokrat Parti seçim propaganda sürecinin kısmen etkilendiği ileri sürülebilir. Bu kapsamda DUK Başkanı Debbie Wasserman Schultz ve bazı üst düzey görevliler istifa etmiş, Demokrat Parti'nin diğer başkan adayı Senatör Bernie Sanders'in pozisyonu güçlenmiş ve adaylık yarışına bir süre daha devam etmesi sağlanmış, Cumhuriyetçi Parti'nin eline Demokrat Parti'nin aleyhine kullanabileceği bir koz verilmiş, Clinton ismi tartışmalı hale gelerek, yıpratılmıştır.[249]

Bununla birlikte söz konusu siber saldırılar neticesinde ifşa edilen e-postaların yarattığı olumsuz etkinin Clinton karşısında Trump'ın zaferini sağlayan en önemli faktör olduğunu gündeme getirmenin de iddialı bir değerlendirme olduğu da düşünülebilecektir. Bu noktada Trump'ın seçim zaferi sonrasında anılanı yıpratmak ve baskı altına almak amacıyla ABD'deki bazı çevrelerin söz konusu siber saldırıları sürekli gündemde tutarak, Trump aleyhine kullanmakta olduğu da bizce dikkate alınması gereken bir durumdur.

Söz konusu siber saldırılar ile ilgili olarak FBI ve DHS tarafından ortak olarak hazırlanmış olan bir raporda ise RF, bu siber saldırıların planlayıcısı olarak doğrudan suçlanmıştır. Ayrıca bahse konu raporla birlikte yayımlanan 29 Aralık 2016 tarihli medya bildirisinde, belirtilen raporda gündeme gelen siber saldırıların da ötesinde, Rus istihbarat unsurlarının ABD hükümet kuruluşlarını, sivil toplum örgütlerini, üniversiteleri, ABD kritik altyapılarını, düşünce kuruluşlarını, teknoloji üreten şirketlerini hedef alan siber

[248] NY Times, **Hackers to the U.S. Election**, https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html, (20.02.2016).
[249] Türk İnternet Haber Sitesi, **Beyaz Saray, Rusya'nın Hackleme Operasyonuna Cevap Verileceğini Açıkladı**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=54247, (20.02.2017).

saldırılar planlamakta olduğu da gündeme getirilmiştir.[250] Bununla birlikte DHS tarafından 30 Aralık 2016 tarihinde yapılan bir başka medya açıklamasında:[251]

-RF sivil ve askeri istihbarat yapılarının son dönemlerde ABD hükümetini ve vatandaşlarını hedef alan sofistike ve agresif siber operasyonlar düzenlediği,

-ABD güvenlik ve istihbarat kurumlarının bu saldırıları "Grizlly Steppe" takma adıyla tanımladığı,

-"*Grizlly Steppe*" faaliyeti ile RF'nin ABD'nin hükümet kuruluşlarına, üniversitelerine sivil toplum ve düşünce kuruluşlarına, siyasi partilerine "spread phishing" şeklinde ifade edilen hedef odaklı ve yemleme yöntemleri ile siber casusluk operasyonları düzenlediği ve elde ettiği gizli bilgileri üçüncü ortaklar vasıtasıyla kamuoyuna ifşa ettiği, belirtilerek, söz konusu "spread phishing" operasyonlarının yazılımlarına ve uygulanma şekillerine ait bazı teknik detaylar kamuoyuyla paylaşılmıştır.

DHS tarafından RF hükümetine yapılan açık suçlamalar sonrasında, Obama yönetimi tarafından çoğunluğu GRU mensubu olduğu iddia edilen 35 Rus diplomatın, ABD başkanlık seçimlerini hedef alan siber saldırılarda görev yaptıkları iddiasıyla sınır dışı edilmesi ile Maryland ve New York'taki Rus diplomatik temsilciliklerinin kapatılması kararı alınmıştır.[252] Söz konusu sınır dışı kararı karşısında ise RF tarafı belirtilen suçlamaları kabul etmediği açıklamıştır. Putin tarafından konuyla ilgili olarak yapılan açıklama ise "*gelişmelerin kendileri tarafından Washington yönetiminin attığı yeni düşmanca adımlar ve provokasyon olarak nitelendirildiği, hiç kimseyi sınır dışı etmeyecekleri ve ABD'ye verilecek yanıtı Trump yönetiminin tutumuna göre belirleyecekleri*" ifade edilmiştir.[253]

---

[250] Department of Homeland Security, **Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity**, https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity, (20.02.2017).

[251] Department of Homeland Security, **ExecutiveSummary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale**, https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary (20.02.2017).

[252] Sputniknews Haber Portalı, **Beyaz Saray ABD, 35 Rus Diplomatı 72 Saat İçerisinde Sınırdışı Edecek**, https://tr.sputniknews.com/abd/201612291026553306-abd-rusya-yaptirim-diplomat-sinir-disi/, (22.02.2017).

[253] Sputniknews Haber Portalı, **Putin'den ABD'ye Yanıt: Biz Hiç Kimseyi Sınır Dışı Etmeyeceğiz.**, https://tr.sputniknews.com/rusya/201612301026565257-putin-abdye-yanit-biz-hic-kimseyi-sinir-disi-etmeyecegiz/, (22.02.2017).

ÜÇÜNCÜ BÖLÜM
RUSYA FEDERASYONU'NUN
SİBER GÜVENLİK STRATEJİSİNİN ANALİZİ

Siber uzay olarak adlandırılan alanda, ağ teknolojileri temelli teknolojik gelişmelere bağlı olarak ortaya çıkan yeni şartlar, uluslararası ilişkiler disiplini kapsamında ele alınan güvenlik yaklaşımlarını da temelden etkilemiştir. Artık devletler siber uzay kaynaklı yeni tehdit ve fırsatlar kapsamında klasik güvenlik anlayışlarında revizyona giderek, ulusal savunma stratejilerinde siber güvenlik merkezli planlamalara yer vermeye başlamışladır.

RF ve ABD'nin ağ teknolojilerinin ortaya çıkardığı yeni imkânları kullanmak suretiyle gerek askeri kapasitelerini ve espiyonaj imkânlarını geliştirmek adına yaptıkları planlamalar gerekse ülkelerinin siber güvenliklerini sağlamak adına ortaya koydukları strateji ve doktrinler çerçevesinde özellikle de 2000'li yılların başından itibaren siber uzay merkezli gelişmeleri domine ettikleri görülmektedir. Ayrıca RF ve ABD'nin siber güvenlik stratejilerini belirleyen faktörlerin, söz konusu yıllardan bu yana karşılıklı olarak etkileşim halinde olması ve adeta bir etki-tepki ilişkisi kapsamında şekillenmesi nedeniyle de siber güvenlik çalışmaların uluslararası ilişkiler disiplini kapsamında özel bir öneme sahip olmaya başladığı iddia edilebilir.

Bu çerçevede siber uzayda meydana gelen gelişmelerin, devletlerin ulusal düzeyde bir siber güvenlik sistematiğinin ve planlamasının geliştirilmesi noktasındaki öncü rolü nedeniyle devletlerin uluslararası sistemdeki temel aktör pozisyonunu pekiştirmekte olduğu açıktır. Ayrıca devletlerin siber uzay alanındaki gelişmeleri askeri kapasitelerini geliştirmek adına yeni bir fırsat olarak okudukları, bununla birlikte siber uzayın anonim yapısının tehdit kavramını asimetrik hale getirmek suretiyle uluslararası sistemi eskiye kıyasla çok daha anarşik hale dönüştürdüğü de son yıllarda çok daha net ortaya konmaktadır.

Öte yandan SSCB, Soğuk Savaş döneminde ABD ile tecrübe ettiği askeri rekabetin bir sonucu olarak sahip olduğu teknolojik altyapısını, Soğuk Savaş sonrası döneme büyük ölçüde RF'ye aktarmıştır. Bu potansiyelin özellikle 2000'li yıllar sonrasında askeri gücünü geliştirme noktasında RF tarafından yeni bir fırsat olarak gördüğü ileri sürülebilir. Bu kapsamda da RF, günümüzde siber savunma ve saldırı kapasitesine yaptığı büyük

teknolojik yatırımlar ile birlikte, istihbarat servisleri, bu servisleri ile bağlantılı olarak faaliyet gösteren siber kriminal suç örgütlenmeleri, silahlı kuvvetlerinin ağ teknolojileri temelli askeri imkânları, tüm bu faaliyetleri küresel ölçekte destekleyen uluslararası medya kuruluşları ve sosyal medya imkânlarından da istifade edebilen diğer enformasyon savaş enstrümanlarını birlikte kullanabilen küresel siber güç haline geldiği değerlendirilebilir. Bu değerlendirmemizin daha net olarak irdelenebilmesi amacıyla da çalışmamızda RF'nin küresel siber güç haline gelme süreci tüm yönleri ile analiz edilecektir.

1. RF'nin Siber Güvenlik Stratejinin Temelleri

RF, siber güç olarak günümüzde siber uzayı domine eden en önemli devletlerden biri konumundadır. RF, internetin genişleyip yayılmaya ve günlük hayatımızın hemen her alanını etkilemeye başladığı 2000'li yılların başından itibaren, siber uzay olarak adlandırılan alanda etkinlik sağlamak amacıyla planlama ve stratejiler geliştirmektedir.

Tarihsel olarak SSCB döneminden günümüze kadar ulaşan stratejik ve teknolojik aklın da etkisiyle, RF'nu siber kapasitesini saldırı ve savunma yönünde genişletme eğilimindedir. Örneğin SSCB döneminde, Komitet Gosudarst Bezopasbosti (KGB)'nin dış operasyonlarının önemli bir bölümünün, Batı bloğundaki teknolojik gelişmeleri yakından takip ederek teknolojik casusluk yoluyla bu buluşları SSCB'ye aktardığı bilinmektedir.

Bu geleneksel yöntem, Soğuk Savaş dönemi sonrasında da Rus İstihbarat Servisleri (RİS)'nin dış operasyonlarında belirleyici bir etken olmuştur.[254] Diğer yandan SSCB Ordusu'nda teknolojik gelişmeleri askeri doktrinlere adapte eden fikirlerin daima teşvik edildiği, söz konusu geleneğin ise günümüz RF Silahlı Kuvvetleri (RSK)'nde de devam ettiği genel kabul görmüştür. Böyle bir uygulamanın neticesi olarak, 1920'li yıllarda Sovyet yazarları tarafından uzayda savaş uçaklarının it dalaşı yapabileceği fikirlerinin ortaya konduğu da bilinmektedir.[255] Diğer yandan 1920'ler için bir hayal olan bahse konu fikirlerin, 1980'lerin başı ile birlikte ABD'nin "Yıldız Savaşları Projesi"[256] ile gerçeğe

[254]WIRTZ J.James, **Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy**,NATO CCD COE Publications, Tallinn 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf, (05.03.2016), p. 30.
[255] Ayrıntılı bilgi için bkz. Ibid., pp. 33-34.
[256]"Stratejik Savunma Girişimi" bilinen adıyla"Yıldız Savaşları Projesi",1980'li yıllarda, ABD BaşkanRonald Reagan tarafından tasarlanan bir askeri planlamadır. Bu proje, ABD'nin Soğuk Savaş dönemindeki rakibi SSCB'nin kıtalararası balistik füzelerini uzaydan kontrol edilen lazer ışınları ile henüz ABD topraklarına ulaşmadan yok etmesi üzerine kurulu bir bilim kurgu ürünü ve gerçek dışı bir projedir. Anılan projede, uzayda belirli koordinatlarda konuşlandırılmış olan ABD uyduların, merkezden veya kendilerinin tespit

dönüştüğü de görülecektir. Bu noktada söz konusu projenin geliştirilmesine ilham veren temel düşüncenin SSCB dönemindeki bahse konu eğilimden kaynaklandığı iddiasının, ABD otoriteleri tarafından hiçbir zaman inkar edilmediği gerçeği de dikkate alınmalıdır.

RF'nin güncel siber politikalarını etkileyen önemli diğer bir tarihsel ve kültürel faktör ise Rus siyaset kültürünün savaş olgusuna bakışı ile ilgilidir. Rus politik elitleri için savaş, tarih boyunca bir politik hareket tarzı ve şerefli bir imge olarak kabul edilmiştir.[257] Bu yaklaşım ile birlikte Rus kültürü için savaşın veya sıcak bir çatışmanın politik çıkarların uygulanması noktasında sıklıkla başvurulmaktan çekinilmeyen bir yöntem olarak geliştiği de belirtilebilecektir. Bu kabulden hareketle, günümüzde RF'nin askeri doktrinlerini belirleyen üst aklın, siber uzayı bir savaş alanı olarak gördüğü ve Rus devletinin çıkarları doğrultunda bu alanda siber saldırı ve savaş yöntemleri ortaya koydukları belirtilebilir.

Bu bağlamda 1980'lerde Sovyet Ordusu'nda üst düzey görev yapan Mareşal Nikolai Orgakov tarafından başlatılan Revoluation in Military Affairs (RMA) Programı, günümüz Rus Siber Stratejisi'nin temeli olarak kabul edilebilir.[258] Orgakov, bu program ile birlikte kitlesel ve hantal bir yapıya sahip Sovyet Silahlı Kuvvetleri'ni ağ teknolojileri ve teknik operasyonlar ile takviye edilen ve yönetilen, daha etkin bir yapılanmaya kavuşturmayı hedeflemiştir. Orgakov'un bu misyonu ile birlikte, 1980'ler boyunca kimi Sovyet askeri stratejistleri, enformasyon teknolojilerindeki önemli gelişmelerin orduların kapasitelerinin artırılması noktasında kullanılabileceğini değerlendirmişlerdir. Ayrıca anılan uzmanlar, silahlanma yarışının 21.yy.'da klasik anlamından çıkarak enformasyon alanına kayacağını tahmin etmişler ve bu alanda planlamalar yürütmüşlerdir.

1990-1991 Körfez Savaşı esnasında, Koalisyon güçlerinin kullandığı iletişim ve enformasyon tekniklerinin, Irak Silahlı Kuvvetleri'nin harekât kabiliyetine verdiği zararın yanı sıra Koalisyon güçlerine kazandırdığı hız, dönemin Rus askeri uzmanları tarafından da yakından izlenmiştir. Bununla birlikte, I. Körfez Savaşı'ndaki sıcak çatışmaların dünya

---

ettikleri balistik füzeleri, güçlendirilmiş lazer ışınlarını bahse konu balistik füzelerin üzerlerine odaklayarak havada yakmaları ve böylece bir tehdit oluşturmadan imha etmeleri hedeflenmiştir. Yıldız Savaşları Projesi, 1980'lerde ekonomisi çökmeye başlayan SSCB'nin kaldıramayacağı kadar büyük bir mali yük getirdiğinden, SSCB bu tasarıya eş değer veya daha üstün değerde bir karşılık verememiştir.

[257]WIRTZ, op. cit., p. 35.

[258]Ayrıntılı bilgi için bkz. MOWTHORPE Matthew, **The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views**, file:///C:/Users/tk44655/Downloads/2011.06.02-Maturing-Revolution-In-Military-Affairs1.pdf, (05.03.2016), pp. 1-5.

kamuoyuna adeta canlı olarak aktarılmasında, kitle iletişim araçlarının ortaya koyduğu imkân ve kabiliyetin anlaşılması noktasında Rus uzmanlarca dikkatle tecrübe edilmiştir. Fakat söz konusu dönemde Rus toplumun içinde bulunduğu ekonomik ve sosyal çöküntü nedeniyle Rus Ordusu'nun iletişim teknoloji konusundaki gelişmeleri silahlı kuvvetlerin mevcut yapısına adapte etme noktasında çalışma yapması için, 2000'li yılları beklemesi gerekmiştir.[259]

1979-1989 arasında devam eden Afganistan Savaşı esnasında, Sovyet Ordusu'nun psikolojik savaş tekniklerini uygulamada ve Afganistan'daki saha birlikler ile Moskova Riyaseti arasında etkili bir iletişim sağlama noktasında yeterince başarılı olamadığı ortadadır.[260] Benzer şekilde 1994-1996 yıllarındaki Çeçen Savaşı sırasında, internet haberleşmesi ve internet haberleşmesinin ortaya koyduğu imkânlar, savaş esnasındaki olayların RF aleyhine yansıtılması kapsamında oldukça başarılı olmuştur.[261] Bu kapsamda RF, uluslararası kamuoyu nezdinde Çeçen Savaşı'nda insanlık dışı yöntemlere başvuran, savaş suçu işleyen bir devlet olarak kabul edilmiştir.[262] Söz konusu iki olayın olumsuz etkisiyle, Rus güvenlik ve askeri bürokrasisinin "*askeri ağ teknolojileri*" ve "*enformasyon savaşı*" alanındaki planlamaları ve hazırlıkları hızla gelişmeye başlamıştır. Bu planlamanın bir sonucu olarak, NATO güçlerinin 1999 yılında eski Yugoslavya'daki Sırp güçlerini bombalamaya başlaması ile birlikte, Sırp ve Rus hackerlar tarafından NATO'ya, üye ülkelerin askeri haberleşme sistemlerine, ABD Savunma Bakanlığı'nın alt yapılarına siber saldırılar gerçekleştirilmiştir.[263]

Yukarıda genel ve soyut olarak aktardığımız üzere RF'nin geçmişte edindiği tecrübeler ile geliştirdiği ve sürekli olarak ortaya koyduğu yeniliklerle de etkinliğini arttırdığı siber gücünün ulaştığı kapasite, günümüzde başta ABD olmak üzere, NATO üyesi ülkelerin yanı sıra RF'nin komşuları için de ciddi bir tehdit olarak değerlendirilebilecek seviyeye ulaşmıştır. Bu noktada, ABD Ulusal İstihbaratı'nın Başkanı James Clapper'ın "ABD İstihbarat Topluluğu'nun Dünya Tehdit Değerlendirmeleri- 2015" başlıklı bir sunumda, RF'nin siber savaş gücü için: *"Burada detaylara giremem ama*

[259]HEICKERO Roland, **Emerging Cyber Threats and Russian Views on Information Warfare and Operation**, Swedish Defense Research Agency Press**,** March 2010, http://www.foi.se/rapport?rNo=FOI-R--2970--SE, (23.06.2016), p. 15.
[260]Ibid.
[261]BIÇAKCI, "21. Yüzyılda Siber …", op. cit.,s.30.
[262]HEICKERÖ, loc.cit.
[263]BIÇAKCI, "21. Yüzyılda Siber …", loc.cit.

Rusya'nın siber tehdidi daha önce tahmin ettiğimizden çok daha ağır..." yorumunu yapması dikkat çekicidir.[264]

RF günümüzde siber espiyonaj, siber kontr/espiyonaj, dezenformasyon, elektronik savaş, psikolojik savaş ve propaganda, siber saldırı gibi faaliyet ve planlamaları kapsayan geniş bir enformasyon savaşı kabiliyetine sahip olma noktasında ciddi gayret içindedir.[265] RF böyle etkin bir siber güce ulaşarak, siber uzaydaki yeniliklerin ortaya koyduğu imkân ve fırsatları, dış politika hedeflerine ulaşmak amacıyla kullanmayı planlamaktadır.

RF için stratejik ve teknolojik mirasın da etkisiyle siber uzayda yaşanmakta olan teknolojik gelişmeler ile askeri operasyonların yanı sıra askeri strateji ve politik çıkarlar arasında bir bağ kurarak, etkili bir siber saldırı ve savunma stratejisi ortaya koyan öncü devlet konumuna gelmek belki de kaçınılmaz bir sonuç olarak görülmelidir. RF günümüzde siber uzayda etkili bir siber savunma ve saldırı imkân ve kabiliyetine sahip ciddi bir aktördür. Bu gücün sistematiğine ve planlamasına yönelik detaylar ise RF'nin 2000'li yılların başından itibaren yayımladığı resmi siber güvenlik doktrin ve savunma stratejileri belgelerinin analiz edilmesi ile ortaya konabilecektir.

Bu bağlamda söz konusu bölümdeRF'nin siber güvenlik strateji belgeleri; RSK ile RİS'lerin siber kapasiteleri; RİS ile irtibatlı siber kabiliyete sahip bazı legal / illegal örgütlerin faaliyetleri ve RF'nin siber alanının yapısal özellikleri analiz edilerek, RF'nin siber güvenlik kapasitesi tespit edilmeye çalışılmıştır.

1.1. RF Ulusal Güvenlik Konsepti

Siber uzay ve siber güvenlik ile ilgili analizlerin uluslararası literatürde yoğun olarak tartışılmaya başlandığı 2000'li yıllar ile birlikte, RF'nin"*bilgi güvenliği*" kelimesinin ilk kez kullanıldığı resmi belgesi**,** 24 Ocak 2000 tarihinde yürürlüğe giren "*National Security Concept of Russian Federation / RF Ulusal Güvenlik Konsepti"* isimli dokümandır. Söz konusu belgede, bilgi güvenliği kavramı ile ilgili olarak:[266]

---

[264]Sputniknews Haber Portalı, **Rusya'nın Artan Siber Gücü, ABD'yi Kaygılandırıyor**, http://tr.sputniknews.com/savunma/20150409/1014919049.html, (21.03.2016).
[265]WIRTZ, loc.cit.
[266]NATO Cooperative Cyber Defence Centre of Excellence, **National Security Concept of Russian Federation**, https://ccdcoe.org/cyber-security-strategy-documents.html, (23.03.2016). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/99.html, (23.06.2016).

-Ekonomik, politik, bilimsel, teknolojik ve enformasyon alanında yaşanan gelişmelerin güvenlik kavramı ile ilgili yeni yaklaşımların oluşmasına neden olduğu,

-RF'nin enformasyon alanı ile ilgili olarak, vatandaşlarının güvenliği ve ekonomik çıkarlarının sağlanması noktasında telekomünikasyon güvenliğine önem vermesi ve bu alana yatırım yapması gerektiği,

-Rus ulusal güvenliğine yönelik olarak enformasyon teknolojileri kaynaklı artan bir tehdit yapılanmasının bulunduğu, bu kapsamda RF'nin asker güvenliğini hedef alan ve dış kaynaklı olan faaliyetler ile bilgi altyapısını etkilemeye ve manipüle etmeye yönelik iç tehditleri bertaraf etmesinin şart olduğu,

-Bu kapsamda Rus hükümetlerinin temel görevinin RF'ninenformasyon güvenliğini sağlamak noktasında, enformasyon güvenliğini tehlikeye düşürecek olan faaliyetleri engelleyecek karşı faaliyetler yürütmesi gerektiği, ifade edilmektedir.

Görüldüğü üzere bahse konu belge temel olarak, enformasyon güvenliğinin öneminden, bu alanda Rus çıkarlarına yönelik iç ve dış tehditlerin varlığından ve bu tehditlere yönelik tedbirler alınmasından bahsetmektedir. Bu genel yapısı ile birlikte düşünüldüğünde belgenin, RF'nin siber güvenlik politikasının gelecekte nasıl şekilleneceğine yönelik olarak ciddi bir emare içermediği de görülmektedir. Bununla birlikte belgenin, Rus güvenlik bürokrasisinin siber uzay alanında meydan gelen gelişmeleri takip etmeye başladığını ve bu alanı bir tehdit algılaması ile anlamlandırma gayreti içerisinde olduğunu göstermesi bakımından önemli kabul edilebilecektir.

1.2. RF Enformasyon Güvenliği Doktrini

9 Eylül 2000 tarihli *"Information Security Doctrine of the Russian Federation / RF Enformasyon Güvenliği Doktrini"*, RF'nin siber güç olma hedefi yolundaki ilk temel belge olduğu belirtilebilecektir. Bu belge, RF'nin enformasyon güvenliği konusundaki yol haritasını, prensiplerini, amaçlarını ve konu kapsamındaki resmi görüşlerini genel hatlarıyla ortaya koymaktadır.[267] Belgede, RF'nin enformasyon güvenliğinin sağlanması konusundaki ulusal çıkarlarının temelde ekonomik yapının, sivil toplumun ve politik sistemin korunması ile sağlanabildiğine işaret edilmektedir.[268]

[267]MEDVEDEV, op. cit.,p. 55.
[268]Ministry of Foreign Affairs of the Russian Federation, **Information Security Doctrine of Russian Federation**,http://archive.mid.ru//bdomp/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd

Diğer yandan anılan belgenin birinci paragrafının üçüncü bölümü incelendiğinde, RF'nin 2000 yılı itibarıyla diğer devletlerden kaynaklanabilecek olası bir enformasyon savaşı tehdidine de göz ardı etmediği de görülebilecektir. Bu itibarla belgenin bu bölümünde özetle;"*yabancı ekonomik, askeri, istihbarat oluşumlarının RF'nin enformasyon güvenliği için tehdit oluşturduğu ve enformasyon savaşı (psikolojik savaş) alanında yeni tekniklerinin gelişmesinin dünya üzerindeki ülkelerin bilgi güvenliği ile ilgili olarak tehlikeler yarattığı*" hususları vurgulanmaktadır.[269]

Belgede RF'ninenformasyon savaşı konsepti 2000'li yılların ilk bölümü için potansiyel iki tehdit kaynağına odaklanmıştır. Söz konusu tehdit kaynaklarının ilki; RF'nin siyasi ve kültürel yapısını etkileyebilecek olan psikolojik savaş yöntemleri, diğeri ise RF'nin enformasyon ve teknoloji güvenliğini tehlikeye atabilecek olan siber savaş teknikleridir.[270] Belgede, ayrıca dünya üzerinde etkinlik sağlamaya çalışan devletlerin enformasyon güvenliği alanına ciddi yatırımlar yaptıkları, bu alanda yeni teknik ve silahlar geliştirdikleri, bu durumunda yeni bir silahlanma yarışına neden olabileceği, bu noktada RF'nin hazırlıklı olması gerektiği hususlarına da vurgu yapılmaktadır.[271]

Bahse konu doktrinin tonu daha çok savunma ağırlıklıdır. Belge bir bütün olarak ele alındığında, saldırgan bir üslup ihtiva eden her hangi bir beyanı ihtiva etmemektedir.[272] Bununla birlikte belgenin özellikle kitle iletişim araçlarının kullanımı ve yayınları ile ilgili olarak, demokratik bir üslup içermediği de ortadadır. Bu durum RF'nin söz konusu dönem için başta ABD olmak üzere, Batılı ülkelerden gelebilecek psikolojik savaş ve istihbarat tehditlerine karşı bir refleksi olarak değerlendirmelidir. Bu itibarla, belgede ister kamuya isterde özel sektöre ait olsun, medya kuruluşlarının Rus milletinin çıkarlarına uygun bir yayın politikası gütmesi gerektiği, bu kapsamda da Rus devletin tedbirler geliştirmesinin şart olduğu vurgusu dikkat çekicidir.[273]

24bc32575d9002c442b!OpenDocument, (23.03.2016). Ayrıntılı bilgi için bkz.http://www.scrf.gov.ru/documents/ 99.html, (23.06.2016).

[269]Ibid.

[270]THOMASL. Timothy, "Russia's Information Warfare Strategy: Can the Nation Cope inFuture Conflicts?", **The Journal of Slavic Military Studies**, Vol.27, No. 1, 2014, p. 275

[271]Ministry of Foreign Affairs of the Russian Federation, **Information Security Doctrine of Russian Federation**,http://archive.mid.ru//bdomp/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument, (23.03.2016)

[272]Ayrıntılı bilgiiçin bkz. GILES Keir, **Information Troops-A Russian Cyber Command?**, Paper presented atthe 3rd International Conference on Cyber Conflict, Tallinn, 2011, "Cooperative Cyber Defense Centre of Excellence", http://conflictstudies.org.uk/files/Russian_Cyber_Command.pdf, (23.03.2016), pp. 1-5.

[273]Ibid., p. 6.

1.3. "2020'ye Doğru Rus Ulusal Güvenlik Stratejisi" Belgesi

"Russia's National Security Strategy to 2020 / 2020'ye doğru Rus Ulusal Güvenlik Stratejisi" tüm açıklığı ile güvenlik meselesine odaklanması bakımından dikkat çekici bir belge olarak karşımıza çıkmaktadır. Söz konusu güvenlik strateji belgesi kabul edildiği tarih itibarıyla Rus güvenlik ve istihbarat servisleri için temel rehber ve plan niteliğine haiz önemli bir resmi dokümandır [274]

Söz konusu belgede, başta ekonomi olmak üzere, sağlık ve güvenlik stratejine ilişkin görüş ve planlamalara yer verilirken, enformasyon güvenliği konusu dolaylı olarak gündeme getirilmiştir. Bu kapsamda enformasyon güvenliği meselesi ile ilgili olarak, anılan belgede:[275]

-Uluslararası siber yeteneğe sahip teknolojik silahların Rus ulusal güvenliği için tehdit oluşturduğu,

-Bilgi teknolojilerindeki yeni gelişmelerin, önemli toplumsal, ekonomik ve kültürel yansımalara neden olduğu,

-Bilgi teknolojileri, telekomünikasyon ve iletişim teknikleri, bilgisayar yazılımları alanlarında dünyanın ciddi bir atılım içinde bulunduğu,

-Teknolojik yeniliklerin, küresel ağlar vasıtasıyla Rus ulusal bilgi altyapısı için önemli bir tehdit oluşturabileceği,

-Belirtilen tehditlerin bertaraf edilmesi noktasında, etkili ve fonksiyonel enformasyon ve telekomünikasyon altyapısı geliştirilmesi gerektiği, bu itibarla da Rus devletinin tekil (merkezi) bir enformasyon-telekomünikasyon destek sistemine ihtiyaç duyduğu, hususları yer almaktadır.

Görüldüğü üzere söz konusu belgede temel olarak güven artırıcı ve işbirliğini hedefleyen bir üslubun hâkim olduğu söylenebilecektir. Diğer yandan anılan belgede, Rus istihbarat ve güvenlik güçlerine Rus toplumun ve Rus devletinin kritik altyapıların korunması noktasında tedbirler alınması gerektiği işaret edilmek ile birlikte, bahse konu tedbirlerin detayı ve mahiyetine ilişkin bilgi verilmediği görülecektir. Bu itibarla da

[274]Ayrıntılı bilgi için bkz. Rustrans Useful Translations, **Russia's National Security Strategy to 2020**, http://rustrans.wikidot. com/russia-s-national-security-strategy-to-2020, (23.03.2016).
[275]Ibid.

belirtilen yumuşak ve savunmacı üslubun RF'nin siber güvenlik stratejilerinin gerçek amacının ve yapısının gizlenmesi hedefinde kaynaklandığı da değerlendirilebilecektir.[276]

1.4. "Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler" İsimli Belge

2011 yılında RF Savunma Bakanlığı tarafından yayımlanan*"Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space / Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler"*isimli belge, siber güvenlik analisti Keir Giles tarafından:*"Rus Ordusu'nun Ön Siber Savaş Doktrini"* şeklinde tanımlanmaktadır.[277] Bu kapsamda belgenin siber uzayda Rus askeri varlığını ve hareketliliğini kabul eden ilk açık belge olduğu da ileri sürülebilir.[278] Mezkûr belge, RF siber uzay konseptine yeni bir bakış açısı getiren tanımlar, kurallar ve güven arttırıcı tedbirlerden oluşan 15 sayfalık resmi bir görüş beyanı şeklindedir.

Bu dokümanda, diğer resmi RF stratejilerinin aksine bilgiyi merkeze alan bir bakış açısıyla siber faaliyetleri operasyonel bir mantık ve çatışma konsepti ile değerlendirme söz konusudur. Bu kapsamda belgede, enformasyon savaşı kavramı:*"bilgi sistemlerine ve kaynaklarına zarar veren, toplumun ve hedef hükümetleri psikolojik savaş yöntemleri ile devirmeyi amaçlayan, politik, ekonomik ve kültürel sistemin altını oyan faaliyetler"* şeklinde tanımlanmıştır.[279]

Defansif bir bakış açısının hâkim olduğu ifade edilebilecek olan belgede, siber uzay ile ilgili olarak Rus Devleti'nin askeri sorumluluklarından da bahsedilmektedir. Bu çerçevede, belgede:[280]

-RF Ordusu'nun, kendi enformasyon güvenliğini sağlamak zorunda olduğu ve bu bağlamda planlamalar geliştirmesi gerektiği,

-Bu bağlamda da ordununenformasyon güvenliğini tehlikeye sokması muhtemel tehditleri belirlemesinin şart olduğu,

---

[276]GILES, "Russia's Public Stance …", op. cit., p. 67.
[277]Ibid., 68.
[278]Ayrıntılı bili için bkz. The Russian Ministry of Defense, **Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space**, https://ccdcoe.org/strategies/Russian_Federation_ unofficial_translation.pdf, (23.03.2016).
[279]Ibid.
[280]GILES, "Russia's Public Stance …", op. cit., p. 69.

-Söz konusu tehditlerin belirlenmesi akabinde ise RF Ordusu'nun ve bu tehditlerin ordunun organizasyon yapısını, lojistik sistemini, kontrol yapısını ve silahlı gücünü olumuz olarak etkilemesini engelleyecek tedbirler almasının önem arz ettiği, vurgulanmaktadır.

Bu belgenin diğer resmi Rus siber güvenlik dokümanlarından bir diğer farkı ise belgede yer alan *"siber uzayda uluslararası işbirliğinin geliştirilmesi"* vurgusudur. Bu kapsamda, anılan belgede, RF'nin uluslararası enformasyon güvenliğinin sağlanması noktasında uluslararası standartların, kurumların, hukuk ve normların belirlenmesi amacıyla Birleşmiş Millet (BM) nezdinde girişimde bulunması gerektiği belirtilmektedir. Bahse konu durum ise RF'nin söz konusu belgeyi hazırlayan uzmanlarının, Rus Ordusu'nun mevcut teknolojik şartları dahilinde enformasyon güvenliğini sağlama noktasında yetersiz kalabileceği endişesinde kaynaklanmakta olduğu da değerlendirilebilmektedir.[281]

1.5. Gerasimov Doktrini

9 Kasım 2012 tarihinde RF Genelkurmay Başkanlığı görevine atanan Valery Gerasimov'un 27 Şubat 2013 tarihinde *"Military Industrial Kurier Dergisi'nde"* yayınlanan *"The Value of Science in Prediction"* adlı makalesinde ortaya koyduğu askeri yaklaşım, uluslararası ilişkiler alanında geniş yankı bulmuş ve "*Gerasimov Doktrini*" olarak tanımlanarak, tartışmaya başlanmıştır.[282]

Diğer yandan bahse konu makale hakkındaki tartışmaları mezkur dönemden günümüzde kadar hararetli bir şekilde sürdüren temel neden ise Gerasimov'un yaklaşımına uygun bir tarzda, RSK'nın 2014 yılındaki Ukrayna müdahalesi esnasında gösterdiği çok yönlü sıcak çatışma performans ile ilgilidir. Bu kapsamdaRSK Ukrayna müdahalesi sırasında, organize bir şekilde yönlendirilen ekonomik tedbirleri, siber saldırı yöntemlerini, yerel Rus azınlıkla koordineli bir şekilde gerilla faaliyeti gerçekleştiren özel piyade kuvvetlerinin operasyonlarını ve psikolojik savaş yöntemlerini kullanmıştır. Bu itibarla da RF tarafından Ukrayna müdahalesi esnasında ortaya koyduğu savaş performansı kimi analistler tarafından *"hibrit savaş, kirli savaş, non-linear war, yeni savaş, bulanık savaş konsepti"* şeklinde de tanımlanan yaklaşımlarla değerlendirilmiştir.

Çalışmanın bu bölümünde, söz konusu yaklaşım ve değerlendirmeler ele

[281]Ibid., p. 70.
[282]MEDVEDEV, op. cit., p. 56.

alınmayarak, doğrudan Gerasimov Doktrini'nin ortaya koyduğu prensipler analiz edilecektir. Diğer yandan bahse konu tartışmalar ile birlikte analiz edilecek şekilde, RSK'nın Ukrayna müdahalesi esnasındaki siber kabiliyetleri çalışmanın ilerleyen bölümlerinde ayrı bir başlık altında detaylıca değerlendirilecektir.

Bu çerçevede Gerasimov Doktrini ile ortaya konan prensipler dahilinde RF; askeri niteliğe sahip olmayan yöntemleri, askeri kapasitesine dahil ederek, daha az konvansiyonel güç ile dolayısıyla da daha az insan kaybı ve maliyet ile sıcak çatışma süreçlerini yönlendirmeyi ve yönetmeyi amaçlamıştır. Bu bağlamda askeri bir müdahale öncesinde; hedef bölge, ülke, topluluk ya da devlete yönelik olarak siber saldırılar ile avantaj sağlanması, hedefin yıpratılması, psikolojik savaş yöntemleri ile baskı altına alınması, moralinin bozulması, savunma direncinin kırılması, kritik altyapılarına zarar verilerek, ekonomisinin zarara uğratılması ortaya konmak istenen hedefler arasında yer almaktadır. Bu kapsamda Gerasimov, makalesinde özetle:[283]

-21. yüzyılda çatışma ile çatışmasızlık arasındaki çizginin giderek bulanık hale geldiğini, çatışma alanlarının siyah (savaş) ve beyaz (barış) alanlar yerine gri alanlara kaydığını, gri alan olarak adlandırılan bölgede ise askeri olmayan kapasitelerin kullanılması suretiyle hedef ülkede etkinlik sağlanabileceğini, klasik askeri kapasitenin ise istenen etkinlik sağlandıktan sonra elde edilen kazanımların korunması aşamasında devreye sokulabileceğini,

-Arap Baharı[284] ve Renkli Devrimler[285] örneklerinde de görüleceği üzere, hedef ülkeye

[283] Ayrıntılı bilgi için bkz. GERASİMOV Valery, "Tsennos' Nauki v Vredvidenii (Value of Applied Science)", **Voyenno-Promyshlennyy Kuryer**, February 27, 2013, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, (24.03.2016).

[284] Arap Baharı (Arapça: Al-Thawrāt al-'Arabiyyah), 2010 yılında başlayan ve günümüzdede süren,Arap dünyasında yaşanan halk hareketlerine verilen ortak addır. Arap Baharı, Arap halklarının demokrasi, özgürlük ve insan hakları taleplerinden ortaya çıkmış; bölgesel, toplumsal bir siyasi-silahlı harekettir. Protestolar, mitingler, gösteriler ve iç çatışmalar ile birlikte yaşanmıştır. Halklar, özgürlük mücadelesi adı altında birçok Arap diktatörünü resmen devirmiştir. Tunus, Mısır, Libya, Suriye, Bahreyn, Cezayir, Ürdün ve Yemen'de büyük çapta; Moritanya, Suudi Arabistan, Umman, Irak, Lübnan ve Fas'ta küçük çapta olmak üzere tüm Arap dünyasında baş gösteren mitingler, protestolar, halk ayaklanmaları ve silahlı çatışmalar kapsamında vuku bulmuştur. İslami demokrasi talepleri artmıştır. Birçok uzman bu eşi görülmemiş halk hareketini, Arap dünyasında yaşanan en büyük değişim olarak yorumlamaktadır. Ayrıntılı bilgi için bkz. PİRİNÇCİ Ferhat, **Arap Baharı'nı Yeniden Düşünmek**, http://www.ferhatpirincci.com/download/orsam_ferhatpirincci.pdf, (03.04.2017)

[285] Renkli Devrimler, 2000'lerin başında eski Doğu Blok'u ülkelerinde ve Balkanlar'da gerçekleşen toplumsal hareketleri tanımlamak için uluslararası basın tarafından kullanılan bir tabir. Renkli Devrimler'e katılanlar çoğunlukla sivil direniş olarak da bilinen şiddetsiz direnişi kullanmışlardır. Bu devrim

yerel toplumsal dinamiklerini manipüle eden bir planlama ile daha fazla zarar verilebileceğini,

-Günümüzde, bir devletin askeri kapasitesinin imkân ve kabiliyetini gösteren emareler değerlendirildiğinde, askeri olmayan faktörlerin rolünün arttığını, bu itibarla da siber savaş teknikleri ile uyumlu bir şekilde faaliyet gösteren özel kuvvet (Spetsnaz) operasyonlarının öneminin günümüzde klasik askeri tedbirlerin ötesine geçtiğini, söz konusu tarzda planlanmış olan faaliyetlerin ise barış zamanında bile "barışı koruma ve kriz yönetimi" maskesi altında kullanılabileceğini,

-Hedef devletin topraklarında sürekli bir cephe bulundurmak için klasik askeri yöntemler yerine bu mahaldeki dost ve akraba toplulukların yanı sıra muhalif hareketlerden de yararlanılabileceğini,

-Psikolojik istihbarat yöntemleriyle, bilgi ortamının manipüle edilerek muhalif hareketlerden de istifade edilmek suretiyle, düşman devlet kademelerinin ve halkının etki altına alınabileceğini, bunun sonucu olarak da düşman kuvvetlerinin muharebe etkinliğini azaltacak asimetrik olanakların yaratılabileceğini, bu amaç doğrultusunda da siber uzayın sağladığı yeni imkânlardan azami ölçüde istifade edilmesi gerektiğini,

-Siber uzayın sağladığı imkânların, aynı zamanda hedef ülke ve bölgedeki iç dinamik unsurlarla birlikte hareket eden özel kuvvet operasyonlarının merkez ile koordinesinin etkin ve doğru bir şekilde sağlanması noktasında da önem arz ettiğini, ileri sürmüştür.

Öte yandanGerasimov, söz konusu askeri yaklaşımı ile temel olarak RF güvenlik bürokrasine askeri olmayan yöntemlerin 21.yy sıcak çatışmalarındaki artan önemine vurgu

---

hareketlerinin çoğunda özel bir renk veya çiçek sembol olarak kullanılmıştır. Renkli Devrimler'de sivil toplum kuruluşlarının ve özellikle öğrenci aktivistlerin önemli rol söz konusu olmuştur. 2000'de Yugoslavya'daki Buldozer Devrimi, 2003'te Gürcistan'daki Gül Devrimi ve 2004'te Ukrayna'daki Turuncu Devrim dâhil olmak üzere bu tür devrimler başarıyla sonuçlanmıştır. Renkli Devrimler'in pek çoğu tartışmalı seçimlerin ardından muhalefetin çağrısıyla halkın sokağa dökülerek adil seçim istemesiyle patlak vermiştir. RF Savunma Bakanı Sergey Şoygu ve Dışişleri Bakanı Sergey Lavrov gibi çeşitli hükûmet üyeleri Renkli Devrimler'i savaş durumunun yeni bir biçimi olarak tanımlayıp suçlamışlardır. RF Devlet Başkanı Putin, 2014 yılındaki bir konuşmasında, Renkli Devrimler'in önlenmesi gerektiğine dikkat çekerek: "*Biz Renkli Devrimler'in trajik sonuçlarını görüyoruz. Bu tür girişimlerin Rusya'da olmasını engellemek için ne gerekiyorsa yapmalıyız. Bu bizim için bir uyarı ve ders."* şeklinde beyanda bulunmuştur. Ayrıntılı bilgi için bkz. OĞAN Sinan, **Turuncu Devrimler Kitabı: Birinci Bölüm**, http://www.turksam.org/tr/makale-detay/410-turuncu-devrimler-kitabi-birinci-bolum, (02.04.2017).

yaparak, bu konuda tedbirler geliştirilmesini önermektedir.[286]Bu kapsamdaGerasimov Doktrini ile RSK'nın:

-Askeri olmayan ve özellikle siber saldırı yöntemlerini kullanan kapasite, planlama ve stratejilere sahip olması,

-RİS ile koordineli bir şekilde planlanan ve hedef ülkedeki dost-akraba topluluklardan da istifade eden gizli operasyonlar geliştirmesi,

-Gerilla taktiklerini kullanan özel kuvvet birimlerinisöz konusu şekilde düzenlenmiş olan hareket planlamalarına dâhil etme yeteneğine ulaşması,

-Asimetrik tehdit yaratan psikolojik savaş yöntemlerine ağırlık vermesi,

-Söz konusu yöntemlerin tamamı kullanma kapasitesine ulaşan bir silahlı gücün, konvansiyonel bir saldırı öncesinde hedef bölge, ülke ve topluluğun savunma direncinin kırılmasına yardımcı olacağına işaret ederek, bu konuda hazırlık ve planlama yapılması için tedbirler geliştirilmesi, kapsamındaki imkan ve kabiliyetini geliştirmesi hedeflenmiştir.[287]

Gerasimov Doktrini'nin, Rus askeri kapasitesine tam anlamıyla uygulanması halinde ise RSK'nın siber imkânlardan ve örtülü istihbarat servisleri ile özel kuvvetler operasyonlarının sağladığı avantajlardan maksimum düzeyde istifade eden, ofansif yönü oldukça gelişmiş bir askeri güç olacağı açıktır.

Bununla birlikte RF'nin 2000'li yılların başı itibarıyla ortaya koyduğu askeri-güvenlik doktrin ve belgelerinde, temel itibarıyla savunma yönü gelişmiş, ekonomik yıkıcılığa neden olabilecek siber faaliyetleri ve Rus toplumunu siyasi eğilimlerini etkilemeyi amaçlayan psikolojik savaş yöntemleriniengellemeye yönelik tedbirler geliştirilmesi gerektiğini savunan, bu alanda da uluslararası işbirliğinin önemine vurgu yapan bir üslubun hakim olduğu açıktır. Öte yandan Gerasimov Doktrini ile RF'nin en azından siber strateji doktrin ve belgelerinde vurguladığı savunmacı ve uluslararası işbirliğine açık siber politikalarını, daha aktif ve caydırıcı yönü güçlü bir stratejiye doğru revize ettiği görülmektedir.

---

[286]Ayrıntılı bilgi için bkz. In Moscow's Shadows, **The Gerasimov Doctrine and Russian Non-Linear War**, https:// inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russiannon-linear-war/., (24.03.2016).
[287]GERASİMOV, loc. cit.

Resmi bir siber güvenlik belgesi olmamasına rağmen Gerasimov Doktrini kapsamında ortaya konan ilkelerin tamamının Ukrayna Krizi esnasında başarı ile uygulanmış olmasından da anlaşılacağa üzere, RF siber kapasitesini aktif ve caydırıcı bir tarzda yeni nesil enformasyon savaşı enstrümanlarından da istifade etmek suretiyle reelpolitik paradigmalara uygun bir şekilde geliştirmek istemektedir. Bu noktada çalışmamızda da belirtildiği haliyle Vladimir Putin iktidarı ile özellikle 2000'li yıllardan itibaren alınan tedbirler ile birlikte RF'nin günümüzde siber uzayı domine eden aktif bir siber güç haline dönüştüğü ortadadır. RF, siber uzay merkezli imkânları askeri kapasitesi için yeni bir fırsat olarak okumakta ve bu teknolojilere yatırım yaparak siber gücünü dış politikada kullanabileceği bir caydırıcı ve baskı unsuru olarak görmektedir.

1.6. "RF Dış Politika Konsepti" İsimli Belge

"Concept of the Foreign Policy of the Russian Federation / RF Dış Politika Konsepti", 12 Şubat 2013 tarihinde RF Devlet Başkanı V. Putin'in onayı ile kabul edilmiş bir belgedir. Esas itibarıyla RF'nin dış politikasının gelecek dönem hedefleri ile ilgili temel yaklaşım ve prensipleri ele alan bu belgede, enformasyon ve siber güvenlik alanında da bazı tespit ve değerlendirmeler mevcuttur.[288]

Bu kapsamda belgede enformasyon alanında yaşanmakta olan yeni teknolojilerin ulusal güvenlik için tehdit olduğu vurgusu yapılarak, geleneksel uluslararası ilişkiler disiplini yaklaşımlarının ötesinde yeni enformasyon teknikleri ve kültürel metotların modern dış politika enstrümanları arasında kabul edilmesi gerektiği ifade edilmektedir. Bu belgede ayrıca:[289]

-Enformasyon alanı kaynaklı yeni suç ve terörist yöntemlerinin, ulusal ve uluslararası güvenlik açısından tehdit olarak kabul edilmesi gerektiği,

-Genel olarak politik, ekonomik ve sosyal tehditlerin bertaraf edilmesi noktasında, RF'nin yeni telekomünikasyon teknolojileri dâhilinde tedbirler almasının şart olduğu,

-Bu noktada, BM sistematiği kapsamında uluslararası tedbirler alınması amacıyla girişimlerde bulunulmasının önem arz ettiği,

---

[288]Ayrıntılı bilgi için bkz. The Russian Ministry of Defense, **Concept of the Foreign Policy of the Russian Federation**,http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D, (24.03.2016). Ayrıntılı bilgi için: http://archive.mid.ru//brp_4.nsf/0/6D84DDEDEDBF7DA644257B160051BF7F, (26.06.2016).
[289]Ibid.

-Rus kamu diplomasisi alanında iç toplumsal dinamiklerin etkilenmesine yönelik yeni enformasyon teknikleri kaynaklı tehditlerin engellenmesi bağlamında, RF'nin ulusal güvenliğini sağlayacak tedbirler almakta olduğuna vurgu yapılarak, bu alanda da uluslararası işbirliğinin sağlanmasının RF'nin dış politika hedefleri arasında yer aldığı, belirtilmektedir.

Bu kapsamda söz konusu belgede de RF'nin enformasyon ve siber güvenlik alanında uluslararası kurum, kuruluş, norm ve standartların belirlenmesine özel önem verdiği ve bu konudaki girişimleri RF dış politikasının temel amaçlarından birisi olarak kabul ettiği görülebilecektir.

Belirtilen yaklaşımın temel dayanak noktası ise*"*Renkli Devrimler" ve "Arap Baharı" olarak adlandırılan sürecin bir devamı olarak, 4 Mart 2012 tarihinde RF'de yapılan ve V. Putin'in altı yıl için yeniden başkanlığa seçildiği dönemde Rus toplumun ve kamuoyunu etkilemeye yönelik olarak, özellikle de sosyal medya aracılığıyla gerçekleştirilen dış kaynaklı psikolojik istihbarat faaliyetleridir. Bu itibarla RF siber güvenlik alanında bahse konu şekilde uluslararası kurum, kuruluş, norm ve standartların belirlenmesini sağlayarak, ülkesine yönelik uluslararası müdahale girişimlerini bir ölçüde de olsa sınırlamayı hedeflemiştir.

1.7. "RF Devlet Politikası'nın Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri" İsimli Belge

2013 yılında kabul edilen*"Basic Principles for State Policy of the Russian Federation in the Field of International Information Security / RF Devlet Politikasının Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri"* isimli belge, RF'nin siber güvenlik kapsamındaki uluslararası girişim ve planlamalarının devamı kapsamında görülebilecektir. Bu itibarla söz konusu belge ile RF'nin uluslararası enformasyon güvenliği alanındaki temel prensiplerini tespit edilerek, uluslararası kamuoyuna ilan edilmiştir.

Söz konusu belgenin başlangıcında, bu belgenin RF'nin ulusal kanunları ve geçmiş dönemde yayımlanan diğer enformasyon güvenliğine ait belgeler ile uyumlu olduğu vurgusu yapılarak, hedeflenen temel amacın;*"RF'nin bilgi ve telekomünikasyon*

teknolojileri alanında dünyanın diğer önemli güçleri ile eşitliği sağlayabileceği şartların oluşturulması" olduğuifade edilmiştir.[290]

Belgede, uluslararası enformasyon güvenliği; "*bireylerin, toplumların ve devletlerin ve devletlerin kritik altyapılarının güvenliğine zarar verebilecek küresel enformasyon alanı kaynaklı faaliyetlerin engellenmesi"* şeklinde tanımlanmıştır. Uluslararası enformasyon güvenliği işbirliği ise*"bu tehditleri engelleyecek ulusal ve uluslararası örgütlerin oluşturulmasının yanı sıra konu kapsamındaki uluslararası norm ve standartların belirlenmesi amacıyla gerekli tedbirlerin alınmasının yönelik faaliyetler"* şeklinde tanımlanmaktadır. Diğer yandan, anılan belgede özetle, uluslararası bilgi güvenliğini tehlikeye sokan tehditler:[291]

-Uluslararası hukuka aykırı olarak ulusal güvenliği, toprak bütünlüğünü, iç işlerine müdahale edilememesi ilkelerine aykırılık taşıyan ve küresel enformasyon alanı kaynaklı,

-Terörist amaçlara hizmet eden, kritik altyapıları ve ulusal güvenliği tehlikeye düşüren, terör örgütleri propagandası yapan, terör örgütlerine eğitim desteği ve adam kazanma imkânı sağlayan,

-Kamu düzenini tehlikeye düşürecek şekilde, ırkçılığı ve yabancı düşmanlığını teşvik eden ve nefret kültürünü yayan,

-Zararlı yazılımlar kullanmak suretiyle adi nitelikli siber suçları uluslararası işbirliği ile organize eden faaliyetler şeklinde tanımlanmıştır.

Bu kapsamda, söz konusu belgede, RF'nin söz konusu faaliyetleri engellemeye yönelik her türlü ulusal tedbirler alacağı ve uluslararası işbirliğinin geliştirilmesine yönelik dış politika inisiyatifleri geliştireceği, belirtilmektedir.

Bu noktada belirtilen amaç bağlamındaki ulusal tedbirler:*"RF'yi oluşturan federal yapılar, RF genelinde faaliyet gösteren özel, kamu ve kamu-özel ortaklığı şeklindeki kurum, kuruluş ve ticari işletmeler, RF Devlet Başkanlığı, RFUlusal Güvenlik Konseyi, RF Dışişleri ve İçişleri Bakanlığı ile diğer resmi kurumlar arasında her türlü işbirliği, yardımlaşma ve koordinasyonu sağlayacak tedbirlerin katı ve kesin suretle, tavizsiz olarak*

[290]NATO Cooperative Cyber Defense Centre of Excellence, **Basic Principles for State Policy of the Russian Federation in the Field of International Information Security**, https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf, (24.03.2016). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/6/114.html, (26.06.2016).
[291]Ibid.

alınması" şeklinde tespit edilmiştir. Diğer yandan anılan belgede, uluslararası tedbirler kapsamında bazı spesifik uluslararası örgütler ve yapılanmalar doğrudan işaret edilerek, RF'nin:[292]

-Özellikle BM'nin mevcut yapısı içindeki işbirliği imkânlarına önem verdiği, bu kapsamda enformasyon teknolojileri alanında uluslararası işbirliği tesis edecek bir uzlaşmayı arzuladığı, BM'nin çatısı altında telekomünikasyon ve enformasyon alanında kalkınmanın sağlanmasına yönelik çalışma yürüten hükümet uzmanları grubunun[293] ortaya koyduğu faaliyetlerin önemsendiği,

-Şanghay İşbirliği Örgütü (ŞİÖ), Kolektif Güvenlik Antlaşması Örgütü (KGAÖ), BRİCS ülkeleri, Asya-Pasifik Ekonomik İşbirliği Örgütü (APEC) üyeleri, Bağımsız Devletler Topluluğu (BDT) ülkeleri, G-8 ve G-20 üyeleri ile konu kapsamındaki işbirliğinin geliştirilmesine katkı yapacağı,

-Uluslararası Telekom Birliği (ITU)'nin bilgi ve internet güvenliği alanındaki faaliyetlerinin geliştirilmesini teşvik edeceği,hususları net bir şekilde ortaya konmuştur.

Belirtilen belgede yer aldığı üzere RF'nin siber güvenlik alanında uluslararası bir konsensüsün oluşmasını hedefleyen ve böylelikle de siber uzayı düzenleyen, internet ve bilgi güvenliği alanında kurallar ortaya koyan bir işbirliğinin geliştirilmesini isteyen bir dış politika sürdürme niyetindedir. Söz konusu niyet ise temelde: "*RF'nin kendi ülkesine hedef alan, ülke kamuoyunu etkilemeyi hedefleyen, ekonomik yıkıcılık faaliyetlerini de bünyesinde barındıran, insan hakları ihlalleri, yargı bağımsızlığı, adil seçimler ve diğer demokrasi uygulamaları noktasında, özellikle Batı ülkeleri kaynaklı iç işlerine müdahaleye varabilecek dış politika inisiyatifleri engelleme amacından*" kaynaklanmakta olduğu da değerlendirilebilir.

[292]Ibid.

[293]RF hükümetinin, 1998 yılında gündeme getirdiği ve BM Genel Kurulu'nun 53.oturumunda ele alınan teklifi,53/70 nolu karar ile sonuçlanmıştır. Söz konusu kararda: *"BM üyeleri, iletişim teknolojileri kaynaklı olarak sürdürülmekte olan terörizm ve adi suç faaliyetleri konusunda uluslararası prensiplerin ortaya konması yönünde çalışma yapmaya"* davet edilmişlerdir. Bu davetin sonucu olarak, BM çatısı altında 15 üyeli bir hükümet uzmanları grubu tesis edilmiştir. Ayrıntılı bilgi için bkz. UN Generel Assembly, **53/70 Resolution adopted by the General Assembly**, https://ccdcoe.org/sites/default/files/documents/UN-021122-ITIS.pdf, (02.04.2017).

1.8. "RF Enformasyon Güvenliği Doktrini"

"RF Bilgi Güvenliği Doktrini / Information Security Doctrine of the Russian Federation" isimli doküman, 9 Eylül 2000 tarihli RF Enformasyon Güvenliği Doktrini'nin yerine yürürlüğe konulmak üzere hazırlanmıştır.

17 sayfadan oluşan ve 6 Aralık 2016 tarihinde kabul edilen belge, RF'nin siber savunma ve bilgi güvenliği alanındaki ulusal çıkarlarını belirlemekte ve bu alanlar kaynaklı olarak Rus çıkarlarını hedef alan tehdit unsurlarına işaret etmektedir. Bu kapsamda, bahse konu belgede özetle:[294]

-Siber uzay ve siber suç alanları kapsamındaki ağ teknolojilerine yönelik tedbirler alınması gerektiği, bu tedbirlerin ise en başta terörist organizasyonların propaganda faaliyetlerine karşı koyma hedefine odaklanmasının şart olduğu,

-Rus hükümetlerinin söz konusu amaç kapsamında ulusal düzeyde kontrol edilebilir ve denetlenebilir bir internet sistematiği kurmasının önem arz ettiği,

-Yabancı istihbarat servislerinin, RF'nin ulusal ve uluslararası düzeydeki çıkarlarını tehlikeye düşürebilecek siber propaganda faaliyetlerine karşı etkili mücadele edilmesinin gerektiği,

-RF'nin uluslararası medya sistematiği içinde daha etkin bir şekilde faaliyet gösterebileceği yapılanmaları geliştirmeye devam etmesinin şart olduğu,

-Rus toplumunun, özellikle de genç Rus nüfusunun manipüle edilmesini amaçlayan siber aktivitelerin engellenmesinin RF'nin öncelikli hedefleri arasında olması gerektiği,

-Rus hükümetlerinin kendi ülkesini hedef alan siber operasyonların yanı sıra kendisine dost ülkelere yönelik siber saldırı ve enformasyon savaşı aktivitelerini de engellemesinin önem arz ettiği, hususları yer almaktadır.

Kısa bir süre önce kabul edilmesi kapsamında, etkilerinin henüz test edilemediği bu belge ile ilgili olarak ise ilk etapda gelecek yıllarda, RF'nin siber uzayda terörist organizasyonların siber propaganda faaliyetlerine karşı etkili bir mücadele ortaya koymak istediği anlaşılabilir. Ayrıca bu belge ile RF'nin ülkesini ve kendisine dost devletleri hedef

[294] RIA Novosti ve Mir24.Tv, **New Kremlin Information-Security Doctrine Calls For 'Managing' Internet In Russia**, http://www.rferl.org/a/russia-informaiton-security-internet-freedome-concerns/28159130.html, (02.01.2017). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/6/135.html, (02.01.2017).

alan siber propaganda faaliyetlerinin engellenmesi amacıyla azami gayret göstereceği, sosyal medya imkânları vasıtasıyla, ayrıca da küresel düzeyde yayın yapan kitlesel medya kurumları aracılığıyla mevcut enformasyon savaşı imkânlarını geliştirmeyi planladığı, ulusal internet alanını ise giderek daha sıkı bir şekilde denetleyerek, bu alandaki teknolojilerinin millileştirmesine ciddi önem vereceği öngörülebilecektir.

Yukarıda genel ve soyut olarak aktardığımız belge ve doktrinler dahilinde RF'nin geliştirmeye devam ettiği Siber Güvenlik Stratejisi'nin tüm detayları ile analiz edilmesi için çalışmanın bir sonraki kısmında RF'nin siber güvenlik alanında işbirliğini geliştirmek amacı ile bugüne kadar ortaya koyduğu dış politika girişimleri bizce irdelenmelidir. Zira ancak bu tarz bir analiz ile büyük resim daha kolay anlaşılabilir.

2. RF'nin Siber Güvenlik Alanındaki Uluslararası İşbirliği Arayışları

RF'nin 2000'li yılların sonu itibarıyla siber savunma ve siber saldırı kapasitesini geliştirmek amacıyla ciddi bir irade ortaya koymuştur. RF'nin gerek savunma, enformasyon güvenliği ve telekomünikasyon teknolojileri alanında, gerekse de dış politika konularındaki resmi doktrin ve belgelerinde, söz konusu irade net bir şekilde görülmektedir. Öte yandan anılan doktrin ve belgelerde dikkat çeken en önemli unsurlardan biri ise RF'nin siber uzay alanındaki gelişmeleri düzenleyecek olan uluslararası bir konsensüsün, özellikle de BM çatısı altında yaratılmasına yönelik çabasıdır.

Bununla birlikte RF'nin belirtilen girişimlerinin ardında siber savunma sistematiğindeki zafiyet ve kırılganlıkların giderilmesi amacı yatmaktadır. Bu itibarla V.Putin'in şahsiyeti etrafında da kimlikleşen ve simgeleşen mevcut ülke sistemindeki demokratik olmayan bazı uygulamaların, başta ABD olmak üzere, Batılı ülkeler tarafından dış politika alanında RF'yi zor durumda bırakmayı amaçlayan bazı girişimlerin konusu olduğu da bilinmektedir. Bu bağlamda uluslararası medya kuruluşlarının konu kapsamındaki düzenli ve ısrarlı yayınları ile sosyal medya alanında, özelliklede 2012 RF Başkanlık seçimleri esnasında zirveye çıkan Rus toplumunu etkilemeye yönelik uluslararası kaynaklı müdahale girişimleri, RF'yi konu kapsamında tedbirler almaya itmiştir.

Bu çerçevede Rus hükümetleri, 2011 yılında ilan edilen *"Bilgi Çağında (Siber Uzayda) Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler / Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space",* 2013 yılında ilan edilen *"RF'nin Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri / Basic Principles for State Policy of the Russian Federation in the Field of International Information Security"*veyine2013 yılında ilan edilen *"RF Dış Politika Konsepti / Concept of the Foreign Policy of the Russian Federation*" isimli belgelerde**,** siber güvenlik alanında uluslararası işbirliğine açık olduğunu net bir şekilde beyan etmiştir. Bu politikanın arkasında yatan neden ise RF'nin siber uzay alanında uluslararası işbirliği geliştirilmesi durumunu, RF'nin ulusal siber savunma sisteminin bir parçası olarak görmesidir.

Bu noktada dikkat çeken bir diğer husus ise RF'nin söz konusu girişimleri esnasında, ülkesindeki kitle iletişim araçları yayın politikası, internet güvenliği sistematiği ve sosyal medya kullanımları ile ilgili olarak, ülke standartlarının liberalleştirmesi yönünde isteksiz olması ve çekingen bir tutum sergilemesidir.

2.1. RF'nin Siber Uzay Alanında İşbirliği Geliştirilmesine Yönelik Olarak BM'deki Girişimleri

RF'nin uluslararası siber tartışmalar alanında BM çatısı altındaki ilk girişimi, 1998 yılında BM Genel Kurulu gündemine getirdiği tekliftir. BM Genel Kurulu'nun 53. oturumunda ele alınan teklif, 53/70 No.lu karar ile sonuçlanmıştır. Söz konusu kararda özetle *"*BM üyeleri, iletişim teknolojileri kaynaklı olarak sürdürülmekte olan terörizm ve adi suç faaliyetleri konusunda uluslararası prensiplerin ortaya konması yönünde çalışma yapmaya*"* davet edilmişlerdir.[295]

Diğer yandan, RF hükümetinin 1998 yılındaki bu girişiminin sonucu olarak, BM çatısı altında uluslararası işbirliği imkânlarının yaratılması konusunda çalışma yapması amacıyla 15 üyeli bir hükümet uzmanları grubu tesis edilmiştir. Grubun ilk girişimleri başarısız olmuş ve konu kapsamında BM Genel Sekreteri'ne bir rapor sunulmuştur.[296]

[295]Ayrıntılı bilgi için bkz. United Nations, 53rd Sess., 1999, A/RES/53/70, **Developments in the Field of Information and Telecommunications in the Context of International Security**, http://www.un.org/disarmament/sgreports/ 68/, (28.03.2016).
[296]Ayrıntılı bilgi için bkz. United Nations, 60th Sess., 2005, A/60/202, **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, http://www.un.org/ disarmament/sgreports/68/, (28.03.2016).

Bununla birlikte bu grubun 2005, 2009 ve 2013 yıllarında hazırladığı raporların içeriği ile ilgili olarak da RF ve ABD'nin arasında anlaşmazlıklar olmuştur. Bu noktada ABD tarafı; temel olarak Rus tekliflerinin siber suçlar ve askeri konulara odaklanmakta başarısız olduğunu savunmuş, bahse konu raporlarda ortaya konan kararların bir ülke genelinde zararlı yazılımların engellenmesine yönelik altyapının oluşturulması noktasında yeteriz kaldığı da iddia edilmiştir.

Bununla birlikte belirtilen çalışma grubun faaliyetlerinin net bir sonuca ulaşamamasına rağmen, RF'nin bahse konu politikası dönem içinde BM üyeleri arasında bir farkındalık yaratmış, BM terminolojisine doğrudan tesir etmiş ve bu konuda BM Genel Kurulu'nda çeşitli ülkelerin teklifleriyle alınan kararların sayısı hızla artırmıştır. Ayrıca BM çatısı altındaki RF merkezli işbirliği arayışları ile birlikte, RF gibi Batılı ülkeler tarafından demokrasi alanında eleştirilere maruz kalan ülkelerin de belirtilen girişimleri destekledikleri görülmüştür. Ayrıca bu ülkeler nezdinde siber uzay alanındaki gelişmeleri daha korumacı ve anti-demokratik metotlarla düzenleme eğilimlerinin artığı da müşahede edilmiştir.[297]

2.2. RF'nin Siber Uzay Alanında İşbirliği Geliştirilmesine Yönelik Olarak Şangay İşbirliği Örgütü Kapsamındaki Girişimleri

RF'nin dış politika çıkarları kapsamında, özellikle ABD ve Batılı ülkeler karşıtlığı temelinde, uluslararası sistemi etkilemek amacıyla kurulmasına temel katkı yaptığı Şangay İşbirliği Örgütü (ŞİÖ), RF'nin siber uzay alanında işbirliği geliştirilmesine yönelik girişimleri için de önemli bir uluslararası zemin durumundadır.

RF'nin girişimleri ile ŞİÖ tarafından 2005 yılında kabul edilen bir kararda, ABD'nin politikalarına odaklanılmak suretiyle, iletişim ve telekomünikasyon alanı kullanılarak, ülkelerin egemenlik haklarının ihlal edildiği, bu kapsamda da uluslararası barış ve güvenliğin tehlikeye düştüğü beyan edilmiştir.[298] Bu beyan itibarıyla Rus hükümetinin BM çatısı altındaki pozisyonun aksine, ŞİÖ bünyesinde siber güvenlik alanındaki girişimlerinde,siber uzay alanına yönelik korumacı ve kısıtlayıcı niyetini daha net olarak ortaya koyduğu ileri sürülebilir.

[297]Ayrıntılı bilgi için bkz. MEDVEDEV, op. cit., pp. 66-68.
[298]Ibid.,p. 69.

RF'nin ŞİÖ bünyesinde ortaya koyduğu uluslararası işbirliği çabalarının belki de en somut sonucu, ÇHC ve RF devlet başkanları tarafından 2015 Mayıs ayında yayınlanan siber güvenlik alanında işbirliği yapılmasına yönelik ortak açıklamadır. Bu açıklama ile iki devlet birbirlerine karşı siber saldırılar gerçekleştirmeme, siber uzay teknolojileri konusunda eğitim ve teknoloji transferi konusunda işbirliği geliştirme, iki ülkenin iç politik yapısını ve sosyo-ekonomik atmosferini bozmayı hedefleyen siber saldırılara karşı ortak tedbir alma, siber uzayı denetleyen uluslararası bir rejim tesis etme yönünde uluslararası örgütler nezdinde ortak hareket etme hususlarında uzlaşma sağlama niyetinde olduklarını deklare etmişlerdir.[299] Bu kapsamda söz konusu ortak beyan ile RF ve ÇHC, siber uzayda temel aktör konumuna gelmek isteyen ABD'ye karşı ortak bir duruş sergilemeyi ve siber uzayda ABD'nin başat devlet olmasını engellemeyi amaçladıkları da iddia edilebilir.

Diğer yandan bu işbirliği arayışlarının, ABD Savunma Bakanlığı tarafından 2015 Nisan ayında yayımlanan ABD Savunma Bakanlığı Siber Stratejisi Belgesi'nde, ÇHC ve RF'nin siber kapasitelerinin ABD için doğrudan bir tehdit olarak tanımlanmasına yöneliktir cevap niteliğinde olduğu da ileri sürülebilir.[300]

ÇHC ve RF arasında siber güvenlik alanındaki bahse konu yakınlaşmanın uluslararası ilişkiler alanına yansıyan ilk pratik etkisi ise 2016 Şubat ayında Avustralya'ya yönelik olarak RF ve ÇHC kaynaklı olduğu iddia edilen siber saldırılardır. Bu kapsamda, mezkûr tarihte, Avustralyalı yetkililer tarafından, "*ülke genelinde hükümet kuruluşları arasında bilgi iletişimin sağlanması için kullanılmakta olan ICON sistemine ciddi siber saldırıların gerçekleştiği, bu nedenle sistemde aksama ve duraksamaların yaşandığı, saldırıların kaynağının ÇHC ve RF olduğu"* belirtilmiştir.[301]

Diğer yandan ŞİÖ üyesi olan ÇHC, RF, Tacikistan ve Özbekistan tarafından 2011 yılında BM Genel Sekreteri'ne hitaben *"Enformasyon Güvenliğinin Yönetim Kuralları / Management Rules of Information Security"* isimli doküman hazırlanmıştır. Dokümanda siber silahların yayılmasını engelleyici ya da siber güvenlik alanındaki düşmanca

[299] RAZUMOVSKAYA Olga, **Russia and China Pledge Not to Hack Each Other**, The Wall Street Journal, USA, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/., (01.04.2016).
[300] Russia Direct News Magazine, **China-Russia cyber-security pact: Should the US be concerned?** http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned, (14.04.2016)
[301] STEWART Cameron,**Chinese and Russian spies, as well as other hackers, have stepped up the number of attacks on the government's secure communications network in Canberra**, http://www.theaustralian. com.au/national-affairs/defence/china-and-russia-step-up-cyber-attacks-on-australia/news-story/ 65ba6baa760c85efe93fb736b270f982,(01.04.2016).

faaliyetlerin tanımına ilişkin olarak her hangi bir ifade yer almamakla birlikte, özellikle siber uzay kaynaklı gelişmelerin ülkelerin egemenliğini tehlikeye düşürdüğü beyan edilerek, bu durumda siber tehdit altındaki ülkelerin kendilerini savunma hakkı olduğu kesin bir dille belirtilmiştir.[302]

Bununla birlikte ŞİÖ kapsamındaki girişimleri dikkate alındığında, Rus devletinin siber uzaydaki gelişmelere yönelik uluslararası işbirliğinin tesis edilmesi noktasında, Batı konseptinin dışında inisiyatifi geliştirme amacı içinde olduğu görülmektedir. Bu itibarla RF'nin "Avrupa Konseyi Sanal Suçlar Sözleşmesi (Council of Europe Convention on Cybercrime)'ni imzalamamasının dikkat çekici olduğu değerlendirilebilecektir.

Öte yandan RF'nin ŞİÖ çatısı altındaki girişimleri ile ÇHC ile gerçekleştirdiği siber uzayda işbirliğini içeren anlaşma dikkate alındığında, 2015 sonrası dönemde siber uzayda ABD ve müttefikleri (NATO ve AB üyesi devletler, Japonya, Avustralya) ile ÇHC ve RF'nin yanı sıra bu iki devlet ile savunma ve nükleer işbirliği anlaşmaları mevcut olan İran arasında bir kutuplaşma sürecinin başladığı da ileri sürülebilir.[303]

2.3. RF'nin Siber Uzay Alanında İşbirliği Geliştirilmesine Yönelik Olarak ABD İle Sürdürdüğü İkili İşbirliği Girişimleri

Siber uzayın iki önemli aktörü olan RF ve ABD, bu alanındaki uluslararası işbirliğinin sağlanması noktasında farklı yaklaşımlara sahiptirler. Bu itibarla ABD siber uzay alanı kaynaklı tehditleri uluslararası işbirliğine açık bir şekilde yerel ve ulusal tedbirler ile bertaraf etmeyi amaçlarken, RF siber uzayın uluslararası bir rejim ile denetlenmesini, özellikle de sosyal medya imkânları için elverişli ortam yaratan internetin kontrol altında tutulmasını hedeflemektedir.[304]

Bu farklı yaklaşıma rağmen, 1998 Eylül ayında RF ve ABD Devlet Başkanları arasında gerçekleşen görüşmede, enformasyon teknolojileri alanındaki gelişmelerin olumlu ve olumsuz yanlarına vurgu yapılarak, bu alanda stratejik işbirliği geliştirilmesinin iki

---

[302]United Nations, 66th sess., 2011, A/66/359,**Letter Dated 12 September 2011 From the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General**, https://disarmament-library.un.org/UNODA/Library.nsf/f446fe4c20839e50852578790055e729/329f71777f4b4e4e85257a7f005db45a?OpenDocument, (01.04.2016).

[303]Chaire Cyber-Défense et Cyber-sécurité, **Conference:China's Cybersecurity and Cyberdefense policies and strategies andChina-Iran-Russia, an Information Communıty?**, Paris, 1 July 2013, http://www.chaire-cyber.fr/IMG/pdf/6.1f_engchina-iran.pdf, (14.06.2016).

[304]GADY Franz Stefan ve AUSTİN Greg, "Russia, The United States, And Cyber Diplomacy Opening the Doors", **East-West Enstitute Report**, http://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_ WEB.pdf, (01.04.2016), pp. 1-2.

ülkenin ortak çıkarı olduğu beyan edilmiştir. Ayrıca bu görüşmede "*Y2K*"[305] problemi dâhilinde ortaya çıkması muhtemel sorunlar için iki ülkenin birlikte çalışması kararlaştırılmıştır.[306]

2006 yılına gelindiğinde, RF'nin dönem başkanı olduğu G-8 grubuna üye ülkeler arasında terörizm, siber güvenlik ve organize suç konularında özel-kamu ortaklığının geliştirilmesine yönelik bir inisiyatif başlatılmasını teklif etmiş ancak ABD'nin olumlu yaklaşımına rağmen, bu teklifin somut bir sonucu olmamıştır.[307]

Öte yandan Barack H. Obama yönetimi ile birlikte ABD'nin siber uzayda işbirliği geliştirilmesine yönelik çabalarının arttığı da ifade edilebilecektir. Bu kapsamda Obama tarafından 2009 Mayıs ayında yapılan bir çağrı ile RF, ÇHC ve Hindistan'ı da dâhil edecek şekilde iletişim teknolojileri alanında belirli bir gelişmişlik içinde olan ülkelerin siber uzaya alanı kaynaklı olarak hükümet dışı aktörler ile haydut devletlerden gelecek olan tehlikelere karşı ortak hareket edebileceğini, bu itibarla da NATO'nun konu kapsamında inisiyatif alabileceğini gündeme getirilmiştir.[308]

2009 Aralık ayında ise ABD ve RF, BM Silahsızlanma ve Uluslararası Güvenlik Komitesi'ndeki bir toplantıda, siber uzayın askeri bir alan olarak kullanımın azaltılması ve uluslararası güvenliğin geliştirilmesine yönelik olarak iki ülke arasında müzakerelerin başlaması kararı vermişlerdir. Bununla birlikte, konu kapsamında bugüne kadar net bir adım da atılmamıştır.

2010 Temmuz ayında ise Moskova'da gerçekleşen, II. ABD-RF İletişim Teknolojileri Toplantısı'nda bir araya gelen üst düzey yetkililer arasında konu kapsamında bazı resmi temaslar gerçekleşmiştir. Bu temaslarda, iki ülke yetkilileri siber güvenlik

[305]2000 yılı problemi (Y2K problemi, milenyum hatası, Y2K hatası ya da sadece Y2K diye de bilinir.), 01 Ocak2000 yılından sonra eski bilgisayar ve yazılımlarında görülen ve tarih ve zamanla ilgili işlemlerde hatalı sonuçlara yol açan bir yazılım hatasıdır. Hata, bazı kurum ve kuruluşlarda (örneğin bankamatiklerde) ve devlet bilgisayarlarındaki çeşitli işlevlerin 31 Aralık 1999 tarihini müteakip 01 Ocak 2000 gecesi kesilmesi şeklinde ortaya çıkmıştır. Buna benzer bir hata da UNIX yüklü 32-bit sistemlerde 2038 yılında ortaya çıkacak olan 2038 yılı problemidir. Ayrıntılı bilgi için bkz. http://www.constitution.org/y2k/y2k.htm, (02.04.2017). Ayrıca bkz. https://www.theguardian.com/technology/2014/dec/17/is-the-year-2038-problem-the-new-y2k-bug, (02.04.2017).
[306]GADY ve AUSTİN, loc.cit.
[307]G8 Summit 2006, Moscow, November 28-30, Working Meetings, **G8 Initiative For Public Private Partnerships To Counter Terrorism: Private Sector Action Beyond 2006**, http://issuu.com/ewipublications/docs/g8-initiative-for-public-private-partnerships-to-c/1, (02.04.2016).
[308]GADY ve AUSTİN, loc.cit.

alanındaki işbirliği arayışına yönelik görüşmelerinin sürdürülmesi kararı almışlardır.[309] Bu karar iki ülke arasında konu kapsamındaki iletişim kanallarının açık tutulmak istenmesi bakımından önemli bir aşama olarak kabul edilebilir.

Bunlarla birlikte ABD ve RF hükümetlerinin siber uzay alanındaki işbirliği girişimleri kapsamında bazı önemli siber suçluların iadesi konusunda oldukça uyumlu çalışmalar gerçekleştirdikleri de görülmektedir. Bu çerçevede ABD ve RF'nin isnat edilen siber suçlar kapsamında aradıkları bazı zanlıları birbirlerine iade etmekten çekinmedikleri de müşahede edilebilmektedir.

Görüldüğü üzere ABD ve RF arasında siber uzay konusunda ikili ve uluslararası düzeyde işbirliğinin tesis edilmesine yönelik bazı girişimler de bulunulmasına rağmen, bu girişimlerin somut bir sonuca ulaşmadığı da ileri sürülebilir. Bu olumsuz durumun nedeni ise iki ülkenin siber uzay konusunda birbirlerine yönelik tehdit algılamaları ve farklı anlayışlarıdır. Bu kapsamda, ABD liderliği için RF sadece siber uzay alanı kaynaklı tehditler için değil, aynı zamanda her türlü askeri kaynaklı tehditler içinde tedbir alınması gereken bir devlet şeklinde konumlandırılmaktadır. Benzer biçimde, RF güvenlik ve askeri bürokrasisi de ABD'nin teknolojik üstünlüğünü dikkate alarak, en önemli askeri ve siber tehdit kaynağı olarak görmektedir.

RF'nin küresel siber uzay alanına yönelik uluslararası bir rejimin tesis edilmesi, bu alanının denetlenmesi ve kurallara bağlanması, internetin sosyal medya kullanıma olanak sağlayan özelliklerine karşı uluslararası denetim mekanizmaları oluşturması kapsamındaki girişimlerinin yanı sıra RF'nin kendi ulusal siber uzay alanın denetlenmesi, kontrol edilmesi ve savunulmasına yönelik tedbirleri de dikkat çekicidir.

Bu itibarla siber uzayı domine eden iki küresel siber güç olan ABD ve RF'nin bu alanda uluslararası işbirliğinin tesis edilmesi noktasındaki farklı yaklaşımlarının uluslararası sistemin yapısını eskisinden çok daha fazla anarşik hale getiren bir faktör olduğu da değerlendirilebilir. Ayrıca siber uzay alanını düzenleyen evrensel nitelikte kesin ve nihai bir uluslararası hukuk düzenlemesinin hala bulunmaması, siber uzayda devletler arasında işbirliği yerine daha rekabetçi politikaların hakim olması ve bu rekabetin şiddetinin giderek artması hususları dikkate alındığında, uluslararası sistemin eskisinden

[309]U.S. Department of State, **Office of the Spokesman, Roundtable on U.S.-Russia Information, Technology: Dialogue on a Range of Topics Including Broadband and Internet Governance**,http://issuu.com/ewipublications/docs/usrussiacyber/12, (02.04.2016).

çok daha fazla belirsiz ve güvensiz bir hal aldığı da bizce ileri sürülebilir.

Öte yandan RF'nin siber güvenlik stratejisinin tüm detayları ile analiz edilmesi amacı kapsamında, RF'nin siber uzay alanına ilişkin ulusal düzenlemeleri, teknolojik altyapısı, bu alanda faaliyet gösteren istihbarat ve güvenlik kuruluşları, siber suç faaliyeti yürüten illegal yapılanmaları ve iletişim teknolojileri alanındaki özel veya kamu şirketlerinin özellikleri de analiz edilmelidir.

3. RF'nin Siber Uzay Alanının Yapısı

RF'nin sürdürmekte olduğu siber stratejinin, sadece ABD'nin değil aynı zamanda tüm uluslararası sistem için geçerli olacak şekilde, devletlerin ulusal siber stratejilerini şekillendirdiğini ifade etmek, zorlama bir yaklaşım olmayacaktır.

Bu kapsamda RF'nin 2007 yılında Estonya'ya, 2008 yılında Gürcistan'a, Kırım Krizi dâhilinde 2014 yılında Ukrayna'ya ve 2015 yılında Türkiye'ye yönelik gerçekleştirdiği iddia edilen siber saldırıları dikkat çekicidir. Öte yandan RF kaynaklı olarak uluslararası boyuta da ulaşmış siber kriminal faaliyetler, bu faaliyetleri yürüten suç organizasyonlarının RİS ile olan olası bağlantıları da konu dâhilinde analiz edilmelidir.

3.1. Rus İstihbarat Servisleri'nin Siber Kapasiteleri

Rus Federal Güvenlik Servisi (Federalnaya Slujba Bezopasnosti /FSB), Rus İstihbarat Servisi (Sluzhba Vneshney Razvedki / SVR) ve Rus Askeri İstihbarat Direktörlüğü'nün (Glavnoye Razvedyvatel'noye Upravleniye / GRU) gerek tek başlarına sahip oldukları siber kapasiteleri gerekse de Rus kriminal örgütleri ile olan illegal bağlantıları kapsamında RF'nin siber savunma ve saldırı kapasitesini belirleyen temel faktörlerdendir. Bu servislerden FSB ve SVR, RF Devlet Başkanı'na doğrudan bağlı durumdayken GRU, Savunma Bakanlığı'nın bir parçası konumunda ve RSK emrinde görev yapmaktadır.[310]

Daha ayrıntılı bir biçimde açıklama gerekirse FSB, SSCB döneminde faaliyet gösteren gizli servisler olan ÇEKA, NVD ve KGB'nin yerini alan ve iç güvenlik alanında faaliyet gösteren bir gizli servistir. Bir iç güvenlik servisi olarak FSB'nin faaliyetleri iki boyutlu olarak düşünülmelidir. FSB'nin ilk görevi ülke genelinde devlet güvenliği aleyhine

[310]HEICKERO, op. cit.,p. 27.

sürdürülen faaliyetler hakkında istihbarat toplamaktır.[311] Örneğin, RF'deki ayrılıkçı Çerkez/Çeçen gruplarının, cihad yanlısı terör örgütlerinin veya organize suç odaklarının faaliyetlerini izlemek, takip etmek ve haklarında istihbarat toplamak FSB'nin görevidir. FSB'nin bir diğer görevi ise RF' ye yönelik olarak sürdürülmekte olan espiyonaj faaliyetlerine karşı koymaktır. Bu karşı koyma faaliyeti, kontr/espiyonaj çalışması olarak adlandırılır ve RF aleyhine dış istihbarat servisler aracılığıyla sürdürülen subversif operasyonların da engellenmesi amacını içerir. Bu kapsamda RF'na yönelik siber saldırılara karşı koymak ve temelde ülkenin siber güvenliğini sağlamak, FSB'nin görevidir.[312] FSB'nin siber güvenlik operasyonlarına doğrudan yöneldiği tarih ise 2008'dir. 2008 yılında, 1978 yılında teknik operasyonları yürütmek amacıyla KGB bünyesinde kurulan "Kvant" isimli departman, FSB'nin adeta siber güvenlik operasyon merkezi haline dönüştürülmüştür.[313]

FSB'nin siber güvenlik alanındaki diğer bir sorumluluğu ise ülke genelindeki Rus vatandaşlarının ve yabancıların telekomünikasyon iletişim bilgilerinin istihbar olunan bilgiler kapsamında takip edilmesidir. FSB, Rus GSM ve telekom şirketlerinin yasal bir zorunluluk olarak kurmak zorunda oldukları, RF'deki internet ve anolog haberleşmesini takip eden ve bir nevi denetleme sistemi şeklinde tesis edilmiş olan "Operatif Denetleme Faaliyetleri Sistemi" (System for Operative Investigative Activities / SORM)'nin kontrolü görevini de üstlenmiştir.

FSB'nin sanayi, teknoloji ve bilişim sektörlerine yönelik espiyonaj faaliyetlerinin engellenmesi noktasında Rusya Teknik ve İhracat Kontrol Servisi (Federal Service for Technical and Export Control of Russia / FSTEC) ile de yakın işbirliği bulunmaktadır. Bu kapsamda 2004 yılında kurulan ve RF Savunma Bakanlığı bünyesinde faaliyet göstermekte olan FSTEC'nin ihracat denetim rejimini kontrol etmek suretiyle sanayi, teknoloji ve bilişim sektörlerini hedef alan espiyonaj operasyonlarına karşı koymada önemli bir rolü bulunduğu belirtilebilir.[314] FSTEC, bir ihracat kontrol servisi olarak Moskova Riyaseti

[311]GADY ve AUSTIN, op. cit., p. 5.
[312]Ayrıntılı bilgi için bkz. The Centre For Counterintelligence and Security Studies, **Russia's SVR/FSB/GRU Intelligence Services**, http://www.cicentre.com/?page=191, (27.03.2016).
[313]Ayrıntılı bilgiiçin bkz. CARR Jeffry, **Intelligence on Russian Information Warfare Activities**, http://jeffreycarr.blogspot.com/2012/01/intelligence-on-russian-information.html, (04.01.2017).
[314]CARR Jeffrey, **Inside Cyber Warfare: Mapping the Cyber Underworld**, O'Reilly Media Inc., USA, 2011, s. 318.

merkez olmak üzere altı bölge ofisi ile birlikte faaliyetlerini sürdürmektedir.[315] FSTEC'in, 1973 yılında tesis edilmiş olan ve SCCB dönemi boyunca devlet teknik sırlarının korunması amacıyla faaliyet gösteren Devlet Teknik Komisyonu (Gostekhkomissiya)'nun günümüzdeki halefi konumunda olduğu da ifade edilebilir.[316] FSTEC'in siber güvenlik ile ilgili olarak görevleri ise şöyledir: [317]

- Bilgi güvenliğinin sağlanması,
- Hassas teknolojilerin ihracatının denetlenmesi,
- Sanayi ve bilişim sektöründeki yeni gelişmeleri hedefleyen espiyonaj faaliyetlerine karşı ulusal düzeyde tedbirler alınması,
- RF'nin teknoloji casusluğu kapsamındaki karşı koyma kapasitesinin geliştirilmesi amacıyla diğer devlet kurumlarıyla gerekli koordinenin tesis edilmesi.

FSB'nin diğer tüm faaliyetlerinde olduğu siber güvenlik alanında da SVR ile koordinasyon kurmaktadır.[318]SVR de KGB'nin devamı olarak RF'nin ülke dışındaki espiyonaj faaliyetlerini yürütmek amacıyla kurduğu dış istihbarat servisidir. SVR, RF'nin dış istihbarat ihtiyaçlarının karşılanmasında, GRU ile birlikte temel aktör konumundadır. SVR, hedef aldığı devlete yönelik askeri, siyasi, biyografik, ekonomik, sosyal, ulaştırma, iletişim, bilim ve teknoloji konularında istihbarat toplar. Örneğin RF'nin ABD'nin dünyanın bir bölgesindeki askeri kapasitesini tespit etmeye yönelik ya da Macaristan'daki başkanlık seçimlerinin sonucunu tahmin etmeyi amaçlayan çalışmaları, SVR tarafından yönetilmektedir. Siber güvenlik stratejisi açısından ise RF'nin bir ülkenin bilim ve teknoloji kapasitesi hedef alan siber casusluk operasyonlarını planlamak, SVR'nin görevleri arasındadır. SVR'nin yurt dışında Belarus, Kazakistan, Tacikistan, Ermenistan, Kırgızistan, Suriye, Küba, Vietnam ile Güney Osetya, Abhazya, Kırım ve Transdinyester bölgelerinde GRU ile birlikte ortak kullandığı elektronik ve sinyal istihbaratı toplama merkezleri de mevcuttur.[319]

[315] FSTEC Internet Sitesi, **FSTEC's Structure**, http://fstec.ru/en/358-structure, (18.06.2017).
[316]Global Security Web, **FSTEC**, http://www.globalsecurity.org/military/world/russia/fstec.htm, (18.06.2017).
[317] FSTEC Internet Sitesi, **FSTEC's Power**, http://fstec.ru/en/359-powers, (18.06.2017).
[318] Ayrıntılı bilgi için bkz. STAAR R. Tocaso, "Russia's Security Services", **Mediterranean Quarterly**, Vol.15, Issue.1, 2010, pp. 1-10.
[319] HEICKERO, op. cit., p. 30

GRU, RF Genelkurmayı'na bağlı olarak faaliyet gösteren askeri istihbarat teşkilatıdır. Daha öncesinde Sovyetler Birliği'nde Kızıl Ordu'ya bağlı olan GRU, RSK'nın büyüklüğü kapsamında RF'nin en geniş sayı ve kapasiteli istihbarat teşkilatıdır. GRU, askeri ve dış istihbarat konularının yanı sıra ülke güvenliği ile ilgili her alanda istihbarat toplama yetkisine sahiptir. Siber güvenlik açısından GRU'nun temel görevleri Rus askeri kapasitesini hedef alan dış servis kaynaklı siber operasyonlara karşı kontr/espiyonaj faaliyeti yürütmek ve imkan bulunması halinde hedef ülkenin askeri kapasitesine yönelik siber casusluk operasyonları planlamaktır. Stratejik Füze Birlikleri'nin faaliyetlerinin sürdürülmesi ayrıca ülkeye yönelik siber saldırlara karşı koymak üzere kurulmuş olan "Computer Emergency Response Team" (RE-CURT)'lerin kontrolü de GRU'nun diğer Rus istihbarat ve güvenlik kuruluşları ile koordineli olarak gerçekleştirdiği görevleri arasındadır.[320]

Bu noktada, GRU'nun RSK'nın 2014 yılındaki Ukrayna Müdahalesi esnasında gösterdiği çok yönlü sıcak çatışma performansına yaptığı katkı ve bu katkının başarısı nispetinde RİS'ler arasında meydana gelen rekabet, RF'nin siber kapasitesinin net bir şekilde ortaya konulması amacı kapsamında ayrıca irdelenmelidir. GRU'nun 2008 yılındaki Gürcistan Müdahalesi esnasındaki başarısızlığı, bu istihbarat örgütünün diğer RİS'lere kıyasla itibarını ciddi biçimde sarsmıştır. Söz konusu kötüye gidiş 2011 yılında Igor Sergun'un GRU direktörü atanması ile sona ermiştir. Bu atama, GRU'nun yönetiminin ve sahip olduğu operasyonel kapasitenin kontrol edilmesi amacıyla FSB tarafından baskı altına alındığı bir tarihte meydana gelmesi bakımından Putin'in oldukça kritik bir kararı olarak okunmalıdır. I. Sergun, diğer RİS'lerde görev yapan rakipleri tarafından; "*iş yapmaktan ziyade, saray dengelerini gözeterek makam sahibi olmuş bir şahsiyet*"[321] olarak ifade edilse de GRU, özellikle Ukrayna Müdahalesi öncesi ve esnasında gerek siber operasyonların planlanmasında gerekse de özel kuvvet birlikleri ile Rus yanlısı ayrılıkçıların faaliyetlerinin koordinasyonunda son derece başarılı olmuştur. I. Sergun direktörlüğündeki GRU, Putin'in iktidarını sürdürme noktasında RF'deki istihbarat servisleri arasında dengeyi gözeten ve hiçbir servisin diğerine üstün olmaması kuralına bağlı olan siyasetini, Ukrayna Müdahalesi esnasında kendisine verilen imkân ve

[320] Ibid., p. 27
[321] Ayrıntılı bilgi için bkz. GALEOTTI Mark. **Putin's Hydra: Inside Russia's Intelligence Services**, European Council on Foreign Relations (ECFR), http://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services, (17.10.2016), pp. 6-9.

kabiliyetleri en üst seviyede kullanmak suretiyle elde ettiği popülerlik ve güç sayesinde ciddi biçimde sarsmıştır.[322]Putin'in söz konusu siyasetinde meydana gelen bahse konu dengesizlik ise 2015 Ocak ayında I. Sergun'un Moskova'da kalp krizi sonucu ani bir şekilde ölmesi ile sona ermiştir Diğer bir ifade ile vurgularsak, I. Sergun'un ölümü sonrasında GRU'nun diğer istihbarat servislerine kıyasla Ukrayna Müdahalesi sonrasında elde ettiği üstünlük ortadan kaybolmuş ve Putin'in istihbarat servisleri arasında gözettiği denge yeniden tesis edilmiştir. Bu gelişmeyi destekleyen bir diğer olay ise Ukrayna İstihbarat Servisi ile irtibatlı bir kaynağın, FSB'nin 2015 Ocak ayı sonrasında Ukrayna'nın doğusunda yer alan RF yanlısı ayrılıkçı gruplar ile tekrar operasyonel planlamalara giriştiğini bildirmesidir.[323] Bu tek örnekten de anlaşıldığı üzere, I. Sergun'un sahneden çekilmesi ve akabinde Putin'in yaptığı yeni atamalar ile birlikte RİS'ler arasındaki güç dengesi yeniden tesis edilmiştir. Böylelikle de Putin, 2018 yılında yapılacak olan RF başkanlık seçimleri öncesinde olası bir iktidar mücadelesi kapsamında kendisine avantaj elde etmeyi amaçlamıştır.[324]

Öte yandan SVR, FSB ve GRU'nun faaliyetlerinin yanı sıra diğer istihbarat ve güvenlik servislerinin yetkilerinin ve görev alanlarının yeniden planlanması kapsamında, 2000'li yılların başı itibarıyla RF'nin siber kapasitesini geliştirme yönünde ciddi adımlar attığı da bilinmektedir. Bu bağlamda RF 1993 yılında kurulmuş olan, elektronik ve sinyal istihbaratı ile kriptoloji alanlarında faaliyet gösteren FABSİ (Federal Agency of Government Communications and Information / Federal İletişim ve Enformasyon Ajansı)'yi 2003 yılında lav ederek, bu kuruluşun yetki ve sorumluluklarını FSB, SVR, RF Savunma Bakanlığı ve Federal Koruma Servisi'ne (Federalnaya Sluzhba Okhrany / FSO) arasında dağıtmıştır. FABSİ'nin kapatılmasının en önemli nedeni ise kurum içerisindeki yolsuzluk ve organize suç örgütleri ile bağlantılı yapılanmalardır.[325]FSO'nun siber güvenlik alanındaki temel görevi ise RF'nin ilgili kurumları ve yöneticileri arasındaki üst düzey ve gizlilik içeren iletişimin güvenli bir şekilde sürdürülmesini denetlemek ve yönetmektir. Doğrudan RF Devlet Başkanı'na bağlı olarak faaliyet yürütür. FSO'nun, ülke genelindeki telgraf, kablolu telefon hatlarının, internet ve iletişim haberleşmesinin kontrolü

[322]Ayrıntılı bilgi için bkz. Ibid. p. 9-13.
[323]MERIÇ Enver, **Rus İstihbarat Savaşları ve Putinizm**, Haber 10 Haber Portalı, http://www.haber10.com /yazar/enver_meric/rus_istihbarat_savaslari_ve_putinizm-620326, (17.10 2016).
[324]Ayrıntılı bilgi için bkz. GALEOTTI, op. cit., pp. 13-19.
[325]HEICKERO, op. cit., p. 28.

ve denetimi, ayrıca Rus uyduları üzerinden toplanan sinyal istihbaratının değerlendirilmesi ve raporlanması, son olarak Rus nükleer silah sisteminin güvenliğin sağlanması şeklinde görevleri de bulunmaktadır. Rus nükleer silahlarını aktif hale getirecek olan "*Cheget*" (siyah kutu / çanta) ve bu süreci yöneten "*Kavkaz*" (iletişim sisteminin) denetimi ve korunması da FSO'nun yetkisi altındadır[326]

RF 2010 yılında enformasyon ve bilgi teknolojileri alanında çalışma yürütmek amacıyla Savunma Bakanlığı bünyesinde bir "bakan yardımcılığı" pozisyonunu da tesis etmiştir.[327] RF, 2013 yılında aldığı bir karar ile RSK bünyesinde bağımsız bir siber savaş birimi kurmayı planlama kapsamına almıştır. 2012 Ekim ayında kurulan RSK Askeri Araştırma Merkezi Direktörü Andrei Grigoryev konu bağlamında: *"Rus ordusu olarak internet kaynaklı bazı faaliyetleri tehdit olarak değerlendirdiklerini, bu nedenle de ordu bünyesinde bağımsız bir siber savaş departmanı kurmayı planladıklarını, bu plan dâhilinde çalışma yürüttüklerini, başında bulunduğu araştırma merkezinin halen 700 civarında gizli proje üzerinde çalıştığını"* beyan etmiştir.[328]

Bu gelişme ile ilgili olarak 2014 Kasım ayında açıklama yapan RF Savunma Bakanı Sergei Shoigu ise *"Rus Ordusu'nun siber tehditlere karşı koymak amacıyla bünyesinde faaliyet gösterecek olan bağımsız bir yapılanmaya gittiğini, bu planlama kapsamında Rus hükümeti olarak 500 milyon ABD Doları tutarında bütçe ayırdıklarını, anılan oluşumun siber tehditler ile mücadelenin yanı sıra yurtdışı kaynaklı iletişimin gözetlenmesi, toplanması ve denetlenmesi görevini de sürdüreceğini, bu nedenle de yazılım uzmanları ile yabancı dil bilen personele ihtiyaç duyduklarını"* belirtmiştir.[329] Diğer yandan RSK bünyesindeki söz konusu siber biriminin 2017 yılı itibarıyla operasyonel faaliyetlerine başlayacağı tahmin edilmektedir.[330]

---

[326]Ibid., p. 29
[327]EastWest Instıtute, **The American and Russian Approaches to Cyber Challenges**, http://www.omicsgroup. org/journals/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf, (14.04.2016).
[328]SRIDHARAN Vasudevan, **Russia Setting up Cyber Warfare Unit Under Military**,http://www.ibtimes.co.uk/russia-cyber-war-hack-moscow-military-snowden-500220**,** (26.03.2016).
[329]GERDEN Eugene, **$500 Million for New Russian Cyber Army**, Security Magazine UK, http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/, (26.03.2016).
[330]State Security Magazine, **Russia Announces Development of Cyber Military Unit**,http://www.tripwire.com/state-of-security/latest-security-news/russia-announces-development-cyberwar-military-unit/, (26.03.2016).

Bununla birlikte 2010 yılında RF hükümeti tarafından devlet istihbarat politikasını belirleyen ve RİS'in hedef önceliklerini şekillendiren dört temel amaç kabul edilmiştir. Söz konusu amaçlar şöyle özetlenebilir.[331]

1. Rus devletinin istihbarat politikalarının temel amacı, Rus toplumu için bir değerler sistemi oluşturma yönünde her türlü tedbiri alınması ve bu yönde faaliyet yürütülmesidir.

2. Rus milli istihbarat stratejileri, ulusal ve uluslararası kamuoyunun, Rus devletinin politikalarına yönelik desteğinin sağlanmasını amaç edinir. Bu amacın, RİS'ne doğrudan psikolojik istihbarat ve dezenformasyon faaliyetleri yürütmek suretiyle, hedef toplum veya toplum kesimlerinin olaylar karşısındaki tutum ve davranışlarını RF lehine etkilemeye yönelik operasyonel çalışma yürütme görevi verdiği açıktır.

3. RİS, yıkıcı ideolojiler, aşırı dini akımlar, RF aleyhine ulusal ve uluslararası kamuoyunu etkilemeye yönelik faaliyetlere karşı koyacak planlamalar geliştirmeyi hedeflemektedir. Böylelikle, bu hedef kapsamında, RF kendi ülkesine yönelik psikolojik istihbarat faaliyetlerini ve dezenformasyon çalışmalarını engelleyeceğini de net bir şekilde beyan etmektedir.

4. Rus istihbarat politikaları, askeri, teknolojik ve siyasi yapılanmaları da içerecek şekilde, RF'nin ulusal enformasyon fonksiyonlarının güvenliğini ve istikrarını sağlamalıdır. Görüldüğü üzere, Rus kamu ve güvenlik bürokrasisi tarafından RİS'in en temel amaçlarından biri, RF'nin ülke genelindekisiber savunmasını sağlamaya yönelik adımlar atılmasıdır.

Yukarıda aktardığımız bilgilerden de anlaşıldığı üzere Rus sivil ve askeri istihbarat servisleri, haber toplama yöntemi olarak geleneksel HUMINT (Human Intelligence / İnsan Kaynaklı İstihbarat), SIGINT (Signal Intelligence / Sinyal İstihbaratı), ELINT (Electronic Intelligence / Elektronik İstihbarat) ve diğer istihbarat toplam tekniklerinin yanı sıra siber saldırı şeklinde düzenlenmiş espiyonaj operasyonlarına dayanan geniş ve sistematik bir yapıya sahip olmayı hedeflemektedir. Böyle bir yapılanma ile RF, Rus toplumunun ekonomik kalkınmasını ve enerji güvenliği açısından hayati öneme sahip ekonomik, finansal ve teknolojik istihbarat ihtiyaçlarını karşılamaya ve ülke güvenliğini sağlamaya

[331]GADYve AUSTIN, op. cit., p. 6.

çalışmaktadır. Son yıllarda yapılan yatırımlar ile RF'nin bu amaca hizmet eden siber kapasitesinde ciddi bir artış söz konusu olmuştur.[332]

RF, istihbarat ve askeri doktrinin temel amacı öncelikle Rus çıkarları doğrultusunda ülkenin enformasyon güvenliğini sağlamaktır. RF, belirtilen amaç doğrultusunda ülkenin siber güvenliğini sağlamaya çalışırken, siber uzayın verdiği imkânlardan azami ölçüde faydalanan ve Rus hükümetlerinin istihbarat ihtiyaçlarının yanı sıra ülkenin ihtiyaç duyduğu stratejik öneme sahip teknolojik yenilikleri elde etmeye yönelik bir siber espiyonaj sistemi de kurmayı hedeflemiştir. Bu çerçevede RF tarafından birbirleriyle eş güdüm halinde çalışan her biri ortak ve farklı amaçlara yönelmiş, siber uzayı kullanma noktasında önemli imkân ve kabiliyete sahip dört istihbarat (FSB, FSO, SVR, GRU) servisi teşekkül ettirilmiştir.

RİS'in günümüzde ulaştığı ofansif, defansif, operasyonel, stratejik, elektronik harp kabiliyetine sahip, psikolojik istihbarat faaliyetlerine uygun, manipülasyona ve dezenformasyona elverişli yapısı, RF'yi siber uzayda faaliyet gösteren en önemli aktörlerden biri konumuna kavuşturmuştur. Öte yandan, RİS'lerinin sahip oldukları siber kapasitelerinin kullanılmasında, illegal siber kriminal şahısların, örgütlerin ve odakların da önemli rolü bulunmaktadır. RİS ile bahse konu illegal çevreler arasındaki siber işbirliği, RF'nin siber kapasitesinin imkân ve kabiliyetinin anlaşılması noktasında ciddi öneme sahiptir.

Yukarıda özetlendiği haliyle RF, istihbarat servislerinin imkân ve kabiliyetlerinin de verdiği destek ile siber uzayda etkili bir siber güç konumuna ulaşmıştır. Öte yandan RF'nin sahip olduğu siber gücün Nye'nin "siber güç" kavramıyla ilgili tanımlamasıyla paralellik arz ettiği de ileri sürülebilecektir.

Çalışmamızın ilk bölümünde de ifade edildiği üzere Nye tarafından "*insan kaynağı ve yeteneği, yazılım ve donanım teknolojiler, altyapılar ve ağ teknolojileri ile ilgili tüm kaynaklar vasıtasıyla yaratılan bir imkân" şeklinde* tanımlanmış olan siber gücün neden olduğu değişim ve güç uygulamaları hem yumuşak güç hem de sert güç kavramı ile birlikte değerlendirilmelidir. Siber gücün, bir yumuşak güç uygulaması olarak kullanılmasına

[332]Ayrıntılı bilgi için bkz. HAGESTAD II William, op. cit. pp. 18-25.

örnek olarak RF'nin yeni nesil enformasyon savaş stratejisi gösterilebilir. RF'nin bahse konu stratejisi ise çalışmamızın ilerleyen safhasında detayları ile analiz edilecektir. [333]

Öte yandan siber gücün başkaları üzerinde kontrol kurmak ve onlara zarar vermek için kullanılması halinde ise bu durum, sert güç kavramı kapsamında ele alınmalıdır. Bu kapsamda Nye, İran'daki nükleer tesislerin yapılan Stuxnet saldırısını sert güç kullanımına örnek olarak göstermektedir.[334] Stuxnet saldırısına benzer şekilde RF istihbarat servislerinin sahip oldukları siber güçler kapsamında planladığı iddia edilen saldırı ve espiyonaj faaliyetleri ise çalışmamızın bir sonraki başlığında detayları ile değerlendirilecektir.

3.2. Rus İstihbarat Servisleri Kaynaklı Olarak Gerçekleştiği İddia Edilen Siber Saldırı ve Espiyonaj Faaliyetleri

RİS'lerin çalışma alanları, operasyonları, imkân ve kabiliyetleri ile siber kapasiteleri sıklıkla dünya kamuoyunda tartışılmasına rağmen, bu servislerin örtülü siber faaliyetleri ile ilgili olarak sınırlı açık kaynak bilgisi mevcuttur. Konu kapsamında hâkim olan kanı; FSB, GRU, SVR ve FSO'nun siber uzay alanında kendi faaliyet alanları ile ilgili olarak, öz kaynaklarını ve uzman personelini kullanmak suretiyle özel operasyonlar sürdürmekte oldukları şeklindedir. Bu servislerin ihtiyaç hissettikleri faaliyetleri için ise siber kabiliyete sahip kriminal şahıslardan da istifade ederek, özel operasyonlar planlayabildikleri de iddia edilmektedir. Ayrıca söz konusu faaliyetlerin sürdürülmesi noktasında ise bu istihbarat örgütlerinin birbirleriyle koordineli bir şekilde faaliyet gösterdikleri ileri sürülmektedir. RİS'lerin uluslararası kamuoyuna yansıyan bazı illegal siber saldırı ve espiyonaj faaliyetleri ise aşağıda genel hatlarıyla açıklanmıştır.

1.2008 yılında ABD Savunma Bakanlığı ve ABD Ordusu'na yönelik olarak gerçekleştirilen siber saldırılarda kullanılan "BTZ" isimli yazılımı üretme kapasitesine sadece RF ile bağlantılı çevrelerin sahip olduğu bilinmektedir. Söz konusu yazılım 2008 yılında bir taşınabilir bellek vasıtasıyla ABD Ordusu'nun bir Ortadoğu ülkesinde bulunan

[333] Ayrıntılı bilgi için bkz. NYE, "Nuclear Lessons for …", op. cit., , pp. 11-15.
[334] Ibid.

üstündeki bilgisayarları kullanılmak suretiyle aktive edilmiş ve 14 ay boyunca etkinliğini sürdürmüştür.[335]

2. Siber güvenlik hizmeti ve yazılımları alanında faaliyet gösteren "Fire Eye" isimli ABD orijinli bir şirket tarafından 2014 yılında yayınlanan bir raporda, RF'nin "APT28" takma adlı bir grup vasıtasıyla bir dönem sürdürdüğü siber casusluk faaliyeti gündeme getirilmiştir. Bu rapora göre "*APT28, casusluk amaçlı bir dizi siber faaliyeti bünyesinde barındıran, 2007 yılından beri aktif olarak kullanılan, özellikle Doğu Avrupa ülkeleri ile NATO ve Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT)'nın savunma kapasitelerini hedef alan bir espiyonaj operasyonu/grubu*" şeklinde tanımlanmıştır.[336]

3. Yine "Fire Eye" tarafından 2013 Ekim ayında yayımlanan bir başka raporda, FBI'ın 2010 yılında Microsoft'ta çalışan Alexey Karetnikoc isimli bir RİS mensubunu ABD aleyhine siber casusluk faaliyeti gerçekleştirdiği gerekçesiyle tutukladığı, 2012 yılında Rus güvenlik şirketi Kaspersky Lab'ın "Red October" takma adlı bir siber casusluk operasyonu kapsamında çoğunluğu eski Doğu Blok'u üyesi ülke vatandaşlarının internet ve kişisel haberleşmelerini takip ettiğinin belirlendiği şeklinde bilgiler yer almıştır.[337]

4. F-Secure isimli bir data güvenlik şirketi tarafından 2015 Eylül ayında yayınlanan başka bir raporda, RF'nin "*The Dukes*" isimli bir yazılımı kullanılmak suretiyle yedi yılı aşkın bir süre için Avrupa, Asya ve Amerika'daki bazı ülkeleri hedef alan bir siber espiyonaj operasyonu sürdürmekte olduğu iddia edilmiştir. Raporda ayrıca, belirtilen faaliyetin RF destekli hackerlar tarafından gerçekleştirildiği, özellikle de Gürcistan'ın NATO'daki Enformasyon Merkezi'ni, Gürcistan Savunma Bakanlığı'nı, Türk Dışişleri Bakanlığı'nı ve ABD, Avrupa ve Orta Asya'daki bazı düşünce merkezleri ile hükümet kuruluşlarını hedef aldığı ifade edilmiştir.[338]

5. Alman Der Spiegel Dergisi'nde, 2016 Şubat ayında yayınlanan bir haberde, 2015 yılı içinde Almanya Federal Meclisi (Bundestag)'ne yönelik olarak GRU kaynaklı siber

---

[335]STEWART Phil ve WOLF Jim, **Old Worm Won't Die after 2008 Attack on Military**,Reuters, June 16 2011, http://www.reuters.com/article/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617, (16.06.2016).
[336]FireEye, **APT28-A Window Into Russia's Cyber Espionage Operations?**, Special Report by FireEye, https://www.fireeye.com/, (01.04.2016).
[337]GEERS Kenneth, Darien Kindlund, Ned Moran, Rob Rachwald,**World War C**:**Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks**, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf, (14.04.2016), p. 12.
[338]Al Jazeera Internet Web, **Report: Russia sponsored cyber attacks**, http://www.aljazeera.com/news/2015/09/report-russian-government-sponsored-cyber-attacks-150917132351595.html, (01.04.2016).

espiyonaj saldırılarının gerçekleştirildiğinin, Almanya Federal Haber Alma Servisi (Bundesnachrichtendienst / BND) tarafından tespit edildiği bilgisi yer almıştır.[339] Bu siber saldırının Rus askeri istihbarat servisi tarafından gerçekleştirildiğinin açıklanması, GRU'nun siber saldırı kapasitesine sahip olduğunu göstermesi bakımından oldukça dikkat çekicidir.

6. Bloomberg Teknoloji Haber Portalı'nda, 14 Ekim 2015 tarihinde yayınlanan bir makalede ise RİS destekli hackerların Polonya Borsası'na yönelik olarak siber saldırılar gerçekleştirdiğinin tespit edildiği haberleştirilmiştir. Polonyalı yetkililer konuyla ilgili olarak, Rus hackerların söz konusu siber saldırının Polonya'nın Irak ve Suriye politikasının intikamı amacıyla cihatçı gruplar tarafından gerçekleştirildiği manipülasyonunu yaptıklarını, bu hedef kapsamında kullandıkları casus yazılıma yönlendirme amaçlı izler bıraktıklarını, ancak bu izlere rağmen saldırının arka planının RF tarafından espiyonaj amaçlı olarak tasarlandığının tespit edildiğini kamuoyuna açıklanmıştır.[340] Saldırıda, RİS'in siber uzayın anonim yapısından da istifade ederek, saldırının kaynağı ile ilgili dezenformasyon faaliyeti gerçekleştirmiş olmaları önemlidir. Bu itibarla siber saldırı ve espiyonaj faaliyetlerinde, aktivitenin kaynağı ile ilgili olarak daima bu şekilde yanıltıcı planlamaların rahatlıkla uygulanabileceği de hatırda tutulmalıdır.

7. ABC Haber Kanalı tarafından 2014 yılında yapılan bir başka haberde, ABD güvenlik ve istihbarat görevlilerince, RF kaynaklı bir yazılım programının 2011 yılından bu yana ABD'nin doğalgaz, petrol, içme suyu ve sulama sistemine zarar verdiğinin tespit edildiği gündeme getirilmiştir. Söz konusu yazılımın belirtilen kritik altyapı sistemlerinin kontrol mekanizmalarını hedef alarak, zarar vermeyi amaçlayacak şekilde tasarlandığı da aynı haberde yer almıştır.[341]

8. 1 Nisan 2016 tarihinde, Flash Critic Cyber Threats News isimli haber ajansının yayınladığı bir haberde ise RF kaynaklı olarak ABD'de faaliyet gösteren JP Morgan Chase&Co Bankası da dâhil, ismi açıklanmayan beş bankaya subversif amaçlı siber

[339]Der Spiegel News Magazine, **Was Russia behind 2015's cyber attack on the German parliament?**, http://www.dw.com/en/was-russia-behind-2015s-cyber-attack-on-the-german-parliament/a-19017553, (01.04.2016).
[340]Bloomberg Tecnology News Portal, **Cyberspace Becomes Second Front in Russia's Clash With NATO**, http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato, (01.04.2016).
[341]ABC News, **Trojan Horse Bug Lurking in Vital US Computers Since 2011**,http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476, (01.04.2016).

saldırılar gerçekleştirildiği belirtilmiştir. Söz konusu haberde, siber saldırıların 2015 Ağustos ayından bu yana devam ettiği, saldırıların oldukça sofistike bir yazılım kullanılarak yapılmış olması nedeniyle ABD'li yetkililerin saldırının arkasında RF'nin olduğuna kesin olarak emin oldukları ifade edilmiştir.[342]

Genel ve soyut olarak aktardığımız bu örneklerden de anlaşılacağı üzere FSB, GRU, SVR ve FSO'nun siber kapasitelerinin kullanımında, illegal siber kriminal şahısların, örgütlerin ve odakların da önemli rolü bulunmaktadır. Bu kapsamda RİS ile bahse konu illegal çevreler arasındaki siber işbirliği, RF'nin siber güvenlik kapasitesinin imkân ve kabiliyetinin anlaşılması noktasında bizce büyük bir öneme sahiptir.

3.3. Rus İstihbarat Servisleri ile İrtibatlı Siber Kabiliyete Sahip Kriminal Örgüt ve Şahısların Faaliyetleri

SSCB, dağılıncaya kadar dünyanın en büyük mühendis ülkesi olduğu kabul edilmiştir. SSCB'nin sahip olduğu mühendislerin büyük bir kısmı ise ciddi bilgi birikimi ve beceri gerektiren savunma, uzay ve ağır sanayi alanlarında istihdam etmiştir. SSCB'nin dağılması sonrasında, bu yetişmiş iş gücü ekonomik sıkıntılar ile karşı karşıya kalmış ve geçim sıkıntısı motivasyonu bu şahısları, başta bilişim sektörü olmak üzere illegal faaliyetlere yöneltmiştir. Bu durumun bir sonucu olarak özellikle 1990–2000 yılları arasında Rus kökenli hackerların sayısında adeta patlama yaşanmıştır. 2000'li yıllar sonrasında Rus ekonomisinde yaşanan iyileşme, siyaset ve devlet düzeninde kavuşulan istikrar ve disiplinin bir sonucu olarak, söz konusu illegal yapılar da Rus devlet kurumları ile uyumlu faaliyet göstermeye başlamış ve günümüzde önemli ölçüde RF devlet sisteminin denetimine girmişlerdir.[343]

Bu gelişmeler kapsamında RF'nin gerek istihbarat servisleri gerekse de bu servisler ile doğrudan bağlantılı illegal örgütler üzerinden sistematik siber saldırılar düzenleme kapasitesine sahip olduğu rahatlıkla ifade edilebilir. Bu illegal örgütlerden en bilineni ise

[342]Flash Critic Cyber Threats News, **Russian cyber warfare suspected in the bank attack**, http://flashcritic.com/russian-cyber-warfare-suspected-bank-attacks-sophisticated-hackers/, (01.04.2016).
[343]LOBANOVA Katerina, **How Russia Became a Hacking Superpower**, https://themoscowtimes.com/articles/russia-hacker-superpower-56704,(04.01.2017).

NATO tarafından da ittifakın varlığı için en tehlikeli suç örgütlerinden biri olarak kabul edilen Russian Business Network (Rus İş Ağı / RBN)'dür.[344]

RBN'nin Rus devleti ile bağlantılı olduğuna dair spekülasyonun da ötesinde birçok makale ve yorum bulunmaktadır. İlk olarak 2006 yılında bir Rus internet sitesi olarak kurulan RBN, zamanla siber imkânlardan yararlanmak suretiyle gelir elde etmeyi amaçlayan illegal faaliyetlere de yönelmiştir.[345]Diğer yandan RBN'nin bu faaliyetlerinin 2007 ve 2008 yılları arasında Rus güvenlik güçleri tarafından takibe alındığı ve RBN'nin bu nedenle IP adres ve domainlerini ÇHC ile Tayvan'a taşımak zorunda kaldığı iddia edilmiştir. Bu tarih sonrasında ise RBN'nin operasyonlarının gerçekten var olup olmadığı sürekli olarak tartışmalara neden olmuştur. Bununla birlikte RBN'nin daha sonraki yıllarda kriminal faaliyetlerini son derece sofistike hale getirme imkânına kavuştuğu, hatta bu tarihlerde ABD Savunma Bakanlığı'nın yönelik olarak siber casusluk faaliyetleri gerçekleştirdiği de çeşitli analizlere konu olmuştur.[346]

RBN'nin temel operasyonları ise "*kimlik hırsızlığı, phishing*[347,] *botnet*[348]*, zararlı yazılım üretme, çocuk pornografisi ile bankacılık ve kredi kart sahteciliği*" şeklindedir.[349]Tüm dünyadaki siber suçların %60'ını tek başına RBN tarafından işlendiği dahi iddia edilmektedir.[350]

RBN'nin dünya genelinde tanınmasını sağlayan olay ise2008 yılındaki RF-Gürcistan Savaşı esnasındaki siber saldırılardır. Bu dönemde, Gürcistan'a yönelik olarak gerçekleştirilen "botnet" saldırılarının büyük bir bölümünün RBN kaynaklı olduğu gündeme getirilmiştir.[351] RBN'nin savaş esnasındaki faaliyetlerini ne şekilde mobilize ettiği ve planlandığı tam olarak ortaya konamamış olmasına rağmen, RBN'nin bu kriz

---

[344]YENER Yavuz, **Rus Krizinin Gözden Kaçan boyutu: Siber Savaş Tehdidi**,http://www.usak.org.tr/tr/usak-analizleri/yorumlar/rus-krizinin-gozden-kacan-boyutu-siber-savas-tehdidi, (12.04.2016).
[345]The Guardian, **Cyber Crimes**, http://www.theguardian.com/technology/2007/nov/15/news.crime, (12.04.2016).
[346]HEICKERO, op. cit., p. 37.
[347]İngilizce password (şifre) ve fishing (balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş "phishing" ifadesinin Türkçe karşılığıdır. "Yemleme" diye tanımlanan yöntemlerle şifre avcıları, genelde e-posta gibi yollarla kişilere ulaşır ve onların kredi kartı gibi ayrıntılarını sanki resmi bir kurummuş gibi ister. Bu ava karşılık veren kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınmaktadır.
[348]Zorla veya hileli bir yöntemle ve kötü bir yazılım da kullanmak suretiyle, tüm kontrolü bir hackerin geliştirdiği koda bırakılmış bilgisayar ve aygıtlardan olusan ağa verilen isim olarak tanımlanabilecektir.
[349]YENER, loc.cit.
[350]Ayrıntılı bilgi için bkz. HEICKERO, op. cit., pp. 37-38.
[351]Project Grey Goose Phase II Report,**Russia/Georgia Cyber War**, https://tr.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report, (12.04.2016).

sırasındaki rolü Gürcü kritik altyapısına zarar verilmesi ve Gürcistan aleyhine internet üzerinden Rus yanlısı propaganda yapılması şeklinde olduğu ileri sürülmüştür.[352]Gürcistan Savaşı sonrasında ise RBN'nin faaliyetleri tamamen yer altına çekilmiştir.

RBN'nin operasyonları dışında Rus hackerlar tarafından özellikle Batılı devlet vatandaşlarını hedef alan ciddi boyutlarda siber kriminal faaliyetler de sürdürülmektedir. Bu itibarla Rus hackerlerin ABD ve AB üyesi devlet vatandaşlarına yönelik olarak, sahte bankacılık işlemleri, çalıntı ve kopya kredi kartları, ele geçirilmiş sosyal güvenlik ve vatandaşlık numaraları vasıtasıyla yıllık 100 Milyon ABD $ tutarında gelir elde ettiği iddia edilmektedir.[353]RF'nin ise bahse konu grupların suç faaliyetlerine Rus vatandaşlarının ve RF'nin çıkarlarını doğrudan etkilemediği sürece görmezden gelmektedir.[354]Bu grupların bir başka faaliyet alanı ise milliyetçilik duyguları ile Rus devleti ve Rus çıkarları aleyhine faaliyet yürüttüklerini düşündükleri düşman devlet kurumlarına ve kuruluşlarına, sivil toplum örgütlerine, uluslararası şirketlere yönelik siber saldırılar gerçekleştirmektir.[355]

Bu noktada Putin'in inisiyatifi ile kurulan Nashi Gençlik Hareketi'nin siber faaliyetlerinin de dikkat çekicidir.[356] Nashi Gençlik Hareketi, Kremlin yönetiminin yönlendirmesi ile özellikle Renkli Devrimler esnasındaki gençlik hareketinin potansiyelini de dikkate alarak, bu devrimlerin RF sınırları içinde de yayılmasını ve etkili olmasını engellemek amacıyla kurulmuştur.[357] Bu kapsamda, hareket, özellikle sosyal medyanın kullanılması yoluyla Putin aleyhine muhalif hareketlerin manipüle edilmesi noktasında önemli propaganda ve toplum mühendisliği faaliyetleri sürdürmüştür.[358]

Diğer yandan kimi Batılı siber güvenlik uzmanları tarafından Nashi Gençlik Hareketi'nin ülke dışındaki internet kaynaklı psikolojik propaganda operasyonlarını planlamak amacıyla, RİS ve RBN ile illegal bağlantıya sahip olduğu ve özellikle de

---

[352] MARKOFF John, **Before the Gunfire, Cyberattacks**, New York Times, August 2008, New YorkEdition, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&; (12.04.2016)
[353]HAGESTAD II, op. cit., p. 3
[354]GILESKeir, **Russian Cyber Security: Concepts and Current Activity**, Chatham House Conflict Studies Research Centre REP Roundtable Summary,https://www.chathamhouse.org/sites/files/chathamhouse /public/ Research/ Russia%20and%20Eurasia/060912summary.pdf, (14.04.2016).
[355]Ibid., p. 4.
[356]JONES James, **Putin's youth movement provides a sinister backdrop to Russia's protests**, http://www.theguardian.com/commentisfree/2011/dec/08/putin-russia-elections, (12.04.2016).
[357]HALHALLI Yusuf, **Kremli'nin Gençlik Hareketi**, https://www.academia.edu/7302656/ KREML%C4%B0N%C4%B0N_GEN%C3%87LER%C4%B0_NASH%C4%B0_GEN%C3%87L%C4%B0K_HAREKET%C4%B0, (12.04.2016).
[358]Voice of America, **Russia Plays Big Role in Cyber Spying, Hacking**,http://www.voanews.com/ content/russia-plays-big-role-in-cyber-spying-hacking/2522915.html**,** (12.04.2016).

RBN'den siber propaganda imkânları sağlayacak yazılımlar satın aldığını da iddia etmiştir.[359]

3.4. RF Siber Alanının Yapısal Özellikleri

Bir devletin siber alanın yapısal özellikleri, o devletin internet ve ağ teknolojilerini düzenleyen ulusal kanunlar ve kurumlar, söz konusu kanunların yaptırım gücü ve etkisi ile bu sektörlerde faaliyet gösteren şirketlerin yapısı ve teknolojik kapasiteleri ile ilintilidir. Bu kapsamda, RF'nin ulusal alanı açısından detaylı bir şekilde analiz edilmesi, RF'nin siber güvenlik stratejisinin ve kapasitesinin anlaşılması noktasında oldukça önemlidir.

Putin'in devlet başkanı olmasında sonra, RF'nin ekonomik ve ticari yapısının giderek bir nevi nepotik kapitalizme (akraba-dost kapitalizmi) doğru evirildiği, bu yapı içinde devlet ve özel sektör arasında sıkı bir birliktelik söz konusu olduğu literatürde genel kabul gören bir yaklaşımdır. Bu özellik RF siber alanının yapısını da etkilemiş ve devlet ile özel sektör sıkı bir işbirliği içine girmiştir.[360]

Örneğin RF'de, mobil telefon sektörünün %92'si 4 şirket, telekomünikasyon sektörünün ise % 62'si 6 şirket tarafından kontrol edilmektedir ve bu şirketlerin faaliyetleri de belirtilen haliyle akraba-dost kapitalizminin özellikleri kapsamında değerlendirilebilir. RF'nin bu şirketler üzerinde ciddi bir hükümet baskısı ve denetimi söz konusu olmakla birlikte, Rus donanım ve yazılım teknolojileri, telekomünikasyon, data ve iletişim altyapısı önemli ölçüde dış kaynaklı dizayn ve yapıya sahiptir. Bu dışa bağımlı yapı RF'deki diğer stratejik sektörler için de (enerji, hizmet, inşaat, altyapı, gıda vb.) geçerlidir [361]

Dışa bağımlı yapının bir stratejik zafiyet yarattığının farkında olan Rus güvenlik ve istihbarat bürokrasisi, bu yapıyı millileştirmek adına bazı girişimlerde bulunmuştur. Bu kapsamda, RF Devlet Başkanlığı, işletim sistemleri ve yazılım altyapısında Microsoft başta olmak üzere diğer ABD orijinli şirketlere olan bağımlılığın azaltılmasını amaçlayan

[359]MEDVEDEV, op. cit., p. 31.
[360]MEDVEDEV, op. cit., p. 34.
[361]KELLY Sanja, **Freedom on the Net 2014:Russia**, Freedom House, 2014,https://freedomhouse.org/sites/default/files/resources/Russia.pdf., (15.04.2016).

planlamalarını tamamlamıştır.[362]Nitekim 2014 Şubat ayında RF Genelkurmay Başkanlığı Askeri Bilimsel Komitesi üyesi General Igor Sherement verdiği bir beyanatta "*RF'nin siber güvenlik altyapısının dışa bağımlılığının azaltılması gerektiğini*"[363] açıkça belirtmiştir. Sherement tarafından 2014 yılında yazılan başka bir makalede ise "*Rusya'nın dışa bağımlı teknolojik yapısının geçici olduğu, alınan tedbirler ile özellikle iletişim, telekomünikasyon ve siber güvenlik teknolojilerinde millileşme oranının kısa sürede arttırılacağı ve Skolkovo İnovasyon Merkezi'nin yakın zamanda bir nevi Rus Silikon Vadisi özelliğine sahip olacağı*"[364] ileri sürülmüştür.

Rus bilgi güvenliği (anti-virüs) alanında faaliyet gösteren en önemli şirket ise bilindiği üzere Kaspersky firmasıdır. Bu firma, McAfee, Norton ve Symantec şirketleri ile birlikte anti-virüs sektöründe küresel alanda ciddi bir rekabet içinde olup, Kaspersky'nin dünya genelinde 400 milyona yakın müşterisi olduğu tahmin edilmektedir.[365] Kaspersky'nin Rus devletinin yanı sıra RİS ile de yakın irtibatının olduğu, bu şirketin ilk kurucusu olan ve şirkete adını veren Eugene Kaspersky'nin de eğitimine KGB destekli bir bilim akademisinde başladığı iddia edilmektedir.[366]

Yukarda belirttiğimiz üzere RF, ulusal siber uzay alanını denetim altında tutmak amacıyla da ciddi çaba göstermektedir. Freedoam House tarafından yayımlanan bir rapora göre, 2014 yılı itibarıyla Rus nüfusunun sadece %61'i internet erişimine sahiptir. Bu oran, ABD'deki %81, Fransa'daki %82, İngiltere'deki %90 oranları dikkate alındığında oldukça düşüktür. RF'nin ulusal internet kullanımına yönelik tedbirleri 2012 yılına kadar görece olarak daha liberal bir tarzda gelişmiştir. Bu liberal ortamında yardımıyla, milliyetçi Rus hackerların Estonya ve Gürcistan'a yönelik siber saldırlar esnasında oldukça etkin rol oynadıkları da ileri sürülmüştür. Rus çıkarlarını hedef almadıkları sürece RF'de genelde bir denetime tutulmayan siber kriminal grupların faaliyetleri de 2012 yılına kadar aktif bir tarzda gerçekleşmiştir.[367] 2012 yılında ise RF Devlet Başkanlığı seçimleri sırasında sosyal

[362]EastWest Instıtute, **The American and Russian Approaches to Cyber Challenges**,http:// www.omicsgroup.org/journals/the-american-and-russian-approaches-to-cyber-challenges216774.1000110.pdf, (14.04.2016).
[363]MEDVEDEV, op. cit., p. 35.
[364]ZINOVYEVA Elena, "U.S. Digital Diplomacy: Impact on International Security and Opportunities for Russia," **A Russian Journal on International Security**, Vol.19, No. 2, 2013, p. 39.
[365]Kaspersky Company, **About Kaspersky Lab**, www.kaspersky.com/about., (15.04.2014).
[366]SHACHTMAN Noah, **Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals**,Wired Magazine, www.wired.com, (15.04.2014).
[367]KELLY Sanja, **Freedom on the Net 2014:Russia**, Freedom House, 2014, https://freedomhouse. org/sites/default/files/resources/Russia.pdf., (15.04.2016).

medyanın Putin karşıtı faaliyetler için uygun ve etkili bir zemin oluşturmasının etkisiyle RF internetin denetlenmesi noktasında bazı tedbirler almıştır.

Bu kapsamda siber saldırıların ve siber kriminal operasyonların planlanması noktasında hayati öneme sahip anonim (tor) bilgisayarların ve proxy servislerinin kontrol edilmesi amacıyla Putin'in talimatıyla RF İçişleri Bakanlığı 2014 Haziran ayında 3,9 Milyon Ruble bütçe ayırmıştır.[368] Bu kapsamda, FSB yöneticisi Alexsandr Bortnikov yaptığı açıklamada: *"tor servislerinin siber suçlar ve çocuk porno dağıtıcıları tarafından sıklıkla kullanıldığını, devlet olarak bunu engelleyeceklerini ve bu servislerin tümünü kapatacaklarını"*[369] beyan etmiştir. Ayrıca, akıllı cep telefonları üzerinden internete bağlanılmasının denetlenmesi amacıyla da cep telefonlarında kullanılan sim kartların ve kamuya açık alanlarda kablosuz ağ girişi (wi-fi) girişi yapan akıllı telefonların kayıt altına alınmasına yönelik bir yasa 2014 Ağustos ayında kabul edilmiştir.[370]2014 Mayıs ayında kabul edilen bir başka yasayla internet üzerinden kolaylıkla açılabilecek blogların günlük olarak 3000 kişi tarafından giriş yapılabilecek bir kapasiteye ulaşması halinde, bu blogların Federal Komünikasyon, İletişim, Teknoloji ve Medya Denetleme Kurumu (Roskomnadzor)'na kayıt olma zorunluluğu getirilmiştir.[371]Söz konusu yasayla ayrıca, blog yazarlarının takma ad kullanmaları yasaklanmış, yazdıkları tüm yazıların doğruluğunu delillendirmeleri zorunluluk haline getirilmiş ve blogların ziyaretçi giriş-log kayıtlarını altı ay süreyle arşivlemeleri mecburiyeti getirilmiştir.[372]

Diğer yandan söz konusu tedbirlerin iki yönlü bir sonucu bulunmaktadır. Anonim bilgisayarların denetlenmesi, RF'nin kendi siber uzay alanını kontrolü düşünüldüğünde oldukça önemlidir.[373]Bununla birlikte bu tür bilgisayarların varlığının ortadan kaldırılması durumu da ters orantılı olarak RF siber alanı kaynaklı siber saldırı ve kriminal faaliyetlerin gerçekleştirilmesini daha zor ve maliyetli hale de getirmektedir. Yani 2014 yılı sonrası için

[368]BBC News, **Russia Offers $110,000 to Crack Tor Anonymous Network**,http://www.bbc.com/news/technology-28526021, (15.04.2014).
[369]Türk İnternet Haber Sitesi, **Rusya Tor Networkünü ve Anonimlik Araçlarını Erişime Kapatmaya Hazırlanıyor.**", http://www.turk-internet.com/portal/yazigoster.php?yaziid=43607, (27.04.2016).
[370]MEDVEDEV, op. cit., p. 39.
[371]BIRNBAUM Michael, **Russian Blogger Law Puts New Restrictions on Internet Freedoms**,Washington Post, http://search.proquest.com/docview/1550033701., (15.04.2016).
[372]Türk İnternet Haber Sitesi, **Rusya'da Yürürlüğe Giren Yeni Yasayla Blog'lara Ağır Sorumluluklar Getiriliyor.**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=46851, (27.04.2016).
[373]MEDVEDEV, op. cit., p. 38.

RF siber savunmasını artırmak isterken, siber saldırı kapasitesinden ödün vermek durumunda kalmıştır.[374]

Bununla birlikte RF siber güvenliğini sağlamak için kabul ettiği ve 2016 yılında uygulanmaya başlanacak olan bir yasayla da Rus vatandaşlarına yönelik kişisel bilgileri, verdiği hizmet gereği elinde tutma imkânına sahip olan şirketlerin, bu verilerin fiziksel bir arşiv ortamına da aktarması zorunlu hale getirilmiştir.[375]

RF ayrıca, siber güvenliğini sağlamak amacıyla 1 Eylül 2016 tarihinde "*Rusya Bilgi Yerelleştirmesi*" (Russia Data Localizitaion) isimli bir kanunu kabul etmiştir. Bu kanuna göre yabancı internet sitelerinin ve yabancı şirket internet sitelerinin RF kanunlarına dahil olması, RF merkezli faaliyetlerinin "ru, .su, .moscow" gibi domain adlarını kullanmaları ve internet sayfalarının Rusça versiyonlarını da hazırlamaları kural altına alınmıştır. Bu kapsamda, RF vatandaşlarına yönelik kişisel bilgileri verdiği hizmet gereği elinde tutma imkânına sahip olan tüm şirketlerin, bu verileri RF resmi kurumlarının denetimindeki bir fiziksel arşiv ortamına aktarmaları da sıkı bir denetim tabi tutulmuştur.[376]

RF'nin siber güvenlik alanında uygulamaya koyduğu belki de en önemli tedbir ise SORM sistemidir. SORM sistemi RF'deki internet ve anolog haberleşmesini takip eden ve bir nevi denetleme sistemi şeklinde tesis edilen bir uygulamadır. SORM'un ilk versiyonu 1990'lı yıllarda geliştirilmiştir. Daha sonra ise teknolojik gelişmelere bağlı olarak iki yeni versiyonu daha tesis edilmiştir. SORM'un kontrolü görevi de FSB'ye verilmiştir.[377]Mahiyeti ve yetkinliği tam olarak bilinmemekle birlikte, SORM sistemi ile FSB'nin sadece RF sınırları içinde değil, ülke dışında gerçekleşen her türlü internet, sabit telefon ve cep telefonu iletişimi üzerinde etkin bir denetim kurduğu tahmin edilmektedir.[378]

Putin iktidarının son yıllarda internet ve sosyal medya kaynaklı muhalif hareketlere yönelik sert tedbirler aldığı ve sansür uygulamalarından kaçınmadığı da gözlemlenmektedir. Bu çerçevede, 2014 Mart ayında RF Başsavcılık Ofisi'nin talimatıyla,

---

[374]GONZALEZ Daniel, **Preventing Cyber Attacks: Sharing Information About Tor**,The RAND Blog, http://www.rand.org/blog/2014/12/preventing-cyber-attacks-sharing-informationabout., (16.04.2016)
[375]SONNE Paul ve RAZUMOVSKAYA Olga , **Russia Steps Up New Law to Control Foreign Internet Companies**,Wall Street Journal, http://www.wsj.com/articles/russia-steps-up-newlaw-to-control-foreign-internet-companies-1411574920., (15.04.2016).
[376]Bloomberg Tecnology News Portal, **Russia Clarifies Looming Data Localization Law**, http://www.bna.com/russia-clarifies-looming-n17179934521/, (23.09. 2016).
[377]GILES, "Information Troops-A Russian …", op. cit., pp. 8-9
[378]SOLDATOV Andrei ve BOROGAN İrina,"Russia's Surveillance State",**World Policy Journal**, Vol. 30, No. 3, Fall 2013, p. 24-25.

isyana teşvik ve illegal içerik barındırdıkları gerekçesiyle, muhalefetin etkili isimlerinden Garry Kasparov ve Alexei Navalny tarafından kontrol edilen toplam 4 adet web sitesine erişim yasağı getirilmiştir.[379]

RF'nin sosyal medya imkânları kullanılarak sürdürülmesi olası siber tehditlere karşı aldığı önemli tedbirlerden bir diğeri de Rus orijinli sosyal medya şirketlerinin RF'de kullanılmasını teşvik etmek ve bu şirketlerin yönetiminde kendisine yakın şahısların yer almasına özel önem vermektir. Bu önemin bir sonucu olarak da e-posta hizmeti veren "mail.ru"; "google.com" ile benzer hizmetleri sağlayan "yandex.com"; "facebook.com" ile aynı işlevi gören "vkontakte.ru" ve "odnaklassniki.ru" isimli şirketlerin sadece RF'de değil eski SSCB üyesi ülkelerdeki pazar payları oldukça yaygınlaşmıştır.Bu durum ise Putin iktidarına, RF'de ve eski SSCB üyesi ülkelerde sosyal medya merkezli planlanabilecek olası muhalif toplumsal hareketlerin kontrolü ve RF lehine propaganda faaliyetleri sürdürülmesi noktasında önemli avantaj sağlamaktadır.Ayrıca söz konusu sosyal medya uygulamaları arasında yer alan ve 50 milyon civarı kullanıcı ile muhalif görüşlerin de sıklıkla gündeme geldiği "vkontakte.ru" isimli ağın kurucuları, Putin iktidarının baskıları sonucunda, şirketlerini 2014 Mart ayı içinde Putin'e yakın Alisher Usmanov isimli bir Rus işadamına satmak zorunda kalmıştır.[380]

Aktardığımız bilgilerden de anlaşılacağı üzere, 2000'li yıllar ile birlikte başlayan planlamaların bir sonucu olarak RF'nin günümüzde gerek istihbarat servisleri ve bu servisler ile bağlantılı illegal organizasyonların faaliyetleri gerekse de silahlı kuvvetlerinin sahip olduğu siber imkânlar kapsamında önemli bir siber güç olarak siber uzayı domine edebildiği ortadadır. RF'nin söz konusu siber gücüne özellikle 2010 yılından sonra, Moskova merkezli uluslararası haber ajansları ve sosyal medya olanaklarından da geniş bir biçimde istifade eden enformasyon savaş kabiliyetleri de eklenmiştir. Tüm bu siber imkânlar ile birlikte RF, sahip olduğu siber gücü uluslararası ilişkilerde sorun yaşadığı devletlere karşı bir baskı ve zorlama aracı olarak kullanmaktan çekinmemekte ayrıca da bu

[379]Türk İnternet Haber Sitesi, **Rusya'da Putin Yönetimi de Internet Sansürüyle Muhalefeti Susturmayı Deniyor.**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=46190, (27.04.2016).
[380]Ayrıntılı bilgi için bkz. THOBURN Hoburn, "Rusya Siyasetini Anlama Kılavuzu", **Siyaset, Ekonomi ve Toplum Araştırmalar Vakfı (SETA) Araştırmaları**, 2015,p. 80-89, http://file.setav.org/Files/Pdf/20151019183121_rusya-siyasetini-anlama-kilavuzu-pdf.pdf, (19.10.2016).

tarzda planlanmış olan siber saldırılarını etkili ve yıpratıcı bir enformasyon savaşı ile destekleyebilmektedir.

4. RF Kaynaklı Olduğu İddia Edilen Siber Saldırılar

RF, internetin ve ağ teknolojilerinin hızla yayılmaya başladığı 2000'li yıllar sonrasında, siber uzaydaki gelişmelerin verdiği avantajları uluslararası ilişkilerde bir zor kullanma ve baskı aracı olarak kullanmak amacıyla planlamalar yapmıştır. RF, siber saldırı kapasitesine yönelik yaptığı yatırımların yanı sıra siber güvenliğini sağlama ve internet teknolojileri kaynaklı siber psikolojik savaş yöntemlerini geliştirme konusunda da günümüzde önemli bir siber güç konumuna gelmiştir.

RF, siber savunma ve saldırı kapasitesinde söz konusu gelişmişliğin bir sonucu olarak, uluslararası ilişkilerde özellikle de komşularıyla yaşadığı dış politika sorunları esnasında siber gücünü sofistike yöntemlerle kullanmaktan çekinmemiştir. İddia edildiği üzere RF'nin 2007 yılında Estonya'ya, 2008 yılında Gürcistan'a ve Litvanya'ya, 2009 yılında Kırgızistan'a, 2014 yıllında Ukrayna'ya ve 2015 yılında Türkiye'ye yönelik siber saldırıları, siber uzayın ortaya koyduğu yeni şartların dış politika sorunlarında ne ölçüde etkili olabileceğine yönelik analiz edilmesi gereken önemli örnekler arasında yer almışlardır.

4.1. Estonya'ya Yönelik Siber Saldırılar

Estonya'ya yönelik olarak 2007 yılında RF kaynaklı olarak gerçekleştirildiği iddia edilen siber saldırılar, siber güvenlik literatürünün yanı sıra uluslararası ilişkilerde disiplininde de birçok yönüyle detaylı olarak analiz edilmiştir. Söz konusu siber saldırı Estonya Parlamentosu'nun Tallinn meydanındaki Bronz Asker anıtını kaldırma kararı almasıyla başlamış olmakla birlikte, saldırının arka planında Estonya RF ilişkilerindeki yıllardan beri süregelen gerginliğin yanı sıra RF'nin başta ABD olmak üzere, diğer NATO üyeleriyle yaşadığı küresel mücadelenin de etkisi bulunmaktadır.[381]

Genel ve soyut olarak RF ile Estonya arasındaki ilişkiler tarihsel olarak ele alındığında, iki ülke arasında Estonya'nın demografik ve sosyo-kültürel yapısı kapsamında ortaya çıkan bir gerginliğin mevcudiyeti görülecektir. 2. Dünya Savaşı sonrasında, SSCB tarafından maksatlı bir politik adım olarak Estonya'ya önemli oranda Rus kökenli nüfus

[381]BIÇAKCI, "NATO'nun Gelişen Tehdit …", op. cit., s.121.

yerleştirilmiştir. İlerleyen süreçte ise demografik denge Rus azınlık lehine değişmeye başlamıştır. Doğu Blok'unun yıkılması sonrasında ise diğer Baltık ülkelerinin aksine, Estonya ülkesinde %40 oranında bulunan Rus azınlığa vatandaşlık hakkı verme noktasında isteksiz davranmış ve bu durum RF ile Estonya ilişkilerinde süregelen bir gerginliğin oluşmasına neden olmuştur.[382]

Diğer yandan teknolojik mirasının ve eğitim seviyesi yüksek nüfusunun yanı sıra 2000'li yıllarda yapılan yatırımlarla ile birlikte, Estonya iletişim, telekomünikasyon, yazılım ve ağ teknolojileri alanlarındaki Avrupa'nın en gelişmiş e-devleti olarak kabul edilmiştir. Bu itibarla elektronik oy kullanma imkânını vatandaşlarına ilk defa sunan Estonya, halkının % 60'a yakının günlük ihtiyaçlarının önemli bir kısmını internet üzerinden karşıladığı, ülkedeki bankacılık işlemlerinin yaklaşık %96'sının internet üzerinden gerçekleştirildiği bir ülke konumuna ulaşmıştır.[383]

26 Nisan 2007 tarihinden yani Tallinn meydanındaki Bronz Asker heykelinin kaldırılması kararının alınmasından kısa bir süre önce, Estonya'nın kritik altyapılarına yönelik olarak geniş çaplı bir servis dışı bırakma (Distributed Denial of Service / DDoS)[384] saldırısı başlatılmıştır.[385] Bu siber saldırılar ile Estonya'nın siyasi partilerinin, devlet kurumlarının, parlamentosunun web sayfalarına, akabinde; medya kuruluşlarının, bankacılık ve finans sistemine siber saldırılar gerçekleştirilerek, Estonya'nın internet altyapısı çökertilmek istenmiştir.[386] Saldırılar, her ne kadar son derece organize ve yoğun bir şekilde gerçekleşse de Estonya hükümetinin ulusal internet ağını yurtdışından erişime

[382]YENER Yavuz, **8. yılında Estonya Saldırılarına çok boyutlu bir bakış**, https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/, (18.04.2016).
[383]OTTİS Rain, **Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective**, In Proceedings of the 7th European Conference onInformation Warfare and Security, Plymouth, Reading: Academic Publishing Limited, 2008, http://www.academic-bookshop. com/ourshop/prod_1355933-ECIW-2008-7th-European-Conference-on-Information-Warfare-and-Security-Plymouth-UK.html, (18.04.2014).
[384]Distributed Denial of Service (DDoS) olarak bilinen siber saldırı yönteminde, ilk aşamada kötü amaçlı yazılımlarla çok sayıda bilgisayar aynı anda ele geçirilmekte ve bu bilgisayarlar *"zombi"* bilgisayar hâline getirilmektedir. Bu aşamada, çoğu zaman kullanıcılar, bilgisayarlarının ele geçirildiğinin farkında olmamaktadırlar. İkinci aşamada ise ele geçirilen bu bilgisayarlardan *"botnet"* adı verilen bir ağ oluşturarak önceden planlı bir şekilde hedeflenen web sayfalarına sistematik olarak saldırmak suretiyle, hedef aldıkları ağ sistemlerini kullanılmaz hale getirmektedirler.
[385]BIÇAKCI, "NATO'nun Gelişen Tehdit …", op. cit., s. 122.
[386]TIKK Eneken, **International Cyber Incidents: Legal Considerations**, Tallinn, Cooperative Cyber Defense Centre of Excellence, 2010, https://ccdcoe.org/publications/books/legalconsiderations.pdf, (16.04.2014).

kapatma kararı alması ile birlikte, saldırıların yoğunluğunun makul bir seviyede tutulması başarılmıştır. 19 Mayıs 2007 tarihine gelindiğinde ise saldırılar sona ermiştir [387]

Siber uzayın anonim yapısından kaynaklanan isnat-ispat ilişkisi kurulması noktasındaki zorluk dikkate alınarak, bu saldırıların RF kaynaklı olduğu hiçbir zaman kesin olarak ispatlanamayacak olsa bile, Estonya'ya yönelik siber saldırıların arka planında dönemin Rus hükümetinin olduğu aslında oldukça nettir. Estonya söz konusu siber saldırıları gerçekleştiren bazı IP'lerin RF kaynaklı olduğunu; saldırganların çoğunlukla Rusça dilini kullanarak blog ve forum sayfalarında organize olduklarını, büyük ölçüde bilgisayar korsanlığı tecrübesi olan kişilerden oluştuklarını iddia ederek, saldırı ile ilgili olarak RF'yi doğrudan suçlamıştır.[388]

Estonya saldırısı, iki komşu ülke arasında gerçekleşen bir yerel hadise olmanın ötesinde, siber saldırılar ve siber güvenlik kavramlarının uluslararası ilişkiler disiplini açısından da analiz edilmesine neden olması bakımından oldukça önemlidir. Ayrıca söz konusu siber saldırının bertaraf edilmesi noktasında başta ABD olmak üzere, NATO'nun oynadığı rol, ABD ile NATO ve RF ilişkileri açısından da siber uzayın yeni bir mücadele alanı olarak ele alınmasına yol açmıştır.[389] Bu kapsamda, saldırıların ilk başladığı andan itibaren Estonyalı yetkililer NATO uzmanlarından büyük destek almış, Tallinn'e gelen NATO uzmanları, ülkenin saldırılara karşı geliştirdiği savunma mekanizmalarında önemli rol oynamışlardır. Tüm bu gelişmeler ile birlikte, Estonya aynı zamanda siber güvenlik açısında sembolik bir önem kazanmıştır. Zira 2008 yılında Tallinn'de NATO tarafından bir siber güvenlik mükemmeliyet merkezinin kurulması kararlaştırılmıştır. Daha sonra bu merkez, 2008 Ağustos ayında Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defense Center of Excellence/ CCD-COE)adıyla faaliyet göstermeye başlamıştır. [390]

CCD-COE, 2008 yılı sonrasında yaptığı çalışmalar ile birlikte, NATO'nun siber güvenlik stratejisinin belirlemesinde, NATO üyesi ülkeler arasında siber güvenlik alanında işbirliği ve koordinasyonun sağlanmasında, siber güvenlik konusunda strateji belgeleri,

[387]OTTİS,loc.cit.
[388]YENER, loc.cit.
[389]ROTH Mathias, **Bilateral Disputes between EU Member States and Russia**, CEPS Working Document (Centre for European Policy Studies), August 2009, http://www.ceps.eu/files/book/2009/09/1900.pdf., (18.04.2016), p. 5-13.
[390]BIÇAKCI, "NATO'nun Gelişen …", op. cit., ss. 122-125.

konferanslar ve akademik çalışmalar yapılmasında ve başta ABD olmak üzere pek çok üye ülkenin siber güvenlik stratejilerinin planlanmasında önemli rol oynamıştır.[391]

Estonya'ya yönelik siber saldırıların uluslararası ilişkiler disiplini açısından bizce aşağıda belirtilen önemli etkileri bulunmaktadır:

1. Siber güvenlik, siber güç, siber uzay, siber saldırı gibi kavramların da uluslararası ilişkiler analizlerinde derinlemesine ele alınması için bu olaya adeta bir milat olmuştur.

2. RF, Estonya saldırısı ile birlikte, 2000'li yılların başı itibarıyla ortaya koyduğu siber güvenlik ve savunma stratejileri kapsamında planladığı haliyle, ciddi bir siber güç olarak uluslararası sistemde yerini almıştır. Bu kapsamda, RF'nin sahip olduğu siber kapasitesinde RİS'in yanı sıra RİS ile bağlantılı siber kapasiteye sahip kriminal suç örgütlerinin önemli rol oynadığı görülmüştür.

3. RF, elde ettiği bu siber kapasite ve gücü, komşuları ile yaşadığı dış politika sorunları başta olmak üzere, uluslararası sistemde bir zor kullanma ve baskı aracı olarak kullanmaktan çekinmeyeceğini göstermiştir.

4. RF'nin Estonya'ya yönelik siber saldırısı başta ABD olmak üzere, NATO tarafından siber uzayın ortaya koyduğu yeni imkânların Batılı ülkeler için yeni bir tehdit algılaması olarak okunmasına neden olmuştur. Bu tarih sonrasında, ABD'nin önderliğinde NATO ortak bir siber güvenlik stratejisi geliştirilmesi noktasında ciddi adımlar atmaya başlamıştır. Bununla birlikte, NATO üyesi ülkelerin her biri de kendi ulusal siber güvenlik stratejilerini planlama konusunda yeni girişimlerde bulunmuşlardır.

5. RF için ise Estonya saldırısı karşısındaki NATO'nun reaksiyonu siber uzayın NATO ile yaşanacak olan yeni bir gerginlik alanı olarak kabul edilmesine neden olmuştur. Bu itibarla RF, 2008 sonrasındaki siber güvenlik stratejilerinde, temel olarak ABD'nin ve NATO'nun ortaya koyduğu caydırıcılık potansiyelinin dengesini bozmayı temel hedef olarak belirlemiştir. Bilindiği üzere NATO, kolektif bir savunma konsepti ile kurulduğu günden buyana faaliyet yürütmüştür. Bu stratejide temel amaçlar ise örgütün kolektif bir anlayışla üyelerine güvenliklerini sağlayacağını garanti etmesi, aynı zamanda da hasım blok ya da ülkelere de olası bir saldırıya karşı topyekûn bir karşı saldırı yapılacağına dair sinyal verilmesi şeklinde belirlenmiştir. Gerçekte, RF'de siber saldırılarla NATO'yu

[391]YENER, loc.cit

topyekûn yenemeyeceğini bilmektedir. Ancak RF, NATO üyesi olan ya da NATO ile yakın güvenlik ilişkisinde olan ülkelere yönelik siber saldırılarla, hem kendi çıkarları kapsamında saldırılan ülkeyi etkisi altına almak istemekte hem de NATO'nun söz konusu caydırıcılık stratejisini mağlup etmek istemektedir.[392]

4.2. Gürcistan'a Yönelik Siber Saldırı

RF tarafından 2008 yılında Gürcistan'a yönelik olarak planlandığı iddia edilen siber saldırılar, Rus Silahlı Kuvvetleri'nin konvansiyonel saldırısını destekleyecek şekilde planlanması bakımında, Gürcistan ile RF arasındaki söz konusu sıcak çatışmayı dünyadaki ilk hibrit savaş örneği haline getirmesi bakımından da önemlidir. [393]

Genel ve soyut olarak tarihsel arka plana bakarsak bilindiği üzere, Abhazya ve Güney Osetya, SSCB'nin dağılması sonrasında de facto bağımsız bölgeler olarak varlıklarını sürdürmüşlerdir. 2008 yaz ayları boyunca süregelen bir dizi milliyetçi provakosyon neticesinde, 7 Ağustos 2008 tarihinde Gürcistan Askeri Kuvvetleri'nin ülkenin toprak bütünlüğünü tesis etmek amacıyla Güney Osetya'ya yönelik operasyona başlamasına cevaben, Rus güçleri de 8 Ağustos 2008 tarihinde Osetya'ya girmiş ve sonrasında da Gürcistan'ı işgal operasyonunu faaliyete geçirmiştir. Gürcistan'ın RF ile yaşadığı gerginliğin arka planında, bu ülkenin NATO'ya tam üyelik hedefi ve Batı Blok'u ile yakınlaşmasının bulunduğu pek çok kaynakta ileri sürülmektedir. Gürcistan'a yönelik siber saldırılar ise 7 Ağustos 2008 gecesinden itibaren Estonya saldırısına benzer şekilde ülkenin kritik altyapılarını hedef alan "DDoS" saldırıları şeklinde başlamıştır. Bu saldırılar da kullanılan siteler incelendiğinde, sitelerin ABD'den çalınan kredi kartlarıyla RF ve Türkiye'de açıldığı belirlenmiş, ayrıca saldırı için gönderilen spam e-postaların hazırlandığında tespit edilmiştir.[394]

Gürcistan'a yönelik siber saldırılar da Estonya saldırısına benzer şekilde, ülkenin hükümet, medya ve finans sektörlerini felç etmeyi amaçlamıştır. Ancak Gürcü nüfusunun sadece %10'unun o dönemde internet erişimine sahip olduğu yani Estonya'nın tersine Gürcistan'ın ağlanma oranı ve e-devlet kapasitesi sınırlı olduğu için bu saldırlar Estonya

[392]WIRTZ, op. cit.,p. 31.
[393]GOBLE A. Paul, **Defining Victory and Defeat: The Information War Between Russia and Georgia**, **In the Guns of August 2008:Russia War in Georgia**, edited by Svantee E. Cornell and S. Frederick Starr, Armonk, New York, 2009, p. 191.
[394]BIÇAKCI Salih, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler**, Cilt 9, Sayı 34, Yaz 2012, s. 218

örneğinin aksine kısmen etkili olmuştur.[395] Ayrıca saldırılar esnasında Gürcistan'ın NATO üyeliği henüz gerçekleşmediği için İttifakın güvenlik şemsiyesinden doğrudan yararlanılamamış fakat NATO uzmanlarından saldırılara karşı koyma noktasında doğrudan destek alınmıştır.[396] Bu kapsamda Gürcistan'ın siber kaynaklarını üçüncü ülkelere taşımasıyla, bahse konu siber saldırılar bir hafta içinde sona erdirilmiştir. Lakin siber saldırıların psikolojik savaş boyutunda RF, Gürcistan tezleri karşısında uluslararası kamuoyunda yeterli desteği bulamamıştır.[397]

Gürcistan'a yönelik olarak düzenlenen siber saldırılardan çıkartılabilecek en önemli sonuç, literatürde genel kabul gördüğü üzere bu saldırıların gerçek bir hibrit savaş niteliği taşıyan ilk sıcak çatışma olduğudur. RF, silahlı kuvvetlerinin operasyonları öncesinde Gürcistan'ı siber saldırılar ile yıpratarak adeta işgale hazırlamak istemiştir. İlerleyen yıllar içerisinde de RF, Estonya ve Gürcistan saldırılarından da edindiği deneyimler ile birlikte, 9 Kasım 2012 tarihinde RF Genelkurmay Başkanlığı görevine atanan Valery Gerasimov tarafından hazırlanan yeni bir savaş stratejisini ortaya koymuştur. Hibrit savaş konsepti veya Gerasimov doktrini seklinde isimlendirilen bu strateji ise RF tarafından ilk olarak 2014 yılında başlayan Ukrayna'ya yönelik askeri müdahale esnasında tüm yönleriyle uygulanmıştır.

Ukrayna müdahalesi öncesinde de RF'nin siber saldırı yöntemleriyle komşularını baskı altına alarak dış politika sorunları çözme stratejisi izlediği ileri sürülebilir. Bu bağlamda 2008 yılında Litvanya'ya, 2009 yılında ise Kırgızistan'a yönelik gerçekleştirilen siber saldırılar çalışmanın bundan sonraki aşamasında analiz edilebilecektir.

4.3. Litvanya'ya Yönelik Siber Saldırı

Litvanya, 2008 Haziran ayında üç gün süreyle RF kaynaklı olduğu iddia edilen siber saldırılara maruz kalmıştır. Söz konusu siber saldırılar, Estonya ve Gürcistan örneklerindeki gibi Litvanya'nın kritik altyapılarının "DDoS" saldırıları ile çökertilmesi ve Litvanya'da faaliyet gösteren popüler web sayfalarının ağırlıklı olarak "orak-çekiç" amblemleriyle hacklenmesi şeklinde gerçekleşmiştir.[398]

---

[395]TİKK, loc.cit.
[396]BIÇAKCI,"21. Yüzyılda Siber …", op. cit.,s.38.
[397]GOBLE, op. cit., p. 191.
[398]WILLIAM C. Ashmore, **Impact of Alleged Russian Cyber Attacks**, "School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas",http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf, (19.04.2016), p. 11

Bu siber ataklar kapsamında çoğunluğu kamu kurumlarına ait 300'den fazla internet sitesi hacklenerek kullanılmaz hale getirilmiş, bu sitelere "orak-çekiç" amblemlerinin yanı sıra Litvanya halkını aşağılayan kimi şarkılar yüklenmiştir. Saldırılar kapsamında özellikle Litvanya güvenlik ve finans kurumları ile RF karşıtlığı söylemlerinin öncülüğünü yapan Litvanya Sosyal Demokrat Parti'nin internet siteleri hedef alınmıştır.[399]

Söz konusu dönemde, Litvanya adına konuya ilişkin resmi bir açıklama yapan Litvanya Vergi Müfettişliği Başkanı Gediminas Vysniauskis: "*saldırıların önceden planlandığının net olduğu, DDoS ataklarının Romanya merkezli ağlar tarafından ülkelerine yönlendirildiğini tespit ettiklerini ve saldırıların 2007 Estonya saldırı ile benzerlik gösterdiğini*" beyan etmiştir.[400]

Bu saldırıların arka planında, RF ile Litvanya arasında yaşanan politik gerginliğin bulunduğu iddia edilebilir. Zira saldırılar, RF'nin SSCB döneminde çalışma kamplarında ölen Litvanyalı kurbanların yakınlarına tazminat ödemeyi reddetmesi, akabinde de RF'nin Litvanya'ya enerji akışını kısıtlaması, buna cevap olarak da Litvanya hükümetinin eski Sovyet sembollerini yasaklayan bir kanunu meclise sunması ve RF-AB ortaklık sürecini bloke etmesi sonrasında başlamıştır.[401]

Söz konusu siber saldırıları planlayan kaynakların, RİS ve RİS ile irtibatlı kriminal potansiyele sahip Rus suç örgütleri olduğu iddia edilmiştir. Litvanya saldırısının da özellikle Estonya saldırısında olduğu gibi Baltık hükümetlerinin Batı Blok'unun da desteğiyle RF'nin ülkelerine yönelik müdahale girişimlerine direnmesinin bir sonucu olarak meydana geldiği ileri sürülebilir. Çünkü bu saldırı da RF, 2000'li yılların ikinci yarısı itibarıyla RF, komşularıyla yaşadığı sorunların çözümü noktasında siber kapasitesi kaynaklı gücünü kullanmaktan çekinmediğini bir kez daha uluslararası kamuoyuna göstermiştir.[402]

---

[399]Internet Law Center's Cyber Report, **A Timeline of Russian Cyber Attacks**, https://ilccyberreport.wordpress.com/2016/11/02/a-timeline-of-russian-cyber-attacks/, (03.04.2017).
[400]Baltic Times, **Lithuania cyber attacks: Round two**,http://www.baltictimes.com/news/articles/20897/, (04.04.20017).
[401]MCLAUGHLIN Daniel, **Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites**, ttp://lumen.cgsccarl.com/login?url=http://proquest.umi.com/pqdweb?did=1503762091&sid=2&Fmt=3&cl ientld=5094&RQT=309&VName=PQD;, (19.04.2016).
[402]WILLIAM, loc.cit.

4.4. Kırgızistan'a Yönelik Siber Saldırı

2000'li yılların ikinci yarısında yaşanan siyasi gerilim neticesinde RF kaynaklı siber saldırı ile karşı karşıya kaldığı iddia edilen bir başka devlet ise Kırgızistan'dır. Kırgızistan'ın iki temel internet servis sağlayıcısı 18 Ocak 2009 tarihinde "DDoS" saldırıları ile karşı karşıya kalmış ve ülkenin tüm web siteleri ve e-posta haberleşmesi kesilmiştir.[403]

RF'nin bu siber saldırıyı gerçekleştirmesinin arkasında yatan nedenin ise RF hükümetinin Kırgızistan'ı Manas'ta bulunan ABD askeri üssünü kapatması noktasında baskı altına almak istemesidir.[404] Bilindiği üzere Manas Askeri Üssü ABD'nin için Orta Asya'daki etkinliği için önemli bir merkez olmasının yanı sıra ABD'nin Afganistan operasyonlarının idamesi için de hayati öneme sahip bir askeri tesistir.

Bu siber saldırıların RF tarafından kontrol edilen internet ağları üzerinden, özellikle de Rus siber kriminal grubu RBN ile irtibatlı hackerlar vasıtasıyla organize edildiği iddia edilmiştir. Öte yandan Kırgızistan'ın zayıf internet altyapısına rağmen bu ölçekte bir "DDoS" saldırısı düzenlemenin çok etkili bir baskı yöntemi olmadığı da düşünülebilir. Bununla birlikte özellikle RF muhalifi genç nüfusun sosyal medya başta olmak üzere, internet kullanımı alışkanlıklarının yüksek olduğu düşünüldüğünde, Kırgızistan'ın tüm web siteleri ve e-posta haberleşmesinin kesilmesi muhalefetin etkisizleştirilmesi noktasında akılcı bir seçenek olarak karşımıza çıkmaktadır. Bu noktada RF ile işbirliği içinde olan kimi Kırgız siyasi çevrelerinden ülke içinden verdiği teknik destek ile söz konusu siber saldırıların etkisinin artmasına katkı yaptığı da ileri sürülmüştür.[405]

Öte yandan bahse konu "DDoS" ataklarının RF'nin Kırgızistan'a yönelik söz konusu dönemde sürdürdüğü baskı politikasının etkili bir parçası olarak başarılı olduğu da ileri sürülebilir. Zira saldırılar sonrasındaki süreçte Kırgızistan Manas Askeri Üssü'nü kapatmış ve RF'den 2 Milyar Dolar kredi temin etmiştir.[406]

---

[403]RHOADS Christopher, **Kyrgyzstan Knocked Offline**, Wall Street Journal, 10, http://www.wsj.com/articles/SB123310906904622741, (19.04.2016).
[404]Ibid.
[405]The Guardian, **The Fog of Cyber War**, https://www.theguardian.com/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access, (04.04.2016).
[406]NBC News, **Timeline:Ten Years of Russian Cyber Attacks on Other Nations**, http://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111?cid=public-rss_20161218, (03.04.2017).

Görüldüğü üzere RF kendi politik girişimlerine muhalefet eden komşu devletlerin hükümetlerini, bu ülkelerin kritik altyapılarını felç etmeyi amaçlayan siber saldırılar planlamak suretiyle baskı altına almaktan çekinmemektedir. Diğer yandan Litvanya ve Kırgızistan'a yönelik siber saldırıların aşağıda belirtilen üç ortak özelliği sahiptir:[407]

1. Tüm saldırılar, "DDoS" atakları şeklinde planlanmıştır ve RİS veya RİS ile bağlantılı Rus suç örgütleri kaynaklıdır.

2. Saldırılar hedef ülkelerin kritik altyapılarını çökertmeyi amaçlamıştır ve siber uzayın anonim yapısının avantajlarından da istifade edilmek suretiyle RF'yi doğrudan suçlayacak herhangi kanıtı geride bırakmayacak şekilde planlanmıştır.

3. Saldırılar, RF hükümetinin dış politika önceliklerini benimsemeyen, bunlara muhalefet eden ve RF' ye karşı ABD başta Batılı ülkelerin desteği ile dengeleme politikası gütmeyi amaçlayan hükümetlerle yaşanan gerginliklerin hemen sonrasında, söz konusu hükümetleri baskı altına almak ve kendi kamuoyu nezdinde zorlamak amacıyla gerçekleşmiştir.

4.5. Ukrayna'ya Yönelik Siber Saldırı

Ukrayna Devlet Başkanı Viktor Yanukovich'in 2014 Şubat ayında görevden uzaklaştırılması, RF ile Ukrayna arasındaki hibrit savaş özelliği de içeren sıcak çatışma sürecinin başlangıcı olarak kabul edilebilir.[408]

Daha öncede belirttiğimiz üzere Rus hibrit savaş konsepti, Valery Gerasimov tarafından detayları şekillendirilen, ancak ilk örneği RF'nin Gürcistan'a yönelik askeri operasyonu esnasında müşahede edilen gayri-resmi savaş doktrinidir. Bu stratejide temel olarak, siber saldırı teknikleri kullanılarak, hasım devletin askeri gücünün sıcak çatışma öncesinde minimize edilmesi, aynı zamanda yoğun bir şekilde küresel ve yerel ölçekte enformasyon savaşı teknikleri ile RF lehine bir propaganda sürecinin işletilmesi, tüm bunlar ile birlikte hasım ülkedeki dost ve akraba topluluklar ile koordineli bir şekilde planlanan özel kuvvet operasyonlarıyla konvansiyonel bir çatışma süreci sonunda amaca ulaşılması hedeflenmektedir.[409]

RF'nin Ukrayna müdahalesi ilk etapta 23 Şubat–1 Mart 2014 tarihleri arasında

[407]WILLIAM, loc.cit.
[408]MEDVEDEV, op. cit., p. 25.
[409]Ibid., p. 27.

"Rus Kuzey Komutanlığı", Kola Yarımadası ile Ukrayna sınırı arasında 150.000 askerin katıldığı bir "şaşırtma" tatbikatı ile başlayan bir süreçtir. Bu tatbikat, düşük tempolu bir güç gösterisi şeklinde icra edilmiştir. Bu aşamada ayrıca RF Parlamentosu1 Mart 2014 tarihinde Kırım'a yönelik askerî güç kullanımına izin veren bir yasayı da onaylamıştır. [410]

Daha sonra, Ukrayna İç Güvenlik Birimi SBU'nun Başkanı Valenty Nalyvaichenko tarafından 2014 Şubat ayı sonundan itibaren, Ukrayna mobil telefon iletişim ve internet altyapılarının saldırıya uğradığı ve büyük oranda çöktüğü, özellikle Ukraynalı bürokratlarla milletvekillerine ait akıllı cep telefonlarının tamamının "hacklendiği ifade edilmiştir. Ayrıca Rus yanlısı bir hacker grubu olan "CyberBerkut" tarafından, Ukrayna Silahlı Kuvvetleri'ne, Ukrayna resmi sitelerine, Ukrayna ile ilgili faaliyet gösteren NATO'nun internet erişimlerine, Ukrayna medya kuruluşlarına yönelik olarak "DDoS" saldırıları da düzenlenmiştir.[411]Bu siber saldırıların, Estonya ve Gürcistan'a yönelik siber saldırılara nazaran çok daha etkili ve sofistike yöntemlerle planladığı da görülmüştür. Saldırılarda kullanılan "Snake/Uroboros" yazılımı, özellikle Ukrayna'nın resmi kurumlarına yönelik siber ataklarda son derece etkili olmuştur.[412]

Ukrayna'ya yönelik siber saldırıların etkili bir şekilde gelişmesinin bir diğer nedeni ise Ukrayna'nın internet altyapısının özellikleriyle ilgilidir. Genel hatlarıyla belirtirsek; bazı Ukrayna hükümetlerin kısıtlayıcı çabalarına rağmen, Ukrayna'nın liberal internet kullanımı politikası bulunmaktadır. Ayrıca Ukrayna'nın küresel internet sistemi ile bağlantısı hem karasal bir yapıyla, hem de uydu üzerinden sağlanmaktadır. Bu nedenle de hem internet kullanım politikaları göreli olarak serbestlik ilkesi ile şekillenen hem de küresel internet sistemi ile çeşitli vasıtalarla erişim halinde olan Ukrayna'nın, RF kaynaklı siber saldırlar esnasında ülkesinin internet erişimini dış dünyaya kapatmaya yönelik girişimleri yetersiz kalmıştır. Bu kapsamda da söz konusu siber saldırılar etkili bir şekilde gelişmiş ve yaygınlaşmıştır.[413]

---

[410]GÜRCAN Metin, **Rusya'nın Ukrayna'daki Bulanık Savaş Konsepti**,http://www.analistdergisi.com/sayi/2014/05/rusya-nin-ukrayna-daki-bulanik-savas-stratejisi, (22.04.2016).

[411]LEE David, **Russia and Ukraine in Cyber 'Stand-Off**, BBC News, http://www.bbc.com/news/technology-26447200, (23.04.2014).

[412]WEEDON Jen ve GALANTE Laura, **Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast**,FireEye Executive Perspectives, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html, (24.04.2016).

[413]KELLY Sanja, **Freedom on the Net 2014, Freedom on the Net (Freedom House, 2014)**, https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf., (24.04.2016).

Bu siber saldırılar ile eş zamanlı olarak, RİS'in provokasyonları ile kışkırtılan Rus yanlısı sivil protestocular Sivastopol'da şiddet içermeyen sokak eylemleriyle RF' ye bağlanma taleplerini beyan eden mitingler düzenlemeye başlamışlardır. Öte yandan, Kırım'daki Rus yanlısı Russkoye Yedinstvo Partisi, Kırım Ruslarının güvenliğini sağlamak maksadı iddiasıyla bir hafta gibi çok kısa sürede 10 bin kişilik silahlı bir güç oluşturduğunu ilan etmiştir. Bu grupların bu kadar kısa sürede silahlanarak organize edilmeleri dikkate alındığında, söz konusu grupların Rus özel kuvvetleri ve RİS ile doğrudan irtibatlı oldukları da rahatlıkla ifade edilebilecektir.

Belirtildiği üzere söz konusu siber saldırılar ile direnme gücü törpülenen Ukrayna'ya yönelik sıcak çatışma süreci başlamadan önce, Kırım'ın Ukrayna ve küresel sistemden izole edilmesine yönelik planlama devreye sokulmuştur. Bu kapsamda, 16–28 Mart 2014 tarihleri arasında yoğunlaşacak şekilde, Ukrayna'nın resmî mobil telefon şirketi olan Ukrtelecom'un altyapısını çökertilmiş, bu sayede de Kırım'daki mobil telefonların sıcak çatışmanın ilk günlerinde kullanılması engellenmiş, internet kısmi bir yavaşlama sağlanmış, kritik altyapıları felç eden siber saldırılar organize edilmiş, Sivastopol limanındaki Rus savaş gemilerinden Kırım'daki televizyon ve radyo yayınlarını kesecek elektronik karıştırmalar yapılmış ve "*kimliği belirsiz kişilerce*" Kırım'daki tüm fiber optik kablo altyapısı zarara uğratılmıştır.[414]

2014 Nisan ayı sonuna kadar Lugansk ve Donetsk Bölgeleri'nin büyük bölümü RİS ve Rus özel kuvvetleri üyelerince eğitilen, yönlendirilen ve silahlandırılan RF yanlısı isyancılar tarafından ele geçirilmiştir. Karakollar ve hükümet merkezlerine isyancıların ve RF'nin bayrakları çekilmiş ve Ukrayna bayrakları indirilmiştir. Donetsk ve Lugansk gibi iki büyük şehir ve oblast başkentleri de isyancıların eline geçmiştir. 2014 Mayıs sonu ve Haziran başlarından itibaren ise Ukrayna Ordusu genel taarruza geçmiş ve sert çarpışmalar başlamıştır. Ordu, havadan ve karadan isyancıların yerleşim birimlerini de yoğun bombardımana tutmuş ve birçok sivil de hayatını kaybetmiştir. Temmuz başından itibaren Ukrayna Ordusu isyancıların elindeki en önemli noktalar olarak değerlendirilen Kramatorsk ve Sloviansk'ı ele geçirmeyi başarmıştır. Donetsk şehri çevreleme harekâtı için uygun konuma gelmiştir. Ağustos başı itibari ile Lugansk ile Donetsk'i birbirine bağlayan ana yol üzerinde çatışmalar şiddetlenmiştir. Ukrayna Ordusu böylece iki büyük

[414]GÜRCAN, loc.cit.

şehir olan Donetsk ile Lugansk'ı birbirinden ayırmaya ve isyancıları ikiye ayırmaya çalışmaktadır. Daha sonra RF'nin desteğini arttırmasıyla Rus yanlısı milisler yeniden önemli kazanımlar elde etmişlerdir. Savaş, 2014 yazın sonuna doğru adeta kilitlenmiştir. 5 Eylül 2014 tarihinde Belarus'un başkenti Minsk'te ateşkes antlaşması imzalanmıştır. Ne var ki ateşkes kısa süreli olmuştur. 2015 Şubat ayının ortasına doğru Rus yanlısı ayrılıkçılar saldırılarını Debaltseve çevresinde yoğunlaştırmışlardır.12 Şubat 2014 tarihinde Minsk II protokolü ile taraflar ateşkes konusunda tekrar anlaşmıştır. Ateşkese önemli ölçüde uyulmakla birlikte, halen Luhansk'ın bazı köyleri, Donetsk Havalimanı yakınları ve Shyrokyne civarında aralıkla devam etmektedir.[415]

Bununla birlikte 23 Aralık 2015 tarihinde Ukrayna'nın Prykarpattyaoblenergo Bölgesi'nde bulunan bir enerji santraline yönelik olarak siber saldırı düzenlenmiş ve bu nedenle ilgili bölgede bir süre elektrik kesintisi yaşanmıştır. SBU tarafından konuyla ilgili olarak yapılan açıklamada:*"kesintilerin siber bir saldırı nedeniyle gerçekleştiğinin düşünüldüğü, saldırının arkasında RF'nin olabileceği ve konunun araştırıldığı"* kamuoyuna duyurulmuştur.[416]RF tarafı ise konuyla ilgili olarak bir açıklama yapmamıştır.

Ukrayna'ya RF kaynaklı olduğu iddia edilen siber saldırılar, RF'nin Gerasimov Doktrin'i kapsamında ortaya koyduğu yeni nesil sıcak çatışma konseptinin sahadaki başarılı bir tatbiki olarak değerlendirmelidir. Ukrayna müdahalesi esnasında RF, 2000'li yılların başı itibarıyla ortaya koymaya başladığı siber güvenlik strateji belgelerindeki hedefleri ile uyumlu bir şekilde etkili bir siber saldırı kapasitesine ulaştığını net bir şekilde ortaya koymuştur. Bu saldırı ile birlikte RF'nin sahip olduğu siber imkân ve vasıtaların başta ABD olmak üzere, küresel ölçekte diğer devlet içinde ciddiye alınması gereken bir tehdit odağı haline geldiği açıktır. Bu saldırı sonrasında RF'nin siber kapasitesinin, diğer devletlerin de siber uzay alanında kendi ulusal savunma ve saldırı kapasitelerini geliştirmeye yönelik yeni adımlar atmasına ve daha sofistike planlamalar geliştirmesine neden olduğu da ileri sürülebilir.

4.6. Türkiye'ye Yönelik Siber Saldırı

24 Kasım 2015 tarihi sabah saatlerinde Türk F-16'larının, hava sahasını ihlal eden bir

[415]Erciyes Üniversitesi Stratejik Araştırmalar Merkezi (ERUSAM), **Ukrayna Krizi Kronolojisi: "Bağımsızlıktan Bölünmeye…**, http://www.erusam.com/makale.php?id=111, (24.04.2014).
[416]Türk İnternet Haber Sitesi, **Ukraynalılar Rusların Güç Santrallerine Saldırdığını İddia ediyor.**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=51862, (27.04.2016).

Rus Su-24 uçağını düşürdüğü haberi tüm dünyada şok etkisi yaratmıştır. Bu olay kısa sürede derinleşerek, Türkiye ve RF arasında ciddi boyutlara ulaşan siyasi gerginliğinde başlangıcını oluşturmuştur.

Bu siyasi gerginlik, 14 Aralık 2015 tarihinde saat 12.00 itibarıyla Türkiye'ye yönelik olarak "DDoS" saldırıları ile yeni bir aşamaya taşınarak, iki ülke ilişkilerindeki gerginliğin derinleşmesine neden olmuştur. Söz konusu siber saldırı ile *".tr"* uzantılı adların tutulduğu sistemin kullandığı bant genişliği hedeflenerek, Türkiye'nin bankacılık ve finans, kamu kurumları, e-devlet sistemini teşkil eden kritik altyapılarının yıpratılması hedeflenmiştir. Bilindiği üzere*".tr"* uzantılı adların tutulduğu sistem, *".tr"* uzantılı alan adlarının yerini yönlendirmekte ve dolayısıyla sitelerin bulunmasını sağlamaktadır. Eğer bu sistem ulaşılamaz olursa, adların nerede olduğu bulunamadığından, sitelere erişim mümkün olamamaktadır. Ayrıca saldırıların, "*DDoS"atakları* şeklinde planlanmış olduğu da ifade edilebilecektir.[417]

Saldırılar devam ettiği esnada ise Anonymous hacker grubu tarafından 23 Aralık 2016 tarihinde bir video yayınlanarak saldırılar üstlenilmiştir. Yayınlanan videoda: "*saldırıların Anonymous tarafından gerekleştirildiği, saldırının Türkiye'nin Şam İslam Devleti (IŞİD)'e verdiği desteğe bir misilleme olduğu, Türkiye'nin IŞİD'nden petrol aldığı, örgütü finansal olarak desteklediği, IŞİD militanlarının Türkiye'de tedavi gördüğü ve saldırıların devam edeceği*" belirtilmiştir.[418] Bu açıklamanın RİS tarafından planlanan "*sahte bayrak (false flag)*" operasyonunun bir parçası olması ise kuvvetle muhtemeldir.[419]

Bu itibarla "DDoS" saldırılarının gerçek planlayıcısının kimliği ile ilgili olarak hiçbir zaman net bir delillendirme yapılamayacak olmasına rağmen, Türkiye'ye yönelik saldırının en az 400.000 sitenin etkileyecek kapasitede olması, bu sitelerin ise e-devlet, üniversite, askeri ya da yerel şirket siteleri şeklinde hedeflenmesi, RF ile Türkiye arasında uçak düşürülmesi olayına bağlı olarak süregelen gerginlik, saldırılar ile Türkiye'deki tüm sistemin değil de yalnızca*".tr"* uzantılı adların hedeflenmesi, saldırıların sadece mesai

[417]Türk İnternet Sitesi, **6. Gününde Nic.tr Saldırısı Sürüyor Ama Açıklama Yok - Onun Yerine Yorumlar Var..**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=51749, (24.04.2016).
[418]IB Times Internet News, **Anonymous: Turkey reeling under cyberattack as government and banks websites paralysed**, http://www.ibtimes.co.uk/anonymous-turkey-reeling-under-cyber-attack-government-banks-sites-paralysed-1534984, (24.04.2016).
[419]Sahte Bayrak (False Flag) Operasyonu: gizli örgütlerin ya da istihbarat servislerinin halkı kışkırtmak, yönlendirmek veya başka bir subversif (yıkıcı/bölücü) amaçlı olarak, kendi yaptıkları bazı faaliyet ve operasyonları hedefteki kişiler yürütüyor gibi göstererek kamuyu aldatmak için tasarladıkları gizli planlamalara verilen isimdir.

saatleri içinde gerçekleşmesi, RF'nin bu ve benzeri saldırılar kapsamındaki kabarık sicili, saldırının RF bağlantılı bir şekilde planlama ihtimalini kuvvetlendirmiştir.[420]

Daha teknik bir yaklaşımla saldırıların basit bir formatta hazırlanmış olmasının, olayın arka planı gizlemek ve saldırıyı bireysel bir hacker grubu saldırısı şeklinde göstermek istenmesi amacından kaynaklandığı da belirtilebilecektir. Bu kapsamda, saldırının günlerce sürmesi için bir motor sistemine ihtiyaç duyması, bu kapasitede sunucuların uzun süreli olarak amatörler tarafından çalıştırılmasının teknik olarak mümkün olmaması, DNS sorgulamasında açık sunucu listelerine sürekli *"aldatıcı (spoof)"* istek göndermek suretiyle *".tr"* DNS sunucularına yansıtma saldırısı yapılabilmesi için belirli bir güce gerek duyması, yapılan bu saldırılarda 30 gbps saldırı trafiği üretebilmek için sürekli olarak 5-10 GBps aralığında bir trafiğin varlığını gerektirmesi, saldırının 276.000 farklı adresten ve zaman zaman 30-40 gb boyuta erişen niteliği, bu teknik kapasitenin ise ancak bir devlet organizasyonu desteği ile sağlanabilecek düzeyde planlanabilecek olması hususları dikkate alındığında, saldırının RF desteği ile gerçekleştiği değerlendirilebilecektir.[421]

Türkiye cevap olarak, saldırıların ilk gününde yurtdışı internet trafiğini kesmiş ve yurtdışından *".tr"* uzantılı sitelere ulaşım da engellenmiştir. Ayrıca saldırılar esnasında Türkiye hizmet sağlayan operatörleri gezdirerek, saldırıya uğrayan operatörleri adeta saldırılardan kaçırarak kamu hizmetinin devamını sağlamaya çalışmıştır. Bu aşamada Siber Olaylarla Mücadele Ekipleri (SOME) rol oynamıştır.[422] Bir diğer tedbir ise saldırıya uğrayan DNS Server'larının geçici olarak Hollanda'ya kopyalanması şeklinde alınmıştır. Böylelikle de saldırıların boyutu hafifletilmeye çalışılmıştır.

Saldırılar ile ilgili olarak dönemin Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım, 24 Aralık 2015 tarihinde yaptığı açıklamada: *"söz konusu saldırılara Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile Telekomünikasyon İletişim Başkanlığı (TİB)'nın anında müdahale ettiğini, 17 Aralık'a kadar bu olayın sürdüğünü, iki saat yavaşlama ve*

[420]The Telegraph Online News**, Could Cyberattack on Turkey be a Russian Retaliation?**,http://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation.html, (24.04.2016).
[421]TürkİnternetHaber Sitesi, **6. Gününde Nic.tr Saldırısı Sürüyor Ama Açıklama Yok - Onun Yerine Yorumlar Var..**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=51749, (24.04.2016).
[422]Haberler İnternet Haber Portalı, **Türkiye'ye Siber Saldırının Arkasında Ruslar Var**,http://www.haberler.com/turkiye-ye-siber-saldirinin-arkasinda-ruslar-var-8006069-haberi/, (25.04.2016).

kesilme olduğunu, Orta Doğu Teknik Üniversitesi (ODTÜ)'nin DNS grubuna da DDoS saldırısı olduğunu, bu durumun 'on binlerce insanın aynı anda kapıya yığılması, içeri girilememesi' gibi değerlendirilebileceğini, saldırıların hangi ülkeden yapıldığını kestirmenin ilk anda kolay olmadığını, bu tür bir tespitin çok detaylı ve zahmetli olduğunu, saldırıların yurt dışı kaynaklı planlandığını, Ulusal Siber Olaylara Müdahale Merkezi (USOM)'nin mücadelede önemli rol oynadığını, siber güvenlikle ilgili zaten yasal altyapı ve ekiplerin bulunduğunu, DNS altyapısının ODTÜ tarafından işletildiğini, yeni yasal düzenlemelere göre bu altyapının BTK'ya devredilmesi gerektiğini, fakat ODTÜ'nün bu devire karşı çıktığını, bu çekişmenin şu an için yargıda olduğunu, hâlbuki siber saldırılar ile tek bir merkezden karşı konulması gerektiğini" belirtmiştir.[423]

Saldırılar, Türkiye'nin siber güvenlik stratejisinde kısmen mesafe aldığını göstermekle birlikte, siber savunma direncinin hala son derece yetersiz, dağınık ve plansız olduğunu da ortaya koymuştur. Örneğin saldırıların üzerinden, neredeyse söz konusu dönemde bir hafta geçinceye kadar hiçbir resmi makam saldırıların mahiyeti ile ilgili olarak bir açıklama yapmamıştır. Bu da siber saldırılar esnasında ciddi dezenformasyonun oluşmasına neden olmuştur. Saldırılara, ODTÜ, BTK, TİB ve SOME'lerin karşı koyduğu ve kendi görev alanları ile ilgili, tedbirler geliştirdiği görülmüştür. ODTÜ'nün saldırılar esnasında yapılan eleştirilerin aksine başarılı bir performans ortaya koyduğu söylenebilir. Ancak ülkenin siber güvenliği söz konusu olduğunda, ODTÜ DNS grubunun yetkilerinin ilgili devlet kurumlarına devredilmesi gerektiği de açıktır. Bu konuda, BTK ve ODTÜ arasında acil bir şekilde uzlaşma sağlanmalı ve ülkenin siber güvenliği ilgili devlet kurumlarına devredilmelidir.

Ayrıca bahse konu siber saldırılar, Türkiye gündeminde yeterli şekilde tartışılmamıştır. Bu durum Türk kamuoyunun siber güvenlik kavramına olan yabancılığı ile ilgilidir. Türk internet kullanıcısı için, internet temelde sosyal medyanın kullanılması ve e-posta haberleşmesinin gerçekleştirilmesi anlamına gelmektedir.[424]

Saldırılar kapsamında ortaya çıkan zararın tespiti ile ilgili olarak net bir değerlendirme yapılması şu an için oldukça zor gözükmektedir. Örneğin, Batılı ülkelerde

[423]HaberTürk İnternet Haber Portalı, **Binali Yıldırım'dan ODTÜ açıklaması**, http://www.haberturk.com/ekonomi/teknoloji/haber/1171682-binali-yildirimdan-odtu-aciklamasi, (25.04.2016).
[424]BBC News, **Türkiye'ye Siber Saldırının 10 Günü: Ne oldu?**, http://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan, (25.04.2016).

bu tür her saldırı ya da virüs salgınları sonunda, ortaya çıkan zararın maliyeti ile ilgili olarak görevli kurumlar tarafından kamuoyuna açıklama yapılması olağandır. Ancak ülkemizde bu tür bir çalışma yapacak bir kurum henüz bulunmamaktadır. Saldırılar sonrasında, dünya geneli için *".tr"* isimlerin itibarsızlaşması söz konusu olabilecektir. Bu durumda *".tr"* uzantılı alan adlarına ilginin azalabileceği süreç içinde beklenebilir. Yani yüksek ziyaretçisi olan ve arama motoru trafiği yüksek olan sitelerin *"com.tr"* gibi adresleri kullanması bir risk olarak görülmeye başlanabilir. Bu itibarla, saldırıların sürdüğü 2015 Aralık ayı için, yüksek ziyaretçi trafiği bulunan *"com.tr"* uzantılı sitelerde %10 ziyaretçi kaybı rapor edilmiş olması bu hususta dikkat çekici olarak görülmelidir. [425]

Diğer yandan RF kaynaklı olduğu iddia edilen bu siber saldırılar esnasında, devlet kurumlarına yönelik bir siber espiyonaj faaliyeti de yürütülüp yürütülmediği konusu belirsizliğini korumaktadır. Bu çerçevede süreç için söz konusu siber saldırı esnasında Türk resmi kurum ve kuruluşlarından devletin stratejik öneme sahip bilgilerinin sızdırılıp sızdırılmadığı da görülecektir.

Bahse konu siber saldırılara karşı alınan tedbirler ile birlikte, bu saldırıların etkisizleşmesi noktasındaki bir diğer husus ise Türkiye'nin internet altyapısının zayıflığı ile ilgilidir. Normalde bu tür büyüklükteki bir saldırının misli bir cevap üretmesi beklenirken, bu durum Türkiye'de farklı gelişmiş ve saldırının etkisi daha düşük olmuştur. Bugün Türkiye'nin fiber altyapısı 250.000 km.dir. Hâlbuki bu rakamın Portekiz ile kıyaslanacak olursa 4 milyon km. Afrika'nın bir ülkesi olan Gana ile kıyaslasak olursak ise3 milyon km. olması gerekmektedir. Bunun yanı sıra Türkiye'de internet kullanımı oldukça pahalıdır. Bu nedenle de sunucu başı trafikler düşük düzeyde kalmaktadır. Avrupa'da sunucu başı 1 Gbps olan trafikler, Türkiye'de 10 Mbps gibi düşünülebilir.

Uluslararası ilişkiler disiplini açısından ise Türkiye'ye yönelik siber saldırılar, RF'nin bugüne kadar Estonya, Gürcistan, Ukrayna, Kırgızistan ve Litvanya'ya yönelik gerçekleştirmiş olduğu iddia edilen saldırlar ile benzer özellikler içermektedir. Tüm bu saldırılarda olduğu gibi söz konusu siber saldırı da *"DDoS"* atakları şeklinde ve Türkiye'nin kritik altyapısını olumsuz olarak etkilemeye etmeye yönelik olarak planlanmıştır. Saldırının başlangıcı ise 24 Kasım 2015 tarihli uçak düşürme olayının hemen sonrasına denk gelmiştir. Bu itibarla saldırı ile RF'nin siber kapasitesini kullanarak,

[425]TürkİnternetHaber Sitesi, **6. Gününde Nic.tr Saldırısı Sürüyor Ama Açıklama Yok - Onun Yerine Yorumlar Var..**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=51749, (24.04.2016).

Türkiye'yi diplomatik baskılar ve ekonomik tedbirlerle birlikte köşeye sıkıştırmak istediği açıktır. Saldırılar ile eş zamanlı bir biçimde, RF'nin Türkiye'ye yönelik olarak sosyal medya olanaklarından da istifade etmek suretiyle ağır bir psikolojik savaş süreci de başlattığı ortadadır. Bu süreçte RF'nin enformasyon savaşı enstrümanlarını kullanma noktasında ulaştığı yeni aşamayı göstermesi bakımından da ayrıca analiz edilmelidir.

Bu aşamada RF'nin siber kapasitesinin etkisi ve gücü, Türkiye'nin de siber savunma stratejisindeki söz konusu çok başlı ve hazırlıksız yapısı dikkate alındığında, RF'nin Türkiye'ye yönelik siber saldırısını bir aşamaya kadar sürdürdüğü, böylelikle de Türkiye'nin siber kapasitesini test ettiği ayrıca Türkiye ile mevcut ilişkilerdeki gerginliği daha fazla derinleştirmek istemediği, Türkiye'ye sadece siber imkân ve gücünü göstermek istediği de değerlendirilebilecektir.[426]

İstihbarat ve gizli faaliyet tekniği açısından olay değerlendirildiğinde ise ilk bulgular kapsamında saldırı da RİS'in herhangi bir eleman (HUMINT) şebekesinden faydalanmadığı ifade edilebilir. Saldırı, belirtildiği üzere *"DDoS"* atakları şeklinde organize edilmiştir. Bu ataklara Türkiye temelde internet trafiğini keserek karşılık vermiş ve saldırının etkisinin yukarıda belirtilen diğer nedenler ile birlikte kısmen etkisizleştirmiştir.

RİS'in, KGB altyapısı, kurumsal servis kültürü ve personelinin Türkiye'nin her türlü sosyal yapısına yatkınlığı, bu konuda aldıkları eğitimleri, Türkçeye hâkimiyetleri ile toplumun her kesimi ile temasa geçebilecek karakter ve entelektüel kapasiteleri dikkate alındığında, Türkiye'de siber saldırılar için kullanılabilecek bir eleman şebekesini istihdam edebilecek (employing) ve bu şebekeyi gizli bir faaliyetin tüm gerekliliklerini uygun şekilde sevk ve idare (running) edebilecek imkân ve kabiliyetinin mevcut olduğu öngörülebilecektir. Bu öngörü kapsamında, 2010 yılında, İran'ın nükleer tesislerinin, Stuxnet[427] isimli gelişmiş bir virüs tarafından fiziksel hasara uğratılması olayı hatırlanmalıdır. Bu olayın, sonradan yapılan analiz ve değerlendirmeler dâhilinde, İsrail ve ABD gizli servisleri tarafından planlanmış olan ve hibrit bir özelliğe sahip yıkıcı bir

[426]YİNANÇ Barçın, **Doç. Dr. Salih Bıçakcı ile Röportaj/Rusya İsterse Türkiye'yi Taş Devrine Döndürebilir**, http://www.radikal.com.tr/turkiye/rusya-isterse-turkiyeyi-tas-devrine-dondurebilir-1495797/, (24.04.2016).

[427]Stuxnet, 2010 Haziran ayında fark edilen ve İran'ın Natanz nükleer geliştirme tesisine saldırmak için geliştirilmiş olan bir siber silahın/yazılımının adıdır. Bu saldırı, resmi olarak hiçbir devlet tarafından üstlenmemiş olsada saldırı çok büyük ihtimalle bir ABD-İsrail ortak yapımıdır. Zira her iki ülkeden de bu konuda herhangi bir yalanlama gelmemiştir

operasyon olduğu ortaya konmuştur. Stuxnet virüsünün geliştirilmesi, mahiyeti gereği gizli bir faaliyettir. Bu virüs gizli haberleşme teknikleri kullanılarak, detaylı keşfi (casing) yapılmak suretiyle, daha önceden ilgili servislerce mimlenmiş (spotting), yaklaşılmış (approaching), angaje (recruiting) ve sevk/idare (running) edilmiş bir veya daha fazla elaman (HUMINT kaynağı) vasıtasıyla, söz konusu nükleer tesislere muhtemelen bir taşınabilir bellek vasıtasıyla bulaştırılmıştır. Bu kapsamda mezkûr operasyon istihbarat ve gizli faaliyet tekniği açısında, hem eleman temin edilmesinde klasik metotların kullanılması hem de sevk ve idare edilen elemanın siber kabiliyetini kullanarak bir sabotaj gerçekleştirmesi bakımından hibrit özellikli olarak tanımlanabilecektir. Bahse konu planlamanın sofistikeliği ve hibrit yapısı da dikkate alındığında, ortaya çıkardığı hasarda ilgili servisler açısından üst düzeyde başarılı olmuştur.

DÖRDÜNCÜ BÖLÜM

AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRILMASI

Günümüzde devletlerin güvenliği ile ilgili konuların teknolojik gelişmelerle ne denli bağlantılı olduğu düşünüldüğünde, siber uzayın devletler açısından ciddi bir güvenlik zafiyeti yaratacağı açıktır. Bu kapsamda 2017 Mayıs ayı içinde tüm dünyada etkili olan "WannaCry" isimli virüsün neden olduğu olumsuz etkilerde oldukça dikkat çekicidir**.** Bu itibarla "WannaCry" yazılımında ortaya çıktığı üzere, günümüzde gerek devletler gerekse de bireyler ve özel şirket siber uzay kaynaklı tehditler ile doğrudan karşı karşıya kalabilmektedirler. Eşi görülmemiş büyüklükte bir fidye yazılımı saldırısı olan "WannaCry", tüm dünyadaki organizasyonları ve bireysel kullanıcıları etkileyebilmiştir. "WannaCry" fidye yazılımı küresel ölçekte en çok sağlık, üretim, enerji (petrol ve gaz), teknoloji, gıda ve içecek, eğitim, kamu, medya ve iletişim sektörlerinde olumuz etkisini hissettirmiş ve büyük çapta maddi zarara neden olmuştur.[428] Bu örnekle de daha iyi anlaşılabileceği üzere, devletlerin güvenliklerini sağlama noktasında, geleneksel güvenlik anlayışına göre şekillenmiş tüm kurum ve stratejilerini, etkili bir siber saldırı ve siber savunma kapasitesi oluşturmak adına yeniden organize etmesi de gerekmektedir.

Bu değerlendirme ile uyumlu şekilde, ABD ve RF'nin Soğuk Savaş sonrası dönemde, özellikle de 2000'li yılların başı itibarıyla gerek ordularını ve istihbarat birimlerini, gerekse de kurumsal yapılarını siber uzayın sağladığı yeni imkânlar kapsamında etkili bir siber savunma ve saldırı kapasitesine sahip olmak amacıyla yeniden organize etmeye çalıştıkları görülmektedir. Gerçekte ise bu yeniden organizasyon süreci, iki devlet arasında Soğuk Savaş dönemi boyunca süregelen askeri kapasitelerini artırmaya yönelik rekabetin olağan bir sonucudur.

[428]Türk İnternet Sitesi, **Türkiye'de WannaCry Bağlantılı 166 çeşit Fidye Yazılımı Tespit edildi**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=56130, (31.05.2017).

1. ABD ve RF'nin Siber Güvenlik Stratejilerinin Tarihsel Arka Planı

Soğuk Savaş'ın en sert haliyle yaşandığı 1950 ve 1960'lı yıllarda ise SCCB'nin 1957 yılında ilk yapay uyduyu dünya yörüngesine yerleştirmesi, ardından aynı yıl içinde canlı bir köpek ile Sputnik II'yi uzaya göndermesi, ABD cephesinde ciddi endişe yaratmıştır. Gelişmeler üzerine, ABD yönetimi bilimsel alanda geriye düştüğü SSCB ile rekabet edebilmek amacıyla Şubat 1958 yılında ARPA isimli projeyi başlatmıştır. ARPA'daki projelerin kapsamı ise uzay araştırmalarının yanı sıra balistik füze savunması, dünya üzerinde nükleer test yapılan coğrafi noktaların saptanması gibi konuları da kapsayacak biçimde düzenlenmiştir.

ARPA bünyesinde, proje kapsamında çalışma yürüten bilim insanlarını tek bir ağ altında toplanmasını sağlayabilecek bir teknolojinin geliştirilmesi ile birlikte, söz konusu proje internet tarihinin başlangıcını teşkil etmiştir. Bu kapsamda ARPA projesi, ARPANET şeklinde isimlendirilmiştir.

Daha sonra ise Küba Krizi ile birlikte olası bir nükleer savaş halinde, ARPANET'in bu saldırılardan etkilenmesi için ne tür önlemler alınması gerektiği şeklinde tartışmalar da yaşanmaya başlamıştır. Bu tartışmalar, Paul Baran isimli bilim adamının "*fiziksel saldırı sonrasında kalan en büyük grupla elektrik bağlantısı sağlayarak*" iletişimi sürdürebilecek bir ağ yapının yaratılabileceğini ortaya koyması ile nihayetlenmiş ve farklı merkezlerde çalışan ağlar belirtilen yaklaşıma göre düzenlenmiştir. Akabinde, bu teknik altyapı ile birbirine bağlı olan ARPANET, ilk olarak İngiltere'deki Ulusal Fizik Laboratuarı'ndaki (National Physical Laboratory) ticari ağ ve Fransa'daki araştırma ağı olan Cyclades ile birleştirilmiştir.[429] Böylelikle de internetin uluslararası boyutta ulaşan ilk çekirdek altyapısı oluşturulmuştur. 1982 yılına gelindiğinde, ABD Savunma Bakanlığı gizli askeri verilerin iletişimin sağlanacağı yeni bir altyapı oluşturulmasına karar vermiş ve ARPANET'e ilave olarak, MILNET isimli bir altyapının oluşturulmasını tesis etmiştir.[430]

İnternetin gelişimini hızlandıran asıl olay ise Soğuk Savaş döneminde NATO tarafından kurulan, Varşova Paktı ülkelerine silah gönderilmesini kontrol etmekte olan ve 1947 yılında faaliyete geçirilen COCOM isimli uluslararası komitenin tasfiyesi ile söz

[429]Ayrıntılı bilgiiçin bkz. BIÇAKCI, "21. Yüzyılda Siber …", op. cit., ss. 6-7.
[430]BIÇAKCI, "NATO'nun Gelişen …", s. 107.

konusu olmuştur. Bu tasfiye ile birlikte 1987 yılında Almanya'dan ÇHC'ye ilk elektronik posta gönderilecek altyapı tesis edilmiştir. COCOM anlaşmasının tasfiyesi, ülkeler arasında teknoloji transferine imkân sağlayarak internet altyapısının gelişimine hızlı bir ivme kazanmıştır.[431]

1980'lerin başı ile birlikte, RF ve ABD arasında süregelen ve günümüz ağ teknolojilerinin temelini oluşturan teknoloji alanındaki rekabet, ABD'nin Yıldız Savaşları Projesi ile yeni bir boyuta taşınmıştır. Yıldız Savaşları Projesi'ne, SSCB'nin cevabı ise Mareşal Nikolai Orgakov tarafından "RMA" programının planlanmasıyla verilmiştir. Orgakov, anılan program ile birlikte kitlesel ve hantal bir yapıya sahip Sovyet Silahlı Kuvvetleri'ni ağ teknolojileri ve teknik operasyonlar ile takviye edilen ve yönetilen, daha etkin bir yapılanmaya kavuşturmayı hedeflemiştir. Orgakov'un bu misyonu ile birlikte, 1980'ler boyunca kimi Sovyet askeri stratejistleri, enformasyon teknolojilerindeki önemli gelişmelerin orduların kapasitelerinin artırılması noktasında kullanılabileceğini değerlendirmişlerdir.[432]

1990-1991 Körfez Savaşı esnasında, ABD önderliğindeki Koalisyon güçlerinin kullandığı iletişim ve enformasyon tekniklerinin, Irak Silahlı Kuvvetleri'nin harekât kabiliyetine verdiği zararın yanı sıra Koalisyon güçlerine kazandırdığı hız, dönemin Rus askeri uzmanları tarafından da yakından izlenmiştir. Bununla birlikte, I. Körfez Savaşı'ndaki sıcak çatışmaların dünya kamuoyuna adeta canlı olarak aktarılması kitle iletişim araçlarının ortaya koyduğu imkân ve kabiliyetin anlaşılması noktasında Rus uzmanlarca dikkatle tecrübe edilmiştir. 1999 yılına gelindiğinde ise NATO güçlerinin eski Yugoslavya'daki Sırp askeri unsurlarını bombalamaya başlaması ile birlikte, Sırp ve Rus hackerlar tarafından NATO'ya, üye ülkelerin askeri haberleşme sistemlerine, ABD Savunma Bakanlığı'nın alt yapılarına siber saldırılar gerçekleştirilmiştir. Öte yandan o dönem için Rus toplumun içinde bulunduğu ekonomik ve sosyal çöküntü nedeniyle Rus Ordusu'nun ABD Silahlı Kuvvetleri'nin tecrübe ettiği ağ teknolojileri konusundaki gelişmeleri askeri kapasitesinin mevcut yapısına adapte etme noktasında çalışma yapması için, 2000'li yılları beklemesi gerekmiştir.

[431]Ayrıntılı bilgi çin bkz. BIÇAKCI, "21. Yüzyılda Siber …", op. cit., ss. 6-7.
[432]Ayrıntılı bilgi için bkz. MOWTHORPE, op. cit., pp. 1-5.

2. ABD ve RF'nin Siber Güvenlik Stratejileri ile Siber Uzay'daki Uluslararası İşbirliği ve Rekabet İnsiyatiflerinin Analizi

RF ve ABD'nin güncel siber savunma ve saldırı stratejilerinin temelleri, 2000'li yıllarla birlikte başlayan aktif faaliyetlerin de ötesinde, belirtilen haliyle iki devletin Soğuk Savaş dönemindeki askeri rekabetinin bir sonucu olarak geliştirilen planlamalar vasıtasıyla atılmıştır. 2000'li yıllarla birlikte başlayan söz konusu aktif faaliyetlerin temel dayanak noktası ise ABD ve RF tarafından dünya kamuoyuna ilan edilmeye başlanan siber güvenlik stratejileri ve doktrinleri oluşturmaktadır. Bu dokümanların tonu, konjonktürel durumlara göre yumuşak veya sert vurgulara sahip olmakla birlikte, muhteviyatlarında iki devletin birbirlerine yönelik tehdit algılamalarının izlerini de içermiştir.

Bu noktada ABD'nin federal sistemi, bu sistemden kaynaklanan birbirinden bağımsız karar mekanizmalarının varlığı, siber güvenlik alanında faaliyet gösteren kurum ve kuruluş sayısının fazlalığı, iktidara gelen yönetimlerin yıllar içinde değişen politika öncelikleri, görece olarak daha açık yönetim yapısı nedenleriyle, ABD'nin RF'ye kıyasla 1990'ların ikinci yarısından itibaren siber güvenlik alanı ile ilgili olarak çok sayıda resmi plan, belge, strateji, doktrin ve başkanlık emri ortaya koyduğu görülmektedir.

Bu belgeler ile ilgili olarak genel bir değerlendirme yapılacak olması halinde ise Clinton'ın başkanlık dönemine denk gelen 1998-2001 yılları arasında yayımlanan dokümanlarda, kritik altyapıların korunması, uluslararası siber suç ile mücadele ve bu konuda devletler arasında işbirliği hususlarına vurgu yapıldığı açıkça görülebilecektir. Bush'un iktidarda olduğu 2000-2009 yılları için ise siber güvenlik alanına ilişkin olarak, bu alanı militarize eden ve daha fazla askeri anlam yükleyen belgelerin ortaya konulduğu belirtilebilecektir. 11 Eylül sonrasında ise ABD'nin kendisini küresel terör ile bir savaş ortamında kabul etmesinden ötürü, siber güvenlik strateji belgelerinde de siber uzayın ABD askeri gücüne destek sağlayan ve bu gücü pekiştiren bir alan olduğu hususu gündeme getirilmiştir. 2009 sonrasında Obama iktidarında yayımlanan dokümanlarda ise siber güvenlik alanı görece olarak daha ılımlı bir üslupla ve kritik altyapıların korunması, ABD siber savunma sisteminin merkezileştirilmesi, siber casusluk faaliyetlerine karşı konulması, siber uzayda küresel işbirliğinin sağlanması, siber suçlarla mücadele edilmesi, siber

farkındalığın ulusal ve uluslararası düzeyde sağlanması gibi önceliklerle hazırlandığı görülmektedir.[433]

Yukarıda bahsedildiği üzere 1990'lı yıllar ile birlikte büyük teknolojik gelişmelerinde bir sonucu olarak, ABD'nin siber güvenlik alanında resmi planlamalarının da başladığı görülmektedir. Bu itibarla Temmuz 1995 tarihinde yayımlanan *"13010 Nolu Başkanlık Direktifi"*, ABD'nin siber güvenlik alanındaki gelişmelere doğrudan vurgu yapan ve ABD kritik altyapılarının güvenliğinin sağlanmasını hedefleyen çalışmaları başlatmayı amaçlayan ilk resmi belge olması bakımından önemlidir. Bu alandaki ikinci önemli belge olan *"The National Strategy to Secure Cyberspace / Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji"* ise Şubat 2003 tarihinde yayımlanmıştır. Bu belge, ABD'nin siber uzay alanını tanımlayan, bu alandaki hedef ve planlamalarını ortaya koyan, ulusal siber uzayın nasıl korunacağına dair planlanan sistemi belirleyen, siber uzay kaynaklı tehditleri tarif eden ilk geniş kapsamlı dokümandır.

Bunlarla birlikte *"Cyberspace Policy Review / Siber Uzay Politika Revizyonu"*, Başkan Obama'nın talimatıyla 2009 yılında hazırlanmış olan bir belge niteliğindedir. Bu belgede temel olarak, ABD siber savunma sisteminde görev alan resmi kurum ve kuruluşların, federal ve yerel düzeyde çok başlı yapısına eleştiride bulunularak, bu durumun giderilmesi için bazı tedbirlerin alınması gerektiği ve ulusal siber güvenlik sistematiğinin ancak bu kuruluşların birlikte ve eşgüdüm halinde hareket etmesi ile etkili olabileceği belirtilmektedir.

Ayrıca 2011 yılında hazırlanan "*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World / Siber Uzay İçin Uluslararası Strateji: Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık"* isimli dokümanda ABD: "*uluslararası düzeyde siber suçlarla mücadele için gerekli çabayı harcayacağını, internetin yaygınlaşmasını ve uluslararası işbirliği ile yönetilmesini destekleyeceğini, internet özgürlüğünün temel önceliği olduğunu ve ekonomik refah için enformasyon teknolojilerinin geliştirilmesin büyük önem arz ettiğini"* dünya kamuoyuna duyurmaktadır. Bu belgenin dış politika ve siber uzay ilişkisi kapsamında ele alınması halinde ise belgede ortaya konan

[433]BISSON David, **A Cyber Study of the U.S. National Security Strategy Reports**,http://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports/, (25.05.2016).

hedeflerin Obama yönetiminin uluslararası ilişkilerde müzakere süreçlerine önem veren stratejisinin bir yansıması olduğu belirtilebilecektir. Söz konusu belgenin analizi bağlamında, Obama yönetiminin siber güvenlik alanında sert ve tekilci politikalar sürdürmeyi tercih eden Bush yönetiminden farklı bir yaklaşımı benimsemiş olduğu da görülmektedir.

"The Department of Defence Cyber Strategy / ABD Savunma Bakanlığı Siber Strateji" isimli belge, 23 Nisan 2015 tarihinde kabul edilmiştir ve bu belge ABD'nin ilan ettiği son resmi siber güvenlik stratejisi dokümanı niteliğindedir. Söz konusu belge ile Silahlı Kuvvetleri'ne "*ABD ağ teknoloji ve sistemleri ile gizli siber bilgilerini savunma, siber ataklara karşı ABD çıkarlarını koruma, askeri ve gizli siber operasyonları planlama ve bu tür operasyonlara rehberlik etme*" görevleri verilmiştir.

RF'de ise ABD'deki sistematikten farklı olarak, çok sayıda kurum ve kuruluş yerine belli bir standardizasyon içinde RF savunma-güvenlik-istihbarat bürokrasisi tarafından siber güvenlik resmi belge, doktrin ve dokümanlarının hazırlandığı görülmektedir. Bu standart yaklaşımın tek istisnası ise RF Genel Kurmay Başkanı Valery Gerasimov tarafından kaleme alınan, 2012 yılında "*Military Industrial Kurier Dergisi'nde"* yayınlanan *"The Value of Science in Prediction"*isimli makale ile kamuoyuna ilan edilence GRU'nun söz konusu dönemdeki direktörü Igor Sergun'un başarılı yöneticiliği ile GRU tarafından 2014-2015 Ukrayna müdahalesi esnasında etkili bir şekilde tatbik edilen Gerasimov Doktrini'dir.

Öte yandan belirtilen standart yaklaşım kapsamda hazırlanan ilk RF siber güvenlik belgesi, 9 Eylül 2000 tarihli "*Information Security Doctrine of the Russian Federation / Enformasyon Güvenliği Doktrini"* isimli dokümandır. Bu belge üslup olarak daha çok savunma ağırlıklıdır. Bununla birlikte belgenin özellikle kitle iletişim araçlarının kullanımı ve yayınları ile ilgili olarak, demokratik bir tavır içermediği de ortadadır. Bu durum, RF'nin söz konusu dönem için başta ABD olmak üzere, Batılı ülkelerden gelebilecek psikolojik savaş ve istihbarat tehditlerine karşı bir refleksi olarak değerlendirmelidir.[434]

[434]Ayrıntılı bilgi için bkz. GILES, "Information Troops-A Russian…", op. cit. pp. 1-5.

"Concept of the Foreign Policy of the Russian Federation (RF Dış Politika Konsepti" ise 12 Şubat 2013 tarihinde RF Devlet başkanı Vladimir Putin'in onayı ile kabul edilmiş bir belgedir. Bu belgede, RF'nin enformasyon ve siber güvenlik alanında uluslararası kurum, kuruluş, norm ve standartların belirlenmesine özel önem verdiği ve bu konudaki girişimleri RF dış politikasının temel amaçlarından birisi olarak kabul ettiği görülebilecektir. Belirtilen yaklaşımın temel dayanak noktası ise *"Renkli Devrimler"* ve *"Arap Baharı"* olarak adlandırılan sürecin bir devamı olarak, 4 Mart 2012 tarihinde RF'de yapılan ve Putin'in altı yıl için yeniden başkanlığa seçildiği dönemde Rus toplumun ve kamuoyunu etkilemeye yönelik olarak, özellikle de sosyal medya aracılığıyla gerçekleştirilen ABD kaynaklı psikolojik istihbarat faaliyetleridir. Bu itibarla RF siber uzayı denetleyen ve yöneten uluslararası kurum, kuruluş, norm ve standartların tesis edilmesini sağlayarak, ülkesine yönelik ağ teknolojileri kaynaklı uluslararası müdahale girişimlerini bir ölçüde de olsa sınırlamayı hedeflemiştir.

"Basic Principles for State Policy of the Russian Federation in the Field of International Information Security / RF Devlet Politikasının Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri" isimli belge de RF'nin siber güvenlik kapsamındaki uluslararası girişim ve planlamalarının devamı kapsamında görülebilecektir. Anılan belgede, uluslararası tedbirler kapsamında bazı spesifik uluslararası örgütler ve yapılanmalar doğrudan işaret edilerek, RF'nin:

-Özellikle, BM'nin mevcut yapısı içindeki işbirliği imkânlarına önem verdiği, bu kapsamda enformasyon teknolojileri alanında uluslararası işbirliği tesis edecek bir uzlaşmayı arzuladığı,

-ŞİÖ ve KGAÖ üyeleri ile konu kapsamındaki işbirliğinin geliştirilmesine katkı yapacağı,

-ITU'nun bilgi ve internet güvenliği alanındaki faaliyetlerinin geliştirilmesini teşvik edeceği, hususları net bir şekilde ortaya konmuştur.

Belirtilen belgede yer aldığı üzere, RF'nin siber güvenlik alanında uluslararası bir konsensüsün oluşmasını hedefleyen ve böylelikle de siber uzayı düzenleyen, internet ve bilgi güvenliği alanında kurallar ortaya koyan bir işbirliğinin geliştirilmesini isteyen bir dış

politika sürdürme niyetinde olduğu görülmektedir. Bu niyet ise temelde: "*RF'nin kendi ülkesine hedef alan, ülke kamuoyunu etkilemeyi hedefleyen, ekonomik yıkıcılık faaliyetlerini de bünyesinde barındıran, insan hakları ihlalleri, yargı bağımsızlığı, adil seçimler ve diğer demokrasi uygulamaları noktasında, özellikle ABD kaynaklı iç işlerine müdahaleye varabilecek dış politika insiyatiflerini engelleme amacından*" kaynaklanmıştır.[435]

Bu amaç çerçevesinde, RF siber uzay alanındaki gelişmeleri düzenleyecek olan uluslararası bir konsensüsün, özellikle de BM çatısı altında yaratılmasına hedeflemektedir. Bu hedefin amacı ise RF'nin siber savunma sistematiğindeki zafiyet ve kırılganlıkların giderilmek istemesidir. Bu itibarla Putin'in şahsiyeti etrafında simgeleşen anti-demokratik uygulamaların, başta ABD olmak üzere, Batılı ülkeler tarafından dış politika alanında RF'yi zor durumda bırakmayı amaçlayan girişimlerin konusu olduğu da bilinmektedir. Bu kapsamda da uluslararası medya kuruluşlarının konu dahilinde düzenli ve ısrarlı yayınları ile sosyal medya alanında, özellikle de 2012 RF Başkanlık seçimleri esnasında zirveye çıkan Rus toplumunu etkilemeye yönelik uluslararası kaynaklı müdahale girişimleri, RF'yi bazı tedbirler almaya itmiştir. Bu tedbirleri ise RF'nin internet erişimini ve internet tabanlı sosyal medya uygulamalarını denetleyen iç hukuk rejimini sıkılaştırması doğrultusunda gelişmiştir.

RF'nin dış politika çıkarları kapsamında, özellikle ABD karşıtlığı temelinde, uluslararası sistemi etkilemek amacıyla kurulmasına temel katkı yaptığı ŞİÖ, RF'nin siber uzay alanında işbirliği geliştirilmesine yönelik girişimleri için de önemli bir uluslararası zemin durumundadır. RF'nin girişimleri ile ŞİÖ tarafından 2005 yılında kabul edilen bir kararda, ABD'nin politikalarına odaklanılmak suretiyle, iletişim ve telekomünikasyon alanı kullanılarak, ülkelerin egemenlik haklarının ihlal edildiği, bu kapsamda da uluslararası barış ve güvenliğin tehlikeye düştüğü beyan edilmiştir.[436] Bu beyan itibarıyla, Rus hükümetinin BM çatısı altındaki pozisyonun aksine, ŞİÖ bünyesinde siber güvenlik

[435]NATO Cooperative Cyber Defense Centre of Excellence, **Basic Principles for State Policy of the Russian Federation in the Field of International Information Security**, https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf, (24.03.2016). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/6/114.html, (26.06.2016).
[436]MEDVEDEV,op. cit.,p. 69.

alanındaki girişimlerinde,siber uzay alanına yönelik korumacı ve kısıtlayıcı niyetini daha net olarak ortaya koyduğu ifade edilebilecektir.

RF'nin ŞİÖ bünyesinde ortaya koyduğu uluslararası işbirliği çabalarının belki de en somut sonucu, 2015 Mayıs ayında ÇHC ve RF arasında siber güvenlik alanın siber işbirliği yapılması noktasında ortak niyet beyanın da bulunulmasıdır. Bu ortak niyet beyanı ile birlikte RF ve ÇHC, birbirlerine karşı siber saldırılar gerçekleştirmeme, siber uzay teknolojileri konusunda eğitim ve teknoloji transferi konusunda işbirliği geliştirme, iki ülkenin iç politik yapısını ve sosyo-ekonomik atmosferini bozmayı hedefleyen siber saldırılara karşı ortak tedbir alma, siber uzayın denetleyen uluslararası bir rejim tesis etme yönünde uluslararası örgütler nezdinde ortak hareket etme hususlarında iyi niyetli politikalar izleyeceklerini ilan etmişlerdir.[437] Bu kapsamda, bahse konu gelişmeler ile RF ve ÇHC'nin, siber uzayda temel aktör konumuna gelmek istediğini iddia ettikleri ABD'ye karşı ortak bir duruş sergilemeyi ve siber uzayda ABD'nin başat devlet olmasını engellemeyi amaçladıkları da ileri sürülebilecektir.

Diğer yandan söz konusu ortak işbirliği insiyatifinin, ABD tarafından yayımlanan Şubat 2015 tarihli *"National Security Strategy / Ulusal Güvenlik Stratejisi"* ile Nisan 2015 tarihinde yayımlanan *"The Department of Defence Cyber Strategy / Savunma Bakanlığı Siber Stratejisi"* isimli resmi belgelere bir cevap niteliği taşıdığı da değerlendirilebilecektir. Bu kapsamda, "*National Security Strategy / Ulusal Güvenlik Stratejisi*" isimli dokümanda, RF'nin artan siber gücünün ve siber meydan okumalarının ABD'nin güvenliği karşısında ciddi tehdit oluşturduğu hususuna vurgu yapılmaktadır. "*The Department of Defence Cyber Strategy / Savunma Bakanlığı Siber Stratejisi*" isimli dokümanda ise RF'nin oldukça ileri bir siber kapasite ve strateji geliştirmiş olduğu belirtilmiştir. Bu kapsamda RF'nin siber gücü *"tespiti ve deşifresi oldukça zor"* şeklinde bir ifade ile tanımlanmıştır. Ayrıca bu belgede, ABD'nin Ortadoğu ve Asya-Pasifik Bölgesi'nde yer alan müttefikleri ile NATO üyelerine yönelik siber tehditler karşısında, müttefiklerine yardım edeceği açıkça ilan edilmiştir. Bahse konu vurgunun ise ABD'nin RF'nin sorun yaşadığı komşu ülkelere yönelik olarak 2000'lerin ikinci yarısından sonra gerçekleştirmeye başladığı siber saldırılara yönelik bir caydırıcılık mesajı olarak değerlendirilebilecektir.

[437] RAZUMOVSKAYA, loc.cit.

Ayrıca ŞİÖ üyesi olan RF, ÇHC, Tacikistan ve Özbekistan tarafından 2011 yılında BM Genel Sekreteri'ne hitaben, ABD karşıtlığı temelinde *"Enformasyon Güvenliğinin Yönetim Kuralları / Management Rules of Information Security"* isimli doküman hazırlanmıştır. Dokümanda siber silahların yayılmasını engelleyici ya da siber güvenlik alanındaki düşmanca faaliyetlerin tanımına ilişkin olarak her hangi bir ifade yer almamakla birlikte, özellikle siber uzay kaynaklı gelişmelerin ülkelerin egemenliğini tehlikeye düşürdüğü beyan edilerek, bu durumda siber tehdit altındaki ülkelerin kendilerini savunma hakkı olduğu kesin dille belirtilmiştir.[438]

Bununla birlikte ŞİÖ kapsamındaki girişimleri dikkate alındığında, RF'nin siber uzaydaki gelişmelere yönelik uluslararası işbirliğinin tesis edilmesi noktasında, ABD önderliğindeki Batı konseptinin dışında inisiyatifi geliştirme amacı içinde olduğu görülmektedir. Bu itibarla RF'nin Avrupa Konseyi Sanal Suçlar Sözleşmesi (Council of Europe Convention on Cybercrime)'ni imzalamamasının dikkat çekici olduğu değerlendirilebilecektir.

ABD ve RF arasında uluslararası sistemde siber güvenlik alanında çetin bir rekabet söz konusu olmakla birlikte, iki ülkenin bazı teknolojik gelişmeler ve adi suç niteliğindeki siber suçlarla mücadele kapsamında özellikle de suçluların karşılıklı iadesi konusunda zaman zaman işbirliği insiyatifleri geliştirdikleri de gözlemlenmektedir. Siber uzayın iki önemli aktörü olan RF ve ABD, bu alanındaki uluslararası işbirliğinin sağlanması noktasında farklı yaklaşımlara sahiptirler. Bu itibarla ABD siber uzay alanı kaynaklı tehditleri uluslararası işbirliğine açık bir şekilde, yerel ve ulusal tedbirler ile bertaraf etmeyi amaçlarken, RF siber uzayın uluslararası bir rejim ile denetlenmesini, özellikle de sosyal medya imkânları için elverişli ortam yaratan internetin kontrol altında tutulmasını hedeflemektedir.

Bu farklı yaklaşıma rağmen ABD ve RF, 2009 Aralık ayında BM Silahsızlanma ve Uluslararası Güvenlik Komitesi'ndeki bir toplantıda, siber uzayın askeri bir alan olarak kullanımın azaltılması ve uluslararası güvenliğin geliştirilmesine yönelik olarak iki ülke

[438]United Nations, 66th sess., **2011-A/66/359, Letter Dated 12 September 2011 From the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General**, https://disarmament-library.un.org/UNODA/Library.nsf/f446fe4c20839e50852578790055e729/329f71777f4b4e4e85257a7f005db45a?OpenDocument, (01.04.2016).

arasında müzakerelerin başlaması kararı vermişlerdir. Bununla birlikte konu kapsamında bugüne kadar net bir adım da atılmamıştır.[439]

Belirtilen girişimden öncede, RF ve ABD yetkilileri tarafından enformasyon güvenliği alanında işbirliği geliştirilmesi yönünde çalışmalar da söz konusu olmuştur. Bu kapsamda, 1998 Eylül ayında RF ve ABD Devlet Başkanları arasında gerçekleşen görüşmede, enformasyon teknolojileri alanındaki gelişmelerin olumlu ve olumsuz yanlarına vurgu yapılarak, bu alanda stratejik işbirliği geliştirilmesinin iki ülkenin ortak çıkarı olduğu vurgusu yapılmıştır.[440] Ayrıca bu görüşmede "*Y2K"* problemi dahilinde ortaya çıkması muhtemel sorunlar için iki ülkenin birlikte çalışması kararlaştırılmıştır.

Hatırlanacağı üzere, 2006 yılına gelindiğinde RF dönem başkanı olduğu G-8 grubuna, üye ülkeler arasında terörizm, siber güvenlik ve organize suç konularında özel-kamu ortaklığının geliştirilmesine yönelik bir insiyatif başlatılmasını teklif etmiş, ancak ABD'nin olumlu yaklaşımına rağmen, bu teklifin somut bir sonucu söz konusu olmamıştır.[441]

Ancak Obama yönetimi ile birlikte ABD'nin siber uzayda işbirliği geliştirilmesine yönelik çabalarının arttığı da ifade edilebilecektir. Bu kapsamda Obama tarafından 2009 Mayıs ayında yapılan bir çağrı ile RF, ÇHC ve Hindistan'ı da dâhil edecek şekilde iletişim teknolojileri alanında belirli bir gelişmişlik içinde olan ülkelerin siber uzaya alanı kaynaklı olarak hükümet dışı aktörler ile haydut devletlerden gelecek olan tehlikelere karşı ortak hareket edebileceğini, bu itibarla da NATO'nun konu kapsamında insiyatif alabileceğini gündeme getirilmiştir.

2010 Temmuz ayında ise Moskova'da gerçekleşen, II. ABD-RF İletişim Teknolojileri Toplantısı'nda bir araya gelen üst düzey RF ve ABD'li yetkililer arasında konu kapsamında bazı resmi temaslar gerçekleşmiştir. Bu temaslarda, iki ülke yetkilileri siber güvenlik alanındaki işbirliği arayışına yönelik görüşmelerinin sürdürülmesi kararı

[439] GADY ve AUSTİN, loc.cit.
[440]Ayrıntılı bilgi için bkz. GADY ve AUSTİN, op. cit., pp. 1-2.
[441]G8 Summit 2006, Moscow, November 28-30, Working Meetings, **G8 Initiative For PublicPrivate Partnerships To Counter Terrorism: Private Sector Action Beyond 2006**,http://issuu.com/ewipublications/docs/g8-initiative-for-public-private-partnerships-to-c/1, (02.04.2016).

almışlardır.[442] Bu karar iki ülke arasında konu kapsamındaki iletişim kanlarlının açık tutulmak istenmesi bakımından önemli bir aşama olarak kabul edilebilecektir.

ABD ve RF arasında siber uzay konusunda ikili ve uluslararası düzeyde işbirliğin tesis edilmesine yönelik bazı girişimler bulunmasına rağmen, bu girişimlerin somut bir sonuca ulaşmadığı da görülmektedir. Bu olumsuz durumun nedeni ise iki ülkenin siber uzay konusunda birbirlerine yönelik tehdit algılamaları ve farklı anlayışlarıdır. Bu kapsamda, RF güvenlik ve askeri bürokrasisi, ABD'nin teknolojik üstünlüğünü dikkate alarak, ABD'ni en önemli askeri ve siber tehdit kaynağı olarak görmektedir. Benzer biçimde, ABD liderliği için RF'nin sadece siber uzay alanı kaynaklı değil, aynı zamanda her türlü askeri kaynaklı tehditler için de tedbir alınması gereken bir devlet şeklinde konumlandırılmaktadır.

RF'nin bahsedilen şekilde, geçmişte edindiği tecrübeler üzerine geliştirdiği ve sürekli olarak ortaya koyduğu yeniliklerle de etkinliğini arttırdığı siber gücünün ulaştığı kapasite, günümüzde başta ABD olmak üzere, NATO üyesi ülkelerin yanı sıra RF'nun komşuları için de ciddi bir tehdit olarak değerlendirilmektedir. Bu noktada, ABD Ulusal İstihbaratı'nın Başkanı James Clapper'ın *"ABD İstihbarat Topluluğu'nun Dünya Tehdit Değerlendirmeleri-2015"* başlıklı bir sunumda, RF'nun siber savaş gücü için; *"Burada detaylara giremem ama Rusya'nın siber tehdidi daha önce tahmin ettiğimizden çok daha güçlü."* şeklindeki değerlendirme yapmış olmasının oldukça önemlidir.[443]

Öte yandan daha öncede ifade edildiği üzere, ABD Ordusu'nun I. Körfez Savaşı esnasında oldukça aktif ve başarılı bir şekilde ağ teknolojilerinden istifade etmeyi başarması bu konuda ABD'nin yeni planlamalar geliştirme sürecini de hızlandırmıştır. Bu çerçevede ABD, Hava Kuvvetleri bünyesinde Bilgi Savaşı Merkezi (Info War Center) isimli bir birim kurmuş, 1995 yılında ise ABD Ulusal Savunma Üniversitesi siber savaşa komuta edecek olan ilk subaylarını mezun etmeye başlamıştır. Ayrıca konu kapsamında ABD Hükümeti tarafından, Uzay Komutanlığı (Space Command),"Stratejik Komutanlık'a (Strategic Command / STRATCOM)" dönüştürülmüş ve bu komutanlığa siber savaşa

[442]U.S. Department of State, **Office of the Spokesman, Roundtable on U.S.-Russia Information, Technology: Dialogue on a Range of Topics Including Broadband and Internet Governance**, http://issuu. com/ewipublications/docs/usrussiacyber/12, (02.04.2016).
[443]Sputniknews Haber Portalı, **Rusya'nın Artan Siber Gücü, ABD'yi Kaygılandırıyor**, http://tr.sputniknews.com/savunma/20150409/1014919049.html, (21.03.2016)

komuta etme yetkisi verilmiştir. Bu gelişmelerin devamında 2009 yılında STRATCOM'da, bir siber komutanlık kurulması emri verilmiş, 2010 yılında ise müstakil bir "Siber Komutanlık (CYBERCOM)" tesis edilmiştir. CYBERCOM, ABD'nin siber güvenlik sistematiğinde önemli bir rol üstlenmektedir.[444]Bu kapsamda CYBERCOM'un temel görevleri, ABD'nin mevcut siber kaynaklarını düzenlemek ve ABD askeri bilgisayar ağları müdafaasını eşzamanlı bir hale getirmek olarak belirlenmiştir.

ABD Silahlı Kuvvetleri bünyesindeki siber savunma ve saldırı kapasitesini artırılmasına yönelik bahse konu planlamaların, RF Ordusu'na yansıması ise 2010 yılında enformasyon ve bilgi teknolojileri alanında çalışma yürütmek amacıyla RF Savunma Bakanlığı bünyesinde bir bakan yardımcılığı pozisyonunu tesis edilmesiyle başlamıştır. Akabinde de RF, 2013 yılında aldığı bir karar ile RSK bünyesinde bağımsız bir siber savaş birimi kurmayı planlama kapsamına almıştır.

Son olarak, 6 Aralık 2016 tarihli *"RF Bilgi Güvenliği Doktrini / Information Security Doctrine of the Russian Federation"* isimli doküman, 9 Eylül 2000 tarihli RF Enformasyon Güvenliği Doktrini'nin yerine yürürlüğe konulmak üzere hazırlanmıştır. Siber güvenlik alanında RF tarafından kabul edilen son resmi doküman niteliğindedir. Bu kapsamda, bahse konu doktrinde özetle:

> "*Siber uzay ve siber suç alanları kapsamındaki ağ teknolojilerine yönelik tedbirler alınması gerektiği,*
>
> *Bu tedbirlerin ise en başta terörist organizasyonların propaganda faaliyetlerine karşı koyma hedefine odaklanmasının şart olduğu,*
>
> *Rus hükümetlerinin söz konusu amaç kapsamında ulusal düzeyde kontrol edilebilir ve denetlenebilir bir internet sistematiği kurmasının önem arz ettiği,*
>
> *Yabancı istihbarat servislerinin, RF'nin ulusal ve uluslararası düzeydeki çıkarlarını tehlikeye düşürebilecek siber propaganda faaliyetlerine karşı etkili mücadele edilmesinin gerektiği,*

[444]YAYLA, op. cit., s. 186.

RF'nin uluslararası medya sistematiği içinde daha etkin bir şekilde faaliyet gösterebileceği yapılanmaları geliştirmeye devam etmesinin şart olduğu,

Rus toplumunun, özellikle de genç Rus nüfusunun manipüle edilmesini amaçlayan siber aktivitelerin engellenmesinin RF'nin öncelikli hedefleri arasında olması gerektiği,

Rus hükümetlerinin kendi ülkesini hedef alan siber operasyonların yanı sıra kendisine dost ülkelere yönelik siber saldırı ve enformasyon savaşı aktivitelerini de engellemesinin önem arz ettiği" hususları yer almaktadır.[445]

3. ABD ve RF Tarafından Birbirleri Aleyhine Planlandığı İddia Edilen Siber Saldırılar

RF ve ABD arasında siber uzay alanında yaşanan rekabet ve hasmane politikaların somutlaşmış örnekleri, ABD ve RF istihbarat servislerinin birbirlerine yönelik siber espiyonaj ve siber saldırılar şeklinde planlanmış olan subversif gizli faaliyetlerinin açık kaynaklara ulaştığı haliyle irdelenmesi neticesinde görülebilecektir.

Bu kapsamda, ABD'nin 1982 yılında Sibirya Gaz Hattı'na yönelik *"mantık bombası"* şeklinde isimlendirilen bir zararlı yazılım ile yaptığı iddia edilen saldırı, gerek iki ülke arasında gerçekleşen ilk siber saldırı örneği olması, gerekse de dünyanın bugüne kadar tecrübe etmediği bir şekilde zararlı yazılım kullanılmak suretiyle planlanmış olması bakımından özellikle vurgulanmalıdır.[446]Ayrıca teknoloji lideri ülke olarak bilişim ortamını en etkin kullanan ABD'nin, 1980'lerde dahi oldukça sofistike yöntemleri kullanabilecek bir siber kapasiteye ulaşabildiğini göstermesi bakımından bu saldırı oldukça önemlidir. *"Mantık bombası"* olarak bilinen yöntemle, ABD bomba gibi her hangi bir savaş ekipmanı kullanmadan, bilgisayar sistemine eklenen bir kod sayesinde ve

[445]RIA Novosti ve Mir24.Tv, **New Kremlin Information-Security Doctrine Calls For 'Managing' Internet In Russia**, http://www.rferl.org/a/russia-informaiton-security-internet-freedome-concerns/28159130.html, (02.01.2017). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/6/135.html, (02.01.2017).

[446]The Telegraph OnlineNews, **CIA plot led to huge blast in Siberian gas pipeline**,http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html, (02.06.2016).

bilgisayarın işletim sisteminin karıştırılmasını sağlayarak SSCB'de bulunan Sibirya Gaz Boru hattını patlatmayı başardığı da iddia edilmiştir.[447]

1998 yılında FBI tarafından ABD Savunma Bakanlığı, Enerji Bakanlığı, bazı kuruluş ve üniversitelerin özellikle de uzay araştırmalarını hedefleyen bir siber espiyonaj operasyonu tespit edilmiştir. Kamuoyunda "Moonlight Moze / Ay Işığı Labirenti" adıyla bilinen söz konusu operasyonun planlayıcılarının ise RİS ile irtibatlı Rus hackerlar olduğu da yapılan araştırmalar kapsamında iddia edilmiştir. Bu operasyon ile ABD'nin gizli araştırma faaliyetleri ve askeri çalışmaları dahilindeki çok önemli bilgiler çalınabilmiştir. Bahse konu iddiaları ise Rus tarafı kabul etmemiştir. Bu olay ABD güvenlik ve istihbarat bürokrasi ile kamuoyunda siber saldırıların yaratabileceği olumsuz etkiler ile ilgili olarak ciddi bir farkındalığın oluşmasına vesile olmuştur.[448]

Bununla birlikte ABD'ye yönelik olarak RF istihbarat servisleri kaynaklı olarak gerçekleştirildiği iddia edilen ve açık kaynaklara yansımış olan bazı siber saldırı vakaları da bulunmaktadır. Bu kapsamda, 2008 yılında ABD Savunma Bakanlığı ve ABD Ordusu'na yönelik olarak gerçekleştirilen siber saldırılarda kullanılan *"BTZ"* isimli yazılımı üretme kapasitesine sadece RF istihbarat servisleri ile bağlantılı çevrelerin sahip olduğu bilinmektedir. Söz konusu yazılım 2008 yılında bir taşınabilir bellek vasıtasıyla ABD Ordusu'nun bir Ortadoğu ülkesinde bulunan üstündeki bilgisayarları kullanılmak suretiyle aktive edilmiş ve 14 ay boyunca etkinliğini sürdürmüştür.[449]

Siber güvenlik hizmeti ve yazılımları alanında faaliyet gösteren *"FireEye"* isimli ABD orijinli şirket tarafından 2014 yılında yayınlanan raporda ise RF'nin *"*APT 28*"* takma adıyla faaliyet gösteren hacker grubu vasıtasıyla sürdürdüğü bir siber casusluk faaliyetini gündeme getirilmiştir. Bu rapora göre: "*APT28*, *casusluk amaçlı bir dizi siber faaliyeti bünyesinde barındıran, 2007 yılından beri aktif olarak kullanılan, özellikle Doğu Avrupa ülkeleri ile NATO ve Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT)'nın savunma kapasitelerini hedef alan, RİS ile doğrudan bağlantılı bir espiyonaj operasyonu/grubu"*

[447]Akademik Portal News, **Bugüne Kadar Gerçekleşmiş Olan Beş Devasa Siber Saldırı**, http://www.akademiportal.com/bugune-kadar-gerceklesmis-olan-5-devasa-siber-saldiri/, (18.02.2016).
[448]INC Comittee on Govermental Affairs US Senate, **Testımony of James Adams Chief Executıve Offıicer**,https://fas.org/irp/congress/2000_hr/030200_adams.htm,(16.02.2017).
[449]STEWART ve WOLF, loc.cit.

şeklinde tanımlanmıştır.[450] RİS ile bağlantılı olarak sürdürülen söz konusu espiyonaj operasyonu raporda belirtildiği haliyle doğru ise bu durum RF'nin siber sisteminin kaynağı anlaşılamayan bir uzaktan kontrol mekanizması ile yönlendirilen, güvenlik sistemlerini aşma kapasitesine ulaşmış, tespit edilmeden uzun bir süre aktive olabilecek ve bilgi manipülasyonu imkânını da bünyesinde barındıran bir kapasiteye ulaştığı ileri sürülebilecektir.

Yine *"FireEye"* tarafından 2013 Ekim ayında yayımlanan başka bir raporda: FBI'ın 2010 yılında Microsoft'ta çalışan Alexey Karetnikoc isimli bir RİS mensubunu ABD aleyhine siber casusluk faaliyeti gerçekleştirdiği gerekçesiyle tutukladığı, 2012 yılında Rus Güvenlik Şirketi Kaspersky Lab'ın *"Red October"* müstear adlı bir siber casusluk operasyonu kapsamında çoğunluğu eski Doğu Blok'u üyesi ülke vatandaşlarının internet ve kişisel haberleşmelerini takip ettiğinin belirlendiği, 2013 yılında android yazılım kullanmakta olan cep telefonlarında, söz konusu cep telefonu üzerinden yapılan haberleşmenin takip etme kapasitesine sahip RF kaynaklı yazılımların ilgili şirket tarafından tespit edildiği, bu kapsamda RF merkezli siber saldırı ve casusluk operasyonlarının başta ABD olmak üzere Batı çıkarlarına zarar verecek teknik özelliklere sahip, oldukça sofistike boyutta planlanmış ve tespiti oldukça güç özelliklere sahip olduğunun belirtilebileceği hususları yer almıştır.[451]

F-Secure isimli data güvenlik şirketi tarafından, 2015 Eylül ayında yayınlanan bir raporda, RF'nin yedi yıldır süre gelen, *"The Dukes"* isimi bir yazılımın kullanıldığı ve Avrupa, Asya ve Amerika'daki bazı ülkeleri hedef alan bir siber espiyonaj operasyonu sürdürmekte olduğu iddia edilmiştir. Raporda ayrıca, belirtilen faaliyetin, RF devleti destekli hackerlar tarafından gerçekleştirildiği, özellikle de Gürcistan'ın NATO'daki Enformasyon Merkezi'ni, Gürcistan Savunma Bakanlığı'nı, Türkiye Dışişleri Bakanlığını ve ABD, Avrupa ve Orta Asya'daki bazı düşünce merkezleri ile hükümet kuruluşlarını hedef aldığı ifade edilmiştir.[452]

---

[450]FireEye, **APT28-A Window Into Russia's Cyber Espionage Operations?**, Special Report by FireEye, https://www.fireeye.com/, (01.04.2016).
[451]GEERS, op. cit., p. 12.
[452]Al Jazeera Internet Web, **Report:Russia sponsored cyber attacks**,http://www.aljazeera.com/news/2015/09/report-russian-government-sponsored-cyber-attacks-150917132351595.html, (01.04.2016).

ABC Haber Kanalı tarafından 2014 yılında yapılan bir haberde, ABD güvenlik ve istihbarat görevlilerince, RİS kaynaklı bir yazılım programının 2011 yılından bu yana ABD'nin doğal gaz, petrol, içme suyu ve sulama sistemine zarar verdiğinin tespit edildiği gündeme getirilmiştir. Bu yazılımın belirtilen kritik altyapı sistemlerinin kontrol mekanizmalarını hedef alarak, zarar vermeyi amaçlayacak şekilde tasarlandığı da aynı haberde yer almıştır. [453]

1 Nisan 2016 tarihinde, Flash Critic Cyber Threats News isimli haber ajansının yayınladığı bir haberde RİS kaynaklı olarak, ABD*"Flash Critic Cyber Threats News"*'de faaliyet gösteren JP Morgan, Chase&Co Bankası da dahil, ismi açıklanmayan beş bankaya subversif amaçlı siber saldırılar gerçekleştirildiği belirtilmiştir. Söz konusu haberde, siber saldırıların 2015 Ağustos ayından bu yana devam ettiği, saldırıların oldukça sofistike bir yazılım kullanılarak yapılmış olması nedeniyle ABD'li yetkililerin saldırının arkasında RF olduğuna kesin olarak emin oldukları ifade edilmiştir.[454]

RF ve ABD arasında siber güvenlik alanında yaşanan ve etkileri hala devam etmekte olan önemli bir kriz ise *"Edward Snowden Olayı"*dır. Amerikan NSA ve CIA görevlisi (sistem mühendisi ve benzeri görevler) Edward Snowden'ın dünya siyasetinin gündemine oturmasının temel sebebi, anılanın ABD ve İngiltere hükümetleri tarafından kullanılmakta olan kitle takip programlarını (PRISM ve Tempora) 2013 yılında kamuoyuna ifşa etmesidir. Bu ifşa süreci ve akabinde yaşanan gelişmeler RF ve ABD ilişkilerinde etkileri hala sürmekte olan ciddi bir diplomatik kriz haline gelmiştir. Bu skandalı dikkat çekici kılan yanı ise ABD'nin sahip olduğu ve sadece hasım ülkeleri değil aynı zamanda müttefiklerini de hedef alabilen küresel siber kapasitesinin ifşasıdır. Snowden hâlihazırda geçici sığınma hakkıyla RF hükümetinin himayesindedir. RF'nin, Snowden'e ABD'nin tüm baskılarına rağmen siyasi sığınma hakkı vermiş olması, aslında siber uzay alanında RF ve ABD arasındaki güç mücadelesinin bir yansımasıdır. RF, Snowden'e verdiği siyasi destek ile adeta siber uzayda ABD'nin tek egemen güç olmasına direneceğini ve bu alanda ABD karşıtlığını sürdüren bloğun liderliğini yapacağını dünya kamuoyuna açıkça ilan etmiştir.

---

[453]ABC News, **Trojan Horse Bug Lurking in Vital US Computers Since 2011**,http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476, (01.04.2016).
[454]Flash Critic Cyber Threats News, **Russian cyber warfare suspected in the bank attack**, http://flashcritic.com/russian-cyber-warfare-suspected-bank-attacks-sophisticated-hackers/, (01.04.2016).

ABD ve RF arasında siber güvenlik alanında yaşanmakta olan rekabetin ve hasmane tutumların en net görüldüğü son olay, RF'nin 2016 yılı içerisinde Demokrat Parti Ulusal Komitesi (DUK)'nin, Clinton'ın seçim kampanyası direktörü olan John Podesta ile ABD eski Dışişleri Bakanı ve aynı zamanda Demokrat Parti'nin seçim çalışmalarına aktif olarak destek veren Colin Powell'ın e-postalarını siber saldırı yöntemleri ile temin ettiği ve bu e-postalardan bazılarını kamuoyuna sızdırdığı, böylelikle de aktif bir şekilde ABD seçim sürecini kendi ulusal çıkarları kapsamında manipüle ettiğine yönelik iddialardır.

Söz konusu siber saldırılar ile ilgili olarak, RF istihbarat örgütlerinin bizzat Putin'in talimatıyla bu saldırıları organize ettiği, bahse konu saldırıların nedeninin 2011 yılında RF başkanlık seçimlerine yönelik olarak Clinton'ın da dışişleri bakanı olarak yer aldığı ABD yönetiminin Putin karşıtı açık ve örtülü faaliyetleri olduğu hususları da gündeme getirilmiştir.

RF tarafından gerçekleştirildiği iddia edilen söz konusu siber saldırılar, 2015 yaz ayları içinde başlayacak şekilde RF iç istihbarat örgütü FSB, RF askeri istihbarat örgütü GRU tarafından bizzat veya bu örgütler tarafından desteklenen hacker grupları vasıtasıyla planlandığı gündeme getirilmektedir. Söz konusu hacker grupları arasında yer alan ve FSB tarafından desteklendiği iddia edilen yapılanmaların adları, Cozy Bear, the Dukes ve APT 29'dur. GRU tarafından desteklendiği iddia edilen grup ise Fancy Bear veya APT 28 olarak isimlendirilmektedir. Ayrıca "Guccifer 2.0" adıyla bireysel olarak faaliyet gösteren bir hacker yapılanması da bahse konu saldırılarda rol oynadığı iddia edilmiştir. Saldırılar, "spread phishing" şeklinde ifade edilen hedef odaklı ve yemleme yöntemleri ile gerçekleştirilmiştir. Bu yöntemle, hedef kurum ve şahısların e-postaları (50-60 bin civarı) siber casusluk amaçlı kötü yazılımlar ile temin edilerek, manipülasyonun amacına uygun olanları çeşitli internet sayfaları ve medya kuruluşları (WikiLeaks, The New York Times, DC Leaks, The Washington Post, The Wall Street Journal) tarafından kamuoyuna ifşa ettirilmiştir.

Söz konusu ifşalar neticesinde ise ABD Demokrat Parti seçim propaganda sürecinin kısmen etkilendiği belirtilebilecektir. Bu kapsamda DUK Başkanı Debbie Wasserman Schultz'un ve bazı üst düzey görevliler istifa etmiş, Demokrat Parti'nin diğer başkan adayı Senatör Bernie Sanders'in pozisyonu güçlenmiş ve adaylık yarışına bir süre daha devam

etmesi sağlanmış, Cumhuriyetçi Parti'nin eline Demokrat Parti'nin aleyhine kullanabileceği bir koz verilmiş, Clinton ismi tartışmalı hale gelerek, yıpratılmıştır.

Bu siber saldırılar ile ilgili olarak FBI ve DHS tarafından ortak olarak hazırlanmış olan bir raporda ise RF, bu siber saldırıların planlayıcı olarak doğrudan suçlanmıştır. Ayrıca bahse konu raporla birlikte yayımlanan 29 Aralık 2016 tarihli medya bildirisinde, belirtilen raporda gündeme gelen siber saldırıların da ötesinde, Rus istihbarat unsurlarının ABD hükümet kuruluşlarını, sivil toplum örgütlerini, üniversiteleri, ABD kritik altyapılarını, düşünce kuruluşlarını, teknoloji üreten şirketlerini hedef alan siber saldırılar planlamakta olduğu da gündeme getirilmiştir.

Bununla birlikte DHS tarafından 30 Aralık 2016 tarihinde yapılan bir medya açıklamasında: "*RF sivil ve askeri istihbarat yapılarının son dönemlerde ABD hükümetini ve vatandaşlarını hedef alan sofistike ve agresif siber operasyonlar düzenlediği, ABD güvenlik ve istihbarat kurumlarının bu saldırıları 'Grizlly Steppe' takma adıyla tanımladığı, 'Grizlly Steppe' faaliyeti ile RF'nin ABD'nin hükümet kuruluşlarına, üniversitelerine sivil toplum ve düşünce kuruluşlarına, siyasi partilerine "spread phishing" şeklinde ifade edilen hedef odaklı ve yemleme yöntemleri ile siber casusluk operasyonları düzenlediği ve elde ettiği gizli bilgileri üçüncü ortaklar vasıtasıyla kamuoyuna ifşa ettiği*" belirtilmiştir.[455]

DHS tarafından RF hükümetine yapılan açık suçlamalar sonrasında, Obama yönetimi tarafından çoğunluğu GRU mensubu olduğu iddia edilen 35 Rus diplomatın, ABD başkanlık seçimlerini hedef alan siber saldırılarda görev yaptıkları iddiasıyla sınır dışı edilmesi, Maryland ve New York'taki Rus diplomatik temsilciliklerinin kapatılması kararı alınmıştır. Söz konusu sınır dışı kararı karşısında ise RF tarafı belirtilen suçlamaları kabul etmediğini açıklamıştır. Putin tarafından konuyla ilgili olarak ise "*gelişmelerin kendileri tarafından Washington yönetiminin attığı yeni düşmanca adımlar ve provokasyon*

[455]Department of Homeland Security, **ExecutiveSummary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale**, https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary (20.02.2017).

olarak nitelendirdiği, hiç kimseyi sınır dışı etmeyecekleri ve ABD'ye verilecek yanıtı Trump yönetiminin tutumuna göre belirleyeceklerini" ifade edilmiştir.[456]

Snowden Olayı ile Demokrat Parti Hack Skandalı'nın ABD ve RF'nin siber güvenlik stratejileri kapsamındaki önemli bir yansıması da iki devlet arasında yeni nesil enstrümanlar ile devam etmekte olan enformasyon savaşını çok daha belirgin hale getirmiş olmasıdır. Bu noktada özellikle RF'nin sosyal medya imkânlarından azami ölçüde yararlanan, yeni tesis ettiği uluslararası medya kuruluşları vasıtasıyla sürdürdüğü yayın politikaları ile kuvvetlendirilen ve ulusal siber güvenlik stratejisinin önemli bir parçası olarak tasarlanan modern enformasyon savaşı kabiliyetlerinin son yıllardaki gelişim ivmesinin dikkat çekici olduğu da ileri sürülebilecektir.

4. ABD ve RF'nin Enformasyon Savaşı Kapsamındaki Rekabeti

"Enformasyon Savaşı" kavramının üzerinde uzlaşılmış tek bir tanımı bulunmamakla birlikte, en geniş haliyle *"birisinin hasmı üzerinde avantaj sağlamak amacıyla; bilgiyi indirgeme, dağıtma, inkâr etme, koruma, transfer etme ve toplama yöntemlerini ihtiva eden teknikler bütünü olarak kullanması"* şeklinde tanımlanabilir.[457]

Uluslararası sistemdeki etkili devletlerin, 1990'lı yıllar ile birlikte siber uzayın sağladığı imkânlardan askeri kapasitelerini destekleme ve dış politikada bir baskı aracı olarak kullanma noktasında faydalandıkları, ayrıca bu devletlerin iletişim ve telekomünikasyon teknolojilerinde yaşanmakta olan gelişmeleri bir enformasyon savaşı tekniği şeklinde okuyarak, bu alanda da stratejiler geliştirdikleri görülmektedir.

Bu kapsamda CNN'in 1991 yılındaki 1. Körfez Savaşı esnasındaki yayın performansı ile başlayan, daha sonra RF'nin 1994-1996 yılları arasındaki Çeçenistan müdahalesi ile internetin bir propaganda yöntemi olarak ilk kez kullanılması ile devam eden, 2010 yılında başlayan Arap Baharı olayları kapsamında El Cezire'nin yayın politikası ile birlikte daha da gelişen, 2013 Gezi Olayları sırasındaki uluslararası medya

[456]Sputniknews Haber Portalı, **Putin'den ABD'ye yanıt: Biz hiç kimseyi sınır dışı etmeyeceğiz.**, https://tr.sputniknews.com/rusya/201612301026565257-putin-abdye-yanit-biz-hic-kimseyi-sinir-disi-etmeyecegiz/, (22.02.2017).

[457]Ayrıntılı bilgi için bkz. BURNS Megan, **Information Warfare: What and How?**, http://www.cs.cmu.edu/~burnsm/InfoWarfare.html, (11.11. 2016).

kuruluşları tarafından yapılan yayınlarla da çok boyutlu hale gelen yeni nesil enformasyon savaşı teknikleri, sosyal medya olanaklarının da muazzam katkısıyla son yıllarda ciddi bir uluslararası müdahale aracı olarak karşımıza çıkmıştır.

Tüm bu gelişmeleri de dikkate almak suretiyle RF'nin de siber güvenlik stratejisinin bir parçası olarak kendi enformasyon savaşı stratejisini geliştirme kapsamındaki gayretleri 2010 yılı sonrasında ivme kazanmıştır. Bu şekilde bir stratejik hamle yapılmasında RF çıkarları aleyhine Batı tarafından desteklenen ve 2000'lerin başında eski Doğu Blok'u ülkelerin ile Balkanlar'da yaşanan Renkli Devrim süreçlerinin de büyük etkisi söz konusu olmuştur.

Bu çerçevede Rusya Bugün (Russia Today / Rus Rossiaya Segodnya) Medya Topluluğu, 9 Aralık 2013 tarihinde Putin'in talimatıyla, RF'nin uluslararası enformasyon alanındaki faaliyetlerini yürütmek amacıyla kurulmuştur. Sputnik Multimedya Haber Grubu ise 10 Kasım 2014 tarihinde Rossiaya Segodnya'nın bünyesinde Rusya'nın Sesi ve RIA Novosti Haber Ajansları'nın birleştirilmesi ile tesis edilmiştir. Gerçekte ise Sputnik'in kuruluş nedeni, RF'nin bir enformasyon savaşı hamlesi olarak, Batılı medya organlarının tek taraflı ve hegemonik yayınlarına karşı Moskova'nın yanıtı olarak değerlendirilebilecektir.

Hem haber ajansı hem de radyoyu kapsayan bir medya ağı şeklinde yapılandırılan Sputnik, faaliyet gösterdiği ülkelerde geniş bir yerel ofis ağı tesis etmek şeklinde örgütlenmiştir. Bu kapsamda Sputnik, Türkiye örneğinde; bir internet haber portalı, etkin bir şekilde kullanılan sosyal medya ağı ve İstanbul, Ankara, İzmir, Antalya ve Bursa merkezli olarak faaliyet gösteren radyo istasyonları şeklinde yapılandırılmıştır. Sputnik evrensel düzeyde ise Sputnik markası altında faaliyet gösteren, İngilizce, İspanyolca, Çince ve Arapça haber merkezleri, multimedya içerikle desteklenecek olan ve Rusça, Türkçe, Abhazca, Afganca, Almanca, Arapça, Azerice, Ermenice, Gürcüce, Fransızca, Kazakça, Kırım Tatarca, Kırgızca, Çince,Kürtçe,Letonyadili, Moldova dili, Tacikçe, Lehçe,Farsça, Portekizce, Sırpça, Özbekçe, Ukraynaca, Fransızca, Hintçe, Estonya dili ve Japonca haber yayın akışları ile İstanbul,Londra, Washington,Yeni Delhi, Kahire, Montevideo, Pekin,Berlin, Riode Janeiro, Paris, Buenos Aires, Belgrad, Helsinki, Minsk, Kiev, Taşkent,

Astana, Bişkek, Duşanbe, Sohum, Tshinvali, Tiflis,Erivan, Bakü ve Kişinev'de bulunan yerel haber ofisleri şeklinde organize olmuştur.

Görülüğü üzere yerel unsurlarla entegre bir şekilde, küresel ölçekte de geniş bir örgütlenme ile dizayn edilmiş olan Sputnik'in faaliyetleri ile ilgili olarak, Rusya Bugün Genel Müdürü Dmitri Kisyelev:*"Bugün hem Batı'ya hem de Doğu'ya kendi isteklerini empoze etmeye çalışan birtakım devletlerin müdahil olduğu coğrafyalarda yıllarca sürecek iç savaşların tohumları atılarak oluk oluk kan akmasına sebep olunuyor. Renkli Devrimler ile devletler yıkılmakta; tıpkı Irak, Libya, Gürcistan, Ukrayna ve Suriye örneklerinde olduğu gibi… Artık pek çok insan bu olaylarda Amerikalılar gibi düşünmenin ve olayları onların penceresinden değerlendirmenin bir zorunluluk olmadığını anlamış durumda. Rusya söz konusu şartlarda insanlığın yararına olacak yeni bir model öneriyor; biz çok renkli bir dünya düzeninden yanayız ve bu hususta bizimle fikir birliği yapan birçok müttefikimiz de bulunmakta. Bu sebeple medya grubumuz, yeni bir dünya markası olan Sputnik'i yaratmıştır. Sputnik, her ülkenin kendi ulusal önceliklerinin, geleneklerinin, kültürünün ve tarihinin ön planda olduğu çok kutuplu bir dünya düzeninin aynası olacaktır. Bizim çok uluslu ve çok kutuplu medeniyet anlayışımızda Japonya*'da *Japon, Türkiye'de Türk, Çin*'de *Çinli ve Rusya'da Rus olarak yer almaktadır. Biz hiç kimseye Rusya'nın ulusal menfaatlerine uygun olan bir yaşamı empoze etmeye çalışmıyoruz. Bize göre her millet kendi değerleri doğrultusunda yaşam hakkına sahiptir ve böyle bir dünya düzeninin temel dinamiği de uluslararası hukuktur. Mevcut küresel düzende bugün devam etmekte olan yeniden şekillendirme süreci insanlığın yararına olacaktır. Faaliyet gösterdiğimiz hiçbir ülkede muhalif bir medya kuruluşu anlayışı ile çalışmıyoruz. Objektif yayın anlayışına uygun olarak toplumun tüm kesimleri ile eşit mesafede ve iyi ilişkiler kuruyoruz. Sputnik'in yayını tamamen yurtdışındaki izleyici kitlesine yönelik olarak hazırlandı.*"şeklinde beyanda bulunmuştur. Bu beyanda da açıkça vurgulandığı üzere, RF'nin Sputnik'in yayın sistematiği ile hedeflediği amacın, küresel ölçekte ABD başta olmak üzere Batı karşıtlığı temelinde, etkili, yerel unsurlarla uyumlu, iyi örgütlü bir propaganda mekanizmasını siber güvenlik stratejisin bir parçası olarak geliştirmek olduğu açıktır.[458]

[458]Ayrıntılı bilgi için bkz. Milliyet Gazetesi, **Rusya'dan Medya Atağı**, http://www.milliyet.com.tr/rusya-dan-medya-atagi/dunya/detay/1968251/default.htm, (21.04.2016)

RF'nin siber güvenlik stratejisinde Sputnik, adeta bir enformasyon savaş aparatı olarak dizayn edilmiştir. Bu itibarla Sputnik'in geleneksel Sovyet propaganda tekniklerinin dışında, Kremlin'in doğrudan sesi olmak yerine, hedef alınan her ülkeye özgü olarak, Rus çıkarları doğrultusunda kafa karıştırıcı, yanıltıcı ve yönlendirici ve manipüle edici bir yayın akışı benimsediği de ifade edilebilecektir. Yani Sputnik bahse konu yayın akışı ile Kremlin'in bir nevi "medya silahı" olarak görülebilir.[459]

Ukrayna krizi kapsamında değerlendirildiğinde Sputnik'in, RF'nin ortaya koyduğu hibrit savaş yönteminin propaganda ayağını önemli ölçüde üstlendiği görülmektedir. Ukrayna müdahalesinden çok önce, Sputnik'in Ukrayna hükümeti aleyhine ve bölgedeki Rus azınlığı da kışkırtacak şekildeki bir yayın akışına ağırlık verdiği açıktır. Fakat bu durum bahse konu dönemde, ÇHC ile Asya-Pasifik'te güç mücadelesi sürdüren, Suriye sorununa angaje olan ABD ile göçmen krizi ile boğuşan AB üyesi ülkeler tarafından yeterince anlaşılamamıştır.[460]

Benzer bir durum, Suriye iç savaşı esnasında Sputnik tarafından sürdürülen yayın politikası içinde geçerlidir. İç savaşın ilk yıllarından bu yana Sputnik Esad rejimine doğrudan destek vererek, Esad rejiminin adeta küresel ölçekteki sesi olmuştur.

Türkiye'nin 24 Kasım 2015 tarihinde sınır ihlali yapan RF'ye ait bir savaş uçağını düşürmesi sonrasında ise Suriye'ye yönelik artan RF'nin askeri desteği esnasında da bu yayın politikası özellikle, Türkiye'nin cihat yanlısı Selefi ve Tekfiri gruplara yardım ettiği şeklindeki agresif bir yıpratma propagandasına dönüşmüştür. Hatta Sputnik Adalet ve Kalkınma Partisi (AK Parti) aleyhtarlığını merkeze koyarak, sosyal medyadaki imkânlardan da istifade etmek suretiyle Türkiye'ye yönelik olumsuz yayın politikasını 2016 Mart ve Nisan aylarında zirveye çıkarmıştır. Bu noktada Sputnik'in 1 Nisan 2016 tarihli maksatlı ve yönlendirici *"BM'ye Türkiye-IŞİD bağlantısını gösteren belgeler..."*[461] başlıklı haberinin, Türkiye'de bazı medya gruplarınca kullanılma şekli dikkat çekici görülebilecektir. Bunun bir sonucu olarak da Türkiye'de Sputnik'in internet sayfasının ve

[459]LUCAS Edward and NIMMO Ben, **Information Warfare: What Is It and How to Win It**, Center for European Policy Analysis (CEPA), http://cepa.org/sites/default/files/Infowar%20Report.pdf, (20.04.2016), p. 1.
[460]Ibid., p. 2
[461]Sputniknews Haber Portalı, **BM'ye Türkiye-IŞİD bağlantısını gösteren belgeler...**,http:// tr.sputniknews.com/rusya/20160401/.../rusya-bm-turkiye-isid.html, (15.04.2016).

sosyal medya hesaplarının erişimi engellenmiş[462] ve Sputnik Türkiye Genel Müdürü Tural Kerimov'un da Türkiye'ye girişi 26 Nisan 2014 tarihinde yasaklanmıştır.[463]

Sputnik'e yönelik yayın yasağına yönelik tedbirler ise 15 Temmuz 2016 darbe girişimi sonrasındaki süreçte, Cumhurbaşkanı Recep Tayyip Erdoğan'ın RF'ye yapacağı ziyaretin hemen öncesinde, iki ülke arasında gerginleşen ilişkilerin iyileştirilmesine yönelik Türkiye'nin arzusunu ifade eden bir jest olarak, 8 Ağustos 2016 tarihinde kaldırılmıştır.[464]

Sputnik ve diğer RF medya kuruluşlarının Türkiye'ye yönelik olarak başlattığı enformasyon savaşının bir başka ayağı ise bahse konu medya kuruluşlarının yerel unsurlarla işbirliği yaparak, kendi yayın akışına uygun politikacıları, siyasi analistçileri, gazetecileri ve sosyal medyayı manipüle etmesi amacıyla da paralı trolleri[465] kullanması şeklinde planlanmıştır.[466] Bu kapsamda özellikle AK Parti ve Cumhurbaşkanı Recep Tayip Erdoğan karşıtlığı temelinde birleşen Türkiye'deki muhalif bazı çevreler bilerek veya bilmeyerek, Rus medya kuruluşları tarafından sürdürülen bu yayın politikasının birer vasıtası haline gelmişlerdir. Bu itibarla bahse konu dönemde "Fuat Avni" takma adlı twitter hesabından yapılan ve RF'nin söz konusu iddialarını[467] manipülatif bir tarzda ele alan kimi paylaşımlar[468] dikkat çekicidir.

---

[462]Anadolu Ajansı, **Sputnik ve DİHA'ya erişim engeli talebi onaylandı.**, http://aa.com.tr/tr/turkiye/sputnik-ve-dihaya-erisim-engeli-talebi-onaylandi-/555880, (20.04.2014).

[463]HaberTürk İnternet Haber Portalı, **Kerimov'a Yasak**, http://www.haberturk.com/gundem/haber/1227586-sputnik-turkiye-genel-muduru-tural-kerimova-giris-yasagi, (20.04.2014).

[464]Ayrıntılı bilgi için bkz. Sputniknews Haber Portalı, **AA: Sputnik'e Erişim Engeli Kaldırıldı.**,https://tr.sputniknews.com/turkiye/201608081024268110-sputnik-tib-erisim-engeli/ , (03.01.2017).

[465]Trol: İskandinavya folklorunda genellikle dev ya da cüce olarak resmedilen, mağaralarda yaşayan efsanevi, çirkin bir yaratıktır. *"İnternet trollüğü"*: insanları tahrik ederek ve kızgınlıkla yazılmış cevaplar vereceklerini umarak, e-postaveya çevrimiçi grup mesajları göndermek şeklinde tarif edilir. Trol olarak faaliyet gösteren şahıslar, internet ve sosyal medya ortamında kasıtlı olarak karşısındaki kişinin ya da toplumun insan doğasından kaynaklanan zayıf noktalarını istismar edip, keyfini kaçırmaya ve işlerini aksatmaya çalışabilirler.

[466]Ayrıntılı bilgi için bkz. Lucas ve Nimmo, op. cit., ss. 8-12.

[467]Ayrıntılı bilgi için bkz. Sputniknews Haber Portalı, **Fuat Avni, Rus Uçağının Düşürüleceğini Nereden Biliyordu?**, https://tr.sputniknews.com/columnists/201607241024055041-Rus-ucagi-darbe-pilot/, (08.11.2016).

[468]Ayrıntılı bilgi için bkz. Birgün Net, **WikiLeaks, Fuat Avni'nin Rus Uçağı İddiasını Paylaştı**,http://www.birgun.net/haber-detay/wikileaks-fuat-avni-nin-rus-ucagi-iddiasini-paylasti-97073.html, (08.11 2016).

Yine benzer şekilde Halkın Demokrasi Partisi (HDP) tarafından AK Parti ile IŞİD irtibatına yönelik olarak RF iddialarını temel alan ve Türkiye Büyük Millet Meclisi (TBMM)'ne taşınan kimi soru önergeleri[469] ile bu konuda HDP'li milletvekilleri tarafından verilen beyanatların da bu kapsamda önemli örnekleri oluşturduğu ileri sürülebilir.[470]

Bununla birlikte RF'nin enformasyon savaşı stratejisinde, sosyal medya olanaklarının da etkili bir siber propaganda enstrümanı olarak kullanılmakta olduğu görülmektedir. Bu itibarla örneğin RF tarafından, sosyal medyanın "uçak düşürme" krizi esnasında ve sonrasında etkili bir enformasyon savaş yöntemi olarak seçilmesinde, sosyal medya olanaklarına ulaşmanın herkes için kolay, hızlı, anonim, önemli oranda propaganda materyalini aynı anda ve çok kısa sürede yönlendirme kabiliyetine sahip ve coğrafi sınır tanımayan yapısı etkili olmuştur.[471]

RF'nin Türkiye ile ilişkileri kapsamında sosyal medya imkânlarının kullanılması, RİS ile irtibatlı kuvvetli ve etkili bir troll ve blogger ağının çeşitli ulusal ve uluslararası sosyal medya platformlarında (Yandex.com, Youtube.com, Facebook.com, VKontakte.ru, Odnaklassniki.ru, Twitter.com, Yaptriot.ru, Whowho.com.ua, Novorus.info, Novorossia.ru vb.) Türkiye'nin Suriye'de bulunan DAEŞ unsurlarıyla irtibatlı olduğunu gösteren dezenformasyon haberlerinin profesyonel imkânlar la hazırlandığı belli olan görsel dokümanlar ile birlikte Rus ve dünya kamuoyuna servis etmesi şeklinde planlanmış ve geliştirilmiştir. Örneğin 24 Kasım 2015 tarihi sonrası dönemde RF'de gerçekleştirilen sosyal medya paylaşımlarında Putin'in konuyla ilgili ifade ettiği *"sırtımızdan bıçaklandık"* ifadesi uzun bir süre en çok konuşulan olaylar arasına yer almıştır.

Bu dönemde Türkiye'ye gitmeme çağrıları, "*Terörist Türkiye*" mesajları ve Cumhurbaşkanı Recep Tayyip Erdoğan'ın DAEŞ'e yardım ederken gösterildiği çizimler sosyal medyada sıklıkla paylaşılmıştır.[472] Yine benzer şekilde bu dönemde Rus sosyal

[469]Ayrıntılı bilgi için bkz. Sputniknews Haber Portalı, **HDP'li Kürkçü Yanıt Alamadığı IŞID Petrolü Sorusunu Yeniden Sordu**, https://tr. sputniknews.com/turkiye/201603301021838524-hdp-isid-turkiye-petrol-rt-belge/, (08.11.2016).
[470]Ayrıntılı bilgi için bkz. Sputniknews Haber Portalı "**Demirtaş: AKP Terör Üreticisi, IŞİD'in Siyasi Uzantısı**", https://tr.sputniknews.com/politika/201602201021016742-demirtas-akp-isid/, (08.11.2016).
[471]NATO Communications Centre of Excellence, "**Social Media as a Tool of Hybrid War**", http://www .stratcomcoe.org/social-media-tool-hybrid-warfare, (19.10.2016), s. 24.
[472]Birgün Net, **Rusya'nın Savaş Uçağının Düşürülmesi Üzerine Sosyal Medyada Tepki**,http://www. birgun.net/haber-detay/rusya-nin-savas-ucaginin-dusurulmesi-uzerine-sosyal-medyada-tepki-95978.html, (08.11.2016).

medyasında Türkiye, AK Parti ve Cumhurbaşkanı Recep Tayyip Erdoğan aleyhine hazırlanmış sosyal medya görsellerinin paylaşımında adeta bir patlama yaşanmıştır.[473]

Diğer yandan söz konusu sosyal medya paylaşımları ile uyumlu şekilde ulusal Rus medyası da konuyu provokatif bir yayın politikası ile ele alarak, adeta körüklemiştir. Bu itibarla konu Vedomosti Gazetesi tarafından; "*Türkiye Rusya'yı sırtından vurdu. Rusya bu işi sonuçsuz bırakmayacak*", Komsomolskaya Pravda tarafından; "*Biz bir ay önce Cumhurbaşkanı Erdoğan'ın Rus uçağı vurmaya hazırlandığını yazmıştık*", İzvestiya Gazetesi tarafından; "*Bizim uçak Türkiye'yi tehdit etmiyordu. Sırtımızdan vurdular*", Moskovskiy Komsomolets Gazetesi tarafından; "*Ankara savunmaya geçti. Vurulan savaş uçağında kime ait olduğuna işaret eden tanıtıcı işaretler bulunmadığını söylüyor*" şeklindeki manşetlerle gündeme getirilmiştir.[474]

Ulusal ve uluslararası Rus medyasında yer alan söz konusu haberler, sosyal medyada yapılan olumsuz paylaşımlar ile birlikte, Türkiye kısa sürede yapılan tehdit değerlendirmesi anketlerinde Rus halkı gözünde "*1 Numaralı Düşman Ülke*" konumuna ulaşmıştır. Türkiye'ye yönelik bahse konu enformasyon savaşının arka planın da yer alan neden ise Putin'in uçak düşürülmesi olayını fırsata çevirerek, iç politika da güç kazanmak amacıyla Rus toplumunda ki tarihi Türk düşmanlığını körüklemek istemesi şeklinde de değerlendirilebilecektir.[475]

Görüldüğü üzere RF'nin Soğuk Savaş sonrası dönemde, özellikle de 2000'li yılların başı itibarıyla gerek ordusunu ve istihbarat birimlerini gerekse de kurumsal yapılarını siber uzayın sağladığı yeni imkânlar kapsamında etkili bir siber saldırı kapasitesine sahip olmak amacıyla yeniden organize etmeye çalıştığı, bu organizasyonu kapsamında da yeni nesil enformasyon savaşı planlamalarına özel önem verdiği ortadadır. RF'nin yaklaşık on yıldır planlı bir şekilde geliştirdiği siber saldırı kapasitesinin en önemli ayağı olan yeni nesil siber propaganda imkânları, Soğuk Savaş döneminde enformasyon savaşı alanında SSCB tarafından ortaya konulan stratejinin çok ötesinde, artık oldukça sofistike niteliktedir.

---

[473]WeirdRussia Haber Portalı, "**How Social Media Users Responded to Turkey's downing of Russian warplane**", http://weirdrussia.com/2015/11/26/how-social-media-users-responded-to-turkeys-downing-of-russian –warplane /, (08.11.2016).

[474]Hürriyet Gazetesi,**Uçak Krizi Dünya'da Manşet**, http://www.hurriyet.com.tr/ucak-krizi-dunyaya-manset-40018345, (08.11.2016).

[475]Ayrıntılı bilgi için bkz. YILMAZ Salih, **Rusya Neden Suriye'de?**, Yazar Yayınları, Ankara, 2016, ss. 261-267.

Bu kapsamda, iddia edildiği üzere RF'nin 2007 yılında Estonya'nın bilişim sistemlerini çalışamaz hale getiren siber saldırılar ile konvansiyonel bir savaşın etkilerini propaganda ile desteklediği; 2008 yılındaki Gürcistan Savaşı esnasındaki siber faaliyetleri; akabinde meydana gelen 2008 yılındaki Litvanya'ya, 2009 yılındaki Kırgızistan'a yönelik siber saldırıları ile 2014 Ukrayna Müdahalesi esnasında ortaya koyduğu *"yeni nesil"* savaş konsepti ve uçak düşürülmesi krizi sonrasında 2015 Aralık ayında Türkiye'ye yönelik *"DDoS"* atakları ile birlikte uygulama koyduğu enformasyon savaşı stratejisi bu devletin siber uzaydaki kapasitesini göstermesi bakımından kayda değer örneklerdir.

RF'nin enformasyon savaşı alanındaki güçlü ve agresif rolü, Türkiye ile yaşadığı "*uçak düşürme*" krizi esnasında net bir şekilde gözlemlenebilmiştir. Türkiye örneğinde de görüldüğü üzere, RF'nin enformasyon savaşını modern güvenlik stratejisinin merkezine koyduğu açıktır. Bu stratejik yaklaşımın bir sonucu olarak, RF merkezli medya kuruluşlarının, etkili ve yaygın bir sosyal medya ağıyla dünyanın her hangi bir bölgesinde ve o bölgedeki her bir ülkede farklı bir enformasyon savaşı yaklaşımı gösterebilme kapasitesine sahip oldukları da ortadadır.

Bu kapsamda RF'nin enformasyon savaşı stratejisinin sahip olduğu esnek yapısı ile birlikte, takip edilen politik amaçlara uygun bir şekilde Baltık ülkelerinde Rus azınlıkları destekleyebilmekte ve Sovyet dönemi nostaljisi ile eski parlak günlere göndermeler yapabilmektedir. Benzer şekilde söz konusu enformasyon savaşı kapasitesi ile RF, Türkiye'de AK Parti muhalifi çevrelerle uyumlu yayınlar izleyebilmekte ve böylelikle AK Parti iktidarının toplum içindeki etkinliği yıpratabilmekte; Azerbaycan'da Türkiye aleyhtarlığı yapılarak Azeri Türklerine 2008-2009 yılları arasında yaşanan Türkiye-Ermenistan yakınlaşmasını sürekli olarak hatırlatabilmekte; Slovakya ve Çek Cumhuriyeti'nde çevreci ve anti-militarist bir eğilimle yayın politikası belirleyebilmekte; Orta Asya'da Türkiye'nin Turancı politikalar sürdürdüğü ifade edilerek, sürekli olarak Türk ve Batı aleyhtarı haberlere yer verebilmektedir.[476]

Görüldüğü üzere RF'nin yeni nesil enformasyon savaşı planlamaları, çalışmamızın daha önceki bölümlerinde analiz ettiğimiz, Nye'nin siber güç kavramına ilişkin tanımlamasıyla paralellik içermektedir. Tekrar kısaca hatırlamak gerekirse "siber güç",

[476]Ayrıntılı bilgi için bkz. LUCAS ve NİMMO, op. cit., pp. 3-5.

Nye tarafından "*insan kaynağı ve yeteneği, yazılım ve donanım teknolojiler, altyapılar ve ağ teknolojileri ile ilgili tüm kaynaklar vasıtasıyla yaratılan bir imkân"* şeklinde tanımlanmakta ve siber güç kavramının neden olduğu değişim ve güç uygulamalarının ise hem yumuşak güç hem de sert güç kavramı ile ilgili olduğu ifade edilmektedir.

Bu kapsamda Nye açısından "*siber güç*"; diğer aktörleri etkilemek ve dikkatlerini çekmek için kullanılması halinde bu durum, yumuşak güç kavramı ile açıklanabilecektir. Örneğin Nye göre, siber imkânlar kaynaklı olarak elde edilen güç, ÇHC'de olduğu gibi 1930'lardan kalma bir ihtilâf nedeniyle öğrencileri internet üzerinden örgütleyerek Japonya aleyhine protesto gösterileri yapmaya sağlayabilmek ise yumuşak güç kapsamında değerlendirilmelidir. Diğer bir deyişle meşru ve demokratik yöntemlerle bir algı yaratılabilmesi amacıyla kullanılması halinde bir yumuşak güç uygulaması olarak görülmelidir.[477]

Bu noktada çalışmamızda detaylarıyla ve örnek vakalarla analiz edildiği üzere RF'nin yeni nesil siber propaganda sistematiğinin Nye'nin siber güç kavramına ilişkin bahse konu kavramsallaştırmalarıyla uyumlu bir şekilde dizayn edildiği iddia edilebilecektir. Bu kapsamda RF'nin modern enformasyon savaşı enstrümanları yerel imkânlardan, sosyal medya merkezli sofistike uygulamalardan, troll unsurlardan ve küresel ölçekte yayın yapan medya yapılanmalarından güç alarak; hedef toplumu, kitleyi, bireyleri ve devletleri meşru, demokratik, barışçıl yöntemler ile manipüle etmeyi ve RF'nin ulusal çıkarları kapsamında etkilemeyi hedeflemektedir.

Öte yandan ABD'nin, RF'nin sofistike ve modern teknikler ile yeniden organize ettiği yeni nesil enformasyon savaş stratejisine karşı tedbirler geliştirme noktasında görece olarak ağır kaldığı da iddia edilebilecektir. Diğer bir deyişle muazzam teknolojik ve ekonomi gücüne karşı ABD'nin RF'nin modern enformasyon stratejisine karşı koymada zorlandığı açıktır. ABD'nin RF'ye karşı enformasyon alanındaki rekabette nispeten gerilemesinin temel nedeni ise ABD'nin federal sisteminin yanı sıra RF'ye kıyasla görece daha demokratik bir sisteme sahip olması çerçevesinde yazılı, göresel ve sosyal medya ile internet alanını düzenleyici, denetleyici ve manipüle edici ulusal yasaları tanzim etmekte zorlanması ile açıklanabilir.

[477]NYE,"Gücün Geleceği", op. cit. p. 41.

Bu durum çok daha net bir biçimde Demokrat Parti Hack Skandalı ve Snowden Olayı kapsamında ifşa olmuş ve ABD'nin konuyla ilgili uzmanlarınca yapılan değerlendirmelerde de açıkça gündeme getirilmiştir. Bu kapsamda 15 Mart 2017 yılında ABD Kongresi'nde yapılan ve kimi siyasiler ile enformasyon savaşı alanında faaliyet gösteren bürokrat ve uzmanlarının katıldığı bir oturumda yapılan tartışmalarda, ABD'nin RF'nin modern enformasyon savaşı enstrümanlarına karşı koymada etkili bir strateji geliştirmede zorlandığı hususu net bir şekilde ifade edilmiştir. Bu itibarla bahse konu oturumda: [478]

-Gerek ABD hükümetlerinde görev alan üst düzey bir yetkilinin gerekse de sıradan bir ABD vatandaşının ABD'nin enformasyon stratejisinin ne şekilde oluşturulduğu ve koordine edildiğine dair her hangi bir bilgisi olmadığı, bu konuda tamamen bir boşluğun ve yetersiz planlamanın söz konusu olduğu;

-Demokrat Parti Hack Skandalı'nın da ortaya koyduğu üzere, ABD ulusal medyasındaki bazı çevrelerin bilerek veya bilmeyerek RF kaynaklı dezenformasyon faaliyetlerinin toplumun tüm katmanlarına ulaşmasına yardımcı oldukları, buna karşı tedbirler alınması gerektiği;

-Enformasyon alanındaki rekabetin yeni nesil bir çatışma alanı olarak kabul edilmesinin şart olduğu;

-Soğuk Savaş'ın sona ermesi ile kapatılan ve bu dönemde SSCC kaynaklı propaganda faaliyetlerine karşı etkili karşı koyma faaliyetleri yürüten ABD Enformasyon Ajansı (United States Information Agency)[479] ile Aktif Tedbirler Çalışma Grupları (Active Measures Working Groups)'nın[480] yeniden organize edilmesi gerektiği;

---

[478]GERTZ Bill, **U.S. Losing Global Information War**, http://freebeacon.com/national-security/u-s-losing-global-information-war/, (03.06.2017).

[479]ABD Enformasyon Ajansı (United States Information Agency);1953-1999 yılları arasında küresel düzeyde SSCB'nin potansiyel olarak etkisi altına bileceği ülkelerde eğitim ve kültürel faaliyetler organize etmek amacıyla tesis edilmiş bir kurumsal yapılanmadır. Ayrıntılı bilgi için bkz; http://dosfan.lib.uic.edu/usia/, (03.06.2017).

[480]Aktif Tedbirler Çalışma Grupları (Active Measures Working Groups); Soğuk Savaş döneminde küresel düzeyde SSCB kaynaklı dezenformasyon faaliyetlerine karşı koyma çalışmaları yürüten, bu alanda gerekli hallerde NATO üyesi devletlerde yerel ofisler açabilen, istihbarı ve gizli faaliyet prensiplerine uygun planlamalar da yürütebilen kurumsal yapılanmaladır. Ayrıntılı bilgi için bkz: https://www.lawfareblog.com/active-measures-working-group, (03.06.2017).

-Sahip olduğu bütçe imkânları ve yasal yetkileri nedeniyle ABD Savunma Bakanlığı'nın özellikle de Pentagon'un ABD'nin yeni nesil enformasyon stratejisinin oluşturulmasında etkili bir rol oynayabileceği;

-ABD'nin tüm bu öngörülen propaganda stratejilerini tek elde planlayacak ve koordine edecek olan, ayrıca da Soğuk Savaş dönemi tecrübelerinden beslenen ve yeni teknikler ile donatılmış dijital bir enformasyon ajansı kurmasının şart olduğu, bu kurumsal yapılanmanın da doğrudan Ulusal İstihbarat Direktörü / Director of National Intelligence (DNI)'ne karşı sorumlu olarak faaliyet yürütmesi gerektiği hususları gündeme getirilerek, ABD hükümetine tavsiye olarak sunulmuştur.

ABD'nin küresel düzeyde RF'nin yeni nesil enformasyon stratejisine karşı müttefikleri ile birlikte almayı planladığı olası tedbirler ise bazı analiz ve değerlendirme raporlarında detayları ile tartışılmaktadır. Söz konusu potansiyel tedbirler ise ana hatlarıyla aşağıda yer aldığı şekilde özetlenebilir.

-Günümüz propaganda teknikleri Soğuk Savaş dönemine göre son derece sofistike ve karmaşıktır. Bu nedenle ABD küresel düzeyde etkili bir enformasyon stratejisi geliştirmek için müttefikleri ile işbirliği halinde çalışmalı, sosyal medya olanaklarından yararlanmalı, yaratıcı ve esnek bir yapılanma tesis etmelidir.[481]

-RF'nin enformasyon stratejisi temelde Batı'nın kendi içindeki anlaşmazlıklarından istifade ederek, RF'yi bir alternatif olarak üçüncü taraflara sunmak şeklinde dizayn edilmektedir. Bu dizayn dahilinde anti-emperyalist ve özgürlükçü bir tutum içinde olunmasına da özel önem verilmektedir. Bu duruma karşı etkili tedbirler geliştirilmesi önemlidir.

-Söz konusu etkili tedbirlerin ise temelde sosyal medya imkânlarından azami istifade etmesi, uluslararası bir medya yapılanmasının yayınları ile desteklenmesi, küresel düzeyde Rusça konuşan halkları, anti-Amerikan tutum içinde olan aşırı sağ ve sol grupları

[481]LUCAS Edward and POMERANTSEV Peter, **Winning the Information War**, Center for European Policy Analysis (CEPA), http://cepa.org/reports/winning-the-Information-War, 03.06.2017, p. 44

hedeflemesi, ayrıca da taktiksel (kısa vade / reaktif), stratejik (pro-aktif / orta vade), uzun vadeli bir planlama ile hazırlanması gerekmektedir.[482]

-Küresel düzeyde oluşturulacak olan analiz birimleri ile lokal sosyal medya trendleri, sıradan bireylerin iletişim öncelikleri ve yerel medya kurumlarının yayın akışları takip edilerek, genel eğilimleri tespit edilmeli ve buna uygun yayın politikaları geliştirilmelidir. Bu noktada yerel sivil toplum kuruluşları ve iletişim kurumlarıyla işbirliğine özel önem verilmelidir. Bahse konu taktiksel planlamalar RF'nin 2014 Ukrayna müdahalesi öncesinde lokal birimleri manipüle ederek tesis ettiği propaganda stratejisi örnek alınarak oluşturulabilir.[483] Tüm bu tedbirler ise bahse konu taktiksel (kısa vade / reaktif) ve planlamalar başlığı altında ele alınmalıdır.

-Stratejik (pro-aktif / orta vade) tedbirler kapsamında, özellikle RF'nin etki altına almak istediği Orta Asya, Doğu Avrupa ve Balkan ülkelerindeki ulusal medya üzerindeki tekel oluşumların etkisi kırılmalıdır. Bu noktada Fox Medya ve CNN International'ın yerel medya gruplarıyla ile işbirliği tesis ederek açtığı yerel televizyon kanallarının desteklenmesi ve sayılarının artırılması önemlidir. Ayrıca "*sızıntı gazeteciliği, blogger yayıncılığı, youtuber'lık, internet haberciliği*" gibi alternatif gazetecilik yaklaşımları ile etkili bir enformasyon stratejisi geliştirilmelidir. Bu tür alternatif gazetecilik oluşumlarının yayınlarının Rusça konuşan hedef kitlesinin ihtiyaçlarına uygun olarak ve Rusça hazırlanması önemlidir. Bu kapsamda yeni bütçe imkânlarının da tahsis edilmesine gayret edilmelidir.[484]

-Uzun vadeli bir tedbir olarak, planlanmakta olan söz konusu taktiksel çalışmaların sıradan bireylere tesir edebilmesi amacıyla başta ABD ve Avrupa olmak üzere küresel düzeyde RF propagandasının hedefi olan coğrafyalarda sıradan bireylerin medya okur-yazarlığı ve takip alışkanlıklarının artırılması gerekmektedir.[485]

---

[482]Ibid, p. 45.
[483]MediaSapiens, **Evaluation of the effectiveness of the authorities in the field of information security**, 2014-15,http://osvita.mediasapiens.ua/trends/1411978127/otsinka_efektivnosti_diy_organiv_vladi_v_sferi_informatsiynoi_bezpeki_v_201415 _rr/, (03.06.2017).
[484]Ayrıntılı bilgi için bkz. LUCAS ve POMERANTSEV, op. cit., pp. 49-50.
[485]Ayrıntılı bilgi için bkz. NATO Communications Centre of Excellence, **Social Media as a Tool of Hybrid War**, http://www .stratcomcoe.org/social-media-tool-hybrid-warfare, (19.10.2016).

-Yine uzun vadeli bir tedbir olarak, ABD ve Batı medyasında toplumsal grupların bazılarını öteleyici niteliğe sahip, özellikle de nefret söylemi içerikli yayınlara son verilmelidir. Bu kapsamda özellikle "*İslamofobia*" körükleyen yayınların RF'nin Batı toplumlarını hedef alan ve Batı toplumu içindeki sorunları kışkırtıcı mahiyetteki yayınlarının etkisini artırdığı dikkate alınmalıdır.[486]

5. ABD ve RF'nin Siber Güvenlik Alanında Faaliyet Gösteren Kurumsal Yapılarının Analizi

Siber güvenlik strateji belgelerindeki mevcut duruma benzer şekilde federal sisteminin yapısı gereği, ABD'nin siber güvenlik alanında faaliyet gösteren kurumsal örgütlenmeler federal ve eyaletler düzeyinde farklılıklar arz etmektedir.

Bu bağlamda ABD'nin resmi siber organizasyonu oldukça karmaşık bir yapıya sahip olduğu rahatlıkla ifade edilebilir. Bu karmaşık yapı ABD'nn federatif yönetim anlayışı ile şekillenen adem-i merkeziyetçi idare şekliyle doğrudan ilintileridir. Bu kapsamda ABD'nin resmi siber organizasyonu temelde aşağıda belirtildiği biçimde üçlü bir yapıya sahiptir.

- *ABD Savunma Bakanlığı (United States Department of Defense),*

- *ABD İç Güvenlik Bakanlığı (The Department of Homeland Security),*

- *ABD Gizli Servisleri (FBI / CIA),*

Bunun dışında, bazı resmi kurumların kendi görev sahalarına yönelik olarak yetki ve sorumlulukları da bulunmaktadır. Ayrıca, eyalet yönetimleri, ulusal siber güvenlik ağı haricinde, kendi siber güvenliklerini sağlamak amacıyla çeşitli yapılanmalar da kurarak, bu yapılardan aktif olarak istifade etmeyi de tercih etmektedirler.[487]

Örneğin ABD Savunma Bakanlığı, ABD'nin siber güvenlik stratejisinin uygulanmasında etkin bir role sahiptir. Savunma Bakanlığı bünyesinde siber güvenlik alanında en etkili rolü, STRATCOM bünyesinde faaliyet gösteren ve 2010 yılında kurulan CYBERCOM üstlenmektedir. ABD Savunma Bakanlığı bünyesinde siber güvenlik

[486]Ayrıntılı bilgi için bkz. LUCAS ve POMERANTSEV, op. cit., pp. 51-55.
[487]TIRRELL, op. cit., p. 55.

alanında faaliyet gösteren bir diğer kuruluş ise NSA'dır. NSA, ABD'nin küresel izleme, şifre çözme, veri toplama, veri analizi, sinyal toplama, çeviri ve yabancı istihbaratlara karşı istihbarat yapma amaçları için tesis ettiği istihbarat kuruluşu ve örgütüdür. NSA, ayrıca ABD'nin ağ savaşları kapsamındaki haberleşme ve bilgi veri sistemlerinin korunmasından da sorumludur.[488] NSA'nın elektronik sistemleri dinlemek için edindiği misyonunu, gizli yöntemler ve subversif yazılım araçları ile sistemleri sabote edecek şekilde kullandığı da iddia edilmektedir.

DHS, ABD'nin İç Güvenlik Bakanlığı olarak 11 Eylül 2001 saldırılarından sonra kurulan ve terörle mücadele konusunda asıl görevli olan devlet kurumudur. ABD Kongresi tarafından 2002 yılında çıkartılan "Kamu Güvenlik Yasası" ile kurulmuştur. Bu kanun, ABD İç Güvenlik Bakanlığı'nın da kurucu belgesidir. Söz konusu kanuna göre; "*İç Güvenlik (Homeland Security), ABD içinde gerçekleşmesi muhtemel terörist saldırıları önlemek, Amerika'nın terörizm konusundaki güvenlik açıklarını (kırılganlıklarını) azaltmak, saldırı olduğunda ise bu saldırıdan dolayı meydana gelen zararları azaltmak ve en kısa sürede onarmak için ulusal imkân ve çabaları bir araya getirmek*" şeklinde tanımlanmaktadır.[489] ABD İç Güvenlik Bakanlığı'nın siber güvenlik alanındaki amaçları ise *"kritik altyapıları korumak, kritik öneme haiz altyapı yatırımlarını ve hayati öneme haiz kaynaklarının direncini güçlendirmek, hükümetin iletişimini ve operasyonel gücünün devamlılığının sağlamak, ulusal siber güvenlik şartlarını ilerletmek"* şeklinde belirlenmiştir.[490]

DHS organizasyon şeması ele alındığında, ülke genelinde 7/24 esasına göre bir füzyon merkezi olarak görev ifa NICIC'in siber güvenlik alanındaki temel sorumlu birim olduğu görülmektedir. DHS bünyesinde siber güvenlik alanında görev yürüten diğer birimler ise US-CERT ve ICS-CERT'dir. Bu takımlar ve servisler 7/24 esasına göre, ülke genelindeki siber saldırıları takip eden operasyonel birimler şeklinde organize edilmiştir. DHS, ABD siber savunma planlamasının şekillenmesinde, önemli bir eşgüdüm merkezi olarak da görev yapar. Bu itibarla DHS, istihbarat ve güvenlik servisleri ile gelecek

[488]National Security Agency, **60 Years of Defending Our Nation**, http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf, (30.05.2016).
[489]BAŞA Şafak, **ABD İç Güvenlik Bakanlığı**, file:///C:/Users/tk44655/Downloads/ABD_IC_GUVENLIK_BAKANLIGI_SUNUM%20(1).pdf, (31.05.2016).
[490]Ibid.

dönemde meydana gelmesi muhtemel siber saldırıların mahiyeti, kaynağı ve organizasyonu ile ilgili duyumlarını paylaşmak, ABD Savunma Bakanlığı ile ülkenin ulusal siber güvenlik savunma sistematiğini geliştirmek, ABD Adalet Bakanlığı (United States Department of Justice) ile ABD'ye yönelik siber saldırıların faillerinin tespiti ve yargılanması sürecinde hukuk destek sağlamak ile sorumludur.[491]

DHS'nin ülke genelinde siber güvenliğin sağlanması amacına yönelik olarak etkin bir şekilde kullandığı sistemin adı ise NCPS'dir. NCPS, federal ağ sistemindeki siber saldırıları tespit ederek, etkisizleştirmek amacıyla sistemin partnerlerine NICIC ve NCSD uzmanları ile bilgi paylaşımı ve koordinasyon noktasında kanuni sorumluluklar yüklemektedir. NCPS'nin etkinleştirilmesini sağlamak amacıyla da "EINSTEIN" adı verilen bir yazılım kullanılmaktadır ve bu yazılım eksikleri ortaya çıkan yeni durumlar kapsamında sürekli olarak teste tabi tutulmaktadır. Böylelikle de bu yazılımın her seferinde daha sıkı kontrol unsurları getiren ve yenilenen üç yeni versiyonu bugüne kadar geliştirilmiştir.[492]

ABD'nin istihbarat alanında faaliyet gösteren iki önemli kuruluşu ise bilindiği üzere FBI ve CIA'dir. FBI, ABD'nin iç istihbarat ihtiyaçlarını karşılar ve diğer devletlerin ABD'ye yönelik casusluk operasyonları ile subversif faaliyetlerine karşı koyan en önemli istihbarat organizasyonu olarak görev ifade eder. Bu görevleri kapsamında, FBI, RF'nin FSB'si ile aynı işlevi gördüğü de ifade edilebilir. Bu itibarla örneğin RF'nin ABD'ye yönelik siber casusluk operasyonlarına karşı koymak, FBI'ın görevleri arasındadır.

FBI'ın ABD'nin siber güvenlik stratejisinin uygulanmasında; siber suçlulardan, devlet destekli unsurlardan ve terörist gruplardan kaynaklanan siber ataklara karşı koyma görev ve yetkisi kapsamında önemli rolü bulunmaktadır. Bu çerçevede FBI siber güvenlik ile ilgili yetki ve sorumluluklarını sürdürmek amacıyla, CNSS ve CCS şeklinde örgütlenmeler tesis edilmiştir. Bu örgütlemelerden CNSS, terörist gruplardan ve hasım devletlerden kaynaklanan siber saldırıları takip etmek, izlemek ve deşifre etmekten

[491]Department of Homeland Security, **National Cybersecurity and Communications Integration Center**, https://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2012-04-30%20Spring%20Conference-Meeting/2%20Lichtenfels%20DHS%20NCCIC%202.pdf, (31.05.2016).
[492]Ayrıntılı bilgi için bkz. Committee on Homeland Security and Governmental Affairs, **A Review of the Department of Homeland Security's Missions and Performance**, file:///C:/Users/tk44655/Downloads/Senator%20Coburn%20DHS%20Report%20FINAL%20(3).pdf, (31.05.2016), pp. 82-85.

sorumluyken, CCS ise adı suç kapsamında olan, ancak federal güvenliği tehlikeye düşüren siber suçlar ile mücadele etmektedir.[493] CCS ve CNSS'nin, söz konusu görevleri kapsamında diğer hükümet kurumları ile olan koordinasyonu ise NCIJTF aracılığıyla sağlanmaktadır. CNSS direktörü ise aynı zamanda NCIJTF'nin de başkanıdır ve siber güvenlik faaliyetlerinden sorumlu FBI direktör Yardımcısı'nın emrinde çalışmaktadır.[494]

CIA, ABD'nin ülke dışındaki istihbarat ihtiyaçlarını karşılayan ve belirlenen stratejiler kapsamında gizli faaliyetlerini planlayan servisi konumundadır. Bu itibarla CIA'in, RF'nin SVR'si ile aynı işlevi gördüğü de ifade edilebilir. Örneğin RF'nin Ukrayna'ya yönelik sürdürdüğü hibrit savaş konsepti kapsamındaki gelişmeleri istihbar etmek, yurtdışındaki gizli bir hedefe yönelik siber espiyonaj veya saldırı operasyonu planlamak CIA'in görev ve sorumluluğundadır. Bu noktada CIA tarafından organize edildiği ve 2010 yılında İran nükleer tesislerine yönelik olarak İsrail ile işbirliği yapılarak planlandığı iddia edilen "Stuxnet" atağı, CIA'in bu tür siber faaliyetlerine örnek olarak gösterilebilecektir. Hatırlanacağı üzere bu operasyon ile "Stuxnet" isimli gelişmiş virüs tarafından İran'ın nükleer tesisleri fiziksel hasara uğratılarak, İran'ın nükleer programını sürdürme süreci geciktirilmiştir.

ABD istihbarat sistemine benzer şekilde, Rus istihbarat yapılanmasının ana omurgasını iç istihbarat alanında faaliyet gösteren FSB ve dış istihbarat konularında faaliyet yürüten SVR üstlenmektedir. FSB ve SVR'nin söz konusu faaliyetlerinin yanı sıra Rus askeri istihbarat örgütü olan GRU'nun da RF'nin istihbarat operasyonların yürütülmesinde etkili bir rolü bulunmaktadır.

Daha ayrıntılı bir biçimde belirtmek gerekirse, FSB'nin ilk görevi ülke genelinde devlet güvenliği aleyhine sürdürülen faaliyetler hakkında istihbarat toplamaktır. Örneğin, RF'de ki ayrılıkçı Çerkez/Çeçen gruplarının, cihad yanlısı Selefi-Tekfiri terör örgütlerinin veya organize suç odaklarının faaliyetlerini izlemek, takip etmek ve haklarında istihbarat toplamak FSB'nin görevidir. FSB'nin bir diğer görevi ise RF'ye yönelik olarak sürdürülmekte olan espiyonaj faaliyetlerine karşı koymaktır. Bu karşı koyma faaliyeti kontr/espiyonaj çalışması olarak adlandırılır ve RF aleyhine dış istihbarat servisler

[493]Ayrıntılı bilgi için bkz. TIRRELL, op. cit., pp. 60-62.
[494]Ayrıntılı bilgi için bkz. Federal Bureau of Investigation, **Cyber Crime**, https://www.fbi.gov/about-us/investigate/cyber/ncijtf, (01.06.2016).

aracılığıyla sürdürülen subversif operasyonların da engellenmesi amacını içerir. Bu kapsamda RF'na yönelik siber saldırılara karşı koymak ve temelde ülkenin siber güvenliğini sağlamak, FSB'nin görevidir.[495]

FSB'nin siber güvenlik alanındaki diğer bir sorumluluğu ise ülke genelindeki Rus vatandaşlarının ve yabancıların telekomünikasyon iletişim bilgilerinin istihbar olunan bilgiler kapsamında takip edilmesidir. FSB, Rus GSM ve telekom şirketlerinin yasal bir zorunluluk olarak kurmak zorunda oldukları, RF'de ki internet ve anolog haberleşmesini takip eden ve bir nevi denetleme sistemi şeklinde tesis edilmiş olan SORM'un kontrolü görevini de üstlenmiştir. Bu noktada RF'nin SORM sisteminin, ABD'nin EINSTEIN sistemi gibi merkezi bir yapıda organize edilmesinin, her iki ülke askeri ve güvenlik bürokrasinin de siber güvenlik alanındaki faaliyetlerin etkinliğini daha fazla merkezi örgütlenmeler ile sağlama eğilimin de olmalarından kaynaklandığı ifade edilebilecektir. FSB, siber güvenlik alanındaki çalışmalarının yanı sıra diğer tüm faaliyetlerini de SVR ile koordinasyon içinde sürdürmektedir.[496]

SVR de KGB'nin devamı olarak RF'nin ülke dışındaki espiyonaj faaliyetlerini yürütmek amacıyla kurduğu dış istihbarat servisidir. SVR, RF'nin dış istihbarat ihtiyaçlarının karşılanmasında, GRU ile birlikte temel aktör konumundadır. SVR, hedef aldığı devlete yönelik askeri, siyasi, biyografik, ekonomik, sosyal, ulaştırma, iletişim, bilim ve teknoloji konularında istihbarat toplar. Siber güvenlik stratejisi açısından ise RF'nin bir devletin bilim ve teknoloji kapasitesini hedef alan siber casusluk operasyonlarını planlamak, SVR'nin görevleri arasındadır. SVR'nin yurt dışında, Belarus, Kazakistan, Tacikistan, Ermenistan, Kırgızistan, Suriye, Küba, Vietnam ile Güney Osetya, Abhazya, Kırım ve Transdinyester bölgelerinde GRU ile birlikte ortak kullandığı elektronik ve sinyal istihbaratı toplama merkezleri de mevcuttur.[497] Bu itibarla SVR'nin sahip olduğu bazı teknik altyapıların ABD'nin NSA yapılanması ile benzerlik içerdiği belirtilebilecektir.

GRU, RF Genelkurmay Başkanlığı'na bağlı olarak faaliyet gösteren askeri istihbarat teşkilatıdır. Daha öncesinde Sovyetler Birliği'nde Kızıl Ordu'ya bağlı olan GRU, RSK'nın

[495]Ayrıntılı bilgi için bkz. The Centre For Counterintelligence and Security Studies, **Russia's SVR/FSB/GRU Intelligence Services**, http://www.cicentre.com/?page=191, (27.03.2016).
[496]Ayrıntılı bilgi için bkz. STAAR R. Tocaso, "Russia's Security Services", **Mediterranean Quarterly**, Vol.15, Issue.1, 2010, pp. 1-10.
[497]HEICKERO, op. cit., p. 30

büyüklüğü kapsamında RF'nin en geniş sayı ve kapasiteli istihbarat teşkilatıdır. Siber güvenlik açısından GRU'nun temel görevleri Rus askeri kapasitesini hedef alan dış servis kaynaklı siber operasyonlara karşı kontr/espiyonaj faaliyeti yürütmek ve imkan bulunması halinde hedef ülkenin askeri kapasitesine yönelik siber casusluk operasyonları planlamaktır. Stratejik Füze Birlikleri'nin faaliyetlerinin sürdürülmesi, ayrıca ülkeye yönelik siber saldırlara karşı koymak üzere kurulmuş olan RE-CURT'lerin kontrolü de GRU'nun diğer Rus istihbarat ve güvenlik kuruluşları ile koordineli olarak gerçekleştirdiği görevleri arasındadır. Bu noktada GRU'nun söz konusu görevlerinin ABD Ordusu bünyesinde yer alan CYBERCOM'a benzer şekilde yapılandırıldığı da görülmektedir.

Öte yandan SVR, FSB ve GRU'nun faaliyetlerinin yanı sıra diğer istihbarat ve güvenlik servislerinin yetkilerinin ve görev alanlarının yeniden planlanması kapsamında, 2000'li yılların başı itibarıyla RF'nin siber kapasitesini geliştirme yönünde ciddi adımlar attığı da bilinmektedir. Bu bağlamda RF, 1993 yılında kurulmuş olan, elektronik ve sinyal istihbaratı ile kriptoloji alanlarında faaliyet gösteren kurum olan FABSİ, 2003 yılında lav ederek, yetki ve sorumluluklarını FSB, SVR, RF Savunma Bakanlığı ve FSO arasında dağıtmıştır. FABSİ'nin kapatılmasının en önemli nedeni ise kurum içerisindeki yolsuzluk ve organize suç örgütleri ile bağlantılı yapılanmalardır. FSO'nun siber güvenlik alanındaki temel görevi ise RF'nin ilgili kurumları ve yöneticileri arasındaki üst düzey ve gizlilik içeren iletişimin güvenli bir şekilde sürdürülmesini denetlemek ve yönetmektir. FSO'nun ayrıca, ülke genelindeki telgraf, kablolu telefon hatlarının, internet ve iletişim haberleşmesinin kontrolü ve denetimi, ayrıca Rus uyduları üzerinden toplanan sinyal istihbaratının değerlendirilmesi ve raporlanması, son olarak Rus nükleer silah sisteminin güvenliğin sağlanması şeklinde görevleri de bulunmaktadır. Bu görevleri kapsamında FSO'nun bazı görevlerinin, NSA'nın faaliyetleri ile benzerlik taşıdığı da ifade edilebilecektir.

Ayrıca RF 2010 yılında enformasyon ve bilgi teknolojileri alanında çalışma yürütmek amacıyla Savunma Bakanlığı bünyesinde bir "bakan yardımcılığı" pozisyonunu tesis etmiştir.[498] RF, 2013 yılında aldığı bir karar ile RSK bünyesinde bağımsız bir siber savaş birimi kurmayı planlama kapsamına almıştır. 2012 Ekim ayında kurulan RSK Askeri

[498]EastWest Institute, **The American and Russian Approaches to Cyber Challenges,** http://www.omicsgroup. org/journals/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf, (14.04.2016).

Araştırma Merkezi Direktörü Andrei Grigoryev, konu bağlamında: *"Rus ordusu olarak internet kaynaklı bazı faaliyetleri tehdit olarak değerlendirdiklerini, bu nedenle de ordu bünyesinde bağımsız bir siber savaş departmanı kurmayı planladıklarını, bu plan dâhilinde çalışma yürüttüklerini, başında bulunduğu araştırma merkezinin halen 700 civarında gizli proje üzerinde çalıştığını"* beyan etmiştir.[499] Bu birimin CYBERCOM ile benzer bir fonksiyona sahip olacağı açıktır. Diğer yandan RSK bünyesindeki söz konusu siber biriminin 2017 yılı itibarıyla operasyonel faaliyetlerine başlayacağı tahmin edilmektedir.[500]

[499]SRİDHARAN Vasudevan, **Russia Setting up Cyber Warfare Unit Under Military**", http://www.ibtimes.co.uk/russia-cyber-war-hack-moscow-military-snowden-500220**,** (26.03.2016).
[500]State Security Magazine, **Russia Announces Development of Cyber Military Unit,** http://www.tripwire.com/state-of-security/latest-security-news/russia-announces-development-cyberwar-military-unit/, (26.03.2016).

SONUÇ

İnternet, en basit tanımıyla, bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağıdır. 1985 yılında kullanılmaya başlayan internet kelimesi, *"kendi aralarında bağlantılı ağlar"* anlamına gelen "*Interconnected Networks"* teriminin kısaltmasıdır. İnternet, günümüzde tartışmasız bir şekilde yaşamımızın ve güvenlik yaklaşımlarımızın ayrılmaz bir öğesi haline gelmiştir. İnternet, dünya dengelerini değiştirmiş ve bu teknolojik ürün, siber saldırılara ve siber savaşlara aracılık eden siber uzay alanının da temel taşı haline gelmiştir.

İnternet ve ağ teknolojilerinde yaşanan gelişmeler ile birlikte, siber uzay kaynaklı saldırılar, devletlerin ulusal ve ekonomik güvenliğini sarsmaya başlamıştır. Gelecek on yıllar içerisinde de internet ve ağ teknolojileri merkezli gelişmelerin ticari, kültürel, askeri, siyasal, finans gibi sektörleri de içine alacak şekilde tüm dünyayı derinden etkileyeceği açıktır.

Bilgisayarın taşınabilir bir hale gelmesi, akıllı cep telefonu teknolojisi ve internet erişimin yaygınlaşması ile birlikte, internetin yarattığı imkânlar ve kolaylıklar, günlük yaşamın da ötesinde siyasal, askeri, ekonomik yaşamda da yeni bir güç faktörünün ortaya çıkmasına neden olmuştur. Bu durum ayrıca güvenlik tartışmalarında ve analizlerinde siber uzay ve siber güvenlik şeklinde tanımlanan yeni kavramların da tartışılmasına yol açmıştır.

Ağ teknolojileri temelli gelişmeler ile birlikte devletlerin savaş, saldırı ve savunma teknikleri de değişmeye başlamıştır. İnternetin 1990 yıllar ile birlikte hızla ticarileşmesi ve yaygınlaşması hem devletler hem de bireyler için yeni bir tehdit kaynağının oluşmasına da neden olmuştur. Bu kapsamda bireysel veya devlet destekli hackerlar, internetin gizemli dünyasını aralamış ve internet aracılıyla ne tür güvenlik risklerinin yaratılabileceğini devletlere ve sıradan insanlara göstermişlerdir.

1990'lı yıllarda ilk hacking işlemleri kişisel menfaatler için yapılırken, günümüzde devletler destekli veya bireysel hackerların faaliyetleri küresel ölçekte yeni nesil tehdit odaklarının oluşmasına neden olmuştur. Değişen dünya değerleri arasında ilk sırayı alan bilgiyi, koruma ve muhafaza etme biçimi de değişiklik göstermiştir. Gizli sistemlere, sistem açıklarından faydalanarak sızan ve önemli sırları ele geçiren hackerlar, artık birer

siber savaşçı olarak devletler adına çalışmaya başlamış, siber saldırılarla devlet sırları ve devlet savunma sisteminin diğer devletlerce ele geçirilme imkânları yaratılmış, sonuç olarak da devletlerin yeni teknolojik gelişmelere uygun siber saldırı ve savunma sistematikleri geliştirilmesine yönelik planlamaları hız kazanmıştır.

Söz konusu süreçlerin itici gücü olan internet ve ağ teknolojileri temelli gelişmeler ile birlikte insan eliyle yaratılan dijital bir alan olan siber uzay, artık devletler tarafından yeni bir mücadele alanı olarak tanımlanmaya başlanmıştır. Mevcut siyasi, ekonomik ve askeri güçleri kapsamında küresel sistemde hegemon güç konumunda olan ABD ve RF, söz konusu güçlerini kaybetmemek ve hatta daha da artırmak amacıyla siber uzay kaynaklı gelişmeleri askeri kapasitelerini geliştirmek adına yeni bir imkan olarak değerlendirmişlerdir. Bu kapsamda Soğuk Savaş dönemindeki rekabet sürecinin bir sonucu olan teknolojik miraslarının da katkısıyla, RF ve ABD ağ teknolojileri merkezli gelişmeleri kullanmak suretiyle etkili bir siber saldırı ve savunma kapasitesi geliştirmeye yönelik planlamalara hız vermişlerdir. Böylelikle her iki devlet de küresel alandaki güç mücadelelerinde siber kapasite ile desteklenmiş askeri güçlerini, dolayısıyla da caydırıcılık imkânlarını artırmayı hedeflemişlerdir.

Bu kapsamda öncelikle ABD, özellikle 1990 yılların ikinci yarısı itibarıyla elinde bulundurduğu teknolojik imkânlar, ekonomik gelişmişlik düzeyi ve kurumsal örgütlenmeleri kapsamında siber uzay alanında etkili rol oynayan ilk hegemon güç olmuştur. İnternetin sivilleşerek ticari bir alan haline dönüşmeye başladığı 1990'lı yıllar ile birlikte, ABD bu mecrayı ilk etapta ekonomik ve kültürel üstünlüğünü kabul ettirebileceği bir alan olarak değerlendirmiştir. Bu değerlendirme kapsamında da ABD'nin çalışmamızda daha önce bahse konu edildiği üzere 1990 yıllarda ortaya koyduğu siber güvenlik ile ilgili resmi belgelerinin ve başkanlık emirlerinin tamamına yakını internetin ticari kapasitesinin geliştirilmesi, korunması ve ABD'nin kültürel hegemonyasının sürdürülmesi adına küresel düzeyde yaygınlaştırılması odaklı hazırlanmışlardır.

Öte yandan SSCB'nin dağılması sonrasında 1990 ve 2000 yılları arasında siyasi ve ekonomik toparlanma süreci yaşayan RF ise 2000'li yıllar ile birlikte ortaya koyduğu strateji ve planlamalar ile birlikte, günümüzde siber uzayda ABD karşıtlığını ve çıkarlarını hedef alan güçlü ve agresif bir etkinliğe ulaşmıştır. RF'nin 2000'li yıllar ile birlikte siyasi

ve ekonomik istikrarını sağlamış olmasının verdiği etkiyle siber uzayda etkinlik sağlamayı hedeflediği açıktır. Bununla birlikte söz konusu tarih sonrasında RF'nin siber kapasitesini artırmaya çalışması, ayrıca küresel düzeyde etkili ve yeni nesil tekniklerden istifade edebilen bir enformasyon stratejisi geliştirmeye yönelmesinin önemli bir nedeni ise RF çıkarları aleyhine Batı tarafından desteklenen ve 2000'lerin başında eski Doğu Blok'u ülkelerinde, Balkanlar'da yaşanan Renkli Devrim süreçleridir. Bu itibarla RF, siber uzay temelli yeni askeri imkanlar ile sosyal medya uygulamalarından istifade eden toplumsal hareketlerin etki ve önemini çok daha iyi anlamıştır. Bu kapsamda da RF, 2000'li yıllar sonrasında siber askeri gücünü, kriminal örgütlenmelerle irtibatlı siber saldırı kapasitesini, milli yazılımlarla tasarlanan ulusal sosyal medya uygulamalarını, anti-virüs programlarını ve şirketlerini, yeni nesil tekniklerle yayın yapan küresel medya yapılanmalarını önemli ölçüde geliştirmiştir.

Öte yandan söz konusu motivasyonların teşviki ile RF'nin ulaşmayı başardığı güçlü siber kapasite ABD'nin resmi savunma ve güvenlik stratejileri belgelerinin yanı sıra konu kapsamında yetkili yüksek bürokratları tarafından da birçok kez teyit edilmiştir. Bu itibarla 2000'li yıllar ile birlikte özellikle de 2010 yılı sonrasında her iki devlet birbirlerinin siber kapasitelerini geliştirmek adına attıkları her adımı hem yakından takip etmeye başlamışlar, hem de bu adımları kendi ulusal çıkarları aleyhine bir gelişme olarak okuma eğilimi göstermişlerdir**.** Bu noktada konu bağlamında çalışmamızda daha önce ayrıntıları ile analiz ettiğimiz üzere ABD'nin Şubat 2015'te yayınlanan *"National Security Strategy / Ulusal Güvenlik Stratejisi"* ile Nisan 2015'te açıklanan *"The Department of Defence Cyber Strategy / ABD Savunma Bakanlığı Siber Strateji*" isimli belgelerde de RF'nin siber imkân ve kapasitesi ABD'nin ulusal çıkarları için yeni bir tehdit odağı olarak tanımlanmıştır. bu husus bizce her zaman hatırda tutulmalıdır.

Ayrıca litaretürde "Demokrat Parti Hack Skandalı" şeklinde tanımlanan ve RF'nin siber saldırılar ile 2015-2016 yılları arasında ABD başkanlık seçim sürecini manipüle ettiği şeklindeki iddialar ABD ve RF'nin gelecek dönemde siber uzayda yaşayacağı rekabet ve gerginliğin de açık habercisi konumundadır.

Bahse konu şekilde RF ve ABD arasında yaşanmakta olan siber rekabet, 21.yy.'da sadece söz konusu devletlerin ulusal siber güvenlik yapılanmalarına değil, aynı zamanda

uluslararası siber güvenlik stratejilerinin şekillenmesine de doğrudan tesir etmektedir. Her iki devlet, karşı devletin siber uzayda ortaya koyduğu her yeniliği, planlamayı ve kapasite arttırımını ülkesine yönelik bir müdahale ve tehdit girişimi şeklinde görmekte bu hamleye cevap vermek adına da hem siber savunma hem de siber saldırı alanında ciddi yatırımlar gerçekleştirmektedir. Bu yatırımlar sonrasında ise RF ve ABD günümüzde oldukça sofistike ve gelişmiş bir siber saldırı kapasitelerine sahip olmayı başarmışlardır.

RF'nin siber teknolojilere sahip olmak amacıyla yaptığı yatırımlar ve komşu ülkelere yönelik gerçekleştirdiği siber saldırılar sonrasında başta ABD olmak üzere diğer devletler uluslararası ilişkilerde siber uzayın saldırı amaçlı olarak kullanılmaya başlanabileceğini de daha net görmüşlerdir. Bir başka ifadeyle 2000'li yılların ikinci yarısından sonra RF'nin siber uzay alanında ortaya koyduğu yenilikler ile geliştirdiği saldırı kapasitesi, bu hamlelere yönelik ABD'nin ortaya koyduğu tedbirler ve karşı girişimler günümüzde uluslararası ilişkilerde etkisini süratle hissettirmiştir. Bu nedenle de süreç içinde, RF ve ABD tarafından karşılıklı etkileşim ve etki-tepki ilişkisi kapsamında geliştirilen siber savunma ve saldırı kapasiteleri, özellikle de 2010 yılı sonrasında devletlerin klasik güvenlik anlayışlarında, ortaya çıkan bu yeni duruma göre, revizyona gitmelerine neden olmuştur. Bu çerçevede, RF ve ABD kaynaklı olarak bugüne kadar gerçekleşen siber saldırıların ve espiyonaj faaliyetlerinin siber uzayın anonim doğasından kaynaklandığı biçimde kolay ve arkada iz bırakmadan planlanabilir oluşu, uluslararası ilişkilerde tehdit, güvenlik ve caydırıcılık konularındaki güncel yaklaşımların uygulanabilirliği noktasındaki yeni nesil sorunlar olarak ele alınmaya başlanmıştır.

RF ve ABD arasında önceleri örtülü siber operasyon ve saldırılar sonrasında ise "Snowden Olayı" ve "WikiLeaks Belgeleri" ile açıkça ortaya çıkan siber rekabet, "Demokrat Parti Hack Skandalı" kapsamındaki iddialar ile birlikte adeta bir siber çatışma eşiğine doğru dünyayı yaklaştırmıştır. Bu kapsamda kısa ve orta vadede ABD'nin RF'nin söz konusu siber saldırısına karşı aktif tedbirler alacağı, bu tedbirlerin ise Rus çıkarlarını küresel düzeyde tehdit eden siber operasyonlar kapsamında gerçekleşeceği açıktır. Ayrıca bu tahminlerin de ötesinde, ABD'nin 2018 yılında yapılacak olan RF başkanlık seçimlerini etkilemeye yönelik kapsamlı enformasyon savaşı stratejileri ve siber saldırları şimdiden plalamakta olduğu rahatlıkla öngörülebilecektir.

RF'nin ise kendi ülkesine yönelik olası siber saldırıları bertaraf etme konusundaki çalışmaları da şimdiden yoğun bir şekilde gerçekleşmektedir. Bu kapsamda önümüzdeki süreçte RF hükümeti milli yazılımların kullanılması, milli sosyal medya uygulamalarının yaygınlaştırılması, ulusal internet sisteminin denetim ve kontrolünün sıkılaştırılması, RSK ve RİS'ler bünyesinde etkili, aktif ve merkezi denetime sahip yeni siber birimlerin tesis edilmesine yönelik planlamaları artacaktır. RF'nin söz konusu siber savunma imkânlarının geliştirilmesine yönelik çabalarını etkili bir enformasyon savaşı stratejisiyle de destekleyeceği de ortadadır. Bu kapsamda küresel düzeyde faaliyet gösteren medya kuruluşları ile sosyal medyada aktif olarak halihazırda faaliyet gösteren troll ağı ile birlikte, RF'nin yeni nesil enformasyon stratejisi geliştirme konusunda yakın gelecekte çok daha etkili olacağı öngörülebilecektir. Bu durumda ise RF'nin etkili siber saldırı ve savunma kapasitesiyle birlikte, gelişmiş bir küresel siber propaganda sistematiği sayesinde siber uzayda ABD ile ciddi bir rekabete girmekten çekinmeyeceği de değerlendirilebilecektir.

Tüm bu rekabet süreçlerinin ise insan eliyle yapılmış, birbiriyle eklemlenmiş ağ teknolojileri vasıtasıyla oluşturulmuş ve beşinci boyut olarak adlandırılan siber uzay alanının şekillenmesine doğrudan tesir edeceği ve bu kapsamda da siber uzayın devletlerarası mücadelenin yoğun bir şekilde yaşanacağı yeni bir mecra olarak uluslararası ilişkiler analizlerinde daha detaylı bir şekilde değerlendirilmesine yol açacağı da ortadadır.

KAYNAKLAR

Kitaplar:

ARI Tayyar, **Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya İşbirliği**, 6 b, MKM Yayınları, Bursa, 2010.

ARIBOĞAN Deniz Ülke, **Tarihin Sonundan Barışın Sonuna**, Timaş Yayınları, İstanbul, 2003.

BIÇAKCI Salih, **21. Yüzyılda Siber Güvenlik**, Bilgi Üniversitesi Yayınları, İstanbul, Ağustos 2013.

BUZAN Barry, **People, States and Fear, Great Britain, London**, Aktaran: Akın Alkan, 21. Yüzyılın İlk Çeyreğinde Karadeniz Güvenliği, Nobel Yayın Dağıtım, Ankara, 2006.

CARR Jeffrey, **Inside Cyber Warfare: Mapping the Cyber Underworld**, O'Reilly Media Inc., USA, 2011.

CLARKE A. Richard ve KANKE K. Robert, **Siber Savaş**, çeviren Murat ERDURAN, İstanbul Kültür Üniversitesi Yayınları, İstanbul, 2011.

DODGE Martin ve KITCHIN Rob, **Mapping Cyberspace**, Routledge, London, 2001.

DONNELY Jack, **Realism and International Relations, Cambridge University Press,** 2000.

DUNNE Tim, **Liberalism, içinde The Globalization of World Politics, ed. John Baylis, Steve Smith**, Oxford University Press, London, 2001.

GIBSON William, **Neuromancer**, Ace Books, New York, 1984.

GOBLE A. Paul, **Defining Victory and Defeat: The Information War Between Russia and Georgia**, **In the Guns of August 2008:Russia War in Georgia**, edited by Svantee E. Cornell and S. Frederick Starr, Armonk, New York, 2009.

JACKSON Robert ve SORENSEN Georg, "International Relations: Theories and Approaches", **Oxford University Press**, 2007.

NYE Joseph S., **Power and National Security in Cyberspace**, America's Cyber Future Security and Prosperity in the Information Age, New York, Public Affairs, 2011.

KEGLEY Jr. ve CHARLES W., **Neoliberal Challange to Realist Theories of World Politics: An Introduction,** St. Martin's Press, New York, 1995.

KLIMBURG Alexander, **National Cyber Security Framework Manual**, NATO CCD_COE Publication, Talinn, 2012.

KOLODZIEJ Edward, **Security and International Relations**, Cambridge University Press, New York, 2005.

MORGAN M.Patrick, **International Security Problems and Solutions**, CQ Pres., Washington DC, 2006.

MORGENTHAU Hans, J., **Uluslararası Politika**, Çevirenler ORAN Baskın ve OSKAY Ünsal, Sevinç Matbaası, Ankara, 1970.

YILMAZ Salih, **Rusya Neden Suriye'de?**, Yazar Yayınları, Ankara, 2016.

WALTZ Kenneth, **Theory of International Politics**,Chicago,Addison-Wesley Pub., 1979.

WALTZ Kenneth, **Political Structures, Robert O. Keohane (Edt.), Neorealism and its Critics**, New York, Colombia University Press, 1986.

WALTZ Kenneth, **Man, the State and War**, Columbia University Press, New York, 2001.

WALTZ Kenneth ve QUESTER H. George, **Uluslararası İlişkiler Kuramı ve Dünya Siyasal Sistemi**, Çev. Ersin Onulduran, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, Ankara, 1982.

WALTZ Kenneth ve ART J. Robert, **The Use of Force: International Politics and Foreign Policy**, Little Brown and Company, Boston, 1971.

Makaleler:

ABBATE Janet, "Government, Business, and the Making of the Internet", **Business History Review**, Vol. 75, No. 1, Spring 2001, pp.147-176.

AYDIN Mustafa, "Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği", **Uluslararası İlişkiler,** Cilt 1, No.1, Bahar 2004, 2004, ss.33-60.

BAYLIS John, "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler**, Cilt 5, Sayı 18, Yaz 2008, ss. 69-85.

BELLAMY Ian, "Towards a Theory of International Security, **Political Studies**, Vol. 29, No.1, 1981, pp.100-105.

BIÇAKCI Salih, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler**, Cilt.10, Sayı 40, Kış 2014, ss. 101-130.

BIÇAKCI Salih, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler**, Cilt 9, Sayı 34, Yaz 2012, ss.205-226.

BOZDAĞLIOĞLU Yücel ve ÖZEN Çınar, "Liberalizmden Neoliberalizme Güç Olgusu ve Sistemik Bağımlılık", **Uluslararası İlişkiler**, Cilt 1, No.4, Kış 2004, ss. 59-79.

BUZAN Barry, "Peace, Power and Security: Contending Concepts in the Study of International Relations", **Journal Of Peace Search**, Vol. 21 No.2, 1989, pp. 109-125.

ERDOĞAN İbrahim, "Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı", **Akademik Bakış**, Cilt. 6, Sayı 12, Yaz 2013, ss. 265-292.

ERIKSSON Johan ve GIACOMELLO Giampiero, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", **International Political Science Review**, Vol.27, No.3, 2006, pp. 221-244.

GÜRKAYNAK Muharrem ve İREN Adem Ali, "Siber Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt 16, No.2, 2011, ss. 263-279.

JERVIS Robert, "Cooperation Under the Security Dilemma", **World Politics**, Vol.30, No.2, January 1978, pp.167-214.

KALKAN KÜÇÜKSOLAK Övgü, "Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Okulu Çerçevesinde Tartışılması", **Turan Stratejik Araştırmalar Dergisi**, Cilt 4, No.14, İlkbahar 2012, ss. 200-204.

MOWTHORPE Matthew, "The Revolution in Military Affairs (RMA): The United States, Russian an Chinese Views", **University of Hull Press**, Vol.5, No.2, 2005, pp.1-18.

ÖZCAN A. Behiç, "Uluslararası Güvenlik Sorunları ve ABD'nin Güvenlik Stratejileri", **Selçuk Üniversitesi İİBF Sosyal ve Ekonomik Araştırmalar Dergisi**, No.22, 2011, ss. 447-465.

REUS-SMIT Christian, "Realist and Resistance Utopias: Community, Security and Political Action in the New Europe", **Millennium,** Vol. 21, No.1, 1992, pp.5-56.

STAAR R. Tocaso, "Russia's Security Services", **Mediterranean Quarterly**, Vol.15, Issue.1, pp.1-10.

STONE Alec, "What is a Supronational Constitution? An Essay in IR Theories", **The Review of Politics**, Vol.56, No.3, 1994 Summer, pp. 441-473.

SNYDER Jack, "One World, Rival Theories", **Foreign Policy**, No.145, November-December 2004, pp. 53-62.

WALTZ Kenneth, "The Origins of War in Neorealist Theory", **Journal of Interdisciplinary History**, Vol.18, No.4, 1988, pp.615-628.

WALTZ Kenneth, "The Emerging Structure of International Politics", **International Security,** Vol.18, No.2, 1993, pp. 44-79.

ZAGARE C. Frank, "Deterrence Is Dead. Long Live Deterrence", **Conflict Management and Peace Science,** Vol.23, No. 2, 2006, pp.115–120.

ZINOVYEVA Elena, "U.S. Digital Diplomacy: Impact on International Security and Opportunities for Russia", **A Russian Journal on International Security**, Vol.19, No.2, 2013, pp. 33-43.

Diğer Kaynaklar:

ABS-CBS News, **1,796 memos from US embassy in Manila in WikiLeaks 'Cablegate**, http://news.abs-cbn.com/nation/11/29/10/1796-memos-us-embassy-manila-wikileaks-cablegate,(16.06.2016).

AFCEA Organization, **The Evolution of US Cyberpower**, http://www.afcea.org/committees/cyber/ documents/ TheEvolutionofUSCyberpower.pdf, (23.05.2016).

Akademik Portal News, **Bugüne Kadar Gerçekleşmiş Olan Beş Devasa Siber Saldırı**, http://www.akademiportal.com/bugune-kadar-gerceklesmis-olan-5-devasa-siber-saldiri/, (18.02.2016)

AKYAZI Uğur, **Uluslararası Siber Güvenlik Stratejisi ve Doktrinler Arasında Alınabilecek Tedbirler**, 6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı, http://www.iscturkey.org/s/2226/i/2013-paper105.pdf, (14.01.2016).

Al Jazeera Internet Web, **Report: Russia sponsored cyber attacks**, http://www.aljazeera.com/news/2015/09/report-russian-government-sponsored-cyber-attacks-150917132351595.html, (01.04.2016).

Anadolu Ajansı, **Sputnik ve DİHA'ya erişim engeli talebi onaylandı.**, http://aa.com.tr/tr/turkiye/sputnik-ve-dihaya-erisim-engeli-talebi-onaylandi-/555880, (20.04.2014).

BAKIR Emre, **Siber Savaşlar-Başlangıç**, http://www.siberguvenlik.org.tr/2012/12/siber-savaslar-baslangc.html, (14.02.2016).

Baltic Times, **Lithuania cyber attacks: Round two**, http://www.baltictimes.com/news/articles/20897/, (04.04.20017).

BARTON Gellman ve MILLER Greg, **U.S. spy network's successes, failures and objectives detailed in 'black budget' summary**, The Washington Post, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html, (30.05.2016).

BAŞA Şafak, **ABD İç Güvenlik Bakanlığı**, http://www.academia.edu/9830086/ABD_%C4%B0%C3%87_G%C3%9CVENL%C4%B0K_BAKANLI%C4%9EI_SUNUM_, (31.05.2016).

BAYRAM Ümit, **Realizme yapılan Eleştiriler Üzerine Bir Yaklaşımı**, http://www.uiodergisi.com/wp-content/uploads/2011/05/%C3%BCmit-8.pdf, (16.01.2016).

BBC News, **Russia Offers $110,000 to Crack Tor Anonymous Network**, http://www.bbc.com/news/ technology-28526021, (15.04.2014).

BBC News, **Türkiye'ye siber saldırının 10 günü: Ne oldu?**, http://www.bbc.com/turkce/haberler /2015/12/151224_siber_saldiri_arslan, (25.04.2016).

BBC News, **What is Wikileaks?**,http://www.bbc.co.uk/news/technology-10757263, (16.06.2016).

Biography Web Page, **Edward Snowden**,http://www.biography.com/people/edward-snowden-21262897, 15.06.2016.

Biography Web Page, **Julian Assange**, http://www.biography.com/people/julian-assange-20688499, (16.06.2016).

BIRNBAUM Michael, **Russian Blogger Law Puts New Restrictions on Internet Freedoms**,Washington Post, http://search.proquest.com/docview/1550033701., (15.04.2016).

BISSON David, **A Cyber Study of the U.S. National Security Strategy Reports**,http://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-u-s-national-security-strategy-reports/, (25.05.2016).

Birgün Net, **WikiLeaks, Fuat Avni'nin Rus Uçağı İddiasını Paylaştı**, http://www.birgun.net/haber-detay/wikileaks-fuat-avni-nin-rus-ucagi-iddiasini-paylasti-97073.html, (08.11 2016).

Birgün Net, **Rusya'nın Savaş Uçağının Düşürülmesi Üzerine Sosyal Medyada Tepki**, http://www. birgun.net/haber-detay/rusya-nin-savas-ucaginin-dusurulmesi-uzerine-sosyal-medyada-tepki-95978.html, (08.11.2016).

Bloomberg Tecnology News Portal, **Russia Clarifies Looming Data Localization Law**, http://www.bna.com/russia-clarifies-looming-n17179934521/, (23.09. 2016).

BREMMER I., Chaarp, **The Siloviki's Putin's Russia: Who they are and What they want**,Washington Quarterly, Centre For Strategic and International Studies and MIT, www.globalsecurity.org, (26.03.2016).

BURNS Megan, **Information Warfare: What and How?**, http://www.cs.cmu.edu/ ~burnsm/InfoWarfare.html, (11.11. 2016).

ÇAĞRI Erhan, **Diplomaside Wiki-Tsunami**, http://www.turkiyegazetesi.com.tr/yazarlar/prof-dr-cagri-erhan/473614.aspx, (17.06.2016).

CARR Jeffry, **Intelligence on Russian Information Warfare Activities**, http://jeffreycarr.blogspot.com/2012/01/intelligence-on-russian-information.html, (04.01.2017).

Committee on Homeland Security and Governmental Affairs, **A Review of the Department of Homeland Security's Missions and Performance**, https://www.google.com.tr/?gfe_rd=cr&ei=v9RlWb4NNGv8wev6rvQBg#q=A+Review+of+the+Department+of+Homeland+Security%E2%80%99s+Missions +and+Performance,, (31.05.2016).

Chairman, President's Commission on Critical Infrastructure Protection, **Critical Foundations: Protecting America's Infrastructure-The Report of the President's Commission on Critical Infrastructure Protection**, https://www.fas.org/sgp/library /pccip.pdf, (24.05.2016).

CHIVERS Ian and SLEIGHTHOLME Jane, **Fortran History and Development**, http://www.fortranplus.co.uk/resources/Fortran_history_and_development.pdf, (23.05.2016).

ÇIKRIKÇI Tolga, **Realizm Güvenlik Anlayışı ve Soğuk Savaş Sonrası Karadeniz'in Güvenliği**, http://www.bilgesam.org/Images/Dokumanlar/0-140-2014091830guvenlik-26.pdf, (15.01.2016).

ÇÖPOĞLU Onur Muhammet, **Muharebe Alanındaki 5. Cephe: Siber Uzay**, http://akademikblog. com/muharebe-alanindaki-5-cephe-siber-uzay/, (17.02.2016).

DEMİRCİOĞLU Cemalettin, "Siber Uzayda Güç ve Güvenlik", **İdareci'nin Sesi**, Mart-Nisan 2014, http://www.tid.web.tr/ortak_icerik/tid.web/160/8%20 Cemalettin%20 DEM%C4%B0RC%C4%B0O%C4%9ELU.pdf, (10.02.2016).

Department of Homeland Security, **Digital Government. Building a 21st Century Platform to Better Serve the American People**, https://www.dhs.gov/sites/default/files/publications /digital-strategy/digital-government-strategy.pdf (20.02.2017).

Department of Homeland Security, **ExecutiveSummary of Grizzly Steppe**

Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale, https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary (20.02.2017).

Department of Homeland Security, **Federal Information Security Management Act of 2002-FISMA**, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, (13.06.2016).

Department of Homeland Security, **Homeland Security Act**, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf, (13.06.2016).

Department of Homeland Security, **Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization,and Protection**, https://www.dhs.gov/homeland-security-presidential-directive-7, (31.05.2016).

Department of Homeland Security, **Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity**, https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity, (20.02.2017).

Department of Homeland Security, **National Cybersecurity and Communications Integration Center**,https://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2012-04-30%20Spring%20Conference-Meeting/2%20Lichtenfels%20DHS%20NCCIC%202.pdf, (31.05.2016).

Department of Homeland Security, **Written testimony of Secretary Napolitano for a Senate Committee on Homeland Security and Governmental Affairs hearing titled Homeland Threats and Agency Responses**, https://www.dhs.gov/news/2012/09/19/written-testimony-secretary-napolitano-senate-committee-homeland-security-and, (13.06.2016).

Der Spiegel News Magazine, **Was Russia behind 2015's cyber attack on the German parliament?**, http://www.dw.com/en/was-russia-behind-2015s-cyber-attack-on-the-german-parliament/a-19017553, (01.04.2016).

DOYLE Charles, **Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws-Computer Fraud and Abuse Act**, https://www.fas.org/sgp/crs/misc/97-1025.pdf, (13.06.2016).

EastWest Instıtute, **The American and Russian Approaches to Cyber Challenges**, http://www.omicsgroup.org/journals/the-american-and-russian-approaches-to-cyber-challenges-2167 0374.1000110.pdf, (14.04.2016).

FARRELL Paul, **History of 5-Eyes**, https://www.theguardian.com/world/2013 /dec/02/history-of-5-eyes-explainer, (15.06.2016).

Federal Bureau of Investigation, **Cyber Crime**, https://www.fbi.gov/about-us/investigate/cyber/ncijtf, (01.06.2016).

Federal Bureau of Investigation, **Wanted by FBI**, https://www.fbi.gov/wanted/cyber, (01.06.2016).

Federal Trade Comission, **Gramm Leach Bliley Act**, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, (13.06.2016).

FireEye, **APT28-A Window Into Russia's Cyber Espionage Operations?**, Special Report by FireEye, https://www.fireeye.com/, (01.04.2016).

FISCHER A.Eric, **Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions**, Congressional Research Service, 2013 https://fas.org/sgp/crs/natsec/R42114.pdf, (20.02.2017).

FSTEC Internet Sitesi, **FSTEC's Structure**, http://fstec.ru/en/358-structure, (18.06.2017).

FSTEC Internet Sitesi, **FSTEC's Power**, http://fstec.ru/en/359-powers, (18.06.2017).

GADY Franz-Stefan ve AUSTİN Greg, **Russia, The United States, And Cyber Diplomacy Opening the Doors**, East-West Enstitute Report, http://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf, (01.04.2016).

GALEOTTI Mark, **Putin's Hydra: Inside Russia's Intelligence Services**, European Council on Foreign Relations (ECFR), http://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services, (17.10.2016),

GEERS Kenneth, Darien Kindlund, Ned Moran, Rob Rachwald, **World War C**:**Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks**,

https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf, (14.04.2016).

GERDEN Eugene, **$500 Millionfor New Russian CyberArmy**, Security Magazine UK, http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/, (26.03.2016).

GERASİMOV Valery, "Tsennos' Nauki v Vredvidenii (Value of AppliedScience)", **Voyenno-Promyshlennyy Kuryer**, February 27, 2013, https://inmoscowsshadows .wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, (24.03.2016).

GILES Keir, **Russia's Public Stance on Cyber space Issues**, 4th International Conference on CyberConflict, Tallinn, NATO Cooperative Cyber Defense Centre of Excellence, 2012, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_ RussiasPublicS, (23.03.2016).

GILES Keir, **Russian Cyber Security: Concepts and Current Activity**", Chatham House Conflict Studies Research Centre REP Roundtable Summary,https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Russia%20and%20Eurasia/060912summary.pdf, (14.04.2016).

GILES Keir, **Information Troops-A Russian Cyber Command?**, Paper presented atthe 3rd International Conference on Cyber Conflict, Tallinn, 2011, Cooperative Cyber Defense Centre of Excellence, http://conflictstudies.org.uk/files/Russian_ Cyber_Command.pdf, (23.03.2016).

GLASER L. Charles,**Deterrence of Cyber Attacks and U.S. National Security**, Professor of Political Science and International Affairs, Elliot School of International Affairs,The George Washington University Report GW-CSPRI-2011-5, June 1, 2011, http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/54b94136e4b0ad6fb5e16716/1421426998290/2011-5_cyber_deterrence_and_security_glaser.pdf, (23.02.2014).

Global Security Web, **FSTEC**, http://www.globalsecurity.org/military/world/russia/fstec.htm, (18.06.2017).

GONZALEZ Daniel, **Preventing Cyber Attacks: Sharing Information About Tor**, The RAND Blog, http://www.rand.org/blog/2014/12/preventing-cyber-attacks-sharing-informationabout., (16.04.2016).

GÜRCAN Metin, **Rusya'nın Ukrayna'daki Bulanık Savaş Konsepti**, http://www.analistdergisi. com/sayi/ 2014/05/rusya-nin-ukrayna-daki-bulanik-savas-stratejisi, (22.04.2016).

HaberTürk İnternet Haber Portalı, **Binali Yıldırım'dan ODTÜ açıklaması**,http://www.haberturk.com/ekonomi/teknoloji/haber/1171682-binali-yildirimdan-odtu-aciklamasi, (25.04.2016).

HaberTürk İnternet Haber Portalı, **Kerimov'a Yasak**, http://www.haberturk.com/gundem/haber/1227586-sputnik-turkiye-genel-muduru-tural-kerimova-giris-yasagi, (20.04.2014).

Haberler İnternet Haber Portalı, **Türkiye'ye Siber Saldırının Arkasında Ruslar Var**, http://www.haberler. com/turkiye-ye-siber-saldirinin-arkasinda-ruslar-var-8006069-haberi/, (25.04.2016).

Haberus İnternet Haber Portalı, **Snowden Rusya'dan Ayrılmayı Düşünmüyor**, http://haberrus.com/politics/2015/08/15/snowden-rusyadan-ayrilmayi-dusunmuyor.html, (15.06.2016).

HAGESTAD II William, **Comparative Study: Iran, Russia and PRC Cyber War**, RSA Conference, 2013 Europe, http://www.rsaconference.com/writable/ presentations/file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf, (05.03.2016).

HALHALLI Yusuf, **Kremli'nin Gençlik Hareketi**, https://www.academia.edu/7302656/KREML%C4%B0N%C4%B0N_GEN%C3%87LER%C4%B0_NASH%C4%B0_GEN%C3%87L%C4%B0K_HAREKET%C4%B0, (12.04.2016).

HEICKERO Roland, **Emerging Cyber Threats and Russian Views on Information Warfare and Operation**, Swedish Defense Research Agency Press, March 2010, pp.1-70, http://www.foi.se/rapport?rNo=FOI-R--2970--SE, (23.06.2016).

HUHNE Chris, **Prism and Tempora: the cabinet was told nothing of the surveillance state's excesses**, http://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state, (15.06.2016).

Hürriyet Gazetesi, **Uçak Krizi Dünya'da Manşet**, http://www.hurriyet.com.tr/ucak-krizi-dunyaya-manset-40018345, (08.11.2016).

IB Times Internet News, **Anonymous: Turkey reeling under cyber attack as government and banks web sites paralysed**, http://www.ibtimes.co.uk/anonymous-turkey-reeling-under-cyber-attack-government-banks-sites-paralysed-1534984, (24.04.2016).

INC Comittee on Govermental Affairs US Senate, **Testımony of James Adams Chief Executıve Offiicer**, https://fas.org/irp/co ngress /2000 _hr/030200_adams.htm,(16.02.2017).

In Moscow's Shadows, **The Gerasimov Doctrine and Russian Non-Linear War**, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russiannon-linear-war/., (24.03.2016).

Internet Law Center's Cyber Report, **A Timeline of Russian Cyber Attacks**, https://ilccyberreport.wordpress.com/2016/11/02/a-timeline-of-russian-cyber-attacks/, (03.04.2017).

ISACA Cyber Security Nexus, **Cybersecurity Information Sharing Act**,http://www.isaca.org/cyber/ pages/cybersecuritylegislation.aspx, (13.06.2016).

Jeo-Politik Araştırmalar Merkezi, **Yumuşak Güç Nedir?**,http://www.stratejikanaliz.com/analizler/ amerika-kitasi/yumusak-guc-nedir/#axzz40PPz61mH, s.1, (19.02.2016).

The Joint Chiefs of Staff (JCS), **The National Military Strategy for Cyberspace Operations**, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, (20.02.2017).

JONES James, **Putin's Youth Movement Provides a Sinister Back drop to Russia's protests**, http://www.theguardian.com/commentisfree/2011/dec/08/putin-russia-elections, (12.04.2016).

Judiciry Committee, **The USA Freedom Act**, https://judiciary.house.gov/issue/usa-freedom-act/, (13.06.2016).

KAÇAR Gamze, **Güvenlik İkilemi**,http://www.tuicakademi.org/guvenlik-ikilemi/, (18.01.2016).

KARA Mahruze, **Siber Saldırılar- Siber Savaşlar ve Etkileri**, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE Bilişim ve Teknolojis Hukuku Yüksek Lisans Programı,2013,http://openaccess.bilgi.edu.tr:8080/xmlui/bitstream/handle/11411/346/Siber%20Sald%C4%B1r%C4%B1lar%20Siber%20Sava%C5%9Flar%20ve%20Etkileri.pdf?sequence=2&isAllowed=y, (17.02.2017).

KASPERSKY Company, **About Kaspersky Lab**, www.kaspersky.com/about., (15.04.2014).

KELLY Sanja, **Freedom on the Net 2014:Russia**, Freedom House, 2014, https://freedomhouse.org/ sites/default/files/resources/Russia.pdf., (15.04.2016).

KOÇ Şanlı Bahadır, **Wikileaks Üzerine Notlar ve Yorumlar**, http://www.21yuzyildergisi.com/assets/uploads/files/16.pdf,(17.06.2016)

KSHETRI Nir, **Cybersecurity and International Relations: The U.S. Engagement with China and Russia,** http://docplayer.net/2657945-Cybersecurity-and-international-relations-the-u-s-engagement-with-china-and-russia.html**, (15.06.2016).**

LOBANOVA Katerina, **How Russia Became a Hacking Superpower**, https://themoscowtimes.com/articles/russia-hacker-superpower-56704,(04.01.2017).

LEE David, **Russia and Ukraine in Cyber Stand-Off**, BBC News, http://www.bbc.com/news/technology-26447200, (23.04.2014).

LEWIS James Andrew, **The Cyber War Has Not Begun**, Center for Strategic and International Studies March 2010, https://www.google.com.tr/webhp?ie=UTF-8&rct=j#q=james+andrew+lewis+the+cyber+war+has+not+ begun, (21.02.2016).

LUCAS Edward and NİMMO Ben, **Information Warfare: What Is It and How to Win It**, Center for European Policy Analysis (CEPA), http://cepa.org/sites/default/files/Infowar%20Report.pdf, pp.1-20., (20.04.2016).

LUCAS Edward and POMERANTSEV Peter, **Winning the Information War, Center for European Policy Analysis (CEPA)**, http://cepa.org/reports/winning-the-Information-War, pp.1-64., 03.06.2017,

MARKOFF John, **Before the Gunfire, Cyber attacks**, New York Times, August 12 2008, New York Edition, http://www.nytimes.com/2008/08/13/technology/13 cyber.html?_r=1&; (12.04.2016).

MCLAUGHLIN Daniel, **Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites**, http://lumen.cgsccarl.com/login?url=http:// proquest.umi.com/pqdweb?did =1503762091&sid=2&Fmt=3&clientld=5094&RQT=309&VName=PQD;, (19.04.2016).

Media Sapiens, **Evaluation of the effectiveness of the authorities in the field of information security**, 2014-15,http://osvita.mediasapiens.ua/trends/1411978127/otsinka_ efektivnosti_diy_organiv_vladi_v_sferi_informatsiynoi_bezpeki_v_201415_rr/, (03.06.2017).

MEDVEDEV A. Sergei, **Offence-Defence Theory Analysis of Russian Cyber Capability**, Master Thesis, Naval Post-Graduate School, Monterey, Colifornia, https://www.google.com.tr/?gfe_rd=cr&ei=qzHZVrreN7Go8wfMuYegDw#q=this+thesis+ represent+mikhail+tsypkin, (05.03.2016).

MERIÇ Enver, **Rus İstihbarat Savaşları ve Putinizm**, Haber 10 Haber Portalı, http://www.haber10.com/yazar/enver_meric/rus_istihbarat_savaslari_ve_putinizm-620326, (17.10 2016).

Milli Güvenlik Kurulu, **Stratejik Yazılar-I, Milli Güvenlik Kurulu Perspektifinden İç ve Dış Meseleler**, http://mgk.gov.tr/calismalar/yayinlar/strateji_ yazilari_1/strateji_yazilari_1.pdf, (09.02.2016).

Milliyet Gazetesi, **Rusya'dan Medya Atağı**, http://www.milliyet.com.tr/rusya-dan-medya-atagi/dunya/detay/1968251/default.htm, (21.04.2016)

Ministry of Foreign Affairs of the Russian Federation, **Information Security Doctrine of Russian Federation**, http://archive.mid.ru//bdomp/nsosndoc.nsf/1e5f0de 28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument, (23.03.2016).

MORGAN M. Patrick, **Applicabilityof Traditional Deterrence Concepts and Theory to the Cyber Realm**,http://www.nap.edu/read/12997/chapter/7, (23.02.2016).

NAKASHİMAEllen, **Obama administration outlines international strategy for cyberspace**, https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html, (24.05.2016).

National Public Radio (NPR), **In Fight Against ISIS, U.S. Adds Cyber Tools**http://www.npr.org/2016/02/28/468446138/in-fight-against-isis-u-s-adds-cyber-tools, (19.04.2017).

National Security Agency, **60 Years of Defending Our Nation**, http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf, (30.05.2016).

National Security Agency, **The Creation of NSA**, https://archive.org/stream/The_Creation_of_NSA_Part_3-nsa/The_Creation_of_NSA_Part_3_djvu.txt, (30.05.2016).

NATO Communications Centre of Excellence, **Social Media as a Tool of Hybrid War**, http://www.stratcomcoe.org/social-media-tool-hybrid-warfare, (19.10.2016).

NATO Cooperative Cyber Defence Centre of Excellence, **National Security Concept of Russian Federation**, https://ccdcoe.org/cyber-security-strategy-documents.html, (23.03.2016).

NATO Cooperative Cyber Defense Centre of Excellence, **The National Strategy to Secure Cyberspace**, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (24.05.2016).

NATO Cooperative Cyber Defense Centre of Excellence, **Cyberspace Policy Review**,https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf, (24.05.2016).

NATO Cooperative Cyber Defense Centre of Excellence, **International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World**, https://ccdcoe.org/cyber-security-strategy-documents.html, (25.05.2016).

NATO Cooperative Cyber Defense Centre of Excellence, **President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity**, https://ccdcoe.org/cyber-security-strategy-documents.html, (24.05.2016).

NATO Cooperative Cyber Defense Centre of Excellence, "**Draft Strategy for Improving Critical Infrastructure Cybersecurity**", http://www.nist.gov /cyberframework/upload/cybersecurity-framework-021214-final.pdf, (24.05.2016).

NATO Cooperative Cyber Defense Centre of Excellence, "**National Security Strategy**, https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf, (25.05.2016).

NATO Cooperative Cyber Defense Centre of Excellence, **The Department of Defence Cyber Strategy**, http://www.defense.gov/home/features/2015/0415_cyber strategy/Final_2015_DoD_CYBER_STRATEGY _for_web.pdf, (25.05.2016).

NBC News, **Timeline: Ten Years of Russian Cyber Attacks on Other Nations**, http://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111?cid =public-rss_20161218, (03.04.2017).

New Times Haber Portalı, **Röportaj/Joseph Nye: Bugün Bireylerin Güç Pastasından Aldıkları Pay, Geçmişe Göre Çok Daha Büyük**, http://newtimes.az/tr/interview/3042/, (13.04.2016).

NIMMO Ben, **Propaganda in the new Orbit**, Center for European Policy Analysis (CEPA) http://cepa.org/files/?id_plik=2083, (23.04.2014).

NTV Internet Haber Portalı, **Kim Bu Assange?**, http://www.ntv.com.tr/dunya/kim-bu-assange,xZtbkT2VJku5p4lk_WHjAA, (16.06.2016).

NYE Joseph S. Jr., "Cyber Power", **Harvard Kennedy School, Belfer Center for Science and International Affairs**, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, (19.02.2016).

NYE Joseph S. Jr., **Nuclear Lessons for Cyber Security?**, Strategic Studies Quarterly, Winter 2011, http://www.au.af.mil/au/ssq/2011/winter/nye.pdf, (14.04.2014).

NY Times, **Hackers to the U.S. Election**, https://www.nytimes.com/interactive/2016/07/27/ us/politics/trail-of-dnc-emails-russia-hacking.html, (20.02.2016).

NY Times, **Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says**, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html, (20.02.2017).

OTTİS Rain, **Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective**, In Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, Reading: Academic Publishing Limited, 2008, http://www.academic-bookshop.com/ourshop/ prod_1355933-ECIW-2008-7th-European-Conference-on-Information-Warfare-and-Security-Plymouth-UK.html, (18.04.2014).

Presidency Of USA, **Executive Order 13010—Critical Infrastructure Protection**, http://www.presidency.ucsb.edu/ws/?pid=53066, (17.02.2017).

Project Grey Goose Phase II Report, **Russia/Georgia Cyber War**, https://tr.scribd.com/doc/6967393/ Project-Grey-Goose-Phase-I-Report, (12.04.2016).

Rand Cooperation, **Perspective on 2015 DoD Cyber Strategy**, http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT439/RAND_CT439.pdf, (25.05.2016).

Reuters, **Obama Budget Makes Cybersecurity Growing U.S. Priarity**, http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurityidUSBRE93913S 20130411, (17.02.2017).

RHOADS Christopher, **Kyrgyzstan Knocked Offline**, Wall Street Journal, 10, http://www.wsj.com/ articles/SB123310906904622741, (19.04.2016).

RIA Novosti ve Mir24.tv, **New Kremlin Information-Security Doctrine Calls For Managing Internet In Russia**, http://www.rferl.org/a/russia-informaiton-security-internet-freedome-concerns/28159130.html, (02.01.2017). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/6/135.html, (02.01.2017).

ROTH Mathias, **Bilateral Disputes between EU Member States and Russia**, CEPS Working Document (Centre for European Policy Studies), August 2009, http://www.ceps.eu/files/book/2009/09/1900.pdf., (18.04.2016).

Rustrans Useful Translations, **Russia's National Security Strategy to 2020**, http://rustrans.wikidot. com/russia-s-national-security-strategy-to-2020, (23.03.2016).

Russia Direct News Magazine, **China-Russia cyber-security pact: Should the US be concerned?**, http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned, (14.04.2016).

SANGER David, **Israeli Test on Worm Called Crucial in Iran Nuclear Delay**,http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0, (02.06.2016).

SANCAK Kadir, **Güvenlik Kavramı Etrafındaki Tartışmalar ve Güvenlik Kavramının Dönüşümü**, http://www.ktu.edu.tr/dosyalar/sbedergisi_69519.pdf, (15.01.2016).

SANDIKLI Atilla ve ERDEM Kaya, **Uluslararası İlişkiler Teorileri ve Barış**, http://www.bilgesam.org/Images/Dokumanlar/0-130-201404079sandikli_kaya.pdf, (06.01.2016).

SANDIKLI Atilla ve EMEKLİER Bilgehan, **Güvenlik Yaklaşımlarında Değişim ve Dönüşüm**, http://www.bilgesam.org/Images/Dokumanlar/0-81-2014040746sandikli_emeklier.pdf, (15.01.2016).

SEZGİN Fatih, Edward Snowden Olayı'nın ABD-Rusya İlişkileri Üzerindeki Etkileri, **Journal of International Management and Social Researches Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi**, http://dergipark.ulakbim.gov.tr/uysad/article/view/5000108153/5000100862, (30.05.2016), ss.1-8.

SFGATE News Portal, **Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cybersecurity**, http://www.sfgate.com/business/article/Former-White-House-aide-backs-some-Net-regulation-2729985.php, (13.06.2016).

SHACHTMAN Noah, **Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals**,Wired Magazine, www.wired.com, (15.04.2014).

Siber Bülten, **Stuxnet ve Uluslararası Hukuk: Bir siber saldırının anatomisi**, https://siberbulten.com/makale-analiz/stuxnet-ve-uluslararasi-hukuk-bir-siber-saldirinin-anatomisi/, (02.06.2016).

SONNE Paul ve RAZUMOVSKAYA Olga , **Russia Steps Up New Lawto Control Foreign Internet Companies**, Wall Street Journal, http://www.wsj. com/articles/ russia-steps-up-newlaw-to-control-foreign-internet-companies-1411574920., (15.04.2016).

SOLDATOV Andrei ve BOROGAN İrina, **Russia's Surveillance State**, World Policy Journal, Vol. 30, No. 3, Fall 2013, http://www.worldpolicy.org/journal/fall2013 /Russia-surveillance, (03.05.2016).

Sputniknews Haber Portalı, **AA: Sputnik'e Erişim Engeli Kaldırıldı.**, https://tr.sputniknews.com/turkiye/201608081024268110-sputnik-tib-erisim-engeli/,(03.01.2017).

Sputniknews Haber Portalı, **Beyaz SarayABD, 35 Rus diplomatı 72 saat içerisinde sınırdışı edecek**, https://tr.sputniknews.com/abd/201612291026553306-abd-rusya-yaptirim-diplomat-sinir-disi/, (22.02.2017).

Sputniknews Haber Portalı, **BM'ye Türkiye-IŞİD bağlantısını gösteren belgeler...**, http://tr.sputniknews.com/rusya/20160401/.../rusya-bm-turkiye-isid.html, (15.04.2016).

Sputniknews Haber Portalı, **Demirtaş: AKP Terör Üreticisi, IŞİD'in Siyasi Uzantısı**, https://tr.sputniknews.com/politika/201602201021016742-demirtas-akp-isid/, (08.11.2016).

Sputniknews Haber Portalı, **Fuat Avni, Rus Uçağının Düşürüleceğini Nereden Biliyordu?**, https://tr.sputniknews.com/columnists/201607241024055041-Rus-ucagi-darbe-pilot/, (08.11.2016).

Sputniknews Haber Portalı, **HDP'li Kürkçü Yanıt Alamadığı IŞID Petrolü Sorusunu Yeniden Sordu**, https://tr. sputniknews.com/turkiye/201603301021838524-hdp-isid-turkiye-petrol-rt-belge/, (08.11.2016).

Sputniknews Haber Portalı, **Putin'den ABD'ye yanıt: Biz hiç kimseyi sınır dışı etmeyeceğiz.**, https://tr.sputniknews.com/rusya/201612301026565257-putin-abdye-yanit-biz-hic-kimseyi-sinir-disi-etmeyecegiz/, (22.02.2017).

Sputniknews Haber Portalı, **Rusya'nın Artan Siber Gücü, ABD'yi Kaygılandırıyor**, http://tr.sputniknews.com/savunma/20150409/1014919049.html, (21.03.2016).

SRIDHARAN Vasudevan, "**Russia Setting up Cyber Warfare Unit Under Military**", http://www.ibtimes.co.uk/russia-cyber-war-hack-moscow-military-snowden-500220 (26.03.2016).

STEWART Phil ve WOLF Jim,**Old Worm Won't Die after 2008 Attack on Military**, Reuters, June 16, 2011, http://www.reuters.com/article/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617, (23.06.2016).

State Security Magazine, **Russia Announces Development of Cyber Military Unit**, http://www.tripwire.com/state-of-security/latest-security-news/russia-announces-development-cyberwar-military-unit/, (26.03.2016).

State of California Department of Justice, **Notice of Security Breach Act**, https://oag.ca.gov/ecrime/databreach/reporting, (13.06.2016).

State of California Department of Justice, **California Assembly Bill-1950**, http://www.steptoe. com/assets/attachments/1477.pdf, (13.06.2016).

Sydney Morning Herald, **International Man of Mystery**, http://www.smh.com.au/technology/ technology-news/international-man-of-mystery-20100409-ryvf.html, (16.06.2016).

The Centre For Counter Intelligence and Security Studies, **Russia's SVR,FSB/GRU Intelligence Services**, http://www.cicentre.com/?page=191, (27.03.2016).

The Department of State (DOD), **The DOD Cyber Strategy**, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, (03.05.2016).

The Guardian, **Cyber Crimes**, http://www.theguardian.com/technology/2007 /nov /15/news.crime, (12.04.2016).

The Guardian, **History of 5-Eyes–explainer**, https://www.theguardian.com /world /2013/dec/02/history-of-5-eyes-explainer, (18.04.2017).

The Guardian, **The Fog of Cyber War**, https://www.theguardian.com/ technology/2009/feb/05/ kyrgyzstan-cyberattack-internet-access, (04.04.2016).

The Guardian, **Assange walks free after nine days in jail**, http://www. theguardian.com/media/2010/dec/16/julian-assange-walks-free-nine-days-jail?intcmp=239, (16.06.2016).

TIRRELL K. William, **United States Cybwer Security Strategy,Policy and Organization: Poorly Postured to Cope With a Post-9/11 Security Environment**, Master Thesis, Washington University, 2012, https://www.hsdl.org/?view&did=729810, (10.01.2016), pp.1-144.

The New York Times, **Leaked Cables Offer Raw Look at U.S. Diplomacy**,http://www.nytimes.com/ 2010/11/29/world/29cables.html, (16.06.2016).

The Telegraph Online News, **Could Cyber Attack on Turkey be a Russian Retaliation?**, http://www. telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation.html, (24.04.2016).

The Telegraph Online News, **CIA plot led to huge blast in Siberian gas pipeline**,http://www. telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html, (02.06.2016).

THOBURN Hoburn, **Rusya Siyasetini Anlama Kılavuzu**, Siyaset, Ekonomi ve Toplum Araştırmalar Vakfı (SETA) Araştırmaları, 2015, pp.1-91, http://file.setav.org/Files/Pdf/20151019183121_rusya-siyasetini-anlama-kilavuzu-pdf.pdf, (19.10.2016).

The Russian Ministry of Defense, **Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space**, https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf, (23.03.2016).

The Russian Ministry of Defense, **Concept of theForeignPolicy of the Russian Federation**,http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D, (24.03.2016).

The USA Air Force Law Review, **Cyber War Edtion**, http://www.afjag. af.mil/shared/media/document/ AFD-091026-024.pdf, (17.02.2016).

TIKK Eneken, **International CyberIncidents: Legal Considerations**, Tallinn, Cooperative Cyber Defense Centre of Excellence, 2010, https://ccdcoe.org/publications /books/legalconsiderations.pdf, (16.04.2014).

TÜRKER Seyda, **Siber Savaş Hukuku ve Uygulama Sorunsalı**, http://www.arastirmax.com/bilimsel-yayin/istanbul-universitesi-hukuk-fakultesi-mecmuasi /71/1/11 77-1227_siber-savas-hukuku-uygulanma-sorunsali, (14.01.2016).

Türk İnternet Haber Sitesi, **Beyaz Saray, Rusya'nın Hackleme Operasyonuna Cevap Verileceğini Açıkladı**, http://www.turk-internet.com/portal/yazigoster.php ?yaziid=54247, (20.02.2017).

Türk İnternet Haber Sitesi, **Clinton'a 4 ay Boyunca Yapılan Siber Saldırılar, Seçimleri Manipule Etti**, http://www.turk-internet.com/portal/yazigoster.php?yaziid =55005, (20.02.2017).

Türk İnternet Sitesi, **6. Gününde Nic.tr Saldırısı Sürüyor Ama Açıklama Yok-Onun Yerine Yorumlar Var.**, http://www.turk-internet.com/portal/yazigoster.php? yaziid=51749, (24.04.2016).

Türk İnternet Haber Sitesi, **Rusya Tor Networkünü ve Anonimlik Araçlarını Erişime Kapatmaya Hazırlanıyor.**, http://www.turk-internet.com/portal/yazigoster .php?yaziid=43607, (27.04.2016).

Türk İnternet Haber Sitesi, **Rusya'da Yürürlüğe Giren Yeni Yasayla Blog'lara Ağır Sorumluluklar Getiriliyor.**, http://www.turk-internet.com/portal/yazi goster.php? yaziid=46851, (27.04.2016).

Türk İnternet Haber Sitesi, **Rusya'da Putin Yönetimi de Internet Sansürüyle Muhalefeti Susturmayı Deniyor.**, http://www.turk-internet.com/portal/yazigoster .php? yaziid=46190, (27.04.2016).

Türk İnternet Sitesi, **Türkiye'de WannaCry Bağlantılı 166 çeşit Fidye Yazılımı Tespit edildi**, http://www.turk-internet.com/portal/yazigoster.php?yaziid=56130, (31.05.2017).

Türk İnternet Haber Sitesi, **Ukraynalılar Rusların Güç Santrallerine Saldırdığını İddia ediyor.**, http://www.turk-internet.com/portal/yazigoster.php? yaziid=51862, (27.04.2016).

Ulusal Siber Olaylara Müdahale Merkezi, **Siber Güvenliğe İlişkin Temel Bilgiler**, https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF001Siber%20Guvenlige%20 Giris%20ve%20Temel%20Kavramlar.pdf, (15.02.2016).

Uluslararası Stratejik Araştırmalar Kurulu (USAK), **WikiLeaks Belgelerinde Türkiye ve Yakın Çevresi- Türkiye, Rusya, Güney Kafkasya ve Ortadoğu ile İlgili Belgeler**, USAK Raporları No:11-03,Nisan 2011, http://www.usak.org.tr/_files/29420161 44245-TYMHBSBGOI.pdf, (17.06.2016).

Uluslararası Politika Akademisi, **Edward Snowden Olayı**, http://politikaakademisi .org/2013/06/28/ edward-snowden-olayi/, (15.06.2016).

United States Department of Defense, **About the Department of Defense (DoD)**,http://www.defense.gov /About-DoD, (30.05.2016).

United States-China Economic and Security Review Commission, **China's Proliferation Practices, And The Development Of Its Cyber and space Warfare Capabilities, United States-China Economic and Security Review Commission**,Washington, 2008, http://origin.www.uscc.gov/sites/default/files/ transcripts/ 5.20.08HearingTranscript.pdf (15.02.2016).

VENTRE Daniel, **A Constructivist Approach of Cybersecurity/Cyberdefense Concepts: Lessons of Security Studies Theories and Discursive Analysis**, http://www.fvv.um.si/knjigarna/eknjige/pdf/ Crime_Social_Control_and_Legitimacy.pdf, (20.02.2016).

United States Department of Defense, **Sustaining U.S. Global Leadership: Priorities for 21st Century Defense**, http://archive.defense.gov/news/Defense _Strategic _Guidance.pdf>, (20.02.2017).

Voice of America, **Russia Plays Big Role in Cyber Spying, Hacking**, http://www.voanews.com/content/russia-plays-big-role-in-cyber-spying-hacking/ 2522915 .html, (12.04.2016).

WALTZ Kenneth, **Anarchic Orders and Balances of Power**, Robert O. Keohane (der.), Neorealism and its Critics, http://www.olivialau.org/ir/archive/wal8.pdf, (18.06.2016).

WebNoloji İnternet Portalı, **Siber Savaşlar ve Online Güvenlik**, http:// webnoloji.net/siber-savaslar-ve-online-guvenlik/, (27.01.2016).

WEEDON Jenand GALANTE Laura, **Intelligence Analysts Dissectthe Headlines: Russia, Hackers, Cyberwar! Not So Fast**, Fire Eye Executive Perspectives,

https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html, (24.04.2016).

WeirdRussia Haber Portalı, **How Social Media Users Responded to Turkey's downing of Russian warplane**, http://weirdrussia.com/2015/11/26/how-social-media-users-responded-to-turkeys-downing-of-russian –warplane /, (08.11.2016).

White House, **Presidential Decision Directive (PDD)-63, Critical Infrastructure Protection**", http://fas.org/irp/offdocs/pdd/pdd-63.htm, (24.05.2016).

WILLIAM C. Ashmore, "**Impact of Alleged Russian CyberAttacks**, "School of Advanced Military Studies United States Army Commandand General Staff College Fort Leavenworth, Kansas", http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf, (19.04.2016).

WIRTZ J. James, **Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy**, NATO CCD COE Publications, Tallinn 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf (05.03.2016).

YAYLA Mehmet, **Hukuki Bir Terim Olarak Siber Savaş**, http://portal. ubap.org.tr/App_Themes/ Dergi/2013-104-1247.pdf, (17.02.2016).

YİNANÇ Barçın, **Doç. Dr. Salih Bıçakcı ile Röportaj/Rusya İsterse Türkiye'yi Taş Devrine Döndürebilir**, http://www.radikal.com.tr/turkiye/rusya-isterse-turkiyeyi-tas-devrine-dondurebilir-1495797/, (24.04.2016).

YENER Yavuz, **Rus Krizinin Gözden Kaçan boyutu: Siber Savaş Tehdidi**, http://www.usak.org.tr/tr/usak-analizleri/yorumlar/rus-krizinin-gozden-kacan-boyutu-siber-savas-tehdidi, (12.04.2016).

YILMAZ Seda ve SAĞIROĞLU Şeref, **Siber Güvenlik Risk Analiz, Tehdit ve Hazırlık Seviyeleri**, "6. Uluslararası Siber Güvenlik ve Kriptoloji Konferansı", http://www.iscturkey.org/s/2226/i/2013-paper105.pdf, (14.01.2016).

ZHENG E. Denise, **2015 DOD Cyber Strategy-Center for Strategic&International Studies**, https://www.csis.org/people/denise-e-zheng, (25.05.2016).

ÖZGEÇMİŞ

Adı - Soyadı: Ali Burak Darıcılı

Doğum Yeri ve Yılı: Ankara-1977

Eğitim Durumu: Başlama Bitirme Yılı: Kurum Adı:

Lise: 1991-1994 İncirli Anadolu Lisesi

Lisans: 1994-1998 Gazi Üniversitesi Uluslararası İlişkiler Bölümü

Yüksek Lisans: 2009-2011 Orta Doğu Üniversitesi Uluslararası İlişkiler Bölümü

Doktora: 2013-2017 Uludağ Üniversitesi Uluslararası İlişkiler Bölümü

Çalıştığı Kurumlar – Başlama –Ayrılma Yılı – Çalışılan Kurum:

1. 2001-2014 Başbakanlık

2. 2014-… Çevre ve Şehircilik Bakanlığı

Yayınlar:

"Enformasyon Savaşı Bağlamında Türkiye ve Rusya Federasyonu İlişkilerinin Analizi", **İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi**, Cilt 4, Sayı 1, Nisan 2017.

"Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi", **Uludağ Üniversitesi Sosyal Bilimler Dergisi**, Cilt 7, Sayı 2, Mayıs 2014.

İleğtişim (e-posta): daricili@yahoo.com

ULUDAĞ ÜNİVERSİTESİ

TEZ ÇOĞALTMA VE ELEKTRONİK YAYIMLAMA İZİN FORMU

Yazar Adı Soyadı	Ali Burak DARICILI
Tez Adı	AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRMALI ANALİZİ
Enstitü	Sosyal Bilimler Enstitüsü
Anabilim Dalı	Uluslararası İlişkiler
Tez Türü	Doktora
Tez Danışman(lar)ı	Prof. Dr. Barış ÖZDAL

Çoğaltma (Fotokopi Çekim) izni

☒ Tezimden fotokopi çekilmesine izin veriyorum

☐ Tezimin sadece içindekiler, özet, kaynakça ve içeriğinin % 10 bölümünün fotokopi çekilmesine izin veriyorum

☐ Tezimden fotokopi çekilmesine izin vermiyorum

Yayımlama izni

☐ Tezimin elektronik ortamda yayımlanmasına izin Veriyorum

Hazırlamış olduğum tezimin belirttiğim hususlar dikkate alınarak, fikri mülkiyet haklarım saklı kalmak üzere Uludağ Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı tarafından hizmete sunulmasına izin verdiğimi beyan ederim.

Tarih : 15.06.2017

İmza :