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

SİBER CAYDIRICILIK KAVRAMININ NÜKLEER CAYDIRICILIK OLGUSU İLE KARŞILAŞTIRMALI ANALİZİ

(YÜKSEK LİSANS TEZİ)

Uğur ERMİŞ

BURSA - 2015

U.Ü. S.B.E.
ULUSLARARASI İLİŞKİLER
ANABİLİM DALI

SİBER CAYDIRICILIK KAVRAMININ NÜKLEER CAYDIRICILIK
OLGUSU İLE KARŞILAŞTIRMALI ANALİZİ
(YÜKSEK LİSANS TEZİ)

Uğur ERMİŞ

BURSA
2015

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

SİBER CAYDIRICILIK KAVRAMININ NÜKLEER CAYDIRICILIK OLGUSU İLE KARŞILAŞTIRMALI ANALİZİ

(YÜKSEK LİSANS TEZİ)

Uğur ERMİŞ

BURSA - 2015

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

SİBER CAYDIRICILIK KAVRAMININ NÜKLEER CAYDIRICILIK OLGUSU İLE KARŞILAŞTIRMALI ANALİZİ

(YÜKSEK LİSANS TEZİ)

Uğur ERMİŞ

Danışman:
Doç. Dr. Barış ÖZDAL

BURSA – 2015

T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Uluslararası İlişkiler Anabilim Dalı'nda 701216003 numaralı Uğur ERMİŞ'in hazırladığı "Siber Caydırıcılık Kavramının Nükleer Caydırıcılık Olgusu İle Karşılaştırmalı Analizi" konulu Yüksek Lisans Çalışması ile ilgili tez savunma sınavı, …../…../ 20…. günü …… - ……..saatleri arasında yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin/çalışmasının …….. (başarılı/başarısız) olduğuna …… (oybirliği/oy çokluğu) ile karar verilmiştir.

Üye (Tez Danışmanı ve Sınav Komisyonu Başkanı)
Akademik Unvanı, Adı Soyadı
Üniversitesi

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi

……/……./ 20…..

ÖZET

Yazar Adı ve Soyadı : Uğur ERMİŞ

Üniversite : Uludağ Üniversitesi

Enstitü : Sosyal Bilimler Enstitüsü

Anabilim Dalı : Uluslararası İlişkiler

Bilim Dalı :

Tezin Niteliği : Yüksek Lisans Tezi

Sayfa Sayısı : X + 136

Mezuniyet Tarihi : …. / …. / 20……..

Tez Danışmanı : Doç. Dr. Barış ÖZDAL

SİBER CAYDIRICILIK KAVRAMININ NÜKLEER CAYDIRICILIK OLGUSU İLE KARŞILAŞTIRMALI ANALİZİ

Son yirmi yıl içinde internet ve mobil iletişim gibi ağ tabanlarının oluşumu, küreselleşme sürecinin etkisiyle her disiplini olduğu gibi uluslararası ilişkileri de etkilemiştir. Siber uzayın devletler açısından kara, deniz, hava ve uzaydan sonra beşinci boyut olarak güvenlik alanı kabul edilmeye başlaması da hiç şüphesiz iletişim teknolojisindeki söz konusu değişimlerin bir sonucudur. Diğer bir deyişle teritoryal sınırların önemini kaybettiği, devletin yanı sıra çok uluslu şirketlerin ve bireylerin aktör olarak yer alabildiği, kontrol edilmesi zor bir güvenlik alanı olan siber uzay, 2000'li yılların başından itibaren uluslararası ilişkilerde etkisini göstermeye başlamıştır.

Çalışmamızda ise nükleer caydırıcılık olgusunun siber caydırıcılık kavramı ile karşılaştırmalı analizi çerçevesinde, nükleer silahlarla sağlanan caydırıcılığın siber uzayda sağlanıp sağlanamayacağı sorusuna cevap verilmeye çalışılacaktır. Bu çerçevede çalışmamızın ilk bölümünde realizm, liberalizm, Kopenhag Okulu ve İngiliz Okulu'nun güvenlik olgusuna bakış açıları karşılaştırmalı olarak ele alınacaktır. İkinci bölümde nükleer caydırıcılık kavramı, II. Dünya Savaşı esnasında Almanya ve ABD'nin çabaları, ilk nükleer bombanın kullanılması, hidrojen bombasının üretilmesi, Küba Ekim Füzeleri Krizi'ne kadar ABD Başkanlarının askeri doktrinleri, nükleer silahların kontrol altında tutulma girişimleri ele alınacaktır. Üçüncü ve son bölümde ise siber uzayda saldırı stratejilerine, araçlarına, siber saldırı türlerine ve siber saldırı örneklerine değinilip, siber caydırıcılığın mümkün olup olmadığı literatürdeki teorisyenlerin yaklaşımları çerçevesinde analiz edilecektir.

Anahtar Kelimeler: Siber Uzay, Nükleer Caydırıcılık, Siber Caydırıcılık, Kritik Altyapı, Güvenlik.

ABSTRACT

Name and Surname : Uğur ERMİŞ

University : Uludağ University

Institution : Social Science Institution

Field :International Relations

Branch :

Degree Awarded : Master

Page Number : X + 136

Degree Date : …. / …. / 20…….

Comparative Analysis of the Nuclear Deterrence and Cyber Deterrence Concept

Formation of networks such as internet and mobile communication systems via globalization process impacted on international relations like in every scientific discipline in last twenty years. Cyber-Space, which is in scope of our work, has been approved as fifth security field with territory, marine-space and aero-space with regards to states is undoubtedly the result of aforementioned changes in communication technology. In other words, Cyber-space is a security field in which territorial borders lost their importance, multinational companies and individuals are approved as actors and also hard to be controlled, have taken efect in international relations from the beginning of 2000s.

In our work, it will be endeavoured to understand whether deterrence with nuclear weapons is possible in cyber-space or not within the frame of comparative analysis of nuclear deterrence and cyber deterrence. In this context, it will be discussed the approaches of realism, liberalism, Copenhagen School and English School on Security concept comparatively in the first chapter. In the second chapter, nuclear deterrence concept, efforts of Germany and the USA during the WWII, using of first nuclear bomb, production of hydrogen bomb, military doctrines of the USA Presidents until Cuban Missile Crisis and initiatives to control nuclear weapons will be discussed. In the third and last chapter, offense strategies in cyber-space, offensive strategy tools, cyber-attack types and cyber-attack examples will be mentioned and it will be analysed whether cyber-deterrence is possible or not within the frame of approaches of theoreticians in literature.

Keywords: Cyber-Space, Nuclear Deterrence, Cyber Deterrence, Critical Infrastructure, Security.

İÇİNDEKİLER

Sayfa

ÜÇÜNCÜ BÖLÜM

SİBER UZAY VE SİBER CAYDIRICILIK

KISALTMALAR

Kısaltma	Bibliyografik Bilgi
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ABM	Anti-Ballistic Missile
APT	Advanced Persistent Threat
Bkz.	Bakınız
BM	Birleşmiş Milletler
CCD COE	Cooperative Cyber Defence Centre Of Excellence
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
çev.	Çeviren
DARPA	The Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DHS	The Department of Homeland Security
DOS	Denial of Service
edt.	Editör
EXE.	Executable File
ICBM	Intercontinental Ballistic Missile
IP	Internet Protocol
KBRN	Kimyasal, Biyolojik, Radyolojik ve Nükleer
MAD	Mutual Assured Destruction
md.	Madde
MIRV	Multiple Independently Targetable Reentry Vehicle
NATO	North Atlantic Treaty Organization
NCSA	National Cyber Security Alliance
NCSAM	National Cyber Security Awareness Month
NPT	Non-Proliferation Treaty
NSA	National Security Agency
NSC	National Security Council
nu.	Numara
p.	Page
RF	Rusya Federasyonu
S.	Sayı
s.	Sayfa
SALT	Strategic Arms Limitation Talks
SBKP	Sovyetler Birliği Komünist Partisi
SCADA	Supervisory Control and Data Acquisition

SDI	Strategic Defense Initiative
SLBM	Submarine-Launched Ballistic Missile
ss.	Sayfadan sayfaya
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
TDK	Türk Dil Kurumu
TNT	Trinitrotoluen
Vol.	Volume
Yy.	Yüzyıl

GİRİŞ

Nükleer silahların varlığı, Soğuk Savaş boyunca bloklar arasında II. Dünya Savaşı gibi büyük bir sıcak savaşın yaşanmamasının en önemli nedenlerinden biri olmuştur. Aynı nedensellik kapsamında devletlerin güvenlik ihtiyaçlarından dolayı nükleer silah kapasitelerinin oluşturulmasından günümüze değin ortaya konulan tüm güvenlik yapılarında aynı caydırıcılık düzeyi sağlanmaya çalışılmıştır. Günümüz itibariyle devletler kara, deniz, hava ve uzaydan sonra beşinci boyut olarak kabul edilen siber uzayı ise güvenliklerini sağlamak için yeni bir alan olarak görmektedirler. Bu doğrultuda çalışmamızda "nükleer caydırıcılık" ve siber uzayda varlığı tartışılan "siber caydırıcılık" olgularının karşılaştırmalı analizi çerçevesinde, nükleer silahlarla sağlanan caydırıcılığın, siber uzayda sağlanıp sağlanamayacağı irdelenecektir.

Bu soru bağlamında çalışmanın birinci bölümünde, uluslararası ilişkilerin ana akımını oluşturan "realizm" ve "liberalizm" teorileri karşılaştırmalı olarak ele alınacaktır. Bu karşılaştırmanın ardından, realizmin ve ondan temellenen neorealizmin güvenlik kavramına ilişkin temel söylemleri ve güvenlik yaklaşımları irdelenecektir. Uluslararası sistemde, en genel manada "işbirliği" yerine "çatışmayı" ön plana çıkaran realist/neorealist kuramların "caydırıcılığa" verdikleri önem ise teorik çerçeve dâhilinde ele alınacak son konudur. Bu yöntemle çalışmamızda, uluslararası ilişkiler teorilerine genel bir çerçeveden bakılarak, bu teorilerde güvenliğin yeri incelenecektir. Akabinde ise güvenliğin işbirliği yerine silahlanma ve gerekli durumlarda çatışmayla sağlanacağını kabul eden teorilerde caydırıcılığın işlevi, genelden özele giden bir sırayla ele alınacaktır.

Çalışmamızın ikinci bölümünde ise "nükleer caydırıcılık" olgusu ayrıntılı olarak incelenecektir. Bu bağlamda Paul H. Nitze'nin ortaya koyduğu nükleer seçenekler üzerinden bu bölüm beş altbaşlıkta ayrıntılandırılıcaktır. İlk olarak "Asgari Caydırıcılık" altbaşlığında nükleer silahların üretilmesi noktasında II. Dünya Savaşı içerisinde Almanya ve Amerika Birleşik Devletleri (ABD)'nin çabaları genel hatlarıyla incelenecek olup, ilk nükleer bombanın savaşta kullanılmasından kitlesel yıkımda büyük değişime yol açan hidrojen bombasının[1] üretilmesine kadar geçen süreç ele alınacaktır. İkinci olarak "Kentsel ve Endüstriyel Bölgelere Kitlesel Mukabele" altbaşlığında özellikle ABD

[1] Hidrojen bombası, füzyon bombası ya da termonükleer bomba olarak da isimlendirilmektedir.

Dışişleri Bakanı John Foster Dulles'ın savunuculuğunu yaptığı "*New Look*" yaklaşımı çerçevesinde ortaya konulan "*Topyekûn Mukabele Doktrini"*nden başlayarak, dünyanın nükleer savaşla yok olmanın eşiğine geldiği Küba Füze Krizi'ne kadar geçen süreç irdelenecektir. "Esnek Mukabele" altbaşlığı ise ABD Başkanı John F. Kennedy döneminde topyekûn mukabeleden vazgeçilmesi sonrasında uygulanmaya başlanan süreç ele alınacaktır. Bu kapsamda birlikte ilk nükleer silahsızlanma girişimi olan Stratejik Silahların Sınırlandırılması Görüşmeleri (Strategic Arms Limitation Talks)'ne[2] kadar olan süreçte nükleer caydırıcılık bağlamında yaşanan gelişmelere de bölüm içerisinde yer verilecektir. 1972 yılında Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) ve ABD arasında SALT I neticesinde yürürlüğe giren anlaşmaların sonucunda iki devlet füzesavar sistemi üretiminden önemli ölçüde vazgeçerek, büyük şehirlerini nükleer silah tehlikesine açık bırakarak hassas bir denge kurmuştur. Bu durum, tehlikeyi arttırmaktan öte her iki devletinde saldırması durumunda mutlak yok oluşa neden olacağı için caydırıcılığın güvenilirliğini arttırmıştır. "Düşman Tarafı Nükleer Savaş Kazanabilecek Bir Kapasiteden Yoksun Bırakmak" altbaşlığında bu durum ayrıntılı olarak ele alınacaktır. 1979 yılında SSCB'nin Afganistan'ı işgali sonrasında ise dönemin ABD Başkanı Ronald Reagan SALT I ile kurulan dengeye son vererek "*Yıldız Savaşları*" olarak da bilinen "*Strategic Defense Initiative*" projesini başlatmıştır. Bu sebeple ikinci bölümün son alt başlığı olan "Nükleer Savaş Kazandıracak Kapasite"'de "*Strategic Defense Initiative*"'den itibaren Soğuk Savaş'ın sona erdiği 1991 yılına kadar geçen süreçte yaşanan gelişmeler ele alınacaktır.

Literatürde genel kabul gördüğü üzere SSCB'nin dağılmasıyla birlikte dünyanın sonunu getireceği düşünülen nükleer çekişme de büyük ölçüde son bulmuştur. Günümüzde başta Birleşmiş Milletler (BM) Güvenlik Konseyi üyesi devletler olmak üzere dokuz devletin nükleer silah sahibi olduğu düşünülse de nükleer silahların devletlerin kutuplaşmasında bir araç olarak kullanılması artık söz konusu değildir. Nükleer silahların yayılması ise uluslararası antlaşmalar sayesinde kontrol altında tutulmaktadır. Bu nedenlerden ötürü çalışmamızın ikinci bölümü, Soğuk Savaş'ın bitimi ile sınırlandırılacaktır.

Çalışmamızın üçüncü bölümünde ise siber uzayda büyük öneme sahip olacağı düşünülen "caydırıcılık" olgusu, bütüncül bir bakış açısıyla sunulmaya çalışılacaktır. Siber

[2] Sonraki süreçte yapılan ilk görüşmeler SALT I olarak tanımlanmıştır.

uzayda saldırı stratejilerini ve araçlarını bilmek, caydırıcılığın işlevselliğine dair kanaat oluşturmak için oldukça önemlidir. Bu doğrultuda üçüncü bölümde öncelikle siber saldırı türleri ve aralarındaki farklar, bu saldırıların teknik kabiliyetleri ve kapasiteleri ele alınacaktır. Sonrasında ise geliştirilen bu strateji ve araçların sahadaki kabiliyetleri ve devletler üzerindeki etkisini göstermek amacıyla siber uzaya bakışta kırılmalara neden olan Kosova Krizi, Estonya Saldırısı, Gürcistan Saldırısı ve İran'a düzenlenen STUXNET Saldırısı ayrıntılı olarak incelenecektir. Çalışma kapsamında yapılan ön okuma doğrultusunda siber uzayda gerçekleştirilen saldırıların, kritik altyapılarla ilişkisi öne çıkmış olup; kritik altyapıların korunmasının caydırıcılıkta oldukça önemli olduğu fark edilmiştir.

Bu bağlamda siber uzayda gerçekleştirilen saldırıların incelenmesinin ardından, siber güvenliğin sağlanmasında kritik altyapılarının korunmasının önemi teorik bir bakışla ayrıntılı olarak irdelenecektir. Siber caydırıcılığa ilişkin oluşmaya başlayan sınırlı literatür, bu alanda genellemelere gidilerek bütüncül bir bakış açısıyla inceleme yapmayı zorlaştırmaktadır. Bu nedenle "Siber Caydırıcılık Mümkün Mü" altbaşlığında, caydırıcılığın siber uzayda sağlanıp sağlanamayacağını incelemek için, kavramlar üzerinden yazarları incelemek yerine literatürü oluşturan yazarların kavramsallaştırmalarına ve bu kavramsallaştırmalar üzerinden oluşturdukları görüşlerine ayrıntılı olarak yer verilecektir.

I. BÖLÜM

TEORİK ÇERÇEVE

Çalışmamızın ana başlığı olan nükleer caydırıcılık olgusunun siber caydırıcılık kavramı ile karşılaştırmalı analizi çerçevesinde, nükleer silahlarla sağlanan caydırıcılığın siber uzayda[3] sağlanıp sağlanamayacağı sorusuna cevap verilmeye çalışılacaktır. Bu soru bağlamında çalışmanın birinci bölümünde uluslararası ilişkilerin ana akımını oluşturan realizm ve liberalizm karşılaştırmalı olarak ele alınacaktır. Bu karşılaştırmanın ardından, realizmin ve ondan temellenen neorealizme ait görüşlerin güvenlik kavramına ilişkin temel söylemleri ve güvenliğe bakışları analiz edilecektir. Uluslararası sistemde, en genel manada işbirliği yerine çatışmayı ön plana çıkaran realist/neorealist kuramların caydırıcılığa verdikleri önem ise teorik çerçeve dâhilinde ele alınacak son konudur. Bu yöntemle çalışmamızda, uluslararası ilişkiler teorilerine genel bir çerçeveden bakılarak, bu teorilerde güvenliğin yeri incelenecektir. Akabinde ise güvenliğin işbirliği yerine silahlanma ve gerekli durumlarda çatışmayla sağlanacağını kabul eden teorilerde caydırıcılığın işlevi, genelden özele giden bir sırayla ele alınacaktır.

1. Klasik Uluslararası İlişkiler Teorilerinin Temel Yaklaşımları

"İngiliz Okulu, 1970'li yıllarda bir grup İngiliz yazar tarafından uluslararası toplumu temel analiz birimi olarak alan bir akım olarak bilinmektedir".[4] II. Dünya Savaşı sonrası dönemde Birleşik Krallık'ta oluşan İngiliz Okulu'nun temelleri Britanya Uluslararası Politika Kuramı Komitesi'nde çalışan Herbert Butterfield, Martin Wight, Adam Watson ve Hedley Bull tarafından atılmış ve sonraki süreçte Tim Dunne ve N. J.

[3] Literatürde "*cyber space*" kavramının Türkçe karşılığı konusunda bir fikir birliği bulunmamaktadır. Space kelimesi İngilizce'den Türkçeye mekân /alan /uzam şeklinde çevrilebileceği gibi uzay olarak da çevrilebilmektedir. Bu iki Türkçe kelimeye alternatif olarak "internet" de yapılan çalışmalarda kullanılmaktadır. Lakin "internet", "siber uzayın" kendisini değil içeriklerinden birini oluşturmaktadır. Çalışmamızda mekan / alan / uzam kelimesi yerine "uzay" kelimesinin seçilmesinin temel nedeni siber uzayın altyapısını oluşturan fiziki altyapıların egemenlik sınırları dâhilinde devletler tarafından yetki sınırları içerisinde görülebilmesine rağmen bu altyapı üzerinde oluşan yapının doğası gereği uzaya benzer şekilde, sınırlarının belirsiz ve klasik egemenlik iddialarına uygun olmamasıdır. Bu nedenle çalışmamız boyunca siber uzay kavramı tercih edilecektir.

[4] Tayyar Arı, *Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İşbirliği*, 8. Baskı, Bursa: MKM, 2013, s. 512

Wheeler'ın okula katkıları olmuştur.[5] Bu anlamda İngiliz Okulu yukarıda adı geçen dört düşünür tarafından şekillendirilirken, söz konusu dönemde Birleşik Krallık'ta çalışan diğer uluslararası ilişkiler teorisyenleri (E. H. Carr gibi) İngiliz Okulu'nun parçası olarak kabul edilmemektedir.[6]

İngiliz Okulu'nun temel iddiası, egemen devletlerin bir toplum oluşturduğudur. Fakat devletler, daha yüksek bir otoriteye boyun eğmek zorunda olmadıklarından bu toplumun yapısı anarşiktir[7]. İngiliz Okulu'na göre uluslararası ilişkiler literatüründe, Hobbescu karamsarlıkla ve Kantçı iyimserlikle aynı görüşleri paylaşmayan, Grotiusçu olarak bilinen ve orta yolu (via media) temsil eden üçüncü bir yaklaşım daha bulunmaktadır. Hobbescular, temelde insan doğasının kötü ve çıkarcı olduğu ön kabulüne sahip olduklarından, içinde yaşadığımız şiddete eğilimli dünyanın ötesine geçmenin mümkün olmadığına inanırlar. Diğer taraftan Kantçılarsa, şiddete dayalı çatışmaları "*aşmanın*" ve daha barışçıl bir yaşam biçimine doğru ilerlemenin mümkün olduğunu savunurlar. Buna karşılık, orta yolu temsil eden Grotiusçu düşünürler, şiddeti ve savaşı bütünüyle yok etmenin imkânsız olmasa bile çok zor olduğunu kabul ederlerken; şiddet ve savaşın aşırılıklarının "*azaltılmasını*" sağlayacak kural ve normları geliştirmenin mümkün olduğunu savunurlar. Groutiusçular realist yaklaşımla birçok noktada aynı kabullere sahip olsalar da son noktada şiddetin kurallarla kontrol altında tutulabileceğine inanırlar. Bu çerçevede Grotiusçular, Hobbesculardan daha iyimser, Kantçılardansa daha karamsardırlar.[8]

İngiliz Okulu'nun, diğer uluslararası ilişkiler kuramları ile karşılaştırıldığında belki de en önemli özelliği yukarıda örneği verilen eklektik yapısıdır. Bu çerçevede İngiliz Okulu, uluslararası ilişkilerin klasik teorilerini bir bütün olarak içermekte ve bunları birleştirip kullanmaktadır denilebilir. Örneğin İngiliz Okulu'nun kurucusu kabul edilen Martin Wight, tarih boyunca insanlığın devletlerarası ilişkilerdeki davranışını

[5] Bu konuda ayrıntılı bilgi için bkz. Balkan Devlen ve Özgür Özdamar , "Uluslararası İlişkilerde İngiliz Okulu Kuramı: Kökenleri, Kavramları ve Tartışmaları", *Uluslararası İlişkiler*, Cilt 7, Sayı 25 (Bahar 2010), s. 45; Chris Brown and Kirsten Ainley, *Understanding International Relations* Third Edition, Palgrave Macmillan, 2005, p. 50.
[6] Devlen ve Özdamar, loc. cit.
[7] Scott Burchill et. al., *Uluslararası İlişkiler Teorileri*, çev. Ali Aslan – Muhammed Ali Ağcan, 2. Baskı, İstanbul: Küre Yayınları, s. 119.
[8] Martin Wight, *Power Politics*, Londra, Penguin, 1979, passim'den aktaran John Baylis, "Uluslararası İlişkilerde Güvenlik Kavramı", çev. Burcu Yavuz, *Uluslararası İlişkiler*, Cilt 5, Sayı 18 (Yaz 2008), s. 70.

betimleyen üç geleneksel okulun önemini ve kendi siyasal düşüncesine katkısını belirtmiştir.[9] Bunlar Makyavelci (ya da Hobbescu) gerçekçilik, Grotiusçu akılcılık ve Kantçı devrimciliktir. Makyavelciler uluslararası ilişkileri çatışma açısından incelerken; Kantçı devrimciler değişik devletlerde yaşayan insan gruplarının veya sınıfların ortak çıkar, fikir ve ideolojiler çerçevesinde hareket edebileceğini iddia ederler. İngiliz Okulu bu iki geleneksel bakış açısı ile doğrudan ilgilidir, bunların bazı varsayım ve önermelerinden yararlanmıştır.[10] Bu bağlamda İngiliz Okulu'nun üyeleri realizmin ve idealizmin bazı söylemlerinin etkisi altında kalsa da orta yola yönelerek bu iki yaklaşım arasından bir tercihte bulunmazlar.[11]

Orta yol olarak kendisini konumlandıran İngiliz Okulu'nun yukarıda bahsedilen eklektik yapısı, iki klasik uluslararası ilişkiler teorisi olan realizmin ve liberalizmin temel yaklaşımlarını karşılaştırılmalı olarak incelemek için de gerekli olan altyapıyı sunmaktadır. Diğer bir deyişle uluslararası ilişkiler kuramlarının temelini oluşturan bu iki büyük teorinin güvenliğe yaklaşımlarını anlayabilmek için temel söylemlerini bilmek büyük bir öneme sahiptir.

1.1 Realizm ve Güvenlik

Antik Çağ'da Thucydides'in "*Peloponez Savaşları*" adlı eserinde ve Orta Çağ'da Niccolo Machiavelli'nin "*Hükümdar (Prens)*" adlı eserinde realist yaklaşımın ilk örnekleri verilmiştir. Thomas Hobbes'un "*Leviathan*" adlı eserinde insanın özüne ve bu noktadan yola çıkarak devletlerin oluşumuna dair söylemleri ve modern zamanda Edward H. Carr, Hans J. Morgenthau'nun yaptığı çalışmalar uluslararası ilişkilerde realizmi kurumsallaştırmıştır.[12]

[9] Wight,"International Theory: The Three Traditions", passim'den aktaran Devlen ve Özdamar, loc. cit.
[10] Devlen ve Özdamar, op. cit., s. 50.
[11] Burchill, et. al., op. cit., p. 120.
[12] Bu konuda ayrıntılı bilgi için bkz. Niccolo Machiavelli, *Hükümdar*, Çeviren: Semih Lim, 1. Baskı, İstanbul: Türkiye İş Bankası Kültür Yayınları, 2008, passim. ; Thomas Hobbes, *Leviathan*, 7. Baskı, İstanbul: Yapı Kredi Yayınları, 2008, passim.; Hans J. Morgenthau, *Politics Amongs Nations The Struggle For Power And Peace*, First Edition, New York: Alfred A. Knoph, 1948, passim.

Realizm dört temel varsayım üzerinde şekillenen güç ve güvenlik merkezli bir uluslararası ilişkiler teorisidir. Genel ve soyut olarak bu varsayımlar:[13]

1. *"Devletler, merkezi meşru bir yönetimin olmadığı anarşik dünyada biricik ve en önemli aktörlerdir,*
2. *Devlet üniter bir aktördür,*
3. *Devlet rasyonel bir aktördür,*
4. *Alçak ve yüksek politika ayrımı vardır ve ulusal güvenlik yüksek politikanın konusudur."*

Realizmde devletler, analizin temel birimlerini oluştururlar. Bunun temel nedeni ise realistlerin, devletin merkezi meşru bir yönetimin olmadığı anarşik dünyada biricik ve en önemli aktör olduğuna ilişkin kabulüdür. Uluslararası ilişkiler ise devletler arasında gerçekleşir. Çokuluslu şirketler ve diğer uluslararası organizasyonlar gibi devlet-dışı aktörler (Nonstate Actors) ya da North Atlantic Treaty Organization (NATO) veya BM gibi uluslararası örgütler kendilerine ait egemenlikleri olmadığı ve kararlarını otonom olarak vermedikleri için aktör olarak kabul edilmezler ve çok az öneme sahiptirler.

Realizmin ikinci varsayımı olan devletin üniter bir aktör olduğu kabulü ise realistlerin devleti mecazi bir kabukla çevrelenmiş olarak kabul etmelerinden ileri gelmektedir. Devlet, uluslararası sistemde bütünleşik bir yapı olarak değerlendirilmektedir. Realist genel kabule göre devlet içindeki farklı politik düşünceler nihayetinde otoriter bir şekilde çözülür ve hükümetler devletin tamamı adına görüş bildiren tek sestirler.

Devleti rasyonel bir aktör olarak kabul eden üçüncü varsayıma göre ise devlet karar verme sürecinde kapasitesi doğrultusunda bütün alternatifleri göz önünde bulundurur ve her olasılığın muhtemel getiri ve götürülerini hesaplar. Bu rasyonel süreç sonunda karar vericiler her alternatifi değerlendirir ve çıkarını maksimize edeni seçer.

Realizmin dördüncü ve son varsayımına göre askeri ve bununla ilişkili politik konular dünya politikasına egemen olmaktadır. Realistler tarafından devletin varlığını

[13] Bu konuda ayrıntılı bilgi için bkz. Paul R. Viotti and Mark V. Kauppi, *International Relations Theory*, Longman, 2010, pp. 42-43.

devam ettirmeye yönelik konular yüksek politika (high politics), bunun dışındaki tüm konular ise alçak politika (low politics) olarak kabul edilmektedir. Realistler, devletler arasında yaşanan veya yaşanması muhtemel çatışmalar üzerine odaklanır. Bu bağlamda uluslararası dengenin nasıl sağlandığını ve devam ettirildiğini, nasıl bozulduğunu ve anlaşmazlıkları çözmede gücün kullanımını incelerler. Tüm bu nedenlerden dolayı güç olgusu realizmin temelindedir.[14]

Realistler yukarıda açıklanan bu dört temel varsayım üzerinden insan bencilliği ile bir uluslararası üst otoritenin yokluğunun yani anarşinin siyaset üzerinde yarattığı işbirliğini zorlaştıran, güvenlik ihtiyacı ve sürekli güçlenmeye neden olan kısıtlamalara vurgu yaparlar.[15] Realizmin insanın doğasına ilişkin söylemleri Thomas Hobbes'un düşünceleri üzerinde şekillenmektedir. Hobbes, Leviathan adlı meşhur eserinde üç temel varsayımda bulunur:[16]

> *1. "İnsanlar eşittir.*
> *2. İnsanların birbirleriyle etkileşime girmeleri, bir anarşi ortamında gerçekleşir.*
> *3. İnsanlar rekabet, güvensizlik ve gurur tarafından harekete geçirilir."*

Hobbes'un ortaya koyduğu bu üç temel varsayım bireyleri karşı karşıya getireceği için savaş durumu ortaya çıkar ve güvenliği sağlamak için doğal hukuk yetersiz kalır. Hobbes, Leviathan'da bu durumu şu şekilde ifade etmiştir: [17]

> "*… güvenlik doğal hukukla sağlanamaz. Çünkü adalet, hakkaniyet, tevazu, merhamet ve özet olarak, bize ne yapılmasını istiyorsak başkalarına da onu yapmak gibi doğa yasaları, bunlara uyulmasını sağlayacak bir gücün korkusu olmaksızın, bizi taraf tutmaya, kibre, öç almaya ve benzer şeylere sürükleyen doğal duygularımıza aykırıdır. Kılıcın zoru olmadıkça ahitler sözlerden ibarettir ve insanı güvence altına almaya yetmez"*

Bahsedilen *doğal duygu hali* ise insanın doğuştan bencil ve çıkarcı olmasından temellenmektedir. Bu durum insanı sürekli bir savaş haline sürüklemektedir ve Hobbes'a göre böyle bir savaşta hiçbir şey adalete aykırı değildir.[18]

---

[14] Bu konuda ayrıntılı bilgi için bkz. Ibid.
[15] Burchill et. al., op. cit., s. 50
[16] Ibid., s.51.
[17] Hobbes, op. cit., s. 127.
[18] Bu konuda ayrıntılı bilgi için bakınız. Ibid., ss. 92-96.

Bir diğer realist yazar olan Edward H. Carr, iki dünya savaşı arası dönemde uluslararası politikada ortaya çıkan idealizmi Thomas Hobbes'un ortaya attığı temeller üzerinden eleştirmiştir. II. Dünya Savaşı'nın çıkmasını bu politikaların engelleyemediğini belirten Carr, "*The Twenty Years Crisis"* adlı eserinde idealizmin/liberalizmin eleştirisini yapmış ve moral değerlerin uluslararası ilişkilerde yeri olmadığını belirtmiştir. Bu bağlamda Carr uluslararası politikanın ne olması gerektiği gibi normatif bir önermeyle değil ne olduğu ile ilgilenilmesi gerektiğine vurgu yapmıştır.[19]

Realizmin kurumsallaşmasında büyük rol oynayan Hans J. Morgenthau ise "Politics Among Nations" isimli çalışmasının ikinci baskısına giriş olarak siyasal realizmin altı ilkesini eklemiştir. Bu ilkelere göre:[20]

> *1. "Genel olarak toplum gibi politikanın da kökleri, insan doğasında bulunan objektif yasalarca yönetilir. Toplumu geliştirmek için önce bu yasalar anlaşılmalıdır. Bu yasaların işleyişi bizim tercihlerimizden etkilenmez. İnsan sadece kaybetme riski olduğunda bu yasalara meydan okuyacaktır.*
> *2. Siyasal gerçekliğin hareket noktasını güç çerçevesinde tanımlanan çıkar kavramı oluşturur. Çıkar, uluslararası ilişkiler ve gerçekler arasındaki bağlantıyı sağlar. Bu kavram politikayı ahlaktan, etikten ve dinden ayırır. Bu bakış açısı olmaksızın, uluslararası veya ulusal hiçbir politikanın anlaşılması mümkün değildir.*
> *3. Realist varsayıma göre çıkar kavramı politikanın özüdür, zaman ve mekândan etkilenmez. Thucydides'in sözüyle "çıkar, devlet ve birey arasındaki en güvenilir bağdır."*
> *4. Evrensel moral prensiplerinin devletlerin dış politikadaki eylemlerine aynen uygulanması mümkün değildir. Devlet, ulusal çıkar peşindeyken bireysel ahlaki ilkeleri gözetemez.*
> *5. Siyasal gerçeklik bir devletin siyasal eylemlerinin ahlaki olup olmadığını, evrensel ahlak prensipleriyle ölçmeye kalkmaz.*
> *6. Siyasal realizmi diğer teorilerden ayıran şey gerçeğin kendisidir. Politik meselelere entelektüel ve ahlaki yaklaşmanın hiçbir kazancı yoktur."*

Morgenthau'nun ortaya koyduğu bu altı ilke realizmin güvenliğe, güce ve çıkara bakışını net bir biçimde ortaya koymuştur. Kısa bir şekilde özetlersek, klasik realizme göre devletlerarası ilişkiler çıkar temelinde gerçekleşir. İlişkilerin çıkar temelinde gerçekleşmesi ahlaki değerler etrafında şekillenen işbirliğine izin vermez. Bu bağlamda

[19] John A. Vasquez, *The Power of Power Politics*, UK: Cambridge University Press, 1998, p. 35.
[20] Bu konuda ayrıntılı bilgi için bkz. Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, Fifth Edition, Revised, New York: Alfred A. Knopf, 1978, pp. 4-15.

devletlerin temel amacı daha fazla güce sahip olmaktır. Elde edilen bu güç aynı zamanda güvenliği de sağlayacaktır.

1.2 İdealizm/Liberalizm ve Güvenlik

Yukarıda genel ve soyut olarak aktardığımız realizmin temellerine ilişkin teorisyenlerin ortaya koyduğu yaklaşımlar ve idealizme/liberalizme getirdikleri eleştiriler, realizmi ontolojik açıdan olmasa da söylem itibariyle liberalizmin tam karşısında konumlandırmıştır. Antik Çağ'dan günümüze gelen düşünürlerinin ortaya koyduğu realizmin ardından, 18. asırda Avrupa'da yaşanan Aydınlanma Çağı ile temelleri atılan liberalizm, uluslararası ilişkilerdeki en etkili ve bir diğer büyük teori olmuştur. Rasyonalizmin, özgürlüğün ve insanoğlunun ilerlemesinin savunusunu yapan liberalizm; tarihsel süreçte Aydınlanma Çağı ile dile getirilen insan hakları, anayasacılık, demokrasi ve kuvvetler ayrılığı gibi günümüz uluslararası ilişkilerinde önemli yer tutan kavramların düşünsel temellerini oluşturmaktadır.[21]

Liberalizmin realizmle söylemlerinde ki farkları ve bu noktadan hareketle güvenliğe bakışını anlayabilmemiz için temel söylemlerini bilmemiz oldukça önemlidir. Uluslararası ilişkilerde liberalizm dört temel varsayım üzerinden şekillenmektedir. Genel ve soyut olarak bu varsayımlar:[22]

> *1. "Devletler ve uluslar-aşırı (transnational) aktörler dünya politikasının önemli öğeleridir,*
> *2. Devletler uluslararası ilişkilerin üniter aktörleri değildir,*
> *3. Devletler ya da devlet-dışı aktörlerin kurdukları ekonomik veya diğer bağlılık/bağımlılıklar devletlerin davranışını etkilemektedir,*
> *4. Uluslararası ilişkileri anlamak için devlet-toplum ilişkisini anlamak kritik öneme sahiptir."*

Realizmin aksine liberalizmde, ilk varsayımdan da anlaşılacağı üzere, uluslararası ilişkilerin yegâne aktörü devlet değildir. Liberal düşünceye göre uluslararası kuruluşlar da bağımsız bir şekilde karar alabilmektedirler. Benzer şekilde devlet dışı örgütler, sivil

[21] Burchill et. al., op. cit., s. 81.
[22] Viotti and Kauppi, op. cit., pp. 118-120.

toplum kuruluşları, çok uluslu şirketler ve hatta bazı durumlarda bireyler de dünya politikasında önemli roller oynayabilmektedir.[23]

Liberalizmin ikinci varsayımına göre devletler uluslararası ilişkilerin üniter aktörleri değildirler. Herhangi bir uluslararası kuruluşun personeli dahi devletin politikasından duyduğu rahatsızlığı gündeme getirebilir ya da kuruluşun ortaya koyduğu bilgiler, devletin çıkarları doğrultusunda yapacağı tercihi değiştirebilir. Liberalizmin üçüncü varsayımına göre ise bağlılık/bağımlılıklar devletlerin davranışını etkilemektedir. Liberallere göre küreselleşmenin de etkisiyle dünya sadece ekonomik olarak değil aynı zamanda kültürel, politik, sosyal ve uluslar-aşırı bağlarla da yakınlaşmaktadır. Gittikçe globalleşen dünyada uluslararası ve devlet-dışı aktörler, çok uluslu şirketler, gruplar yada bireyler çok karmaşık ilişkiler kurabilmekte koalisyonlar oluşturabilmektedirler. Liberalizmin dördüncü ve son varsayımına göre ise devlet-toplum ilişkisini anlamak oldukça önemlidir. Devlet-toplum ilişkisinin sonucunda devletlerin dış politik tercihleri genişleyebilir. Bu bağlamda liberaller, realistlerin ortaya attığı güvenliği ilgilendiren genelde askeri odaklı konuların yüksek politika, diğer konuların alçak politika olduğu şeklindeki ayrımı da reddederler. Liberallere göre yüksek-alçak politika ayrımı yanlıştır. Zira ekonomik ve sosyal konular da oldukça önemlidir.[24]

Liberalizmin uluslararası ilişkilere yönelik yukarıda bahsedilen bu dört temel varsayımının temellerine ve insan doğasına ilişkin yaklaşımlarına ilk olarak Aydınlanma Çağı düşünürlerinin eserlerinde rastlanmaktadır. 17. asırda yaşayan ve 18. asrın başında ölen John Locke liberalizmin kurucusu olarak kabul edilmektedir. Ortaya attığı düşünceler kendisinden sonra gelen J. J. Rousseau, Immanuel Kant, Adam Smith gibi politik ve/veya iktisadi açıdan liberalizmi savunanlara temel olmuştur. Aydınlanma Çağı düşünürlerinin ortaya koyduğu bu fikirler, diplomasi tarihinde önemli yeri olan Amerikan Bağımsızlık Bildirgesi'nde, Büyük Fransız Devrimi ve ardından yaşanan 1830 ve 1848 Devrimlerinde oldukça etkili olmuştur.

Liberalizmin kurucusu olarak kabul edilen John Locke insan doğasını, Thomas Hobbes'un aksine barışçıl ve işbirliğine yatkın görmektedir. Locke'a göre insan zihni boş bir levha (tabula rassa)'dır. Bu noktadan hareketle fikirlerimiz olmadan doğarız,

[23] Ibid., p. 118.
[24] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 119-120.

edindiğimiz bilgiler algı ve tecrübelerimizle belirlenir. İnsanların doğuştan hangi haklara sahip olduğunu anlamamız için doğa durumunda nasıl hareket ettiklerini düşünmeliyiz. İngiliz düşünüre göre doğa durumu herkesin herkesle savaş içinde olduğu durum değildir. Doğa durumu başına buyrukluktan ziyade özgürlük durumudur.[25] Zamanın çeşitli evrelerinde birçok insan doğa durumunda birbirlerine saygı duyarak yaşamışlardır. Bu fikir Hobbes'un aksine sadece düşünsel bir deneme değildir. Locke, Kuzey Amerika yerlilerini bu durumu örnek göstermektedir.[26]

Locke 1683'te kaleme aldığı "*Two Treaties of Government*" adlı eserinde yukarıda genel ve soyut olarak belirttiğimiz görüşleri çerçevesinde İngiltere'de yaşanan kral-parlamento çatışmasında krala karşı parlamentonun tarafını tutmuştur. Bu bağlamda bireylerin doğuştan gelen haklarını devlet karşısında savunmuş ve yönetilenlerin rızasının yönetimin meşruiyetini sağladığı fikrini ortaya atmıştır.[27]

Bir diğer önemli liberal düşünür Jean-Jacques Rousseau ise "*Eşitsizliğin Temeli ve Kökenleri*" ve "*Toplum Sözleşmesi*" gibi eserleriyle modern siyasi ve sosyal düşüncenin temelini oluşturmuştur. Toplum Sözleşmesi'nde Rousseau görüşlerini "*insan özgür doğar ve şu an her yerde zincirlere vurulmuştur. Kim kendini ötekilerin efendisi olarak görürse, o onlardan daha büyük köledir"*[28] şeklinde ifade etmiştir. Rousseau'ya göre insan doğası Locke'a benzer bir şekilde barışçıldır ve insanların sivil toplumun bir parçası olmaya başlaması, onun diğer bireylerle rekabete ve nihai aşamada çatışmaya girmesine neden olmaktadır. Rousseau devleti ise yurttaşların doğuştan, vazgeçilmez hakları ve kendi yazgılarını belirleme güçleri yoluyla katıldıkları, özgürlük ve eşitlik için bir toplumsal sözleşme üzerine dayalı politik bir örgüt olarak tanımlamaktadır[29].

Liberalizmin kurumsallaşmasında çok önemli yeri olan ve dünya toplumu düşüncesinin felsefi temellerini atan Immanuel Kant'a göre *"tarih, kendisi ahlaki olmasa bile, ahlaki bir sona doğru ilerlemektedir."* Bu ahlaki son ebedi barıştır (perpetual peace). Kant'a göre savaşlar yeryüzünde bir anda ortadan kaldırılamaz. Bu devletlerin sorunlarını

[25] Arı, op. cit., s. 294.
[26] John Locke, *Two Treaties of Government and A Letter Concerning Toleration*, Ian Shapiro (ed.), New Haven and London: Yale University Press, 2003, p. 106.
[27] Richard J. Arneson (edt.), *Liberalism Volume I*, Great Britain; Edward Elgar, 1992, pp. xi-xvi.
[28] Jean Jacques Rousseau, *Discourse on Political Economy and The Social Contract*, New York: Oxford University Press, 1999, p. 45.
[29] Arı, op. cit., s. 297.

barışçıl yollardan çözmeyi adet edineceği ve devlet üstü kurumların ve evrensel bir hukukun oluşumunu gerektirir. Kant 1795 yılında yazdığı *"Ebedi Barış Üzerine Felsefi Bir Deneme"* adlı eserinde halkların nasıl kardeşçe ve savaşsız yaşayabileceğini anlatmaya çalışmıştır. Bunun içinde ebedi barış düşüncesini akılla, ahlakla ve hukukla temellendirmiştir[30]. Kalıcı barışın sağlanması için 6 temel, 3'de nihai madde sıralamaktadır[31]:

> • *"İçinde gizlenmiş yeni bir harp vesilesi bulunan hiçbir anlaşma, bir barış anlaşması sayılamaz.*
> • *İster küçük ister büyük olsun, hiçbir bağımsız devlet, diğer herhangi bir devletin hâkimiyeti altına tevarüs, mübadele, alım-satım veya hibe yollarıyla asla geçmemelidir.*
> • *Daimi ordular zamanla tamamıyla ortadan kalkmalıdır.*
> • *Devletler, dış menfaatlerini desteklemek için borçlanmalara girişmemelidir.*
> • *Hiçbir devlet, diğer bir devletin esas teşkilatına veya hükümetine zor kullanarak karışmamalıdır.*
> • *Hiçbir devlet, harpte, ileride barış akdedileceği zaman devletlerin birbirlerine karşılıklı güven duymalarını imkânsız kılacak yollara başvurmamalıdır. Bu yollara örnekler şunlardır: Düşman ülkesinde katiller, zehirleyiciler kullanmak, kapitülasyonlara aykırı hareket etmek, düşman tebaasını kendi devletine karşı ihanete kışkırtmak vs.*
> • *Devletlerin anayasaları cumhuriyetçi olmalıdır. (Anayasa unsurları özgürlük, kanun koyucuya bağlılık ve eşitlik olmak üzere üç başlık altında toplanmaktadır.)*
> • *Devletler hukuku, hür devletlerden kurulu bir federasyona dayanmalıdır. Devletler, sadece bir savaşı bitirmeyi hedefleyen barış anlaşmasından ziyade, tüm savaşları sonsuza kadar bitirmeyi hedefleyen barış ligi altında yaşamalıdırlar.*
> • *Dünya vatandaşlığı hukuku, evrensel misafirlik şartlarıyla sınırlandırılmalıdır Barış yanlısı yabancılara düşman muamelesi yapılmamalıdır. Kant'a göre misafirlik yabancı bir ülkede düşmanca muamele görmeme hakkıdır."*

Yukarıda genel ve soyut olarak aktardığımız realist ve liberal düşünürlerin insan doğası, devlet ve bu bağlamda devletin yönetimine ilişkin ortaya koyduğu düşünceler realizmin ve liberalizmin güvenliğin sağlanması noktasındaki yaklaşımlarını da etkilemektedir. Çünkü liberalizm, insan doğasını barışçıl ve işbirliğine yakın gördüğü gibi devletlerinde işbirliği ile güvenliklerini sağlayabileceklerini hatta demokrasi ile

[30] Arneson, op. cit., xvi-xx.
[31] Özet olarak belirttiğimiz bu maddeler için bkz. Immanuel Kant, *Ebedi Barış Üzerine Felsefi Deneme*, Çev. Yavuz Abadan – Seha L. Meray, Ankara, 1960, ss. 9-26

yönetilen devletlerin birbirleri ile savaşmayacağı savını öne sürmektedir. Realizm ise liberal yaklaşımın aksine devletleri sürekli çıkar odaklı bir güç mücadelesinin içinde görmekte ve işbirliği yapılması halinde dahi mutlak kazanç yerine, nispi kazancın önemli olduğunu savunmaktadır. Realizm ortaya koyduğu bu yapı devletin güvenliğinin askeri güçten geçtiği (hard power) ve sürekli çatışma halinde olunduğu için silahlanma ve bu bağlamda caydırıcılığın önem kazandığı bir güvenlik algısı oluşturmaktadır.

2. Kopenhag Okulu Bağlamında Realizm ve Neorealizmde Güvenlik Algısı

1985'te Barry Buzan ve Ole Waever gibi düşünürlerin fikirleri çerçevesinde ortaya çıkan Kopenhag Okulu, ismini Kopenhag Üniversitesi'nde yapılan güvenlik merkezli çalışmalar neticesinde almıştır. Okul özellikle güvenlik tehditlerinin içeriği ve ortaya çıkışı üzerindeki çalışmaları ile bilinmektedir. Okulun ortaya attığı "*güvenlikleştirme*" kavramı ve bu bağlamda politikacılar tarafından herhangi bir konunun nasıl ulusal güvenlik meselesi haline getirildiği ile ilgili ortaya koydukları fikirler, literatüre yaptığı en önemli katkıdır.[32]

Buzan, "*Askeri Güvenliğin Değişen Gündemi*" isimli makalesinde *"güvenlikleştirme, bir şeyin, değerli olduğu kabul edilen bir öznenin varlığına yönelik bir tehdit olarak kurgulanması ve bu kurgulamanın buna mukabil alınan istisnai tedbirleri desteklemek için kullanılmasıdır"* şeklinde tanımlamaktadır.[33] Kopenhag Okulu'nun kurucularının bir diğeri olan Waever ise "*Toplumsal Güvenliğin Değişen Gündemi*" isimli makalesinde güvenlikleştirmeyi şu şekilde tanımlamıştır: "*Güvenlikleştirme söylemsel ve siyasi bir süreçtir. Bu süreçte, intersübjektif bir anlama kurgulanmaktadır. Böylece, bir siyasi topluluk içerisinde bir şeyin referans nesnenin varlığını tehdit ettiği ve bu tehditle mücadele için istisnai önlemler alınması gerektiğini ifade edilmektedir."*[34]

[32] Sinem Akgül-Açıkmeşe, "Algı mı, Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri", *Uluslararası İlişkiler*, Cilt 8, Sayı 30 (Yaz 2011), s. 43-73, s. 57.
[33]Barry Buzan, "Askeri Güvenliğin Değişen Gündemi", *Uluslararası İlişkiler*, Çev. Burcu Yavuz, Cilt 5, Sayı 18 (Yaz 2008), s. 107-123, s. 108.
[34] Ole Waever, "Toplumsal Güvenliğin Değişen Gündemi", *Uluslararası İlişkiler*, Çev. Birgül Demirtaş Coşkun, Cilt 5, Sayı 18 (Yaz 2008), s. 151-178, s. 152.

Bu tanımlardan anlaşıldığı üzere güvenlikleştirme yaklaşımına göre güvenlikleştirme askeri konuları içerse de sadece askeri konularla sınırlı kalmamakta ve daha geniş bir tehdit spektrumuna yayılmaktadır. Herhangi bir konunun topluma ulusal güvenlik meselesi olarak kabul ettirilebilmesi yani güvenlikleştirilmesi için konunun politik liderler tarafından söylem yoluyla tehdit olarak algılandığının lanse edilmesi ve bu bağlamda tehdidin varlığı ve kapsamının inşa edilmesi gerekmektedir. Bu şekilde aktörler güvenlikleştirilen tehdide karşı rutin süreçler dışında toplumun kabul edeceği önlemler alabilir.[35]

Buzan'a göre güvenlikleştirme sürekli ya da, sınırlı başarı sağlayabilir veya başarısız olabilir. Başarılı bir güvenlikleştirme için birbirini izleyen üç aşamadan bahsedilebilir: [36]

> *1. "Öncelikle sorunun varlığa yönelik bir tehdit olarak liderler/karar vericiler tarafından belirlenmesi ve kitleye sunulması gerekmektedir,*
> *2. Sunulan tehdidin mahiyeti olağan politik süreçler dışında güvenlik tedbirleri alınmasını gerektirmelidir,*
> *3. Nihai aşamada ise güvenlikleştirmenin başarılı olabilmesi için varlığa tehdit olarak sunulan soruna ve buna karşı alınmak istenen tedbirlere dair söylemin kitle tarafından kabul edilmesi gerekmektedir."*

Genel ve soyut olarak bahsedilen üç aşamadan da anlaşılacağı üzere güvenlikleştirme söylem üzerinden geliştirilmektedir ve kamuoyunda bu söylemin oluşturduğu algı ölçüsünde başarılı olmaktadır. Güvenlikleştirme sonucunda güvenlikleştirilen alan üzerinde özgürlük-güvenlik dengesinde güvenlik kısmı baskın gelmekte ve devletin kontrolü hızla artmaktadır. Buzan'a göre güvenlikleştirme dış tehditlere yöneldiğinde, aktörlerin savunma ve saldırıya yönelik askeri kapasiteleri ve bu kapasitenin doğuracağı yetenekler ile aktörlerin niyetleri arasında iki aşamalı bir etkileşim meydana gelmektedir. Nihayetinde böyle bir güvenlikleştirme savaştan silahsızlanmaya kadar her durumu içerisinde barındırmaktadır. Bu kapsamda ayrıca bir aşamada askeri manada taktik ve stratejik üstünlüğü ele geçirebilmek için silahlanma ve caydırıcılığa yönelik ulusal politikalar geliştirilebilirken bir diğer aşamada ortaya çıkan

[35] Bu konuda ayrıntılı bilgi için bkz. Akgül-Açıkmeşe op. cit., ss. 58-59.
[36] Ibid, s. 61.

güvenlik ikilemini ortadan kaldırma ya da azaltmaya yönelik silahsızlanma çağrıları ve/veya savunmaya yönelik ittifaklar içerisine girilebilir.[37]

2.1. Kopenhag Okulu ve Siber Uzayın Güvenlikleştirilmesi

Son yirmi yıl içinde hiçbir iletişim aracının yayılmadığı hızda yayılan internet ve mobil iletişim gibi ağ tabanlı araçların oluşturduğu siber uzay, beşinci boyutu[38] temsil etmektedir.[39] Devletlerin koyduğu sınırların olmadığı bu alanda, siber uzayın sağladığı kendine has avantajlardan dolayı bireyler, ulus aidiyetleri dâhilinde ve/veya bunun çok daha ötesinde küresel ölçekte iletişim kurabilmekte, örgütlenebilmekte, tepkilerini gösterebilmektedir. Buna paralel olarak belli bir amaç doğrultusunda bireyden devlete uzanan farklı aktörler siber saldırılarda bulunabilmektedir. Siber uzayın çoğu noktada kontrolden uzak bu yapısı, devletlerin ve bu bağlamda lider/karar vericilerin siber uzayı varlıklarına hem iç hem de dış kaynaklı tehdit olarak görmesine neden olmakta ve bu alan hızla güvenlikleştirilmektedir.

Siber uzayın kullanımının hızla yayılması ve buna paralel olarak etkisini arttırması karşısında ABD, Rusya Federasyonu (RF), Japonya ve Avrupa Birliği (AB) gibi önde gelen aktörlerin karar vericileri/liderleri tarafından siber güvenliğin sağlanması kritik öneme sahip, en öncelikli ya da acil konulardan biri olarak lanse edilmiştir.[40] Bu süreçte

- RF, 2000 yılında *Rusya Federasyonu'nun Bilgi Güvenliği Doktrinini*[41] ve bunu desteklemek için 2011 yılında iki farklı belge olarak askeri ve siyasi yaklaşımını[42],

[37] Buzan, op. cit., s. 109.
[38] Siber uzay; kara, hava, deniz ve uzaydan boyutlarının ardından beşinci boyut olarak kabul edilmektedir.
[39] "The Internet Users (per 100 people)", http://data.worldbank.org/indicator/IT.NET.USER.P2/countries?display=graph (E.T. 06.02.2014).
[40] Katerina Klingova, " Securitization of Cyber Space in the United States of America, The Russian Fedaration and Estonia", Yayımlanmamış Yüksek Lisans Tezi, Danışman: Paul Roe, Central European University Department of Political Science, 2013, pp. 49-55.
[41] Bu konuda ayrıntılı bilgi için bkz. "Information Security Doctrine of the Russian Federation", *MFA of Russia*, 29.12.2008, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument (E.T. 06.02.2014).
[42] Bu konuda ayrıntılı bilgi için bkz. "Convention of International Information Security (Consept), *MFA of Russia*, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument

- ABD, 2011 yılında *Siber Uzay için Uluslararası Stratejisi'ni*[43] *ve* 2015 yılında *Savunma Bakanlığı Siber Stratejisi'ni*[44],
- Japonya, 2010 yılında *Ulusun Korunması İçin Bilgi Güvenliği Stratejisi'ni*[45],
- Birleşik Krallık, 2009 yılında *Birleşik Krallık Siber Güvenlik Stratejisi'ni*[46] ve 2011 yılında Birleşik Krallığı dijital dünyada korumak ve desteklemek alt başlığıyla yeni *Birleşik Krallık Siber Güvenlik Stratejisi'ni*[47],
- Almanya, 2011 yılında *Almanya için Siber Güvenlik Stratejisi'ni*[48],
- Fransa, 2011 yılında *Fransa'nın Bilgi Sistemleri Güvenliği ve Savunma Stratejisi'ni*[49],
- ÇHC, 2015 yılında *Çin'in Askeri Stratejisi* içerisinde siber stratejisini[50],
- Hindistan, 2013 yılında *Ulusal Siber Güvenlik Politikası'nı*[51],

---

(E.T. 06.02.2014), "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space", *NATO Cooperative Cyber Defence Centre of Excellence*, http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf (E.T. 06.02.2014)

[43] Bu konuda ayrıntılı bilgi için bkz. "International Strategy For Cyberspace Prosperity, Security, and Openness in a Networked World", *The White House*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (E.T. 06.02.2014)

[44] Bu konuda ayrıntılı bilgi için bkz. "The Department of Space Cyber Strategy", *United States of America Department of Defence*, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (E.T. 14.05.2015)

[45] Bu konuda ayrıntılı bilgi için bkz. "Information Security Strategy for Protecting the Nation", *National Center of Incident Readiness and Strategy for Cyber Securtiy*, 11 May 2010, http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf (E.T. 06.02.2014)

[46] Bu konuda ayrıntılı bilgi için bkz. "Cyber Security Strategy of the United Kingdom Safety, Security and Resilience in Cyber Space", *Cabinet Office*, June 2009, http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (E.T. 06.02.2014)

[47] Bu konuda ayrıntılı bilgi için bkz. "The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World", *Cabinet Office*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (E.T. 06.02.2014).

[48] Bu konuda ayrıntılı bilgi için bkz. "Cyber Security Strategy for Germany", *Federal Ministry of the Interior*, February 2011, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (E.T. 06.02.2014).

[49] Bu konuda ayrıntılı bilgi için bkz. "Information Systems Defence Security France's Strategy", *Premier Ministre Agence Nationale de la Sécurité des Systémes d'Information*, February 2011, http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (E.T. 06.02.2014).

[50] China's Military Strategy, *The State Council Information Office of the People's Republic of China*, Beijing, May 2015, http://cryptome.org/2015/05/prc-military-strategy-cctv-america-15-0526.pdf (E.T. 02.07.2015).

- Türkiye ise 2013 yılında *Ulusal Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı*[52] yayımlamıştır.

Devletlerin siber güvenlik stratejilerini oluşturmalarına paralel olarak siber uzayın kontrolüne ilişkin oluşturdukları yapı ve kurumlarda güvenlikleştirmenin gerektirdiği şekilde savunma bakanlıkları, istihbarat örgütleri ve güvenliğe ilişkin devlete bağlı diğer kurumlar içinde oluşturulmuştur.[53]

Hızla güvenlikleştirilen siber uzayın ulusal güvenlik ve bu bağlamda askeri açıdan savunulacak ve saldırılacak bir alan olarak görülmeye başlanması ise devletlerin siber kapasitelerinin diğer devletler tarafından tehdit olarak algılanmasına neden olmuştur.[54] Günümüz itibarıyla devletler diğer devletleri yaptıkları siber saldırılar/ siber espiyonaj faaliyetleri nedeniyle suçlamakta ve karşılık vermekle tehdit etmektedirler. Örneğin ABD siber uzayda en büyük tehdidin ÇHC hükümeti tarafından desteklenen hacker / cracker'ların[55] ABD sitelerinden veri çalma girişiminde bulunmaları olduğunu iddia etmiştir. Bu duruma karşı ise siber kapasite geliştirdiğini ve gerektiğinde kullanacağını deklare etmiştir.[56] Daha da önemli olan husus ise ABD ve RF'nin caydırıcılıklarını siber

---

[51] National Cyber Security Policy, *Department of Eloctronics and Information Technology*, 2013, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf (E.T. 02.07.2015).

[52] "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", *Resmi Gazete*, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf (E.T. 06.02.2014).

[53] Siber güvenlik stratejilerini kamuya açık yayınlayan devletlerin belgelerine ulaşmak ve ulusal yapılanmaları içindeki yeri hakkında ayrıntılı bilgi edinmek için bkz. "National Cyber Security Strategies in the World", *European Union Agency for Network and Information Security*, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (E.T. 06.02.2014).

[54] Siber uzayın askeri açıdan elverişli bir saha olup olmadığı hakkında ayrıntılı bilgi için bkz. Stuart H. Starr, "Towards an Evolving Theory of Cyber Power ", *The Virtual Battlefield: Perspectives on Cyber Warfare*, Eds. C. Czosseck and K. Geers, Ios Press, 2009, p.22.

[55] Hacker ve cracker kelimesi birbirinden farklı anlamlar ve niyetler içermesine rağmen, dünyada medya tarafından pejoratif şekilde hacker kelimesinin kullanılması sonucu gerçekle algı arasında büyük bir fark oluşmuştur. Hackerlar en temelde teknik anlamda üst düzey bilgiye sahip ve kullandıkları yapıyı geliştirme amaçlı kişilerken, crackerlar hackerlardan farklı olarak sistemde buldukları açıkları belli amaçlar doğrultusunda zarar vermek suretiyle kullanan kişilerdir. Tanımlardan da anlaşılacağı üzere medyanın kullanım şeklinin aksine hackerlar iyi niyetli ve zararsız kabul edilebilirken crackerlar bunun tam tersidir. Bu konuda ayrıntılı bilgi için bkz. Chad Perrin, "Hacker vs. cracker", 17 April 2009, http://www.techrepublic.com/blog/it-security/hacker-vs-cracker/ (E.T. 05.04.2014); Gary Scott Malkin and Tracy LaQuey Parker, "Internet User's Glossary", January 1993, http://tools.ietf.org/html/rfc1392#appendix-H (E.T. 05.04.2014).

[56] Bu konuda ayrıntılı bilgi için bkz. Wendell Minnick, "Experts: Chinese Cyber to US is Growing", *Defence News*, 9 July 2013, http://www.defensenews.com/article/20130709/DEFREG03/307090009/Experts-Chinese-Cyber-Threat-US-Growing (E.T. 07.02.2014); Philip Rucker, "Obama warns Xi that continued cybertheft would damage

karşılıkla sağlayamama durumunda, siber saldırılara karşı konvansiyonel ya da envanterlerinde bulunan herhangi bir silahı kullanabileceklerini açıklamış olmalarıdır.[57]

2.2. Güvenlikleştirilen Siber Uzay ve Neorealizm

Bir realist olan Kenneth Waltz'un "*Theory of International Politics*" adlı eserinde ortaya attığı görüşler ve klasik realizmden farklı olarak devletlerin güç ve güvenlik isteğine ilişkin yaklaşımları, onu neorealizmin (yapısal ya da bilimse realizm) kurucusu haline getirmiştir.[58] Süreç içinde neorealist yaklaşıma John Mearsheimer'ın "*The Tragedy of Great Powers Politics*" adlı eseriyle yaptığı katkılar neticesinde kuram içinde defansif ve ofansif realizm ayrımına gidilmiştir. Bu nedenle Mearsheimer ofansif realizmin savunucusu kabul edilmektedir.[59]

Daha geniş bir biçimde belirtirsek neorealizmde, klasik realizmden farklı olarak devletlerin amacı güç ve çıkar maksimizasyonu değil güvenliktir. Bu noktadaki temel soruysa güvenliğin nasıl sağlanacağıdır. Bilindiği üzere realizmde temel olan güç isteği, güvenliğin sağlanmasında sadece bir araçtır. Devletlerin güçlerini nasıl arttıracağı ve bu çerçevede diğer devletlerle nasıl ilişki kuracağına verilen cevaplar ise neorealizmdeki defansif/ofansif realizm ayrımına neden olmuştur. Neorealizm ve klasik realizm arasındaki en temel fark "devletlerin neden güç istediği" sorusuna verilen cevapta yatmaktadır. Klasik realizmin kurumsallaşmasında büyük öneme sahip olan Morgenthau'nun klasik realizme ilişkin ortaya koyduğu altı prensibe göre insanlar güç

---

relations, US officials said", *The Washington Post*, 8 June 2013, http://www.washingtonpost.com/politics/obama-warns-xi-that-continued-cybertheft-would-damage-relations-us-officials-said/2013/06/08/04843edc-d075-11e2-8845-d970ccb04497_story.html (E.T. 07.02.2014); Antone Gonsalves, "US commission fingers China as biggest cyberthreat", *CSO*, 8 November 2012, http://www.csoonline.com/article/721032/u.s.-commission-fingers-china-as-biggest-cyberthreat (E.T. 07.02.2014).

[57] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War", *The Wall Street Journal*, 31 May 2011, http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304563104576355623135782718.html (E.T. 07.02.2014); David J. Smith, "Russian Cyber Capabilities, Policy and Practice", *The Jewish Policy and Practice*, http://www.jewishpolicycenter.org/4924/russian-cyber-capabilities (E.T. 07.02.2014); Keir Giles, "Russia's Public Stance on Cyberspace Issues", *NATO Cooperative Cyber Defence Centre of Excellence*, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf (E.T. 07.02.2014).

[58] Arı, op. cit., s. 157.

[59] Ibid., ss.167-169.

edinme isteği ile doğarlar ve devletler de tıpkı bireyler gibi doğaları gereği güç edinme arzusu içindedirler.[60]

Neorealizme göre ise insan doğası ile devletin güç isteği arasında önemli bir ilişki yoktur. Uluslararası sistemde bir üst otoritenin olmayışı yani sistemin anarşik yapısı, devletlerin güvenliklerini garanti altına alması için güce ihtiyaç duymalarına neden olmaktadır. Özünde büyük devletlerin anarşik sistemde varlıklarını devam ettirmeleri için güç mücadelesine girmek dışında seçenekleri bulunmamaktadır. Bu çerçeveden bakıldığında büyük devletler "demir bir kafese hapsolmuş" gibidirler.[61] Neorealizmin özellikleri genel ve soyut olarak;

- Neorealist teoriye göre uluslararası sistemde bir üst otorite olmadığı yani sisteme anarşi hâkim olduğu için devletler çıkarlarını kendileri korumalıdır.[62]
- Bir devletin en temel amacı hayatta kalmaktır. Sistemin anarşik yapısı nedeniyle karşılıklı bağımlılığın sağlanması ya da işbirliği mümkün olmadığı için devletlere kendisinden başka yardım edecek herhangi bir güç yoktur. [63]
- Sistemde yaşanan güç dengesi savaşları önlemektedir.[64]
- Uluslararası sistem anarşik, iç siyasal sistem ise hiyerarşiktir.[65]
- Askeri ve ekonomik kapasitelerde değişiklik olabilmesine rağmen sistemin anarşik yapısında değişiklik olmamaktadır. Aktörler, sistem onları belli bir yönde politika yapmaya iteceği için klasik realizmin aksine sistem karşısında daha az öneme sahiptir.[66]

Yukarıdaki tespitlerden de anlaşıldığı üzere neorealizm, gücün tanımı konusunda klasik realizmden daha farklı bir içerik sunmaktadır. Güç devletin sahip olduğu

[60] Morgenthau, op. cit., p. 4.
[61] J. J. Mearsheimer, "Structural Realism", Tim Dunne, Milja Kurki, Steve Simith, *International Relations Theories Discipline and Diversity*, Second Edition, Oxford University Press, p. 78.
[62] Bu konuda ayrıntılı bilgi için bkz Vasquez, op. cit., p.191.
[63] Mearsheimer, "Structural Realism", op. cit., p. 80.
[64] Bu konuda ayrıntılı bilgi için bkz. Ibid.
[65] Bu konuda ayrıntılı bilgi için bkz. Arı, op. cit., ss. 157-158.
[66] Bu konuda ayrıntılı bilgi için bkz. Robert Jackson and Georg Sorenson, *Introduction to International Relations*, Oxford University Press, 1999, p. 85.

ölçülebilir fiziksel kapasitedir. Bu bağlamda sistemde güç dengesi devletin yönettiği somut askeri varlıklar üzerinden şekillenmektedir. Bununla beraber Mearsheimer'a göre devletler henüz harekete geçirilmemiş ikinci bir güce (latent power) sahiptir. Harekete geçirilmemiş bu güç, askeri güce dönüşebilecek sosyo-ekonomik yapı üzerine inşa edilir. Harekete geçirilmemiş ham gücün büyüklüğünün belirlenmesinde devletlerin fiziki büyüklüğü ve toplam nüfus gibi veriler birer etmendir. Büyük devletler güçlü bir askeri yapılanma oluşturabilmek için para, teknoloji ve personele ihtiyaç duyarlar ve bu çerçevede ham gücü oluşturabilmek rakip devletlerle mücadelede büyük bir öneme haizdir. Savaş ise tek güç edinme yolu değildir. Bu bağlamda devletler nüfuslarını ve harekete geçirilmemiş güçlerini arttırarak küresel refahtan pay alabilirler. ÇHC'nin son birkaç on yılda yaşadığı gelişme bu durumun en iyi örneğidir.[67]

Öte yandan, Waltz'a göre ise sistemin üç temel temel ilkesi vardır. "*Anar*şi", "*birimlerin özelliği*" ve "*kapasitelerin dağılımı*" şeklinde kavramsallaştırılan bu üç ilke aynı zamanda uluslararası sistemin yapısını ulusal sistemlerin yapısından ayırmaktadır. Belirtilen bu üç özellikten ilk ikisi olan sistemin anarşik yapısı ve birimlerin özelliği yani uluslararası sistemden herhangi bir desteğin olmaması (self-help) sabitken, üçüncü özellik olan kapasitelerin dağılımı değişken nitelik göstermektedir. Bu bağlamda güç dağılımının eşit olmadığı anarşik sistemde devletler güvenlik ikilemi ile karşı karşıya kalmaktadırlar.[68] Diğer bir deyişle düzenin ve hegemon gücün olmadığı uluslararası sitemde sürekli saldırı endişesiyle karşı karşıya kalan devletler, rakip devletler hakkında en kötüsünü düşünmek zorundadırlar. Devletlerin diğer devletlerin niyetlerinden emin olmamasından kaynaklanan bu korku ise devletleri devamlı yeni önlemler almaya itmekte ve savaşa sürüklemektedir.[69]

Daha önce de belirttiğimiz üzere neorealistler arasında devletin ne kadar bir gücü kontrol etmesi gerektiği ve bu gücün niteliği noktasında yaşanan görüş farklılığı defansif ve ofansif realizm ayrımına neden olmuştur. Stephan Walt gibi defansif realistlere göre gücü maksimum kılmak ve dünya üzerinde hakimiyeti arttırmak akıllıca olmayan bir

[67] Bu konuda ayrıntılı bilgi için bkz. Mearsheimer, op. cit., pp. 78-79; R. Kutay Karaca, *Çin Halk Cumhuriyeti'nin Orta Doğu ve Orta Asya Politikaları ve Bu Politikaların Türkiye'ye Muhtemel Etkileri*, Ankara: SAREM Yayınları, 2006, pp. 2-14.
[68] Arı, op. cit., ss. 157-167
[69] Ali Bilgiç, ""Güvenlik İkilemi"ni Yeniden Düşünmek: Güvenlik Çalışmalarında Yeni Bir Perspektif", *Uluslararası İlişkiler*, Cilt 8, Sayı 29 (Bahar 2011), s.123-142, s. 125.

harekettir çünkü sistem fazla güç elde etmeye çalışan devleti cezalandırılabilmektedir.[70] Bu çerçeveden bakan defansif realistler, uluslararası sistemin devletlerin gücünü arttırmasını teşvik ettiğini kabul etse de hegemonyanın ele geçirilmesini doğru bir yaklaşım olarak kabul etmemektedirler. Devletler güçlerini maksimize etmek yerine ölçülü bir güce sahip olmalıdırlar.[71] Bu kısıtlama üç nedene dayanmaktadır;[72]

> *1. "Defansif realistler bir devletin çok güçlü olması halinde, dengeleme için bir başka devletin de gücünü arttıracağını savunurlar. Bu duruma Napolyon Fransası, İmparatorluk Almanyası ve Nazi Almanyası örnek olarak gösterilebilir.*
> *2. Saldırı-savunma dengesi savunmacının lehinedir. Bir devlet daha fazla güç edinme girişiminde bulunursa bu durum o devlet aleyhine uzun bir savaşla sonuçlanır. Bu varsayıma göre devletler saldırının yersiz olduğunu anlayıp güç dengesi içinde varlıklarını devam ettirmeye yoğunlaşmalıdır.*
> *3. Defansif realistler şartlar uygun olsa bile fethe girişilmesinin yarardan çok zarar vereceğini savunurlar. Milliyetçilik nedeniyle fethedenin, fethedilene boyun eğdirmesi çok zor ve hatta imkânsızdır. Milliyetçilik ideolojisi ele geçirilenin ele geçirene karşı geleceğini garanti eder."*

Defansif realistlere göre bu üç nedenden dolayı devletler daha fazla güce olan arzularını sınırlamalıdır. Aksi halde kendi varlıklarını riske sokarlar. Devletler güçlerini, diğer devletleri yok etmeye değil tehditlere karşı önlem almaya yani savunma merkezli silahlanmaya harcamalıdır. Eğer tüm devletler bu zihniyete sahip olursa büyük güçler arasında çok az savaş hatta tüm devletlerin karıştığı merkezi bir savaş görülmeyecektir.[73]

Ne kadar gücün 'yeterli' olacağı ve bu gücün niteliğine ilişkin başta Mearsheimer, Fareed Zakaria ve Eric J. Labs teorisyenler defansif realist görüşlerden farklı olarak getirdikleri yaklaşım ise ofansif realist görüşü oluşturmaktadır[74]. Ofansif realizmin görüşleri beş başlıkta ele alınabilir:

> *1. "Büyük güçler dünya politikasının temel aktörleridir. Bu devletler anarşik sistemi yönlendirir.*
> *2. Her devlet ofansif bir askeri kapasiteye sahiptir. Bu kapasite devletten devlete ve zaman içerisinde değişiklik gösterebilir.*

[70] Mearsheimer, op. cit., p. 81.
[71] Bu konuda ayrıntılı bilgi için bkz. Ferhat Pirinççi, *Silahlanma ve Savaş*, 1. Baskı, Bursa: Dora Yayınları, ss. 49-52.
[72] Bu konuda ayrıntılı bilgi için bkz. Mearsheimer, op. cit., pp. 79-82.
[73] Bu konuda ayrıntılı bilgi için bkz. Arı, op.cit., ss. 167-168.
[74] Pirinççi, op. cit., s.59.

3. Devletler hiçbir zaman diğer devletlerin niyetlerinden emin olamaz."[75]
4. "Devletler temel amacı hayatta kalmaktır. Devletler iç politika üzerindeki otonomilerinin devamlılığını ister.
5. Devletler rasyonel aktörlerdir. Bu doğrultuda bekalarını sürdürebilmek için güçlerini maksimize ederler."[76]

Mearsheimer'ın büyük güç olarak belirttiği devletler birbirlerinden çekinirler. Bu devletler arasında güven düşüktür. Bu devletlerin en büyük korkusu bir başka devletin kendisine saldıracak kapasiteye ve motivasyona sahip olmasıdır. Bu korkuyu daha tehlikeli hale getiren ise devletlerin anarşik sistem içinde varlıklarını sürdürmeye çalışmalarıdır. Uluslararası sistemin anarşik yapısından dolayı bir devlet bir başka devletin saldırısına uğrarsa, saldırılan devleti kendi gücünden başka koruyacak hiç bir şey yoktur. Ortaya konan bu durumun altında yatan neden ise ofansif realist anlayışa göre devletlerin birbirlerinin niyetlerinden tam olarak emin olamamalarıdır. Devletler, diğer devletlerin güç kullanarak sistemde kurulan dengeyi değiştirmek isteyip istemediğini öğrenmek istese de bu durumdan tam olarak emin olunması imkânsızdır. Konvansiyonel gücün aksine niyetler ampirik olarak doğrulanamaz. Güvenlikleştirmenin aşamalarından da anlaşılacağı gibi niyetler karar vericilerin zihnindedir. Devletin kendini korumak ve varlığını sürdürmek için tek çıkar yolu karşısındaki devleti kendisine saldırmaktan caydıracak kadar güçlü olmasıdır. Uluslararası sistemde bulunan tüm devletler barışı sağlayacak koşulları kabul etse dahi uzun süreli barışın sağlanması imkan dâhilinde değildir. Çünkü devletlerin mevcut ve özellikle gelecekteki niyetlerinden emin olunması imkânsızdır. Bu durum büyük güç politikasının trajedisidir.[77]

Mearsheimer "*The Tregedy of Great Power Politics*" adlı eserinde sık sık anılan büyük güçleri, sistemdeki en güçlü aktöre ciddi bir savaşta meydan okuyabilecek konvansiyonel askeri güce sahip devletler şeklinde tanımlamıştır.[78] Bu bağlamda büyük güçlerin nükleer güce sahip olması da ofansif realistlere göre bir gerekliliktir. Nükleer gücün ortaya çıkardığı caydırıcılığın önemini hem defansif hem ofansif yazarlar kabul etmektedir. Defansif ve ofansif yazarlar ekseriyetle çatışma içindeki iki taraftan sadece birinin bu silaha sahip olması durumu dışında nükleer gücün bir saldırıda çok az işlevi

[75] Ofansif realizme ilişkin verilen ilk beş balıktan üçü hakkında ayrıntılı bilgi için bkz. John J. Mearsheimer, *The Tragedy of Great Power Politics*, New York: W. W. Norton & Company, 2003, p. 3.
[76] Ofansif realizme ilişkin verilen ilk beş başlıktan son ikisi hakkında ayrıntılı bilgi için bkz. Mearsheimer, "Structural Realism", op. cit., pp. 79-80
[77] Ibid., pp. 80-82.
[78] Mearsheimer, "*The Tragedy…*", op. cit., p. 5.

olduğunu kabul ederler. Bunun nedeni ise her iki tarafta ikinci vuruş kapasitesine sahipse, taraflardan hiçbiri için ilk vuruş gücünün kazanç sağlamayacak oluşudur. Bunun da ötesinde defansif ve ofansif realistler nükleer güce sahip devletler arasında konvansiyonel bir savaşın olma ihtimalini kabul etmelerine karşın çatışmanın büyümesiyle ortaya çıkacak nükleer savaş ihtimalinden dolayı gerçekleşmesinin çokta mümkün olmadığını savunurlar[79].

Çalışmamızın temel sorusu daha öncede belirtildiği gibi hem defansif hem ofansif yazarların da kabul ettiği nükleer alanda sağlanabilen bu caydırıcılığın siber uzayda sağlanıp sağlanamayacağıdır. Bu noktada caydırıcılığın nasıl ortaya çıktığı ve sonrasında ortaya koyduğu gelişimin nasıl olduğu sorusu önem kazanmaktadır.

3. Realizm ve Neorealizmde Caydırıcılık Olgusu

Morgenthau devletin güç mücadelesi çerçevesinde ortaya koyabileceği üç hareket tarzı olduğunu öne sürmektedir. Bunlar "müttefik aramak", "hasımlarına karşı ittifakı reddetmek" ve "kendi gücünü arttırmak"tır. Eğer devlet bu seçeneklerden ilk ikisi içerisinde hareket ederse, politikasını ittifak ilişkileri üzerine kurması gerekmektedir. Sonuncusunu seçmesi durumunda ise ittifak ilişkilerinden bağımsız olarak silahlanma üzerinden caydırıcılığı sağlama yoluna başvuracaktır.[80]

Caydırıcılığın sözlük anlamı Türk Dil Kurumu (TDK) tarafından "*bir saldırganlığı önlemek ve engellemek için önlem alma işi*" şeklinde tanımlanmaktadır.[81] K. J. Holsti ise caydırıcılığı "*bir devletin diğer bir devleti askeri güçle etkileme girişiminin engellenmesi"* şeklinde tanım ortaya koymuştur.[82] Tanımdan da anlaşılabileceği üzere caydırıcılığın sağlanması, savunmaya ilişkin bir hareket tarzıdır. Lakin caydırıcılığın ittifaklar yerine silahlarla sağlanması yani uluslararası sistemde işbirliğiyle barışın sağlanamayacağına ilişkin kabul, caydırıcılığın realist bakış açısının bir sonucu olduğunu

[79] Bu konuda ayrıntılı bilgi için bkz, Mearsheimer, "Structural Realism", op. cit., p. 83; Mearsheimer, "*The Tragedy…*", op. cit., pp. 32-36, 63-64.
[80] Steve Chan, *International Relations in Perspective*, Macmillan Publishing Company, 1984, p. 144.
[81] Caydırıcılık kavramının tanımı için ayrıca bkz. http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.55355d01abed21.36704295 (E.T. 07.02.2014).
[82] K. J. Holsti, *International Politics A Framework for Analysis*, Prentice-Hall International, Seventh Edition, 1995, p. 219.

göstermektedir. Bu çerçeveden bakıldığında caydırıcılık devletlerarası ilişkilerin başlangıcından bu yana var olan bir olgudur. Bir strateji olarak değerlendirildiğinde ise Holsti'ye göre caydırıcılık, altı temel üzerine inşa edilmektedir:[83]

> *1. "Hem savunmada olan hem de meydan okuyan devlet, karar verirken rasyonel davranmaktadırlar. Bu süreçte elde edilecek muhtemel kazanç ve kaybın oldukça iyi bir şekilde değerlendirilmesi esastır. Bu noktada caydırıcılığın özünde yatan şey, kazancın muhtemel kayıptan fazla olması gerektiğidir.*
> *2. Yüksek düzeyli tehdit, etkin bir caydırıcılık için oldukça önemlidir. Tehdidin boyutu karşıdakini caydıracak etkiyi göstermezse onu daha da agresif bir hale getirebilir. Bu noktada nükleer silahlar caydırıcılıkta kullanılabilecek en yüksek tehdit olarak karşımıza çıkmaktadır.*
> *3. Değerler hiyerarşisi savunmacı için de buna meydan okuyan devlet için de benzerdir. Bu bağlamda her iki devlet için de önem arz eden şeyler arasında bir paralellik bulunmaktadır. Son noktada savunmacı devlet de buna meydan okuyan devlet de çıkarları doğrultusunda hareket etmektedirler ve büyük bir savaş her ikisinin de aleyhinedir. Büyük bir savaştan kaçınma isteğindeki benzerlik savunmacının caydırıcılığını güçlendirmektedir.*
> *4. Her iki devlet de benzer çözümleme süreçlerine sahiptirler. Bu nedenle devletlerin birbirlerine karşı oluşturdukları tehdit ve verdikleri güvencelere dair mesajlar oldukça net olarak algılanır ve yorumlanır.*
> *5. Alınan kararlar iç politikanın tersine konunun muhatapları haricinde gelecek mülahazalar karşısında hassas değildir.*
> *6. Stratejik silahların kullanımına neden olacak kararların verilmesinde her iki tarafta sıkı bir şekilde merkezi kontrolü sürdürmektedir. Bu durum devlet içerisinde farklı aktörlerin ya da bölgesel güçlerin bu sürece ilişkin kararlar almasına mani olmaktadır."*

Caydırıcılığın inşa edilmesine ilişkin çalışmamızda verilen altı noktadan da anlaşıldığı üzere caydırıcılık aslında verilen mesajlar üzerinden şekillenmektedir. Bu bağlamda caydırıcılık gerçek gücün ötesinde yaratılan algı; caydırılan taraf üzerinde yarattığı etki ölçüsünde başarılı olmaktadır. Caydırıcılık için oluşturulan algı gerçekler üzerinde inşa edilmese de gerçekle arasındaki bağ oldukça önemlidir. Zira devletin caydırmak istediği tehdit karşısında gücünü olduğundan çok daha fazla göstermesi ya da bunun tam tersi şekilde, tehdidi ciddiye almayıp gerçek gücünün altında bir profil göstermesi de caydırıcılıkta başarısızlığa neden olabilmektedir. Bu çerçeveden bakıldığında başarılı bir caydırıcılık algısı yaratılabilmesi için iki kavram önem kazanmaktadır: inanılırlık ve istikrar.

[83] Ibid., p.220.

Yukarıda belirttiğimiz gibi etkili bir caydırıcılığın sağlanması için iki temel gereklilikten biri inanılırlıktır. Tehdit edilen devletin, çıkarlarını gerçekleştirmek için hareket etmesi halinde bu devlet nezdinde gerekli ve yeterli bir güçle misillemede bulunma kapasitesine sahip olunduğu inancı yaratılması caydırıcılığın sağlanmasında oldukça önemlidir. Bu noktada kapasiteyle vurgulanan sadece caydırıcılığı sağlama amacıyla tehdit eden devletin silahlarının sayısı, gücü ve kullanılabilirliği değildir. Asıl önemli husus kapasitenin varlığına dair karşı tarafta oluşturulan inançtır. Devletlerin bahsedilen bu varlıklarını gösterebilmek için kullandıkları en geleneksel yöntem, kazandıkları zaferlerin yıldönümlerinde envanterlerinde bulunan en güçlü silahları gösterdikleri askeri geçit törenleridir.[84] Günümüz savaş alanlarındaki en etkili kuvvet çarpanı olan hava unsurları ile güç göstermek amacıyla yapılan *fil yürüyüşü*[85] *(elephant walk)* da bu duruma örnek olarak verilebilir.

Caydırıcılık aynı zamanda bir iletişim süreci olarak da görülebilir. Devletin karar vericileri, muhataplarını istenmeyecek politik hareketlerde bulunması halinde kazanacağı edinimden daha fazlasını misilleme ile ödetecekleri mesajını vererek vazgeçirmeye çalışması, caydırıcılığın iletişim yönünü ortaya koymaktadır. Caydırılmak istenen devlete verilecek olan bu iletişimsel mesaj en az caydırmada etkin olan askeri güç kadar önemlidir. Diplomatik görüşmeler esnasında savunmada olan devlet, başvuracağı tehdidin inanılırlığını kanıtlamak zorundadır. Holsti eserinde caydırıcılığı şu şekilde formüle etmiştir:[86]

> "*A'nın B Üzerindeki Caydırıcılık Etkisi: B'nin A'nın Kapasitesi Hakkındaki Tahmini Bilgisi X B'nin A'nın Niyeti Hakkında Tahmini*."[87]

Holsti'nin ortaya koyduğu formülden de anlaşılabileceği gibi niyetin saldırgan devlete doğru bir şekilde yansıtılamaması durumunda askeri güç anlamını yitirmektedir.

---

[84] Ibid., pp. 220-223.

[85] 2 Mart 2012'de Güney Kore'nin Kansun Hava Üssü'nde, ABD ve Güney Kore'nin, askeri güç göstermek amacıyla yaptıkları fil yürüyüşü (düzinelerce savaş uçağının tam silah yüküyle pist başı yapması) hakkında ayrıntılı bilgi için bkz. Craig Hoyle, "USAF, South Korean F-16s walk the walk", *Flightglobal*, 9 March 2012, http://www.flightglobal.com/blogs/the-dewline/2012/03/usaf-south-korean-f-16s-walk-t/ (E.T. 20.03.2014) ; David Cenciotti, "Sixty F-16s Taxiing at Kunsan Air Base in One of the Greatest Show of Force Ever: That's a Record-Breaking Elephant Walk", *The Aviationist*, 6 March 2012, http://theaviationist.com/2012/03/06/elephant-walk/ (E.T. 20.03.2014).

[86] Holsti, op. cit., p. 221.

[87] Holsti eserinde ortaya koyduğu bu formülü Singer'in modeli üzerinden geliştirdiğini söylemektedir. Singer'in modeli hakkında ayrıntılı bilgi için bkz. J. David Singer, *Deterrence, Arms Control, and Disarmament*, Columbus, Ohio University Press, 1962, p. 162.

Fakat çalışmamızın neorealizme ilişkin temel varsayımlarını ele aldığımız bölümde de belirttiğimiz gibi niyetler ampirik olarak doğrulanamaz. Bu nedenle devletler birbirlerinin niyetleri hakkında hiçbir zaman emin olamazlar.[88] Şüphesiz bu durum, niyetin karşıya yansıtılmasında eylem ve söylem arasındaki dengeyi çok önemli hale getirmektedir. Savunmacı devletin tarihsel referansları, niyetine dair söylemin etkisini arttıracak önemli bir faktördür. Savunmacının daha önce yaşanan benzer bir krizde saldırgan devlete ya da bir başka devlete verdiği reaksiyonla mevcut duruma vereceğini söylediği tepki arasındaki benzerlik, caydırıcılığın iletişimsel yönünde müspet bir etki yaratacaktır. Bu sayede saldırgan devlet, tehdidin blöf olmadığını inancına sahip olacaktır. Diplomasi tarihinde, caydırıcılıkta elzem olan iletişimsel kısımda başarısız olunduğu için yaşanan savaşlara Irak'ın Kuveyt'i işgali sonrası ABD ve müttefikleri tarafından gerçekleştirilen Körfez Harekâtı, Arjantin'in işgali sonrası yaşanan Falkland Savaşı, ÇHC desteğinde Kuzey Kore yönetiminin Güney Kore'ye saldırması sonrasında yaşanan Kore Savaşı örnek verilebilir.[89]

Etkili bir caydırıcılığın sağlanması için inanılırlık kadar önemli olan diğer unsur ise istikrardır. Caydırıcılığı değerli kılan temel neden savaşa gerek kalmaksızın savunmacının saldırganı niyetinden vazgeçirebilmesidir. Bu bağlamda savaşın çıkması caydırıcılığın başarısız olduğu anlamına gelmektedir. Bu nedenle caydırıcılığı sağlamak için güdülecek politika askeri tehdit içeriğiyle eşzamanlı olarak makul güvenceyi de içermelidir. Aksi halde caydırıcılık sağlanmaya çalışılırken, karşılıklı saldırı korkusu ve bu korkunun altında yatan önleyici ya da önalıcı saldırı yapacak devletin daha fazla kazanca sahip olacağı gerçeğinden ötürü, taraflardan herhangi birinin ani saldırısıyla savaşa dönüşebilecektir. Bu çerçeveden bakıldığında verilecek mesaj, karşı tarafta sadece savaşın kaçınılmaz olduğu hissini uyandırmamalı aksine saldırgan devletin politikalarından vazgeçmesi halinde krizin tırmanmayacağı mesajını da açık bir şekilde içermelidir. Diğer bir şekilde ifade edersek caydırıcılık, askeri güç üzerinden savaş tehdidi içeren mesajlar verilse de savaş çıkmasıyla değil karşı tarafın savaştan vazgeçmesiyle başarılı olur. Bunu sağlamak için savunmacı devletin yapması gereken söyleminde krizi tırmandıran ve savaşı kaçınılmaz hale getirecek olan provakatif mesajlar

[88] Supra, pp. 22-23.
[89] Holsti, op. cit., p. 222.

yerine aksi yönde istikrarı barındıran bir söylem geliştirmesi ve bu şekilde hareket etmesidir.[90]

Tehdidin gerçekliği ve doğru mesajların verilmesi dünyanın bir nükleer savaş yaşamasını engellemiştir. II. Dünya Savaşı sonunda ABD tarafından nükleer silahların ilk kez kullanımıyla caydırıcılıkta karşı tarafa yöneltilen tehdit boyut değiştirmiştir. Nükleer silah tehdidi caydırılan tarafı varlığının bütünüyle ortadan kaldırabileceği gerçeğiyle karşı karşıya bırakmıştır. 1949 yılında SSCB'nin de ilk nükleer silahını edinmesi ve 1957'de uzaya gönderdiği Sputnik uydusu ile ABD'nin tek nükleer güç olduğu dönem sona ermiştir. SSCB'nin Sputnik uydusu ile aynı altyapıyı kullanarak, başka bir kıtadaki devleti füzelerle vurabilecek güce erişmesinin ardından dünya iki nükleer süper güç etrafında kümelenmiştir. Her ne kadar bu dönem Soğuk Savaş olarak adlandırılsa da nükleer silahların karşı tarafın varlığını tamamen ortadan kaldırabileceği gerçeği üzerinden sağlanan caydırıcılık, iki süper gücün birbiriyle doğrudan savaşmasını engellemiştir. Bu bağlamda bahse konu olan dönem bizce, karşı tarafın varlığına duyulan tüm rahatsızlığa ve savaş isteğine karşın nükleer silahların gölgesi altında sağlanmış bir barış dönemi şeklinde de adlandırılabilir.

Defansif realistler savunma – saldırı dengesinde savunmadan yana olmanın daha doğru olduğunu belirtmektedirler. Bunun altında yatan neden ise savunmanın saldırı yapmaktan çok daha kolay olmasıdır. Nükleer silahla sağlanan caydırıcılığın tarih boyunca varlığını devam ettiren caydırıcılıktan çok daha etkili olmasının altında yatan temel neden ise nükleer silahlara karşı savunma yapılmasının zorluğudur. Nükleer silahla saldırı yapılması durumunda nükleer bombanın taşındığı taşıyıcı aracın bomba aktif hale gelmeden vurulması dışında yapılabilecek herhangi bir savunma yöntemi bulunmamaktadır. Saldırılan güç de nükleer kapasiteye sahip ise bu durumda yok olmadan önce ya da saldırıyla paralel kullanacağı nükleer silah marifetiyle karşılıklı yok olmayı hatta kullanılacak silahların etkisi itibariyle Dünya'da ki tüm yaşamın ortadan kalkmasını sağlayacaktır. Bu durum Soğuk Savaş esnasında "dehşet dengesi" olarak kavramsallaştırılmıştır.[91] Nükleer silahların savunmacının aleyhine koyduğu bu yapı,

[90] Ibid., pp. 222-224.
[91] Bu konuda ayrıntılı bilgi için bkz. Chan, op. cit., pp. 144-147

nükleer silahlar üzerinden geçmişte sağlanmaya çalışılan caydırıcılığın çok daha üst noktaya taşıdığının en büyük göstergesidir.

Daha öncede belirtildiği gibi çalışmamızın temel sorusu ise nükleer silahlarla sağlanan bu caydırıcılığın aynı aktör (devlet) düzeyinde siber uzayda devletlerin edindikleri siber kapasiteler ile sağlanıp sağlanamayacağıdır. Soğuk Savaş'ın sona ermesiyle 45 yıl boyunca dünyada büyük önem arz eden sınırlar, ticaretin de etkisiyle hızla eski önemini kaybetmiş ve küreselleşme olarak kavramsallaştırılan sürece girilmiştir. Soğuk Savaş sonrasında Dünya'da kapitalizm ve bu ideolojinin en büyük temsilcisi olan ABD'nin tek güç haline gelmesine paralel olarak gelişen teknolojininde etkisiyle internet kullanımı tarihte hiçbir iletişim aracında görülmediği hızda[92] artmıştır.[93] Öncelikle The Defense Advanced Research Project Agency (DARPA) tarafından ABD Savunma Bakanlığı içerisinde iletişimi sağlamak amacıyla icat edilen internet daha sonra 1969 yılında Amerikan üniversitelerinin kullanımına açılmıştır. Üniversitelerin kullanımına açılmasının ardından hızla dünyaya yayılan internet yapılış amacı gereği güvenlik kaygısı taşımamasından ötürü açıkları da beraberinde getirmiştir.[94]

İnternet ve diğer sanal iletişim altyapılarının oluşturduğu siber uzayda bulunan açıklara Kosova Krizi ile başlayan dönemde gerçekleştirilen siber saldırılar, devletlerin siber güvenliklerinin fiziki güvenlikleri kadar önemli olduğu gerçeğini ortaya koymuştur.[95] Bu aşamadan sonra siber uzay devletlerin diğer devletlere karşı güvenliğini sağlaması gereken bir alan haline gelmiştir. Güvenlik ihtiyacı ile kurulan yapılar ve 2000'li yıllar boyunca gerçekleşen saldırılar, siber uzayı uluslararası ilişkilerin bir parçası haline getirmiştir. Zaman içerisinde akademisyenler, siber uzayın güvenliğinin sağlanması temelli çalışmalar yerine siber uzayın devletin politikaları neticesinde kullanılmanı öngören eserler üretmeye başlamıştır. Bu çalışma alanını günümüzde siber caydırıcılığın sağlanıp sağlanamayacağı sorusu takip etmektedir.

---

[92] "Internet Growth Statistics", http://www.internetworldstats.com/emarketing.htm (E.T. 20.03.2014).
[93] Starr, "Towards an Evolving…", op. cit., p.25.
[94] Bu konuda ayrıntılı bilgi için bkz. "Partial Bibliography of the Internet/Arpanet", http://www.darpa.mil/About/History/PARTIAL_BIBLIOGRAPHY_OF_THE_INTERNETARPANET.aspx (E.T. 20.10.2014).
[95] Bu konuda ayrıntılı bilgi için bkz. Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", The Computer Security Journal, Vol. XVI, No. 3, Summer 2000, pp. 15-35. http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf (E.T. 20.03.2014).

Çalışmamızın ilerleyen bölümlerde ayrıntılı olarak değerlendirilecek olan asıl konu ise siber uzayın caydırıcılık maksadı ile kullanılıp kullanılamayacağı ve nükleer silahlar ile sağlanan caydırıcılığın siber silahlarla sağlanmasının mümkün olup olmadığıdır.

II. BÖLÜM

NÜKLEER SİLAHLANMA VE NÜKLEER CAYDIRICILIK

16 Temmuz 1945 Pazartesi günü "*Tritinity Projesi*" olarak isimlendirilen ilk nükleer deneme saat 05:00'te ABD - Meksika sınırında bulunan Alamagadro Hava Kuvvetleri Üssü içerisinde gerçekleştirilmiştir. Deneme sonrasında gerçekleşen patlama 80 kilometre çapında duyulmuş, 400 kilometre uzaklıktan fark edilmiş, 200 kilometre uzaklıkta bulunan bir evin camları kırılmış, bombanın atıldığı hedef noktasında bulunan 30 metrelik çelik kule ise buharlaşmıştır.[96]

İlk denemenin üzerinden bir ay bile geçmeden ABD, Pasifik'teki Japonya direnişini kırmak için 6 Ağustos 1945'te Hiroşima'ya "*Little Boy*" adı verilen uranyum bombasını ve 9 Ağustos 1945'te Nagazaki'ye "*Fat Man*" adlı plütonyum bombasını atmıştır.[97] On binlerce insanın ölümüne ve iki şehrin büyük ölçüde yok olmasına neden olan bu iki nükleer saldırıdan günümüze, dünyayı birden fazla kez ortadan kaldırabilecek, binlerce nükleer silah üretilse de hiçbir savaşta kullanılmamıştır. Hiroşima ve Nagazaki'deki yıkım, nükleer silahları cephanelikte bulunan bir askeri objeden dünyadaki en kuvvetli caydırıcı unsura çevirmiştir. Bu unsur Soğuk Savaş boyunca caydırıcılığın merkezinde bulunmuş, farklı caydırıcılık stratejilerinin oluşturulmasını sağlamıştır.[98]

Bu kapsamda önemle vurgulanması gereken kavram "strateji"dir. Zira çalışmamızda ikinci bölümünde bir olgu olarak ele alacağımız "nükleer caydırıcılık" ve "siber caydırıcılık" her şeyden önce birer stratejidir. Strateji en temel anlamda "*…istenilen hedefin elde edilebilmesi için yapılacak işlerin ve eylemlerin ana yönünü belirleyen ve bunların koordinasyonunu sağlayan kapsamlı karar ve planlama çabasıdır…*" şeklinde tanımlanmaktadır.[99] Tarih boyunca stratejilerin uygulanmasında

[96] Nezihi Özden, *Nükleer Çağın İlk 40 yılı,* Cilt 1, İstanbul: İ.T.Ü. Nükleer Enerji Enstitüsü Genel Yayınları No. 17, 1983, ss. 52-53.
[97] Bu konuda ayrıntılı bilgi için bkz. Ibid., ss. 79-81.
[98] Bu konuda ayrıntılı bilgi için bkz. Lawrence Freedman, *The Evolution of Nuclear Strategy*, Third Edition, Great Britain: Palgrave Macmillan, 2003, passim.
[99] Mehmet Tanju Akad, *Modern Savaşın Temel Kavramları*, 1. Baskı, İstanbul: Kitap Yayınevi, 2011, s. 192.

kullanılan askeri doktrinlerde[100] farklı silahlar ve bunların entegre olarak kullanımı bulunsa da hiçbiri nükleer silahlar kadar doktrinlerin merkezinde yer almamıştır.

Soğuk Savaş boyunca ABD nükleer stratejisinin oluşturulmasında büyük etkisi olan Paul H. Nitze "*Foreign Affairs*"'ta yayınlanan makalesinde, bir devletin nükleer kapasitesi doğrultusunda ortaya koyabileceği seçenekleri beş başlıkta ele almaktadır. Bu başlıklar:[101]

1. *Asgari Caydırıcılık*
2. *Kentsel ve Endüstriyel Bölgelere Kitlesel Mukabele*
3. *Esnek Mukabele*
4. *Düşman Tarafı Nükleer Savaş Kazanabilecek Bir Kapasiteden Yoksun Bırakmak*
5. *Nükleer Savaş Kazandıracak Kapasite*

Nitze'nin 1976 yılında ortaya koyduğu bu beş seçenek, sadece ilk nükleer bombanın savaşta kullanıldığı 1945 yılından makalenin yayınlandığı 1976 yılına kadar geçen süreci doğru bir şekilde tasnif etmekle kalmamış, aynı zamanda büyük bir öngörüyle Soğuk Savaş'ın sonuna kadar olan süreçte gerçekleşecek stratejik değişimleri de ortaya koymuştur.

Bu bağlamda Paul H. Nitze'nin ortaya koyduğu nükleer seçenekler üzerinden bu bölüm beş altbaşlıkta ayrıntılandırılıcaktır. İlk olarak "Asgari Caydırıcılık" altbaşlığında nükleer silahların üretilmesi noktasında II. Dünya Savaşı içerisinde Almanya ve ABD'nin çabaları genel hatlarıyla incelenecek olup, ilk nükleer bombanın savaşta kullanılmasından kitlesel yıkımda büyük değişime yol açan hidrojen bombasının üretilmesine kadar geçen süreç ele alınacaktır. İkinci olarak "Kentsel ve Endüstriyel Bölgelere Kitlesel Mukabele" altbaşlığında özellikle ABD Dışişleri Bakanı John Foster Dulles'ın savunuculuğunu yaptığı "*New Look*" yaklaşımı çerçevesinde ortaya konulan "*Topyekûn Mukabele*

[100] Akad tarafından askeri doktrin "*savaşın nasıl yapılacağına dair ortak bir bakış sağlamak için silahlı kuvvetler içinde geliştirilen düşüncedir… Doktrin her ordunun savaş olayına bakışı, savaş prensiplerini anlama biçimi ve yönetim ile geleneklerinin toplamından çıkan düşünce biçimi olup, gene de her komutan tarafından farklı (veya yaratıcı) yorumlanmaya açıktır"* şeklinde tanımlanmıştır. Bu konuda ayrıntılı bilgi için bkz. Akad, op. cit., s. 78.

[101] Bu konuda ayrıntılı bilgi için bkz. Paul H. Nitze, "Assuring Strategic Stability in on Era of Detanté", *Foreign Affairs*, Vol. 54, January 1976, No. 2., pp. 207-232, pp. 212-213.

*Doktrini"'*nden başlayarak, dünyanın nükleer savaşla yok olmanın eşiğine geldiği Küba Füze Krizi'ne kadar geçen süreç irdelenecektir. "Esnek Mukabele" altbaşlığı ise ABD Başkanı John F. Kennedy döneminde topyekûn mukabeleden vazgeçilmesi sonrasında uygulanmaya başlanan süreç ele alınacaktır. Bu kapsamda birlikte ilk nükleer silahsızlanma girişimi olan Strategic Arms Limitation Talks'a kadar olan süreçte nükleer caydırıcılık bağlamında yaşanan gelişmelere de bölüm içerisinde yer verilecektir. 1972 yılında SSCB ve ABD arasında SALT I neticesinde yürürlüğe giren anlaşmaların sonucunda iki devlet füzesavar sistemi üretiminden önemli ölçüde vazgeçerek, büyük şehirlerini nükleer silah tehlikesine açık bırakarak hassas bir denge kurmuştur. Bu durum, tehlikeyi arttırmaktan öte her iki devletinde saldırması durumunda mutlak yok oluşa neden olacağı için caydırıcılığın güvenilirliğini arttırmıştır. "Düşman Tarafı Nükleer Savaş Kazanabilecek Bir Kapasiteden Yoksun Bırakmak" altbaşlığında bu durum ayrıntılı olarak ele alınacaktır. 1979 yılında SSCB'nin Afganistan'ı işgali sonrasında ise dönemin ABD Başkanı Ronald Reagan SALT I ile kurulan dengeye son vererek "*Yıldız Savaşları*" olarak da bilinen "*Strategic Defense Initiative*" projesini başlatmıştır. Bu sebeple ikinci bölümün son alt başlığı olan "Nükleer Savaş Kazandıracak Kapasite"'de "*Strategic Defense Initiative*"'den itibaren Soğuk Savaş'ın sona erdiği 1991 yılına kadar geçen süreçte yaşanan gelişmeler ele alınacaktır.

Literatürde genel kabul gördüğü üzere SSCB'nin dağılmasıyla birlikte dünyanın sonunu getireceği düşünülen nükleer çekişme de büyük ölçüde son bulmuştur. Günümüzde başta BM Güvenlik Konseyi üyesi devletler olmak üzere dokuz devletin nükleer silah sahibi olduğu düşünülse de nükleer silahların devletlerin kutuplaşmasında bir araç olarak kullanılması tezimin yazıldığı 2015 yılı itibariyle söz konusu değildir. Nükleer silahların yayılması ise uluslararası antlaşmalar sayesinde kontrol altında tutulmaktadır. Bu nedenlerden ötürü çalışmamızın ikinci bölümü, Soğuk Savaş'ın bitimi ile sınırlandırılacaktır.

1. Asgari Caydırıcılık

Literatürde genel kabul gördüğü üzere "*enerjisini atom çekirdeğinin parçalanmasından (atom bombası) ya da birleşmesinden (hidrojen bombası) alan kitle*

imha silahları"[102] şeklinde tanımlanmaktadır. Nükleer bombanın ilk kez 1945'te üretilmesine rağmen nükleer çağın başlaması yaklaşık 50 yıl geriye gitmektedir.

1.1. Asgari Caydırıcılığın Sağlanmasında İlk Nükleer Mücadele

Nükleer çağın başlangıcını oluşturan ilk gelişme 1896 yılında Fransız Henri Becquerel ve yardımcı Marie Curie'nin radyoaktiviteyi keşfetmeleridir.[103] İnsanoğlu böylece nükleer olayların farkına varmaya başlamış ve bu tarihten itibaren Avrupa merkezli olarak buluşlar birbirini izlemiştir. Ernest Rutherford, 1911 yılında çekirdekli atom modelini ortaya koymuştur. Niels Bohr, atom altı parçacıkların hareketlerini 1913 yılında açıklayarak Rutherford'un modeline katkıda bulunmuştur. Maddenin enerjiye dönüşebileceğini ortaya koyan Albert Einstein ise gelecekte nükleer silah yapmak isteyenlerin kendilerine teorik olarak temel alacağı noktayı oluşturmuştur. Bu alanda yaşanan ikinci önemli gelişme ise Rutherford'un 1919 yılında alfa ışınları kullanarak azotu oksijene dönüştürmeyi başarmasıdır.[104] Rutherford bir elementi bir diğerine çevirerek atom çekirdeğine insanlığın ilk kez müdahalesini gerçekleştirmiştir.

Yaşanan üçüncü büyük gelişme ise atomun parçalanması olayı olan fisyondur. Fisyon teorik olarak temellendirildikten sonra farklı milletlere ait bilimadamlarının oluşturdukları gruplar tarafından ortaya konulan beş yıllık bir yarış sonrasında 1938 yılında, başında Otto Hahn'ın bulunduğu Alman grubu tarafından keşfedilmiştir.[105] Fisyon yarışında Alman grubuyla rekabet eden İtalyan grubunun başındaki Enrico Fermi ise fisyonun bir sefer başlatıldıktan sonra kendi kendine devam etmesi olan zincirleme reaksiyonu, II. Dünya Savaşı'nın devam ettiği 1942 yılında ABD'ye göç ettikten sonra keşfederek yeni kıtayı nükleer yarışa sokmuştur.[106] 1938'de Faşist İtalya'dan kaçan

[102] Akad, op. cit., s. 154.
[103] "The Discovery of Radioactivity", Berkeley Lab., U. S. Deparment of Energy, http://www2.lbl.gov/abc/wallchart/chapters/03/4.html (E.T. 10.04.2015).
[104] "Ernest Rutherford – Biographical", http://www.nobelprize.org/nobel_prizes/chemistry/laureates/1908/rutherford-bio.html (E.T. 10.04.2015).
[105] "Otto Hahn" Atomic Heritage Foundation, http://www.atomicheritage.org/profile/otto-hahn (E.T. 10.04.2015); Michael Madsen, "Pioneering Nuclear Science: The Discovery of Nuclear Fission", International Atomic Energy Agency, https://www.iaea.org/newscenter/news/pioneering-nuclear-science-discovery-nuclear-fission (E.T. 10.04.2015).
[106] "Enrico Fermi and the First Self-Sustaining Nuclear Chain Reaction", Research and Development of the U. S. Depertment of Energy, http://www.osti.gov/accomplishments/fermi.html (E.T. 10.04.2015); "Enrico Fermi – Biographical", http://www.nobelprize.org/nobel_prizes/physics/laureates/1938/fermi-bio.html

Enrico Fermi ve Nazi Almanyası'ndan kaçan diğer bilimadamları ABD'ye nükleer yarışta çok büyük üstünlük sağlamıştır. Öte yandan ABD ile aynı zamanda nükleer silah üretmek için zincirleme reaksiyon çalışmalarına başlayan bir diğer devlet de Nazi Almanyası'dır. Zincirleme reaksiyon yaratmak için oluşturulacak reaktörde kullanılmak üzere Nazi işgali altındaki Norveç'teki Rjukan Ağır Su Üretim Fabrikası'ndan temin edilecek ağır su ise 27-28 Şubat 1943 gecesi Birleşik Krallık komando birliklerinin yaptığı operasyon ve 16 Kasım 1943 günü ABD hava bombardımanı ile sabotaja uğratılmıştır.[107] Nazi Almanyası'nın müttefikler tarafından işgali esnasında zincirleme reaksiyon ve atom bombasını gerçekleştirmekle görevlendirilen Erich Bagge, Kurt Diebner, Walther Gerlach, Otto Hahn, Paul Harteck, Werner Heisenberg, Horst von Laue, Carl Friedrich von Weizsacker ve Karl Wirtz'ten oluşan Alman ekibi ele geçirilmiştir. Cambridge Farm Hall'da esir tutulan ekip ABD'nin 6 Ağustos 1945'te attığı atom bombasını BBC Radyosu'nda öğrenmiştir.[108]

ABD nükleer çağın başlangıcında her ne kadar Avrupa'nın gerisindeyse de büyük bir hızla II. Dünya Savaşı'nın sonunda tüm devletlerin önüne geçerek nükleer güç haline gelmiştir. Bu konuda ABD'ye en büyük dolaylı desteği kıta Avrupa'sının iki büyük diktatörü olan Adolf Hitler ve Benito Mussolini vermiştir. Zira bu iki liderin oluşturduğu dikta rejimleri ve Nazi Almanyası'nın Yahudi karşıtı politikaları Avrupa'nın en iyi bilimadamlarının büyük kısmının ABD'ye göç etmesine neden olmuştur. ABD'ye göç eden bu bilimadamları savaşta ABD'nin ilk nükleer silahı üretmesini sağlamıştır. ABD'nin atom bombası çalışmalarının 2 Ağustos 1939'da Albert Einstein'ın, F. D. Roosevelt'e yazdığı mektupla[109] başladığı iddia edilebilir. Mektubunda 1942 yılında zincirleme reaksiyon oluşturmayı başaracak olan Enrico Fermi'nin çalışmalarını aktaran Einstein, ortaya çıkan gelişmelerin gelecekte çok büyük kuvvete sahip bombaların yapılmasına müsaade edeceğini belirtmiştir. Uranyum elde edilmesinin önemine değinen Einstein, Nazi Almanyası'nın Çekoslavakya'da bulunan uranyum madenlerini ele

(E.T. 10.04.2015); "Enrico Fermi (1901 - 1954)", http://www.atomicarchive.com/Bios/Fermi.shtml (E.T. 10.04.2015).

[107] Bu konuda ayrıntılı bilgi için bkz. Özden, op. cit., ss. 1-32.

[108] Bu konuda ayrıntılı bilgi için bkz. "World War II: Operation EPSILON Detention of German Nuclear Scientists British Intelligence Files", http://www.paperlessarchives.com/wwii-operation-epsilon.html (E.T. 10.04.2015); "Farm Hall Transcripts", 6 Ağustos 1945, http://www.aip.org/history/heisenberg/p11a.htm (E.T. 10.04.2015).

[109] Albert Einstein'in yazdığı mektubun orjinali için bkz. http://research.archives.gov/description/593374 (E.T. 10.04.2015).

geçirdiğini de belirtmiştir. Bu noktada Einstein'in talebi ABD'nin destekleyeceği bir grup fizikçinin bu alanda çalışmasının sağlanmasıdır.[110]

Einstein'ın mektubunu ABD Başkanı Roosevelt dikkate alınmış ve daha sonra "*Manhattan Projesi*" ismini alacak çalışmalar başlatılmıştır. Projenin amacı ABD'de bulunan en iyi bilimadamlarını bir araya getirip devletin imkânlarını kullanarak ilk atom bombasını diğer devletlerden önce üretmektir. Bu noktada bilgi ve kaynak kullanımında Birleşik Krallık ile işbirliğine giden ABD, diğer müttefiki SSCB'yi bu işbirliğinin dışında bırakmıştır. 65 bin işçinin farklı kademelerinde yer alacağı "*Manhattan Projesi"* ordu kontrolüne verilmiştir. ABD ordusunu temsilen yönetimde General Leslie Groves'un bulunduğu projede, bilimadamlarının başında ise Los Alamos Ulusal Laboratuvarı'nın müdürü J. Robert Oppenheimar bulunmuştur. ABD ve Kanada'da otuzdan fazla yerde devam eden çalışmaların nihai ürünü olan atom bombası ise gizlilik dereceli Las Alamos Ulusal Laboratuvarı'nda üretilmiştir.[111]

Üretilen ilk atom bombasının denemesi "*Trinity Projesi*" kod adıyla 16 Temmuz 1945'te ABD - Meksika sınırında bulunan Alamagadro Hava Kuvvetleri Üssü alanında gerçekleştirilmiştir. Deneme sonrasında gerçekleşen patlama 80 kilometre çapında duyulmuş, 400 kilometre uzaklıktan fark edilmiş, 200 kilometre uzaklıkta bulunan bir evin camları kırılmış, bombanın atıldığı hedef noktasında bulunan 30 metrelik çelik kule ise buharlaşmıştır. Denemede gerçekleştirilen patlamanın yaklaşık 19 bin ton Trinitrotoluene (TNT) patlamasıyla eşdeğer olduğu ölçülmüştür. New York Times muhabiri William Laurance gerçekleşen patlamayı yeni doğmuş dünyanın ilk ağlaması olarak tarif etmiştir.[112]

1.2. Nükleer Silahların Kullanımı

İlk nükleer silah denemesinin başarılı olmasının ardından, ABD yönetimi ve "*Manhattan Projesi*" kapsamında nükleer silah üreten bilimadamları arasında atom

[110] Joseph Siricusa, *Nuclear Weapons A Very Short Introduction*, Oxford University Press, 2008, p. 12.
[111] Bu konuda ayrıntılı bilgi için bkz. Siricusa, op. cit, pp. 12-14, 17-19.
[112] Bu konuda ayrıntılı bilgi için bkz. Özden, op. cit., ss. 52-53; Siricusa, op cit., p. 19; James Gleick, After The Bomb, A Mushroom Cloud Of Metaphors, *The New York Times*, 21 Mayıs 1989, http://www.nytimes.com/1989/05/21/books/after-the-bomb-a-mushroom-cloud-of-metaphors.html (E.T. 10.04.2015).

bombasının kime karşı ve nasıl kullanılacağı konusunda görüş ayrılıkları ortaya çıkmıştır. Nükleer silahın üretim aşamasında Nazi Almanyası'nı yenmek için kullanılacağı düşünülürken, silahın üretimi tamamlandığında Avrupa'da yaşanan savaş büyük ölçüde sona ermiştir. Pasifik'te ise Japonya büyük kayıplarına rağmen direnmeye devam etmiştir. Pasifik adaları boyunca adım adım süren savaş ABD birliklerine büyük kayıplar verdirmiştir. Bu noktada ABD'nin Pasifik'te daha fazla kayıp vermemek için atom bombasını kullandığı açıklaması literatürde oldukça sık kullanıldığı gibi savaş sonrası düzenin belirlenmesi ve SSCB ile olan ilişkilerde yeni bir caydırıcılık unsuru olarakta kullanıldığına ilişkin görüşler de bulunmaktadır.[113] Örneğin İngiliz deneysel fizikçi Patrick Maynard Stuart Blackett, Japonya'ya 6 ve 9 Ağustos'ta atılan atom bombalarının II. Dünya Savaşı'nın sonu değil Soğuk Savaş'ın başlangıcı olarak görülmesi gerektiğini iddia etmektedir.[114] Bir diğer önemli tartışma konusu ise silahın kullanım şekli olmuştur. Bu noktada bazı bilimadamları silahın etkilerinin gösterilmesinin yeterli olduğunu düşünerek, insansız bir bölgede kamuya açık bir deneme yapılmasını önermiştir. Bir diğer grup bilimadamı ise silahın şehirlere değil Japon Donanması'na karşı kullanılmasını önermiştir. Öte yandan asıl amacın Blackett'inde ortaya koyduğu gibi Japonya'yı savaşta yenmek değil SSCB'ye karşı ABD'nin silahın gücünü göstermek olduğunu, kullanılacak silahın savaş sonrası Avrupa'nın kontrolünü kolaylaştıracağını düşünenlerde olmuştur.[115]

Yaşanan tüm bu tartışmaların ardından 200 bin ton TNT gücündeki *"Little Boy"* kod adlı uranyum bombası 6 Ağustos 1945'te Hiroşima'ya, 220 bin ton TNT gücündeki *"Fat Man"* kod adı verilen plütonyum bombası 9 Ağustos 1945'te Nagazaki'ye atılmıştır. Nükleer silahların tam olarak verdiği zararı radyasyonun uzun süreli zarar verme kapasitesinden dolayı ölçmek mümkün olmasa da Hiroşima'da yaklaşık 150 bin ve Nagazaki'de yaklaşık 74 bin insanın öldüğü tahmin edilmektedir. Nagazaki'ye daha güçlü bir bomba atılmasına rağmen daha az insanın hayatını kaybetmesi bölgenin coğrafi özellikleri ile alakalıdır.[116] Bu açıdan nükleer bombalar, kullanılan birim başına verdiği

[113] Bu konuda ayrıntılı bilgi için bkz. Siricusa, op. cit., pp. 22-26.
[114]Bu konuda ayrıntılı bilgi için bkz. P. M. S. Blackett, *Fear, War and The Bomb*: *Military and Political Consequences of Atomic Energy*, New York, 1948, p. 139'dan aktaran Lloyd J. Graybar, " The 1946 Atomic Bomb Test: Atomic Diplomacy or Bureaucratic Infighting?", *The Journal of American History*, Vol. 72, No. 4, March 1986, pp. 888-907, p. 888.
[115] Siricusa, op. cit., p. 22.
[116] II. Dünya Savaşı'nda nükleer bombaların kullanımı sonucunda verdiği zarar hakkında farklı rakamlar bulunmaktadır. Bu konuda ayrıntılı bilgi için bkz. Özden op. cit., ss. 113-117; Siricusa, op. cit., pp. 22-24;

zarar ölçüldüğünde dünyada o zamana kadar hiçbir silahın yakalamayacağı bir oranı yakalamıştır. Ortaya konulan kapasite ise en tehlikeli caydırıcılık türü olan nükleer caydırıcılığın temellerini atmıştır.

Savaşı bitiren atom bombalarının kullanılmasının ardından ABD içerisinde, stratejinin bir parçası olarak atom bombasının nasıl kullanılması gerektiği ve sonuçlarının ne olacağı ile ilgili tartışmalar başlamıştır. 1940'lı yılların ikinci yarısı boyunca sürecek olan bu tartışmalar ABD nükleer stratejisinin temellerini atmıştır. Bu tartışmalar başta, özellikle Manhattan Projesi'ni yürüten bilimadamları tarafından yürütülürken zaman ilerledikçe diğer bilimadamları ve siyasetçilerde bu tartışmaya katılmıştır. Bu tartışmaları başlatan ayrımın temellerinin 16-17 Kasım 1945'te Philadelphia'da yapılan "*Atomic Energy and Its Implications*" konulu konferansta atıldığı iddia edilebilir. Bu konferansta Manhattan Projesi'nin yürütücülerinden biri olan doğa bilimci Robert Oppenheimar'ın ortaya attığı yaklaşımla sosyal bilimci Jacob Viner'ın yaklaşımı arasındaki fark, sonraki yıllarda nükleer silah stratejisi üzerine çalışanları etkilemiştir.

Oppenheimer ve Manhattan Projesi'nde yer alan diğer doğa bilimcilerin görüşleri, atom bombasının savaşları başlar başlamaz kesin bir galibiyetle sona erdirecek bir şok ve terör silahı olduğu yönündedir. Onlara göre Almanya'nın II. Dünya Savaşı'nda uyguladığı askeri doktrin olarak "*Blietzkrieg*" (Yıldırım Savaşı) çok daha başarılı bir şekilde nükleer silahlarla uygulanabilir. Nükleer silahların kullanılacağı hedefler noktasında ise Japonya'nın Pearl Harbor Baskını ya da Almanya'nın yıldırım savaşı doktrininden farklı olarak düşünülmüştür. Doğa bilimciler tarafından nükleer silahlar askeri hedeflere karşı kullanılmayacak kadar değerli olarak kabul edilmiştir. Bunun yerine silahlar doğrudan düşmanın sosyo-ekonomik yapısını ortadan kaldırmak için şehirlere ve sanayi merkezlerine karşı kullanılmalıdır. Bu şekilde yapılacak bir saldırıda silahların hedefleri silahlar değil şehirler ve fabrikalar olmuştur.[117] Bu yaklaşım, 1950'li yıllarda ortaya çıkan "*topyekun mukabele yaklaşımı*" içerisinde belli bir ölçüde kabul

---

Lawrance Freedman, *The Cold War*, London: Cassel & Co, 2001, pp. 31-34; Lawrance Freedman, "The Evolution of…", op. cit., pp. xii-xv; Pirinççi, op. cit., s. 95.

[117] Nükleer silahların hedefleri olarak silahlar yerine şehirlerin seçilmesi anlayışı, şehirler üzerine atılacak atom bombalarının etkilerini gösteren haritalar yapılmasına neden olmuştur. Bu konuda 1 megaton gücündeki bombanın Taksim Meydanı üzerinde patlatıldığı senaryosu ve 20 kiloton gücündeki bir bombasının Londra Victoria Tren İstasyonu üzerinde patlatıldığı senaryosu üzerine hazırlanan haritalar için bkz. Özden, op. cit., s.114; Freedman, "The Cold War", op. cit., pp. 50-51.

edilse de doğa bilimcilerin yaklaşımları stratejik düşünmekten öte atom bombalarının potansiyelini vurgulamaktadır.[118]

Oppenheimer'dan farklı olarak sosyal bilimci Jacob Viner ise potansiyelden öte büyük bir öngörü ve stratejik düşünce ortaya koymuştur. Şehirlere atılacak atom bombalarının savaşı bir anda sona erdirmeyeceğini ve devletlerin savaşmaya devam edeceğini düşünen Viner, henüz SSCB'nin nükleer silah geliştirmesine beş sene varken, gelecekte nükleer silaha sahip devletlerin artacağı, bu artışın ise misilleme tehdidiyle beraber istikrara katkıda bulunacağını ortaya koymuştur.[119] Sosyal bilimci olarak devletlerin davranışlarını daha isabetli tahmin eden ve uluslararası sistemi okuyan Viner'ın görüşleri kendisinden sonra gelen Bernard Brodie, P. M. S. Blackett, Albert J. Wohlstetter, Liddell Hart gibi bilimadamları tarafından nükleer stratejilerin oluşturulmasına büyük katkı sağlamıştır.

ABD, ilk nükleer bombalarının kullanılmasının ardından doğa bilimciler ile sosyal bilimciler arasında başlayan tartışmada, nükleer alanın 1950'li yıllarda bilimden çok diplomasinin bir konusuna haline geldiği döneme kadar doğa bilimcilere taraf olmuştur. Bu bağlamda nükleer silahların yıkıcı gücüne ve savaşları başlangıcında sona erdiren etkisine dayanarak ABD ordusu küçülmeye gitmiştir. Savaşın sona erdiği 1945 yılında 8 milyon üzerinde mevcudu olan ordu 1946'da 2 milyon sınırının altına, 1948 yılında ise yaklaşık yarım milyona inmiştir. ABD askeri mevcudunun ve bütçesinin küçülmesinden etkilenmeyen iki alan ise nükleer silah imalatı ve o yıllarda bu silahların tek sevk yöntemi olan uzun menzilli ağır bombardıman uçaklarına sahip Stratejik Hava Komutanlığı (Strategic Air Command) olmuştur. ABD'nin ordusunu terhis edip kendi kıtasına çekilmesini ise sadece nükleer silahların sağlayacağı güvenliğe bağlamak tarihsel referanslarla uyuşmamaktadır.[120] 1823 yılında ABD Başkanı James Monreo tarafından

[118] Nükleer silahların kullanım stratejisi tartışmalarında doğa bilimcilerin görüşleri için bkz. Ali L. Karaosmanoğlu, "Nükleer Stratejinin İlk On Yılı", *Ankara Üniversitesi SBF Dergisi*, Cilt: 51, Sayı:1, 1996, ss. 323-345, ss. 325-326; J. R. Oppenheimer, "Atomic Weapons", *Proceedings of the American Philosophical Society*, Vol. 90, No. 1, Symposium on Atomic Energy and Its Implications (Jan., 1946), pp. 7-10, passim; Freedman, "The Evolution of …", op. cit., pp. 37-39.

[119] Jacob Viner, "The Implications of the Atomic Bomb for International Relations", *Proceedings of the American Philosophical Society*, Vol. 90, No. 1, Symposium on Atomic Energy and Its Implications (Jan., 1946), pp. 53-58, passim.

[120] ABD ordusunda mevcut azalması hakkında ayrıntılı bilgi için bkz. Karaosmanoğlu, op. cit., s. 331; William W. Epley, *America's First Cold War Army 1945-1950*, The Institute of Land Warfare Association Of The United States Army, 1999, pp. 9-10. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA383639

ilan edilen ve onun ismiyle anılan Monreo Doktrini[121], devletin barış zamanlarında eski kıtanın oldukça karışık ittifak ilişkilerine girmemesi yönünde bir yaklaşım ortaya koymuştur. Bu doktrinden hareketle ABD kendi çıkarlarını tehlikede gördüğünde savaştan çekinmemişse de savaş sona erdiğinde kendi kıtasını koruma altına alacak yapıyı sağlayacak şekilde varlığını geri çekmiştir. I. Dünya Savaşı sonrasında ABD Başkanı Woodrow Wilson'un tüm çabalarına rağmen değişen ABD iktidarı Monreo Doktrini'ne sadık kalmak amacıyla Wilson'un fikirsel bazda kurucusu olarak kabul edilebileceği Milletler Cemiyeti'ne üye olmamıştır. II. Dünya Savaşı sonrası benzer politikaları uygulama arzusunda olan ABD yönetimi ise SSCB'nin her alandaki revizyonist olarak görülebilecek politikaları karşısında bir daha geri dönemeyeceği şekilde Monreo Doktrini'nden vazgeçmiştir.

SSCB ise ABD nükleer silahlarının sınırlı alanlardaki yoğun yerleşimler olan şehirlere etkisini gördükten sonra Soğuk Savaş başlangıcında ordusunu bu tehlikeye karşı konumlandırmıştır. Bu bağlamda ABD ordusu kadar mevcut azaltışına gitmeyen SSCB, 1945'te 11.3 milyon kişiden oluşan ordusunu 1948 yılına kadar kademeli olarak 2.8 milyon kişiye indirmiştir. Mekanizasyonunu II. Dünya Savaşı sonunda tamamlayan SSCB ordusu bir yandan hızla nükleer silah geliştirmeye çalışırken diğer yandan da yaklaşık 3 milyon kişilik mekanize ordusuyla Batı Avrupa'yı konvansiyonel işgal tehdidi altında tutarak, ABD nükleer tekelini dengelemeye çalışmıştır.[122]

ABD bir yandan kendi ordusunu terhis edip nükleer silahlar ve bunların sevkini sağlayacak stratejik bombardıman kabiliyetini geliştirirken öte yandan SSCB'nin Avrupadaki revizyonist politikalarının fark edilmesi üzerine Monreo Doktrini'ni terk etmiştir. 1946 yılında temelleri George F. Kennan tarafından ortaya konulan komünizmi çevreleme stratejisi[123], 1947 yılında Sovyet tehdidi altındaki Yunanistan ve Türkiye'ye

---

(E.T. 10.04.2015); Richard W. Stewert (Gen. Edi.), *American Military History Volume II The United States Army In A Global Era, 1917-2008,* Second Edition, Washington: Center of Military History United States Army, 2010, pp. 204-205.

[121] Fahir Armaoğlu, *20. Yüzyıl Siyasi Tarihi 1914-1980*, Ankara: Türkiye İş Bankası Kültür Yayınları, 1983, ss. 69-76; Rifat Uçarol, *Sayasi Tarih [1789-2012]*, Gözden Geçirilmiş ve Genişletilmiş 9. Basım, İstanbul: Der Yayınları, 2013, ss. 308-312.

[122] Bu konuda ayrıntılı bilgi için bkz. Roger R. Reese, *The Soviet Military Experience*, London: Routladge, 2001, pp. 138-139; William E. Odom, *The Collapse of the Soviet Military*, USA: Yale University Press, 1998, p. 39; Karaosmanoğlu, op. cit., p. 334.

[123] Çevreleme stratejisi, stratejinin uygulanışı ve George Kennan'ın uygulanışına ilişkin getirdiği eleştiriler için bkz. Martin Griffiths, Steven C. Roach vd., *Uluslararası İlişkilerde Temel Düşünürler ve Teoriler,* çev.

askeri, ekonomik yardımı içeren *"Truman Doktrini"*[124] ve 1948'de Avrupa'nın ekonomisini kalkındırmak için ortaya konan *"Marshall Planı"*[125] ile hayata geçmiştir. Marshall Planı ile gerçekleştirilen destek her ne kadar ekonomik bir yardım olarak gözükse de arkasındaki asıl amaç Batı Avrupa ekonomilerini kalkındırarak Doğu Avrupa'da bulunan SSCB konvansiyonel gücüne karşı yardım alan devletlerin tekrar büyük kara orduları kurmasını sağlayarak konvansiyonel dengeyi oluşturmaktır. Bu sayede ABD'nin tekrar büyük ordular kurması gerekmeyecek, stratejik bombardıman kabiliyeti ve nükleer silahlarla Avrupa'yı komünizme karşı koruma taahhüdünü yerine getirecektir.[126]

ABD'nin II. Dünya Savaşı'nın sonundan SSCB'nin ilk nükleer silahını geliştirdiği 1949'a kadar tek nükleer güç olmasına rağmen bu gücü yeterince etkin kullanamayıp konvansiyonel ve ekonomik yardımlarla SSCB'ye komşu devletleri güçlendirmesinin en büyük nedeni ise henüz emekleme çağında olan nükleer silah teknolojisidir. Daha net bir ifade ile belirtirsek 1948 yılına kadar ABD'nin elinde bulunan nükleer silahlar ve bu silahların sevkinde kullanılan uçaklar oldukça az sayıdaydı. Özellikle nükleer silah yapmak için gereken uranyumu elde etmek bu süreçte ABD için oldukça zor olmuştur. Bunun sonucunda ABD'nin 1945 yılında 2, 1946 yılında 9, 1947 yılında 13, 1950 yılındaysa 50 adet nükleer silaha sahip olabilmiştir.[127] Bu silahlar ise her an kullanıma hazır değil montajı yapılmamış halde saklanmıştır. Bir atom bombasını hazır hale

---

CESRAN, İkinci Basımdan Çeviri, Ankara: Nobel Yayınevi, 2011, ss. 36-40; "Kennan and Containment, 1947", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/kennan (E.T. 10.04.2015).

[124] Truman Doktrini hakkında ayrıntılı bilgi için bkz. Göksel İşyar, *Karşılaştırmalı Dış Politikalar Yöntemler Modeller Örnekler ve Karşılaştırmalı Türk Dış Politikası*, 1 Baskı, Bursa: Dora Yayınevi, 2009, ss. 605-608; Tayyar Arı, *Irak, İran, ABD ve Petrol*, Güncellenmiş 2. Baskı, Bursa: Alfa, 2007, ss. 239-241; Uçarol, op. cit., ss. 929-930, Oral Sander, *Siyasi Tarih 1918-1994*, 8. Baskı, Ankara: İmge Kitabevi, 2000, ss. 231-233; Armaoğlu, op. cit., ss. 441-443; Çağrı Erhan, "ABD ve NATO'yla İlişkiler", Baskın Oran (ed.), *Türk Dış Politikası, Kurtuluş Savaşından Bugüne Olgular, Belgeler, Yorumlar, Cilt I.*, 13 Baskı, İstanbul: İletişim, 2008, ss. 528-537; "The Truman Doctrine, 1947", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/truman-doctrine (E.T. 10.04.2015); Pirinççi, op. cit., ss. 132-133.

[125] Marshall Yardımı hakkında ayrıntılı bilgi için bkz. Erhan, op. cit., ss. 537-542; Armaoğlu, op. cit., ss. 443-445; İşyar, op. cit., ss. 609-613; Uçarol, op. cit., ss. 930-931; Sander, op. cit., ss. 233-234; Çağrı Erhan, "Ortaya Çıkışı ve Uygulanışıyla Marshall Planı", *Ankara Üniversitesi SBF Dergisi*, Cilt: 51, Sayı:1, 1996, ss. 275-287, passim; "Marshall Plan, 1948", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/marshall-plan (E.T. 10.04.2015).

[126] Karaosmanoğlu, op. cit., ss. 331-332.

[127] Bu konuda ayrıntılı bilgi için bkz. Robert S. Norris and Hans M. Kristensen, "Global nuclear weapons inventories, 1945–2010", *Bulletin of the Atomic Scientists*, July 2010, Volume 66, Issue 4, pp. 77-83, p. 81. http://bos.sagepub.com/content/66/4/77.full.pdf+html (E.T. 10.04.2015); Karaosmanoğlu, op. cit., 332.

getirmek için 39 teknisyen ve 2 günlük bir çalışma gerekmiştir. Hazırlanan atom bombalarını 1948 yılına kadar hedefe götürecek sadece 30 adet B-29 Superfortress[128] uzun menzilli ağır bombardıman uçağı bulunmaktadır. II. Dünya Savaşı'nda ABD'nin Pasifik Cephesi'nde gerçekleştirilen stratejik bombardımanın arkasında olan General Curtis LeMay'in 1948'de ABD Stratejik Hava Komutanlığı'nın başına geçirilmesi sonrasında yukarıda verilen tablo hızla değişmiştir. Bu tarihten sonra B-50 Bomber[129], B-47 Strojet[130], B-36 Peacemaker[131] gibi ağır bombardıman uçakları hızla servise alınmaya başlamıştır.

Bu aşamada ABD stratejisinin bir parçası olarak planlanan, SSCB ile yaşanacak bir savaşta bombardıman uçaklarının Birleşik Krallık ve Japonya'da bulunan üslere kaydırılarak tepki süresinin kısaltılmasıdır. Bu şekilde gerçekleştirilen saldırılardan elde edilecek zamanla Batı Avrupa'da bulunan devletlerin seferberliklerini tamamlamayacak süreyi kazanması planlanmıştır. Nükleer silahların Avrupa'ya kaydırılan uçaklardan atılması dahi, şehirlerden daha stratejik olabilecek askeri hedeflere ya da kritik altyapılara karşı saldırı planı yapılmasını sağlayamamıştır. Bu durumun birden fazla sebebi bulunmaktadır. Öncelikle II. Dünya Savaşı'nda gelişen radar teknolojisi ve uçaksavar sistemleri devletlerin kritik değere sahip varlıklarını korumasını sağlamıştır. Bu nedenden ötürü uçaklar düşman ülke içerisinde mümkün olan en büyük ve korunaksız hedefe en az riskle yaklaşmak zorunda kalmıştır. Bir diğer önemli sebep ise nükleer silahların o dönemdeki özellikleriyle ilgilidir. O esnada üretilen nükleer silahlar, uçaklardan en basit olarak kabul edilebilecek teknik olan serbest düşüşle atılan bombalardır. Serbest düşüş bombaların vuracağı hedefe olan isabetini oldukça etkilemiştir. Son olarak ele alınması gereken sebep ise SSCB içerisindeki sınırlı istihbarat kapasitesidir.[132] Sınırlı istihbarat hedef tespit etmeyi ve bazı alanlarda hangi hedefin diğerinden daha değerli olduğunun

[128] Bu konuda ayrıntılı bilgi için bkz. "B-29 Superfortress", http://www.boeing.com/boeing/history/boeing/b29.page (E.T. 10.04.2015).
[129] Bu konuda ayrıntılı bilgi için bkz. "B-50 Bomber", http://www.boeing.com/boeing/history/boeing/b50.page (E.T. 10.04.2015).
[130] Bu konuda ayrıntılı bilgi için bkz. "B-47 Stratojet", http://www.boeing.com/boeing/history/boeing/b47.page (E.T. 10.04.2015).
[131] Daniel Ford, "B-36: Bomber at the Crossroads", *Air&Space Magazine*, April 1996, http://www.airspacemag.com/history-of-flight/b-36-bomber-at-the-crossroads-134062323/?no-ist (E.T. 10.04.2015).
[132] Bu konuda ayrıntılı bilgi için bkz. Robert Wallace, H. Keith Melton, *CIA Kendini Anlatıyor Casusluk*, Çev. Algan Sezgintüredi, 1. Baskı, İstanbul: NTV Yayınları, Aralık 2010, passim.

mukayesesini zorlaştırmıştır. Yukarıda verilen sebeplerden dolayı temel strateji 1950'li yıllarda değişene kadar, ABD için alan hedefleri öncelikli hedefler olarak kalmıştır.[133]

ABD içerisinde dört yıl boyunca nükleer silahların kullanım stratejisi ile ilgili tartışmalar sürerken 29 Ağustos 1949[134] tarihinde SSCB, ilk nükleer denemesini[135] Sibirya'da başarıyla gerçekleştirmiştir. SSCB'nin ilk nükleer denemesi ABD için büyük bir sürpriz olmuştur çünkü Manhattan Projesi sonucunda nükleer silaha sahip olduğu günden sonra nükleer sırları korumaya ve tek nükleer güç olarak uzun süre varlığını sürdürmeye çalışmıştır. Bu süreçte nükleer silah üretim çabalarının başında büyük katkısı bulunan müttefik Birleşik Krallık dahi nükleer sırların dışarısında tutulmaya çalışılmıştır. Bu durum neticesinde Birleşik Krallık ilk nükleer silah denemesini ancak 1952 Ekim'inde[136] gerçekleştirebilmiştir. Nükleer sırlarını korumak için büyük çaba gösteren ABD aynı zamanda bu alanda uluslararası denetim mekanizmaları kurarak atom enerjisinin uluslararası kontrol altında olmasını BM üzerinden önermiştir. Öneriyi ABD adına gerçekleştiren ise Soğuk Savaş'ın isim babası ve ABD'nin BM nezdinde temsilcisi olan Bernard Baruch olmuştur.[137] Dünyada o esnada tek nükleer gücün ABD olduğu ve diğer devletlerin henüz nükleer silah geliştirme kapasitesinden uzak olduğu fikrinin ABD'de hâkim olduğu düşünüldüğünde, oldukça idealist olan bu teklif SSCB tarafından reddedilmiştir. Bu durum ABD tarafından, SSCB'nin nükleer teknolojide oldukça geride olduğu şeklinde yorumlansa da teklifin üzerinden iki yıl dahi geçmeden SSCB ilk başarılı denemesini gerçekleştirmiştir.[138] SSCB'nin denediği ilk nükleer silahın arkasında Andrei Sakharov ve Igor Kurchatov'un başında bulunduğu 1942'den 1949'a kadar devam eden geliştirme çalışmaları olsa da bombanın yapılmasını sağlayan gerçek güç ABD'de bulunan SSCB ajanlarıdır. Klaus Fuchs, Theodore Hall, Harry Gold, David Greenglass, Ethal Rosenberg, Julius Rosenberg, Lona Cohen gibi SSCB ajanları Manhattan Projesi

[133] Bu konuda ayrıntılı bilgi için bkz. Karaosmanoğlu, op. cit. ss. 332-334.
[134] SSCB'nin ilk nükleer denemesi hakkında çalışmada kullanılan eserlerde farklı tarihler tespit edilmiştir. Karaosmanoğlu çalışmasında ilk deneme için Eylül 1949 tarihini verirken, Özden 29 Ağustos 1949 tarihini vermiştir. Freedman ise eserinde Ağustos 1949 şeklinde bir tarihlendirme yapmıştır. Bu konuda ayrıntılı bilgi için bkz. Karaosmanoğlu, op. cit., s. 334; Özden, op. cit., s. 71; Freedman, "The Cold War", op. cit., p. 35.
[135] ABD, Joseph Stalin'e atfen bu denemeye Joe-1 kod adını vermiştir.
[136] Özden, loc. cit.
[137] Bu konuda ayrıntılı bilgi için bkz. "The Acheson-Lilienthal & Baruch Plans, 1946", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/baruch-plans (E.T. 10.04.2015); Özden, op. cit., ss. 125-126.
[138] Freedman, op. cit., pp. 34-36.

içerisinde yer almış yada ilişkili sanayii sırlarının çalınmasına yardım etmiştir. Elde ettikleri sırlar sayesinde ABD'nin Nagazaki'ye attığı *"Fat Man"* kod adlı plütonyum bombası büyük ölçüde kopyalanmıştır.[139]

SSCB'nin 1949'da ABD atom tekelini ortadan kaldırması, nükleer silahların kullanımını öngören stratejilerde büyük değişimlere yol açmıştır. Bu noktadan itibaren nükleer silahlara başvurup başvurmama kararı ABD'nin tercihi olmaktan çıkmıştır. Artık SSCB nükleer savaşı elindeki nükleer silahlarla başlatabilecek ve ABD'yi bir nükleer savaşa zorlayabilecektir. Bu yeni durum nükleer silahları ABD için savaşları bitirebilecek bir araç olmaktan çıkarmış ve karşılıklı nükleer silahlar üzerinden sağlanacak bir caydırıcılık stratejisi oluşturulması sürecine sokmuştur. Bu caydırıcılığı sağlamak ve üstünlük kurmak amacıyla nükleer silahlarda atom bombasının bir üst aşaması olan ve patlayıcı etkisini kilotonlardan megatonlara çıkaran hidrojen bombasını yapım sürecine girilmiştir.

1947 yılında "*The National Security Act of 1947*"[140] ile ABD başkanına dış politikada yardımcı olması amacıyla kurulan "*National Security Council*" (NSC)[141], Soğuk Savaş boyunca ABD'nin ihtiyaç duyduğu stratejilerin oluşturulmasında büyük pay sahibi olmuştur. SSCB'nin başarılı nükleer denemesinin ardından ABD Başkanı Truman 31 Ocak 1950'de hidrojen bombası kararını halka açık bir şekilde deklare etmekle

[139] SSCB'nin nükleer silah geliştirme süreci ve bu süreçte SSCB ajanlarının katkısı hakkında ayrıntılı bilgi için bkz. "The Soviet Nuclear Weapons Program", http://nuclearweaponarchive.org/Russia/Sovwpnprog.html (E.T. 10.04.2015); Pavel V. Oleynikov, "German Scientists in the Soviet Atomic Project", *The Nonproliferation Review*, Summer 2000, pp. 1-30, passim, http://cns.miis.edu/npr/pdfs/72pavel.pdf (E.T. 10.04.2015); Michael I. Schwartz, "The Russian-A(merican) Bomb: The Role of Espionage in the Soviet Atomic Bomb Project", *Journal of Undergraduate Science, Summer 1996, pp. 103-108, passim*, http://www.hcs.harvard.edu/~jus/0302/schwartz.pdf (E.T. 10.04.2015); "Creatıon Of Nuclear Center, Arzamas-16", http://www.sarovlabs.com/history_sarov_nc/ (E.T. 10.04.2015); "Espionage And The Manhattan Project (1940-1945)", U. S. Department of Energy-Office of History and Heritage Resources, https://www.osti.gov/manhattan-project-history/Events/1942-1945/espionage.htm (E.T. 10.04.2015); Marian Smith Holmes, "Spies Who Spilled Atomic Bomb Secrets", 19 Nisan 2009, http://www.smithsonianmag.com/history/spies-who-spilled-atomic-bomb-secrets-127922660/?all (E.T. 10.04.2015); Mehmet Tanju Akad, *Askeri Tarihte Stratejik Düşünce*, 2. Basım, İstanbul: Türkiye İş Bankası Yayınları, Şubat 2014, pp. 126-127.

[140] NSC'nin kuruluşu için bkz. "National Security Act of 1947", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/national-security-act (E.T. 10.04.2015).

[141] Kurulduğu günden 2011'e kadar NSC hakkında yapılmış ayrıntılı bir değerlendirme için bkz. Richard A. Best Jr., *The National Security Council: An Organizational Assessment*, Congressional Research Service, 28 Aralık 2011, https://fas.org/sgp/crs/natsec/RL30840.pdf (E.T. 10.04.2015).

beraber[142] aynı gün yapılan NSC toplantısında ABD'nin bundan sonraki süreçte stratejisini belirleyecek bir raporun oluşturulması talimatını da vermiştir.[143] Bu kapsamda Paul Nitze'nin başkanlığındaki ekibin[144] oluşturduğu *"NSC 68: United States Objectives and Programs for National Security"* adlı rapor, 7 Nisan 1950'de ABD Başkanı'na sunulmuştur. [145]

ABD stratejisinin oluşturulmasında büyük bir aşama olarak kabul edilebilecek *"NSC 68"*, SSCB tehlikesinin her geçen gün arttığının altını çizmiştir. Bu noktada 1950'li yıllarda kabul gören *"New Look"* yaklaşımı ve bunun kaynağı olan *"NSC 162/2*"'den daha öngörülü olan *"NSC 68"*, SSCB tehdidine karşı nükleer silahlanmaya devam edilmesini tavsiye etse de 1954 yılına kadar ABD'nin SSCB karşısındaki nükleer üstünlüğünün sona ereceğini iddia etmiştir. *"NSC 68"* bu doğrultuda gelecekte yaşanacak bir nükleer kilitlenme halinde konvansiyonel silahların önem kazanacağını öngörerek, üstünlük henüz kaybedilmemişken konvansiyonel silahlanmaya ağırlık verilmesini önermiştir. *"NSC 68"*'in ortaya koyduğu gerçeklik 1950'li yıllar boyunca kabul edilmemişse de 1962 yılında ortaya çıkan Küba Füze Krizi sonrasında esnek mukabele doktrinine geçildiğinde, doğru bir yaklaşım olduğu ortaya çıkmıştır.[146]

Truman tarafından 31 Ocak 1950'de ortaya konan direktif sonrasında başlayan hidrojen bombası çalışmaları ise atom bombası çalışmalarına göre çok daha kısa sürede meyvesini vermiştir. Macar asıllı Edward Teller ve Polonya asıllı Stanislaw Ulam'ın dizayn ettiği ilk hidrojen bombası yaklaşık 35 ay sonra 1 Aralık 1952'de Marshall Adaları bölgesinde başarılı bir şekilde denenmiştir. ABD'ye hidrojen bombasının sağladığı üstünlük ise atom bombasının sağladığı üstünlüğe göre çok daha kısa sürmüştür. Yaklaşık dokuz ay sonra 12 Ağustos 1953'te SSCB de ilk başarılı hidrojen bombasını denemesini yapmıştır. Hidrojen bombalarının atom bombalarına kıyasla yüzlerce kat büyük yıkım kapasine sahip olması yaşanacak olası bir savaşta her iki taraf

---

[142] Başkanın Hidrojen bombası kararını açıkladığı konuşmanın tam metni için bkz. http://trumanlibrary.org/publicpapers/index.php?pid=642&st=&st1 (E.T. 10.04.2015).
[143] Elizabeth Edwards Spalding, *The First Cold War Warrior Harry Truman, Containment,and the Remaking of Internationalism*, USA: The University Press of Kentucky, 2006, p.177.
[144] NSC 68'in oluşum süreci için bkz. "NSC-68, 1950", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/NSC68 (E.T. 10.04.2015).
[145] NSC 68'in tam metni için bkz. NSC 68: United States Objectives and Programs for National Security, Washington, 7 Nisan 1950, http://fas.org/irp/offdocs/nsc-hst/nsc-68.htm (E.T. 10.04.2015).
[146] Karaosmanoğlu, op. cit., ss. 335-336.

için de kesin yok oluşun temellerini atmıştır.[147] Bu bağlamda ABD ve SSCB'nin nükleer denemeleri çalışmamızın teorik çerçevesinde Holsti üzerinden açıkladığımız realizm ve neorealizmde caydırıcılığın sağlanması noktasında kapasitenin gösterimine örnek verilebilir.

2. Kentsel ve Endüstriyel Bölgelere Kitlesel Mukabele

1950'li yılların ortasına gelindiğinde tarihte daha önce görülmemiş yıkım kapasitesi geliştiren iki devlet arasında dünya ikiye bölünmüştür. Bu devletlerin geliştirdikleri kapasiteler kendilerinin asgari caydırıcılıklarını sağlamaktan öte artık düşmanın mutlak yenilgisini sağlamayı amaçlamıştır. Mutlak yenilgiye karşı ikincil vuruş kapasitesi fikrinin ortaya çıkması ve bu kapasiteleri sağlamak ya da düşmanın kapasitesini ortadan kaldırmak için daha fazla nükleer silah üretimi, 1960'lı yılların sonundaki silahsızlanma görüşmelerine kadar sürecek olan büyük silahlanma yarışını başlatmıştır. Genel olarak bakıldığında SSCB'nin nükleer silah üretmesi, SALT I'e kadar aralıksız sürecek olan nükleer silah yarışının başlangıç noktası olmuştur.

2.1. Eisenhower Öncesi ABD Nükleer Kapasitesi

Franklin D. Roosevelt'in II. Dünya Savaşı bitmeden ölmesi üzerine ABD başkan yardımcısıyken başkan olan Harry S. Truman, iki dönem sonunda görevi 1953 yılında Dwight Eisenhower'a bırakmıştır. II. Dünya Savaşı'nda Avrupa'da Hitler Almanyası'nı yenmek için Normandiya çıkarmasını yapan müttefik kuvvetlerin komutanı olan Eisenhower, ABD başkanı olarak göreve geldiğinde Truman'dan askeri ve politik alanda büyük bir miras devralmıştır. George Kennan'ın 22 Şubat 1946'da Dışişleri Bakanlığı'na gönderdiği *"Long Telegram"*[148] ve 1947'de *"X"* kod adıyla *"Foreing Affairs"*'ta yayınlanan *"The Sources of Soviet Conduct"* başlıklı makalesi[149] çevreleme politikasının temellerini atmıştır. Bu politikanın Batı Avrupa'daki en büyün yansımalarından biri de

[147] Ibid, s. 335; Özden, op. cit., s. 71.
[148] "The Charge in the Soviet Union to the Secretary of State" adıyla gönderilen telgrafın tam metni için bkz. http://nsarchive.gwu.edu/coldwar/documents/episode-1/kennan.htm (E.T. 10.04.2015).
[149] X, "The Sources of Soviet Conduct", *Foreign Affairs*, July 1947, Vol. 25, Issue. 14, pp. 566-582, passim. http://www.foreignaffairs.com/articles/23331/x/the-sources-of-soviet-conduct (E.T. 10.04.2015).

1949 yılında *"North Atlantic Treaty Organization"*'nın (NATO) kurulmasıdır.[150] 1950 yılında Soğuk Savaş'ın ilk sıcak çatışması olan Kore Savaşı'nın başlamasıyla beraber ABD konvansiyonel kuvvetlerinde tekrar artış başlamıştır. Bilindiği üzere Kore Savaşı'nda 84 sayılı BM Güvenlik Konseyi kararı[151] ile oluşturulan BM Kuvvetleri'ne destek veren Türkiye'de 1952 yılında Yunanistan ile beraber NATO'ya üye olarak kabul edilmiştir. Böylece Eisenhower göreve geldiğinde Atlantik kıyılarından Orta Doğu ve Kafkasya'ya uzanan hatta, büyük ve sıkı bir ittifaka sahip olmuştur.

Truman'ın bıraktığı bir diğer önemli miras ise özellikle nükleer alanda olmakla beraber askeri alanda sağlanan gelişimdir. Truman başkan olduğu süreçte nükleer silahlara dayanarak konvansiyonel kuvvetleri ihmal etmesine rağmen stratejik hava kuvvetlerinin gelişmesine büyük destek vermiştir. Bunun yanında atom bombasıyla yetinmeyen Truman, hidrojen bombasının üretilmesi direktifini vermiş ve görev süresinin dolmasına birkaç ay kala hidrojen bombasına sahip olmayı başarmıştır.

2.2. Eisenhower, Khruşçev ve Stratejide Değişim

1952 yılı sonunda yapılan seçimler sonucunda görev değişikliği olmuş ve Ocak 1953'te ABD'de başkanlık görevini D. Eisenhower alırken, SSCB'de 5 Mart 1953'te ölen Stalin'in yerine Eylül 1953'te Nikita Khruşçev geçmiştir. Seleflerinin miras bıraktığı nükleer teknoloji üzerine bu iki lider aşağıda genel hatları ile belirttiğimiz yeni stratejileri inşa etmişlerdir.

Eisenhower göreve başlamasının hemen ardından, Truman'ın kendisine bıraktığı miras üzerinden bir genel strateji oluşturulmasını talep etmiştir. Yapılan çalışmalar sonucunda *"NSC 162/2"*[152] isimli rapor 30 Ekim 1953 tarihinde başkanın onayıyla Milli Güvenlik Kurulu'na sunulmuştur. *"NSC 162/2"*'nin önerdiği yaklaşım topyekûn mukabele doktrininin temelini oluşturmuş ve Eisenhower döneminde SSCB'ye karşı alınan önlemlerin tümüne genel olarak *"New Look"* adı verilmiştir. Eisenhower ortaya

[150] NATO'nun kuruluşu hakkında ayrıntılı bilgi için bkz. "A short history of NATO", http://www.nato.int/history/nato-history.html (E.T. 10.04.2015).
[151] Kararın tam metni için bkz. Resolution 84, UN Security Council, 7 Haziran 1950, http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3b00f1e85c (E.T. 10.04.2015).
[152] NSC162/2'nin tam metni için bkz. "NSC 162/2: A Report to National Securtiy Council", http://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf (E.T. 10.04.2015).

koyduğu bu yapı ile ABD'nin nükleer stratejisini oluşturan ilk lider olmuştur. ABD'nin *"New Look"* yaklaşımı ve topyekûn mukabele doktrini ile özdeşleşen ismi ise Eisenhower'in Dışişleri Bakanı olan John Foster Dulles'tır. Ocak 1954'te yaptığı bir konuşmasında Truman dönemindeki yaklaşımların değiştiğini ilk kez Dulles deklare etmiştir. [153] Dulles'ın açıklamalarından dolayı yaşanacak en ufak bir çatışma halinde dahi SSCB ve ÇHC merkezinde bulunan şehirlerin nükleer bombardımana tutulacağı şeklinde algılanan *"New Look"* daha sonra Dulles tarafından *"Foreign Affairs"*'ta yayınlanan makale ile net bir biçimde ortaya konulmuştur. *"New Look"* yaklaşımı konvansiyonel kuvvetlerinde kullanıldığı esnek bir yaklaşımdır ve "topyekûn mukabele doktrini" kullanılacak yaklaşımlar içerisindedir.[154]

"New Look"'un temeli olan *"NSC 162/2"*, ABD askeri kapasitesi ve bunun içerisinde olan nükleer silahları kullanacağını deklera edilmesi yani çatışmada silah ayrımı gözetmeksizin misillemede bulunacağı mesajının düşmana verilmesi ile caydırıcılığın sağlayacağı varsayımı üzerine inşa edilmiştir. Ortaya konulan bu varsayım, nükleer silahları stratejik hedeflere karşı kullanılacak stratejik silahlar olmaktan çıkarmış ve stratejik amaçlara hizmet eden taktik silahlar haline getirmiştir. Şüphesiz nükleer silahların stratejikten öte taktik silah olarak görülmesi çıkarımının altında Truman döneminde başlayan ve devam eden Kore Savaşı'nın etkisi bulunmaktadır. Sınırlı bir savaş olarak görülen Kore Savaşı'nda ABD tarafından nükleer silah kullanılmamıştır. Bu durum savaşın yaklaşık 3 yıl sürmesine ve 300 binden fazla ABD askerinin savaşa katılmasına neden olmuştur.

"NSC 162/2" ise bloklar arasındaki savaşın uzun süreceği varsayımından hareketle ABD'nin ekonomik kuvvetini korumasından yanadır. Nükleer silahların kullanımına ilişkin getirilen yeni görüş ile personel sayısında aşırı artışın önüne geçilerek konvansiyonel kuvvetler için yapılan harcamaların azalmasını sağlanacaktır. *"NSC 162/2"* konvansiyonel kuvvetlerin kullanımını azaltacak şekilde plansa da bu durum konvansiyonel kuvvet kullanımını reddetmemektedir. Konvansiyonel kuvvetlerin kullanılacağı her çatışma seviyesinde nükleer silahların kullanımını temin ederek, konvansiyonel kuvvetlerin optimum noktada tutulmasını amaçlamaktadır. *"NSC 162/2"*

[153] Freedman, "The Evolution of …", op. cit., pp. 72, 79-84.
[154] Bu konuda ayrıntılı bilgi için bkz. John Foster Dulles, "Policiy For Security and Peace", *Foreign Affairs*, Vol. 32, April 1954, No. 3., pp. 353-364, passim.

ve bunun üzerinden şekillenen *"New Look"* ile konvansiyonel kuvvetlere verilen görev stratejik öneme sahip bölgelerin tutulmasını sağlamak, ikmal ve intikal yollarını güvenlik altına almak ve ABD'ye topyekûn mukabelenin de arasında olduğu seçeneklerden ne tür bir mukabelede bulunacağına ilişkin karar vermesini sağlayacak zamanı kazandırmaktır.[155]

Savaşın her kademesinde nükleer silahların kullanılmasına ilişkin yaklaşım nükleer silahların nitelik ve niceliklerini de etkilemiştir. Bu noktada Truman zamanında başlayan geliştirme çalışmaları, Eisenhower döneminde sonuçlarını vermeye başlamıştır. Nükleer silahların herhangi bir çatışmada kullanımına ilişkin yaklaşım neticesinde farklı seviyelerdeki kullanıma uygun nükleer silah üretimine hız verilmiştir. Hidrojen bombası ile bir şehir tamamen ortadan kaldırabileceği gibi Truman dönemindeki nükleer silahlarla şehirlerin ve sanayi bölgelerinin karşılaştırılma yaklaşımından farklı olarak askeri çatışmalarda kullanılmak üzere boyut olarak çok daha küçük ve etki olarak çok daha az güce sahip taktik nükleer silahlar da üretilmiştir. Bu üretim neticesinde ABD envanterine obüs mermisi ebatlarında 1-40 kiloton arasında güce sahip nükleer silahlar girmiştir.[156] Mart 1955'te yapılan bir basın konferansında Eisenhower üretilen taktik nükleer silahların askeri hedeflere kullanılmasını, konvansiyonel mühimmat kullanımından farklı olarak görmediğini belirtmiştir.[157]

ABD *"New Look"* yaklaşımını benimserken, Şubat 1956'da toplanan Sovyetler Birliği Komünist Partisi 20. Kongresi'nde Khruşçev SSCB'nin yeni yaklaşımını ortaya koymuştur. Stalin'in kapitalist devletlerle kaçınılmaz savaş yaklaşımını bir kenara bırakan Khruşçev, *"barış içerinde bir arada yaşama"* yaklaşımını açıklamıştır. Bu yaklaşıma göre ekonomik ve politik alandaki tüm çözümsüzlüğe rağmen nükleer savaşı da içeren bir askeri çatışmadan kaçınmak ve bir arada yaşamak mümkündür. Khruşçev'in bu yaklaşımı ABD'nin hızla nükleer silahlarını çeşitlendirdiği ve topyekûn mukabele söylemini ortaya attığı bir zamanda SSCB'yi korumayı amaçlamaktadır. Khruşçev'e göre yaşanacak bir nükleer savaş, sadece SSCB ya da ABD'yi değil tüm medeniyeti ortadan

[155] Bu konuda ayrıntılı bilgi için bkz. Freedman, "The Evolution of …", op. cit., pp. 76-79; Karaosmanoğlu, op. cit., ss. 336-340.
[156] Richard Weitz, "The Historical Context", Tom Nichols, Douglas Stuart, Jeffrey D. McCausland(edt.), *Tactical Nuclear Wepons and Nato*, US Army War College, Strategic Studies Institute, April 2012, pp. 3-12. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1103.pdf (E.T. 10.04.2015).
[157] Freedman, "The Evolution of …", op. cit., p. 73.

kaldırma tehlikesini barındırmaktadır. Barışçıl söyleminin yanında Khruşçev, SSCB nükleer silahlanmasını desteklemeyi de sürdürmüştür. SSCB, ABD Stratejik Hava Komutanlığı karşısındaki eksikliğini füze programıyla kapamaya çalışmıştır. Temelleri Nazi Almanyası'nın geliştirdiği dikey kalkışlı "*V2*" roketlerine dayanan füze teknolojisi, Khruşçev'in verdiği destekle 1950'li yıllar boyunca hızla gelişmiştir. 20 Şubat 1956'da nükleer başlık takılı ilk orta menzilli balistik füzeyi[158] başarıyla deneyen SSCB, Ağustos 1957'de ilk kıtalararası füze[159] olan *"R-7 Semyorka"*'yıda başarıyla test etmiştir. 4 Ekim 1957'de *"R-7 Semyorka"* füzesi üzerine konuşlandırılmış ilk yapay uydu olan *"Sputnik"*'in başarıyla yörüngeye yerleştirilmesi ise silahlanma yarışına yeni bir boyut olan uzayı eklemiştir.[160]

SSCB'nin geliştirdiği füze teknolojisi ve bu teknolojinin son noktası olan kıtalararası balistik füzeleri kullanarak yörüngeye *"Sputnik"*'i yerleştirebilmesi ABD için korunmasız olduğu bir boyut üzerinden kendi kıtasında saldırıya uğraması ihtimalini ortaya çıkarmıştır. SSCB'nin kıtalararası balistik füzelerle yapacağı sürpriz bir nükleer saldırıyla ABD nükleer kapasitesini ortadan kaldırabilme ihtimali, ABD nükleer kapasitesinin ne kadar korunmasız olduğunu ortaya çıkarmıştır. Ortaya çıkan bu gerçeklik ise uygulanılan stratejilerde daha önce tartışılmayan ikinci vuruş boyutunu eklemiştir.

ABD ve SSCB'nin 1950'li yıllar boyunca girdikleri bu silahlanma yarışı, çalışmamızın teorik çerçevesi içerisinde incelediğimiz ofansif realizmde devletlerin silahlanmasına örnek olarak gösterilebilir. Zira uluslararası sistemin büyük güçleri, herhangi bir üst otorite olmadığı için güvenliklerini sağlamak ve sistemde etkin unsur olabilmek için güçlerini arttırmak yoluna gitmişlerdir.

ABD'li stratejistler tarafından, SSCB'nin füze kabiliyeti gelişmeden önce bu ülkeye gerçekleştirilecek bir nükleer saldırı karşısında, mukabele olarak ABD'nin nükleer silah kabiliyetinin değil şehirlerinin ve sanayi merkezlerinin asıl hedef alacağı hesaplanmıştır. Savunma önlemleri de bu doğrultuda SSCB uçaklarının taarruzuna karşı

[158] Balistik füzeler menzilleri ve gelişimleri hakkında ayrıntılı bilgi için bkz. "Ballistic Missile Basics", Federation of American Scientist, http://fas.org/nuke/intro/missile/basics.htm (E.T. 10.04.2015); Pirinççi, op. cit., 101-103.
[159] Ibid.
[160] Bu konuda ayrıntılı bilgi için bkz. Vladislav M. Zubok, *A Failed Empire: The Soviet Union In The Cold War From Stalin To Gorbachev*, USA: The University of North Coralina Press, 2007, pp. 123-132; İşyar, op. cit., ss. 623-624.

şehirleri ve sanayi bölgelerini korumak üzerine şekillendirilmiştir. SSCB füze kabiliyeti ise herhangi bir hava taarruzuna gerek kalmaksızın, ABD'nin daha önce güvenliğini planlarken hesaplamalarına dahil etmediği nükleer mukabele yeteneğini ortadan kaldırma kapasitesini SSCB'ye sağlamıştır. RAND'ın bu doğrultuda yaptığı çalışmalar, ABD hava üslerinin ve nükleer kapasitesinin, olası bir nükleer saldırıda mukabele yeteneğini kaybedecek kadar zayıf olduğunu göstermiştir. Bu durumun tespiti, savunma tedbirleri geliştirilmeden zafiyetten haberdar olabilecek SSCB için sürpriz bir saldırıyı çok daha değerli hale getirme tehlikesini ortaya çıkarmıştır.1958 yılında RAND araştırmacısı Albert Wohlstetter bu güvenlik zafiyetine işaret ederek ABD'nin caydırıcılığını sağlamak için, karşılaşabileceği nükleer saldırıda ikinci vuruş kapasitesini koruması gerektiğini belirtmiştir. Nükleer dengenin ne kadar istikrarsız olabileceğini gösteren bu çalışma nükleer strateji konusunda gelecekte yapılacak çalışmaları etkilemiştir.[161]

Caydırıcılığı bir mukayeseli riskler sorunu olarak tanımlayan Wohlstetter'ın[162] görüşlerinden etkilenen Bernard Brodie ikinci vuruş kapasitesinin sağlanması için Wohlstetter'e paralel şekilde kapasitenin saldırıya duyarlığının azaltılması gerektiğini vurgulamıştır.[163] Wohlstetter ve Brodie'nin görüşleri ABD yönetimi tarafından dikkate alınmış ve Eisenhower 1958 bütçesine ek olarak bir milyar dolar bütçe istemiştir. Alınan ek bütçeyle ve sonraki yıllarda yapılan yatırımlarla hava üslerinin sayısı çoğaltılmış, erken uyarı sistemleri oluşturulmuş, füzesavar füze sistemlerinin geliştirilmesine öncelik tanınmış ve ABD kendi kıtalararası füze ve denizaltıdan ateşlenebilen füze sistemlerinin geliştirilmesine hız vermiştir.[164]

3. Esnek Mukabele

1950'li yılların ikinci yarısı boyunca obüs mermileri ile hedeflere gönderilebilen taktik nükleer silahlardan, stratejik hidrojen bombalarına kadar tüm alanlarda silahlanma hız kazanmıştır ve bu silahlanma sadece nükleer silahların üretimiyle sınırlı kalmamıştır. Her iki devlet de bu silahların düşman tarafından durdurulmadan hedefe varmasını ya da

[161] Albert Wohlstetter, "The Delicate Balance of Terror", *Foreign Affairs*, Vol. 37, January 1959, No. 2., pp. 211-234, passim, http://www.rand.org/about/history/wohlstetter/P1472/P1472.html (E.T. 10.04.2015); Karaosmanoğlu, op. cit., ss. 341-344.
[162] Wohlstetter, op. cit., p. 222.
[163] Bu konuda ayrıntılı bilgi için bkz. Bernard Brodie, *Strategy In The Missile Age*, New Jersey: Princeton University Press, 15 January 1959, pp. 281-285.
[164] Karaosmanoğlu, op. cit., s. 345.

ikinci vuruş kapasitesini sağlamak için bekalarını korumak amacıyla, kıtalararası balistik füzelerden, jet motorlu ağır bombardıman uçaklarına, deniz tabanında aylarca kalıp muhtemel bir nükleer savaştan yara almadan kurtulacak ve okyanustan nükleer füzeler gönderecek denizaltılara kadar onlarca farklı silah sistemi üretmiştir. Gelişmelerin sonucunda 1960'lı yıllara gelinirken sadece iki devleti değil dünyadaki tüm yaşamı birden fazla kez ortadan kaldırabilecek farklı boyutlarda binlerce nükleer silah üretilmiştir.[165]

İki devletin yarattığı binlerce nükleer silah üzerinden geliştirdikleri ilişki, literatürde *"dehşet dengesi"* adıyla kavramsallaştırılmıştır. Dehşet dengesi devam ederken ortaya çıkabilecek bir nükleer savaşın kazananı olmayacağı için bu durum *"Mutual Assured Destruction"*(MAD / Karşılıklı Kesin Yok Oluş) olarak nitelendirilmiştir. Ortaya çıkan MAD durumu bir yandan her iki devletin nükleer silaha başvurmasını engelleyip nükleer caydırıcılıkta bir denge hali yaratırken diğer yandan da binlerce nükleer silahın olduğu bir ortamda yanlış anlaşılma ya da kazara çıkacak bir nükleer savaş ihtimalini arttırmıştır. Bu doğrultuda 1960 yılında ABD ve SSCB arasında dehşet dengesini kontrol altına alma konusunda bir irade oluşmuşken çıkan U2 Krizi, bu görüşmelerin dünyanın nükleer savaşa en çok yaklaştığı nokta olarak kabul edilen Küba Füze Krizi sonrasına ertelenmesine neden olmuştur.

Genel hatları ile belirtirsek keşif gözlem görevine sahip ABD U2 casus uçağı 1 Mayıs 1960'da SSCB toprakları üzerinde Kızıl Ordu tarafından düşürülmüştür. 3 Mayıs'ta bu bilginin Khruşçev tarafından dünya ile paylaşılması üzerine ABD düşen uçağın bir meteoroloji uçağı olduğunu iddia etmiştir. Bu noktada ABD'li karar alıcıların meteoroloji uçağı iddiası pilotun yaşamadığı varsayımı üzerine kuruluyken, U2 uçağının pilotu Francis Gary Powers SSCB tarafından sağ olarak ele geçirilmiş ve sorgulanmıştır. Powers sorgusunda CIA adına Peşaver-Norveç hattı boyunca SSCB tesislerini tespit etmekle görevlendirildiğini itiraf etmiştir. Khruşçev 5 Mayıs'ta yaptığı ikinci açıklamada bu durumun ABD-SSCB arasında yapılacak görüşmelere büyük zarar verdiğini söylemiştir. Ayrıca ABD üslerinin kurulmasına izin veren ülkeleri de uyaran Khruşçev, SSCB'ye yapılacak herhangi bir saldırıya nükleer füzelerle karşılık verileceğini

[165] 1960 yılında ABD'nin 18638, SSCB'nin 1605 ve Birleşik Krallık'ın 42 nükleer silaha sahip olduğu düşünülmektedir. Bu konuda ayrıntılı bilgi için bkz. Norris and Kristensen, op. cit., p. 81.

belirterek, üslere izin veren ülkelerin de hedef olacağını deklare etmiştir. Pilotun sağ olduğunun anlaşılması ABD'nin uçağın gerçek amacını kabul etmesine ve 25 Mayıs'ta Eisenhower uçuşların durdurulduğunu deklare etmesini sağlasa da yaşanan kriz SSCB ve ABD arasındaki yumuşamanın ertelenmesine neden olmuştur.[166]

Ocak 1961'de ABD Başkanı olan John Fitzgerald Kennedy dönemi ise ABD'nin nükleer stratejisi ve Eisenhower döneminde gittikçe gerginleşen SSCB-ABD ilişkileri için büyük bir kırılma oluşturmuştur. Bu kırılmanın en büyük nedeni 1962 yılında meydana gelen Küba Füze Krizi'dir. 1960'ta meydana gelen U2 Krizi sonrasında ABD-SSCB arasında gerginleşen ilişkilerin yansıması olarak Khruhçev Küba'da 1959 yılında yönetimi ele geçiren sosyalist Fidel Castro yönetimine olan desteğini arttırmıştır. Bu doğrultuda ABD'nin Küba'daki yeni yönetimi devirmek amacıyla planladığı Domuzlar Körfezi Çıkarması[167] harekatına karşı Castro yönetimini desteklemiştir. Ekonomik yardım amacıyla Küba'nın ürettiği şeker satın alınmıştır. SSCB ve Küba arasında gelişen ilişkilerin sonucu olarak 1962 yılında Küba'ya SSCB füzeleri konuşlandırılmaya başlanmıştır. ABD tarafından durumun fark edilmesi üzerine, Kennedy bu durumu açıkça eleştirmiş ve adaya SSCB tarafından üs kurulması halinde müdahale edileceğini dile getirmiştir. Daha sonra yapılan incelemelerde adadaki füzelerin henüz kuruluş aşamasında ve ateşlemeye hazır olmadığının anlaşılması üzerine Kennedy, eksik parçaların adaya ulaşmasını engellemek amacıyla Küba'ya abluka uygulama kararı almıştır. 22 Ekim 1962'de abluka uygulanmaya konulsa da SSCB gemileri Küba'ya olan güzergâhlarından vazgeçmemişlerdir. Khruşçev'in adaya yerleştirilen silahların saldırı değil savunma amacı güttüğünü belirterek gemilere durma emri vermeyeceğini açıklaması, iki devlet arasında yaşanan gerilimin daha da artmasına neden olmuştur.[168]

[166] Freedman, "The Cold War", op. cit., pp. 54-56; Richard Aldrich, "Intelligence", Saki D. Dockrill and Geraint Hughes(edt.), *Palgrave Advances in Cold War History*, USA: PALGRAVE MACMILLAN, 2006, pp. 226-229; Christopher John Bright, "U2 Incident", James R. Arnold and Roberta Wiener(edt.), *Cold War The Essential Reference Guide*, USA: ABC-CLIO, 2012, pp. 221-222; Armaoğlu, op. cit., ss. 599-602; Khrushchev and Eisenhower: Summit Statements, 16 Mayıs 1960, http://legacy.fordham.edu/halsall/mod/1960summit-statements1.asp (E.T. 10.04.2015).

[167] Freedman, "The Cold War", op. cit., pp. 71-74; James H. Wilbarka, "Bay of Pigs", James R. Arnold and Roberta Wiener(edit.), *Cold War The Essential Reference Guide*, USA: ABC-CLIO, 2012, pp. 15-16.

[168] Bu konuda ayrıntılı bilgi için bkz. Freedman, "The Cold War", op. cit., pp. 75-78; Siricusa, op. cit., p. 72; Priscilla Roberra, "Cuban Missile Crisis", James R. Arnold and Roberta Wiener(edt.), *Cold War The Essential Reference Guide*, USA: ABC-CLIO, 2012, pp. 221-222; Armaoğlu, op. cit., ss. 602-612.

Bu noktadan sonra başlayan mektuplaşma trafiği Khruşçev'in asıl amacını ortaya koymuştur. Khruşçev, Kennedy'ye gönderdiği mektubunda, SSCB'nin Küba'ya kurmak istediği füzelere benzer füzelerin ABD tarafından SSCB'ye karşı Türkiye'de kurulduğunu belirtmiştir. ABD'nin Türkiye'de bulunan *"Jüpiter Füzeleri"*'ni sökmesi halinde SSCB'nin Küba'da kurmaya başladığı füzeleri sökeceğini, Türkiye'yi işgal etmeyeceğini ya da içişlerine karışmayacağını bildirmiştir. Kennedy cevabını içeren mektupta, Küba'daki füzelerin sökülmesi durumunda adaya uygulanan ambargoyu kaldıracağını açıkça belirtse de Türkiye'de bulunan füzeler konusunda açık taahhütte bulunmamıştır. Bu durumun füzelerin kaldırılması durumunda yaşanacak yumuşamada müzakere edilebileceğini belirtmiştir. Khruşçev bu konuda gönderdiği son mektubunda Kennedy'nin tutumunu yeterli bulduğunu belirtmiştir. Son mektuplarda SSCB ve ABD liderleri tarafından Türkiye'deki *"Jüpiter Füzeleri"*'nden bahsedilmese de iki devlet arasında yapılan diplomatik görüşmeler sonucunda kamuoylarından gizli kalması kaydıyla füzelerin kaldırılması hususunda mutabakat sağlanmıştır. Küba'da bulunan füzeler diplomatik görüşmeler sonrasında SSCB tarafından sökülse de yaşanan krizin etkileri çok daha kalıcı olmuştur. Küba Füze Krizi'nde SSCB ve ABD ilk defa doğrudan askeri olarak karşı karşıya gelmiştir. Nükleer savaş tehlikesi her iki devleti savaşı çıkaracak son adımı atmaktan uzaklaştırsa da Küba Füze Krizi nükleer savaşa en yaklaşılan nokta olarak Soğuk Savaş'ın zirvesini temsil etmiştir.[169]

Küba Füze Krizi sonrasında iki devlet arasında dehşet dengesinin risklerini azaltacak görüşmeler başlamıştır. Bu doğrultuda atılan önemli adımlardan biri yanlış anlaşılmalardan kaynaklı bir nükleer savaşı önlemek için SSCB ve ABD liderleri arasında doğrudan iletişimi sağlayacak *"Kırmızı Telefon Hattı'"*nın kurulmasıdır. Bunun yanında 5 Ağustos 1963 tarihinde atmosfer, uzay ve sualtında nükleer denemeleri sınırlayan *"Nükleer Denemeleri Sınırlama Anlaşması"* imzalanmıştır. Bu anlaşmayı ilerleyen süreçte imzalanacak olan 27 Ocak 1967 tarihli *"Dış Uzay Anlaşması"* ve halen oldukça

[169] Bu konuda ayrıntılı bilgi için bkz. Vladislav M. Zubok and Hope M. Harrison, "The Nuclear Education of Nikita Khrushchev", Jonhn Lewis Gaddis Philip Gordon, Enrnest May, Jonathan Rosenberg(edt.), *Cold War Statesman Confront The Bomb Nuclear Diplomacy Since 1945*, New York: Oxford University Press, 1999, pp. 157-161; James G. Hershberg, " The Cuban Missile Crisis", Melvyn P. Leffler and Odd Arne Wasted(edt.), *The Cambridge History of Cold War, Volume II Crises and Detente*, New York: Cambridge University Press, 2010, pp. 65-87.

önemli olan 1 Temmuz 1968 tarihli *"Nükleer Silahların Yayılmasının Önlenmesi Anlaşması"* (NPT) takip etmiştir.[170]

Küba Füze Krizi'nden itibaren yaşanan süreçte topyekun mukabele anlayışı bir kenara bırakılarak, nükleer silahlarında seçenekler arasında bulunduğu ama en son seçenek olarak düşünüldüğü esnek mukabele anlayışına kademeli olarak geçilmiştir. Bu doğrultuda nükleer savaşa varacak nizami çatışma ihtimallerini azaltmak adına, gayri nizami harp unsurlarını uygulamak için ABD tarafından özel birlikler yetiştirilmeye başlanmıştır. Bu birliklerin ve ABD gizli servisi Central Intelligence Agency'nin (CIA) çalışmaları 1960'lı yıllardan itibaren hızla artmıştır. Gayri nizami harp unsurları ile yürütülen mücadele nükleer savaşa varacak krizlerin baş göstermesini büyük ölçüde engellemiştir. Yumuşama ortamının sonucu olarak 1969'dan itibaren nükleer silahların, bu silahların iletim vasıtalarının ve bu silahlara karşı koruma sağlayan vasıtaların sınırlandırılmasına ilişkin müzakereler başlamıştır.[171]

4. Düşman Tarafı Nükleer Savaş Kazanabilecek Bir Kapasiteden Yoksun Bırakmak

Kasım 1969'da Helsinki'de başlayan Stratejik Silahların Sınırlandırılması Görüşmeleri Soğuk Savaş boyunca nükleer alanda yaşanan büyük kırılmalardan biridir. Küba Füze Krizi sonrası başlayan yumuşama dönemi boyunca *"NPT"* dâhil nükleer silahların kullanımı ve yayılmasıyla ilgili anlaşmalar yapılsa da SALT ile ilk defa bu silahların üretiminin sınırlandırılması tartışılmaya başlanmıştır.

SALT görüşmelerinin yapılmasının birden fazla sebebi bulunmaktadır. Öncelikle 1962'de yaşanan Küba Füze Krizi sonrası dünyanın nükleer savaşın eşiğine gelmesi ve bu savaşı hiçbir devletin kazanamayacak olması barış içerisinde bir arada yaşamaktan başka bir seçenek olmadığını açıkça ortaya koymuştur. Bu süreçte SSCB ve ÇHC arasında yaşanan görüş ayrılıkları ile ABD ve Fransa arasında yaşanan görüş ayrılıkları

[170] Haluk Gerger, *Soğuk Savaş'tan Yumuşama'ya*, 1. Baskı, Ankara: Işık Yayıncılık, 1980, ss. 96-97.
[171] Bu konuda ayrıntılı bilgi için bkz. Philip Nash, "Bear Any Burden? John F. Kennedy and Nuclear Weapons", Jonhn Lewis Gaddis Philip Gordon, Enrnest May, Jonathan Rosenberg(edt.), *Cold War Statesman Confront The Bomb Nuclear Diplomacy Since 1945*, New York: Oxford University Press, 1999, pp. 124-127; Akad, "*Askeri Tarihte…*", op. cit., pp. 249-254.

da Doğu ve Batı Bloklarında çatlaklar oluşmasına neden olmuştur. [172] Bloklar içerisindeki problemler, iki kutup lideri devleti de belli ölçüde anlaşmaya zorlamıştır.

Ele alınması gereken bir diğer hususta gelişen silah teknolojisinin getirdiği sonuçlardır. 1960'lı yıllar boyunca yumuşama dönemi yaşansa da silah teknolojisinde ki gelişmeler iki devlet arasındaki nükleer dengeyi bozucu unsurların geçici süreyle ortaya çıkmasına neden olmuştur. Bu teknolojilerden ilk olarak ele alınması gereken füze teknolojisinde yaşanan gelişimdir. Nazi Almanyası'nın *"V2"* Roketleri üzerinden gelişen bu teknoloji 1960'ların sonuna gelindiğinde saldırı doktrinlerinin değişmesinde büyük bir etken olmuştur.

Öncelikle kısa menzilden hızla kıtalararası menzillere ulaşan füze teknolojisindeki diğer değişim füzenin taşıdığı başlık sayısı ve füzenin konumlandırılmasında olmuştur. Başlarda tek bir hedefe gönderilen füzelerin yerini, içerisinde birden fazla küçük füze olarak tarif edilebilecek başlıkların olduğu çok başlıklı füzeler almıştır. Birden fazla hedefe çok başlıklı tek füze (Multiple İndependently Targetable Reentry Vehicle / MIRV)[173] ile ulaşılabilmesi, savunulması oldukça zor olan bir saldırı türünü daha da zor hale getirmiştir. Ayrıca füzeler artık sadece karada bulunan silolarda konuşlandırılmakla kalmamış bunun yanında denizaltından atılabilen nükleer füzeler (Submarine-Launched Ballistic Missile) de iki devletin envanterine girmiştir. Füze teknolojisinde yaşanan bu ilerleme füzesavar füze (Anti-Ballistic Misilse / ABM) teknolojisinin geliştirilmesi yolunda adım atılmasına neden olmuştur. Geliştirilmesi oldukça maliyetli radarlar, sensörler ve hedef hassasiyeti olan füzelerden oluşan bu sistemlerin ise yaşanacak bir nükleer savaşta başarı şansının ne olacağı belirsizdir. Füzesavar füze teknolojisi aynı zamanda iki devlet arasındaki nükleer caydırıcılığın temeli olan saldırıya açık şehirlerin korunması ihtimalini ortaya çıkararak, oldukça hassas olan nükleer dengeye zarar vermektedir.[174]

Arka planda yukarıda verilen gelişmeler ışığında başlayan SALT, iki aşamadan oluşmuştur. SALT ya da SALT I olarak ifade edilen ilk tur 1969-1972 arasında süre

[172] Armaoğlu, op. cit., ss. 769-770.
[173] Milton Leitenberg, *Studies of Military R&D and Weapons Development,* Case Study 3 The Origin of MIRV, passim, http://fas.org:8080/man/eprint/leitenberg/index.html
[174] Bu konuda ayrıntılı bilgi için bkz. Freedman, "The Evolution of …", op. cit., pp. 334-338.

gelmiştir. Sonucunda ise füzesavar füze teknolojisinin sınırlandırılması konusunda kesin bir anlaşma ve geçici anlaşmalar imzalanmıştır. 1972'de başlayan SALT II ise 1979'a kadar sürmüş sonucunda anlaşma imzalansa da imzalanan anlaşma Afganistan'ın SSCB tarafından işgali sonrasında ABD tarafından iç hukukta usulüne uygun olarak onaylanmadığı için hukuksal geçerlilik kazanmamıştır.[175]

1969 yılında başlayan SALT görüşmelerinin ana müzakere konusu gelişen füze teknolojisinin üç alanında gerçekleşmiştir. Bu alanlar kıtalararası balistik füzeler arasında özellikle çok başlı taşıyan MIRV'lar; denizaltından ateşlenebilen SLBM'ler ve füzesavar füze sistemleri olan ABM'lerdir. Yapılan görüşmeler sonucunda ABM'ler hakkında nihai anlaşma olan *"Anti-Ballistic Missile Anlaşması"* imzalansa da MIRV'lar ve SLBM'ler hakkında beş yıl süreli geçici anlaşmalar yapılmıştır. Anlaşmalar, 26 Mayıs 1972'de ABD Başkanı Richard Nixon ile SSCB Komünist Partisi Genel Sekreteri Leonid Brejnev arasında Moskava'da imzalanmıştır.[176]

Varılan uzlaşmaya binaen imzalanan *"Anti-Ballistic Missile Anlaşması"*[177] sonucunda her iki devlette sahip olduklarını ABM sayısını biri başkentlerini biri de Inter Continental Ballistic Missile (ICBM) kapasitelerini koruyacak şekilde ikiye indirmişlerdir. Daha sonra 3 Temmuz 1974'te imzalanan *"ABM Protokolü"*[178] ile bu sayı ikiden bire düşürülmüştür. *"Anti-Ballistic Missile Anlaşması"* ile beraber beş yıl süreli yapılan geçici anlaşma ile de ABD 44 denizaltı ve bu denizaltılardan atılabilecek 710 SLBM ile SSCB ise 62 denizaltı ve bu denizaltılardan atılabilecek 950 SLBM ile sınırlandırılmıştır.[179] ICBM'ler de ise yeni füze üretilmemesi kararı alınmıştır.[180] ABD,

[175] Bu konuda ayrıntılı bilgi için bkz. Tayyar Arı, *Uluslararası İlişkiler ve Dış Politika*, 7 Baskı, Bursa: MKM, 2008, ss. 601-602.
[176] Bu konuda ayrıntılı bilgi için bkz. Armaoğlu, op. cit., ss. 769-772; Sibel Kavuncu, "Nükleer Silahsızlanma Yolunda Start Süreci", *Bilge Strateji*, Cilt 5, Sayı 8, Bahar 2013, ss.119-148, ss. 121-124.
[177] Anti-Ballistic Missile Anlaşması'nın tam metni için bkz. "Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Limitation Of Anti-Ballistic Missile Systems", 26 May 1972, http://www.state.gov/www/global/arms/treaties/abm/abm2.html (E.T. 10.04.2015).
[178] 1974'te düzenlenen ABM Protokolü için bkz. "Protocol To The Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Limitation Of Anti-Ballistic Missile Systems", 3 July 1974, http://fas.org/nuke/control/abmt/text/abmprot1.htm (E.T. 10.04.2015).
[179] SALT I neticesinde imzalanan 5 yıl süreli geçici anlaşma için bkz. "Interim Agreement Between The United States Of America And The Union Of Soviet Socialist Republics On Certain Measures With Respect To The Limitation Of Strategic Offensive Arms", 26 May 1972, http://fas.org/nuke/control/salt1/text/salt1.htm (E.T. 10.04.2015).
[180] Gerger, op. cit., ss. 96-97.

SALT neticesinde süre şartı konulmadan imzalanan *"Anti-Ballistic Missile Anlaşması"'*dan, 11 Eylül 2001 Saldırıları sonucunda geliştirdiği yeni politika doğrultusunda 13 Aralık 2001'de tek taraflı olarak çekilmiştir.[181]

18 Haziran 1979'da Viyana'da ABD Başkanı Jimmy Carter ile SSCB Komünist Partisi Genel Sekreteri Leonid Brejnev arasında imzalanan anlaşma[182], SALT I sonucunda çözüme varılamayan ya da geçici süreli anlaşmalara bağlanan konuların çözümünü içermiştir.[183] Yapılan anlaşma neticesinde her iki devlet belli konulardaki askeri kapasitesini karşı tarafa bildirmiş, ICBM ve SLBM tipi füzelere miktar sınırlanması yapılmış, seyir füzelerine (cruise missile)[184] 600 km menzil limiti getirilmiş ve birden fazla başlık taşıması yasaklanmıştır.[185]

SALT I sonucunda yapılan anlaşmanın en büyük sonucu her iki devletin de aralarındaki nükleer dengenin bozulması için çaba harcamak yerine bilinçli olarak dengeyi devam ettirme iradesini göstermiş olmasıdır. SALT I'in sonucunda imzalanan *"Anti-Ballistic Missile Anlaşması"* her iki devletin de şehirlerini korumasını engellemiştir. Bu engelleme iki devletinde birbirlerinin şehrini rehin konumda tutarak dehşet dengesinin varlığını korumuş ve karşılıklı yok olma ihtimalini garanti altına almıştır. Bu istikrar arayışı 1979'da SSCB'nin Afganistan'ı işgalinden sonra *"İkinci Soğuk Savaş"* olarak adlandırılacak süreçte ortadan kalkmıştır. ABD Soğuk Savaş'ta dengeyi kendi lehine son kez değiştirmek için 1984'de *"Strategic Defense Initiative (SDI)"* adını alan yeni askeri programını açıklamıştır.

5. Nükleer Savaş Kazandıracak Kapasite

23 Mart 1983'te ABD Başkanı Ronald Wilson Reagan'un konuşmasıyla başlayan yeni silahlanma yarışı, SSCB'nin ekonomik kötü gidişatını hızlandırarak Soğuk Savaş'ın

[181] ABD'nin Anti-Ballistic Missile Treaty'den çekilme açıklaması için bkz. "ABM Treaty Fact Sheet", White House Press Secretary, http://2001-2009.state.gov/t/ac/rls/fs/2001/6848.htm (E.T. 10.04.2015).
[182] SALT II girişimi anlaşma imzalanmasına rağmen başarısızlıkla sonuçlandığı için çalışmamızda ayrıntılı olarak ele alınmayacaktır.
[183] Salt II anlaşmasının tam metni için bkz. "Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Limitation Of Strategic Offensive Arms, Together Wıth Agreed Statements And Common Understandings Regarding The Treaty" 18 June 1979, http://fas.org/nuke/control/salt2/index.html (E.T. 10.04.2015).
[184] Seyir füzeleri hakkında ayrıntılı bilgi için bkz. "Cruise Missiles", Federation of American Scientist, http://fas.org/nuke/intro/cm/index.html (E.T. 10.04.2015).
[185] Bu konuda ayrıntılı bilgi için bkz. Armaoğlu, op. cit., ss. 772-778.

bitmesine katkıda bulunmuştur. Reagan yaptığı konuşmada[186] SSCB'nin gösterilen tüm barışçıl tutuma rağmen stratejik füze olarak kabul edilen ICBM teknolojisini, geliştirmeye devam ettiğini vurgulayarak, ABD ve müttefiklerinin bu tehlikeden korunması için ekonomik fedakârlıklarda bulunarak önleyici teknoloji geliştirmesi gerektiğini belirtmiştir.

Reagon'un yaptığı konuşma, SALT I sonrası başlayan yumuşama süreciyle beraber tehdit algısından çıkmaya başlayan SSCB'yi yeniden hedef haline getirmiştir. Çalışmamızın teorik çerçevesi içerisinde incelediğimiz Kopenhag Okulu'nun güvenlikleştirme kavramına bu durum örnek olarak verilebilir. Çünkü Reagon konuşmasıyla ABD toplumu nezdinde SSCB'yi tekrar tehdit algısı içine sokarak güvenlikleştirmiş, SDI için yapılacak ekonomik harcamalara kaynak sağlanmasının önünü açmıştır.

Ocak 1984'te resmi olarak *"Strategic Defense Initiative"* olarak isimlendirilen proje gerçekçi gözükmeyen teknolojik taleplerinden dolayı yönetmen George Lucas'ın 1977'de yayınlanan bilim kurgu filmi *"Star Wars"*'a benzetilerek *"Yıldız Savaşları Projesi"* olarak anılmaya başlanmıştır. Proje, temelde silahlanma yarışını yeni teknolojilerle uzaya taşımaktadır. Bu bağlamda SDI; uzaya yerleştirilecek lazer ışını kullanan silahlar, dünya çapında radarlar, sensörler, diğer tespit ve imha sistemlerini bir bütün olarak barındırmaktadır. SSCB topraklarından yada SLBM kullanan denizaltılardan atılacak kıtalararası füzeler ateşlendikten sonra farklı katmanlarda öncelikle füzelerin tespitini içeren proje, ardından uzayda bulunan lazer silahlarıyla füzenin imha edilerek ABD ve müttefiklerine kalkan olmayı hedeflemektedir.[187] SSCB ise SDI ile başlatılacak bir yarışa girmemek için 1985'ten itibaren ABD'yi projeden vazgeçirmeye çalışmıştır. Bu doğrultuda 19-20 Kasım 1985'te Cenevre'de, 11-12 Ekim 1986'da Rejkjavik'te, 7-10 Aralık 1987'de Washington'da, 29 Mayıs-2 Haziran 1988'de Moskova'da yapılan zirveler ABD'nin projeyi devam ettirme iradesi neticesinde başarısız olmuştur.[188]

[186] ABD Başkanı Ranold Reagan'ın 23 Mart 1983 tarihli "Address To The Nation On Defense And National Security" isimli konuşmasının tam metni için bkz. http://www.atomicarchive.com/Docs/Missile/Starwars.shtml (E.T. 10.04.2015).
[187] Bu konuda ayrıntılı bilgi için bkz. Freedman, " The Cold War", op. cit., pp. 193-194; Freedman, "The Evolution of …", op. cit., pp. 394-397; Siricusa, op. cit., pp. 92-100.
[188] Armaoğlu, op. cit., ss. 1087-1088.

ABD'nin ortaya koyduğu proje her ne kadar dönemin bilimsel imkanları içerisinde üretilmeye müsait görülmese de nükleer dengede yarattığı kırılma oldukça önemlidir. ABD, 1950'li yıllardan SDI'ya kadar özenle korunmaya çalışılan dehşet dengesi ve bunun sağladığı istikrarı yeni yaklaşımıyla ortadan kaldırmayı hedeflemiştir. Bu durumda ABD'nin kazanacağı ilk vuruş kabiliyeti, SSCB silahlarını ve ikincil vuruş kapasitesini anlamsız hale getirecektir. Karşılıklı kesin yok oluşun olmadığı bir ortamda ise ABD, Soğuk Savaş'ın başında nükleer güç olduğu 1945-1949 döneminden daha güçlü bir hale gelecektir. SSCB'nin SDI projesinin 1972'de imzalanan *"Anti-Ballistic Missile Anlaşması"*'na aykırı olduğu iddiası sonuçsuz kalmış ve SSCB uzayın silahlandırılması yarışında ABD'ye karşılık verememiştir.

Burada belirtilmesi gereken bir diğer önemli hususta, SDI projesinin SSCB'nin durdurma taleplerine rağmen devam ettirilse de başarıya ulaştırılamamış olmasıdır. SDI projesinin adı 1993'te ABD Başkanı Bill Clinton tarafından *"Ballistic Missile Defense Organization"* olarak, 2002'de ise ABD Başkanı George W. Bush tarafından *"Missile Defense Agency"* adıyla değiştirilmiştir. Proje aynı ad altında günümüzde sürdürülmeye devam etmektedir. Projedeki lazer silahlarından radarlara, kinetik enerji silahlarından sensörlere uzanan geniş sistemin büyük bir kısmı 2010'lu yıllarda dahi ABD ordusunun kullanımına girecek kabiliyete erişememiştir. Reagan'un, dönemin bilimsel kapasitenin dışındaki teknolojiden oluşan SDI projesini başlatması, ABD'li astrobiyolog Carl Sagan'ın da belirttiği gibi[189] başarıya ulaşmaktan öte SSCB'nin ekonomik çöküşünü hızlandırılması için yapılmış bir girişim olduğu iddiasını kuvvetlendirmektedir.

SSCB, ABD'nin SDI projesine karşılık verememekle kalmamış, askeri harcamalarda yıllarca yaşanan artış SSCB halklarının refahını da büyük ölçüde düşürmüştür. SSCB'nin son lideri Mihail Gorbaçov'un *"Glastnost"* ve *"Perestroyka"* gibi reform çabaları bu süreçte yeterli olmamıştır. Tüm bu gelişmelerin neticesinde neticesinde 1989'da Avrupa'da SSCB gücünün simgelerinden biri olan Berlin Duvarı yıkılmıştır. Orta ve Doğu Avrupa'daki hakimiyetini hızla yitiren SSCB 21 Aralık 1991 yılında *"Alma Ata Deklerasyonu"* ile hukuken ortadan kalkmıştır. Bu süreçte SSCB'nin

[189] Carl Sagan'ın 1986 tarihli "How to Reduce the Risk of Nuclear Warfare: Carl Sagan on Space Exploration" isimli basın konferansının tamamı için bkz. https://www.youtube.com/watch?v=fVUk30GFsL4 (E.T. 10.04.2015).

dağılması sonrası bağımsızlık elde eden ülkelerde kalan nükleer silahlar da yeni kurulan RF'ye iade edilmiştir.[190]

[190] Bu konuda ayrıntılı bilgi için bkz. Sibel Turan, Yasin Usta, "Küresel Ve Bölgesel Nükleer Güçlerin Kıskacında Orta Asya", *ISSA II. Uluslararası Sosyal Bilimler Kongresi Kongre Kitabı*, Kocaeli: Kocaeli Üniversitesi Yayını, 2009, pp. 874-892, passim.

III. BÖLÜM

SİBER UZAY VE SİBER CAYDIRICILIK

Çalışmamızın üçüncü bölümünde ise siber uzayda büyük öneme sahip olacağı düşünülen "caydırıcılık" olgusu, bütüncül bir bakış açısıyla sunulmaya çalışılacaktır. Siber uzayda saldırı stratejilerini ve araçlarını bilmek, caydırıcılığın işlevselliğine dair kanaat oluşturmak için oldukça önemlidir. Bu doğrultuda üçüncü bölümde öncelikle siber saldırı türleri ve aralarındaki farklar, bu saldırıların teknik kabiliyetleri ve kapasiteleri ele alınacaktır. Sonrasında ise geliştirilen bu strateji ve araçların sahadaki kabiliyetleri ve devletler üzerindeki etkisini göstermek amacıyla siber uzaya bakışta kırılmalara neden olan Kosova Krizi, Estonya Saldırısı, Gürcistan Saldırısı ve İran'a düzenlenen STUXNET Saldırısı ayrıntılı olarak incelenecektir.

Çalışma kapsamında yapılan ön okuma doğrultusunda siber uzayda gerçekleştirilen saldırıların, kritik altyapılarla ilişkisi öne çıkmış olup; kritik altyapıların korunmasının caydırıcılıkta oldukça önemli olduğu fark edilmiştir. Bu bağlamda siber uzayda gerçekleştirilen saldırıların incelenmesinin ardından, siber güvenliğin sağlanmasında kritik altyapılarının korunmasının önemi teorik bir bakışla ayrıntılı olarak irdelenecektir. Siber caydırıcılığa ilişkin oluşmaya başlayan sınırlı literatür, bu alanda genellemelere gidilerek bütüncül bir bakış açısıyla inceleme yapmayı zorlaştırmaktadır. Bu nedenle "Siber Caydırıcılık Mümkün Mü" alt başlığında, caydırıcılığın siber uzayda sağlanıp sağlanamayacağını incelemek için, kavramlar üzerinden yazarları incelemek yerine literatürü oluşturan yazarların kavramsallaştırmalarına ve bu kavramsallaştırmalar üzerinden oluşturdukları görüşlerine ayrıntılı olarak yer verilecektir.

1. Siber Saldırı Türleri

Siber uzayda ofansif kapasiteye sahip aktörler diğer dört boyutta olduğu gibi kendisine özgü saldırı araçları kullanmaktadırlar. Savunmanın gelişmesine paralel olarak saldırı araçları evrim geçirmekte ve daha kompleks hale gelmektedir. Çalışmamızın bu bölümünde siber uzayda saldırı amaçlı kullanılan yöntemler ve bu yöntemlerin araçları genel hatları ile ele alınacaktır.

1.1. Advanced Persistent Threat[191]

Advanced Persistent Threat (APT) saldırıları, niteliği nedeniyle siber saldırı için kullanılan bir araçtan öte strateji olarak değerlendirilebilir. APT saldırılarının en ayırt edici özelliği belli bir amaç doğrultusunda yapılmasıdır. Bu amaç bir devletin hedef alınan endüstriyel sistemlerine sabotaj düzenlemek, belli bir veriye ele geçirmek veya veri üzerinde değişiklik yapmak olabilir. Bu bağlamda saldırı yapılmadan önce gerçekleştirilmek istenen amaca yönelik hedef tespiti yapıldıktan sonra, siber saldırı araçları bu hedefi ele geçirmek için kullanılır. Ele geçirilmek istenen hedef hakkında fiziki istihbarat ve/veya sosyal mühendislik yöntemleri de APT'yi oluşturmak için kullanılabilmektedir. Ele geçirilmek istenen hedef, değerinden dolayı çoğu zaman iyi korunacağı için APT'ler oldukça kompleks saldırı kapasitesine sahiptir.

Bu bağlamda APT'ler, saldırılarını yapabilmek için genellikle "Zero Day"[192] açıklarını kullanmaktadır. "Zero Day" açıklar üzerinden sisteme sızan saldırı araçları, hedeflenen amaç doğrultusunda işlevlerini yerine getirmektedir. APT'ler amacını yerine getirdikten sonra sistemden kendini kaldırabileceği gibi varlığı tespit edilmeden çok uzun süre sistemde de kalabilir. Mandiant firması, ÇHC'nin espiyonaj amaçlı gerçekleştirdiği APT'ler üzerine yaptığı araştırmada, saldırı araçlarının ortalama bir yıl fark edilmeden sistemde kaldığını tespit etmiştir.[193] APT geliştirmenin göreli zorluğu ve maliyeti, kullanacak aktörü de değiştirmektedir. Yapısı itibariyle APT'ler, crackerlardan öte devlet destekli grupların ya da ulus-devletlerin kullanacağı bir strateji haline gelmektedir. [194]

---

[191] APT hedef odaklı ve kararlı bir saldırı türüdür. APT'nin literatürde Türkçe karşılığı bulunmadığı için çalışma boyunca İngilizce olarak kullanılacaktır.

[192] Kullanılan yazılımda, geliştiriciler ya da güvenlik şirketleri tarafından varlığı tespit edilememiş açıklara "Zero Day" denmektedir. "Zero Day" açıkların, yapılan siber saldırı sonrasında ilk defa ortaya çıkması, saldırıya karşı savunma yapılmasını çok zor hale getirmektedir. "Zero Day" açıklar crackerlar tarafından keşfedilmesinin ardından kullanılabilmekte ya da bu açığa kullanmak isteyenlere satılabilmektedir. "Zero Day" açıklar ve bu açıkların ticareti hakkında ayrıntılı bilgi için bkz. Tony Bradley, "Zero Day Exploits", http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm (E.T. 05.04.2014); Graham Cluley, "Zero-day exploit in Apple's iOS operating system "sold for $500,000"", http://grahamcluley.com/2013/07/zero-day-ios-exploit/ (E.T. 05.04.2014)..

[193] "Exposing One of China's Cyber Espionage Units", Mandiant Report, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (E.T. 10.04.2014). , p. 3.

[194] Bu konuda ayrıntılı bilgi için bkz. Margaret Rouse, "Advanced Persistent Threat (APT)", http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT (E.T. 10.04.2014); "Advanced Persistent Threats: A Symantec Perspective Preparing the Right Defense for the New Threat Landscape", Symantec Report, http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (E.T. 10.04.2014); "Advanced Persistent Threats: A

1.2. Denial of Service Attack/ Distrubuted Denial of Service Attack

Siber uzayda yapılabilecek en basit ve ses getiren saldırı türlerinden biri Denial of Service Attack/ Distrubuted Denial of Service Attack (Dos/DDos) saldırılarıdır. Dos/DDos saldırıları siber uzayda gerçekleştirilen oturma eylemleri olarak kabul edilebilir. Temelde zararsız olan bu saldırılar belli bir web sayfasına ulaşılmasını engellemek amacıyla yapılmaktadır. Politik motivasyona sahip hacktivist gruplar tarafından tercih edilen bu saldırı tipi, oldukça basit bir yapıya sahiptir. İnternete belli bir bant genişliğiyle bağlı olan web sayfasına, bant genişliğinin alabileceği sayının üzerinde Internet Protocol (IP)'nin bağlanmaya çalışarak bant genişliğini doldurması, saldırının temel yöntemidir.

Bahsedilen bağlanma girişimi birden fazla şekilde olabilmektedir. Politik motivasyona sahip bir kitlenin internette örgütlenerek ortak hareket etmesiyle bu saldırı gerçekleşebileceği gibi bir kişinin Botnetler[195] aracılığıyla tek başına bu saldırıyı gerçekleştirmesi de mümkündür. Dos/DDos saldırılarına karşı, saldıran IP sayısının dolduramayacağı bir bant genişliğine çıkmak, web sayfasının geçici olarak hizmet dışı hale getirmek ya da saldırılan IP'leri bloklamak genellikle uygulanan çözümlerdir. Bant genişliği değiştirmek maliyetliyken, IP'leri bloklamak ise genellikle Botnet kullanılan saldırılarda oldukça zorlaşmaktadır. Web sayfasını geçici olarak hizmet dışı bırakmak ise saldırganların amacını yerine getirmektedir.[196]

Brief Description", https://www.damballa.com/advanced-persistent-threats-a-brief-description/ (E.T. 10.04.2014); Emre Bâkır, "5. Boyutta Savaş: Siber Savaşlar – I", 20.12.2012, https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html (E.T. 10.04.2014); "FireEye Advanced Threat Report: 2013", FireEye, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf (E.T. 10.04.2014).

[195] Uygun yazılımın kabul edilmesi ya da gizlice bilgisayara yüklenmesi sonucu ağ üzerinden komuta kontrol edilerek yönlendirilen bilgisayarlara, robot bilgisayar/köle bilgisayar ya da Botnet denmektedir. Botnet kelimesi robot ve internet kelimelerinin birleştirilmesiyle oluşturulmuştur. Botnetler özellikle DDos saldırılarında kullanılmaktadır. Bu konuda ayrıntılı bilgi için bkz. "Botnet nedir?", http://www.microsoft.com/tr-tr/security/resources/botnet-whatis.aspx (E.T. 10.04.2014); Ramneek Puri, "Bots &; Botnet: An Overview", SANS Institute InfoSec Reading Room, 08.07.2003, http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299 (E.T. 10.04.2014).

[196] Bu konuda ayrıntılı bilgi için bkz. Candan Bölükbaş, "Yeni Nesil Teknolojik Silahlar: DoS/DDoS", 22.12.2014, http://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/ (E.T. 10.01.2015); "What is a DDoS Attack?", http://www.verisigninc.com/tr_TR/website-availability/ddos-protection/what-is-a-ddos-attack/index.xhtml#infograph (E.T. 10.04.2014); Mindi McDowell, "Understanding Denial-of-Service Attacks", 06.02.2013, https://www.us-cert.gov/ncas/tips/ST04-015 (E.T. 10.04.2014) ; "Types of DDoS Attacks", http://web.archive.org/web/20100808153343/http://www.anml.iu.edu/ddos/types.html (E.T. 10.04.2014); "What is a DDoS Attack?", http://www.digitalattackmap.com/understanding-ddos/ (E.T. 10.04.2014).

1.3. Virüs, Solucan ve Trojan Horse

Virüsler, solucanlar ve Trojan Horse'lar işletim sistemlerine zarar vermek için yazılmış kodlardır. Bu zararlı yazılımlar işletim sistemi içerisinde kendilerini silinmemek için kopyalayabilir, ağa yayılmaya çalışabilir ya da gizli kalmak için önlemler alabilir. Sistemdeki açıkları kullanan zararlı yazılımlar, işlemciyi daha fazla işlem yapmaya zorlayabilir ya da geçici hafızada yer işgal ederek bilgisayarı yavaşlatabilir, bulunan verileri silebilir ya da değiştirebilir. Genellikle hedef odaklı olmayan zararlı yazılımlar, sistemlerin yönetimlerini ele geçirerek, daha büyük bir amaca hizmet etmek için Botnet haline getirebilir ya da basit bir reklam uygulamasını çalıştırmak için kullanılabilir.

Virüs, solucan ve Trojan Horse arasında bazı temel farklılıklar bulunmaktadır. Virüsler temelde bir program ya da dosyaya eklenerek bir bilgisayardan diğerine hareket eder ve konak noktalarına bulaşarak zarar verir. Genellikle tüm virüsler executable (.exe) dosya ve programlara ekli olarak bulunurlar. Executable dosya çalıştırılmadan virüs aktif hale gelmez ve zarar verme eylemi gerçekleştiremez. Virüslerin bir bilgisayardan diğerine kendi başlarına gitmesi mümkün değildir. Böyle bir yayılma için bilinçsiz kullanıcının dosyayı paylaşması ve çalıştırması gerekmektedir.[197]

Solucanlar yazılımları itibariyle virüslere benzerlik göstermektedir. Virüslerin bir alt kategorisi olarak da değerlendirilebilecek olan solucanın en önemli farkı yayılma şeklidir. Solucanlar virüslerin aksine yayılmak için herhangi bir kullanıcıya ihtiyaç duymazlar. Kendisini bir dosya içerisinde saklayabilen solucanlar, kullanıcı müdahalesine gerek duymaksızın işlevsel hale gelip kendisini yüzlerce kez kopyalayarak büyük zararlar verebilir. Bunun ötesinde kendisini adres defterinde bulunan herkese göndererek yayılmaya devam edebilir. Solucanlar, kullanıcı müdahalesine ihtiyaç duymadığı için virüslere oranla çok daha tehlikelidir.[198]

---

[197] Bu konuda ayrıntılı bilgi için bkz. "Bilgisayar virüsü nedir?", http://www.microsoft.com/tr-tr/security/pc-security/virus-whatis.aspx (E.T. 10.04.2014); Vangie Beal, "Computer Virus (virus)", http://www.webopedia.com/TERM/V/virus.html (E.T. 10.04.2014); http://home.mcafee.com/virusinfo/anti-virus-tips?ctst=1 (E.T. 10.04.2014); "Computer Virus Information", http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses (E.T. 10.04.2014).

[198] Bu konuda ayrıntılı bilgi için bkz. "What is a Computer Worm?", http://www.pctools.com/security-news/what-is-a-computer-worm/ (E.T. 10.04.2014); "How Are Email Viruses Still So Effective?: Lessons

Trojan Horse'lar ise ismini Homeros'un İlyada ve Odysseai destanlarında anlatılan Truva Savaşı'ndan almaktadır. Mitolojideki Truva Atı'na benzer şekilde Trojan Horse'lar da dış görüşünden farklı amaçlara hizmet eden yazılımlardır. Solucanlar gibi Trojan Horse'lar da virüslerin bir alt kategorisi olarak değerlendirilebilir. Trojan Horse'ların ayırıcı özelliği kullanıcıyı kendisini olumlu anlamda işe yarar ve istenen bir yazılım olarak göstermesidir. Trojan Horse'lar yüklenip çalıştırıldıktan sonra ise geniş ölçekte zarar verme işlevlerini yerine getirirler. Trojan Horse'lar kendilerini kopyalayamazlar yada yayılmak için ağları kullanamazlar.[199]

2. Siber Saldırı Örnekleri ve Diplomasiye Etkisi

Kosova Krizi sürerken 1999 yılında NATO sunucularına Sırbistan-Karadağ üzerinden yapılan ilk saldırılardan[200] günümüze kadar olan süreçte siber saldırılar, nitelik olarak çok daha etkili ve nicelik olarak çok daha sık ve fazla yapılır hale gelmiştir. CISCO'nun 2014 yılı başında yayınladığı güvenlik raporuna göre 2013 yılında siber saldırılar 2012 yılında yapılan siber saldırılara kıyasla %14'lük bir artış göstermiştir.[201] 1999 yılında NATO'ya Sırbistan-Karadağ menşeli yapılan DDoS saldırı ve mail bombardımanı[202] birkaç yüz bin maille başarılı olmuştur. Alınan tüm önlemlere karşın Botnetlerinde desteğiyle günümüzde bu tipte saldırılar çok daha güçlü bir şekilde tekrarlanabilmektedir.

Nicelik olarak ortaya konan artıştan daha önemli olan asıl husus ise siber saldırıların niteliğinde yaşanan değişimdir. 1999 yılında NATO sunucularına yapılan

---

We Can Learn from the "Here you have" Worm", 16.09.2010, http://www.pctools.com/security-news/email-viruses-here-you-have-worm/ (E.T. 10.04.2014); Mike Barwise, "What is an Internet Worm?", 09.09.2010, http://www.bbc.co.uk/webwise/guides/internet-worms (E.T. 10.04.2014); Bradley Mitchell, "Worm - Computer Worm", http://compnetworking.about.com/cs/worldwideweb/g/bldef_worm.htm (E.T. 10.04.2014); "Worm", http://www.sans.org/security-resources/glossary-of-terms/?pass=w (E.T. 10.04.2014).

[199] Bu konuda ayrıntılı bilgi için bkz. "Trojan Horse", http://www.sans.org/security-resources/glossary-of-terms/?pass=t (E.T. 10.04.2014) ; Vangie Beal, "The Difference Between a Computer Virus, Worm and Trojan Horse", 12.03.2014, http://www.webopedia.com/DidYouKnow/Internet/virus.asp (E.T. 10.04.2014) ; Margaret Rouse, "Trojan Horse", July 2006, http://searchsecurity.techtarget.com/definition/Trojan-horse (E.T. 10.04.2014) ; "What is a Trojan Virus?", http://usa.kaspersky.com/internet-security-center/threats/trojans#.VJlxI_8NQCM (E.T. 10.04.2014) ; "What is a Trojan Virus?", http://www.pctools.com/security-news/what-is-a-trojan-virus/ (E.T. 10.04.2014).

[200] Bu konuda ayrıntılı bilgi için bkz. Chris Nuttall, "Sci/TechKosovo Info Warfare Spreads", 01.04.1999, http://news.bbc.co.uk/2/hi/science/nature/308788.stm (E.T. 10.04.2014).

[201] "Cisco, 2014 Annual Security Report", Cisco, p. 21. "https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf (E.T. 10.04.2014).

[202] Denning, op. cit., pp. 6-7.

DDoS saldırısı ve mail bombardımanı günümüzde yapılan saldırılarla karşılaştırıldığında oldukça basit kalmaktadır. 2010 yılında İran nükleer tesislerine saldıran STUXNET isimli solucan, APT saldırılarına verilebilecek en etkili örnektir. STUXNET saldırısında ilk defa dört adet "Zero Day" açık bir arada kullanılmıştır.[203] Hedefli yapısı ve kullandığı açıklar sayesinde bu zararlı yazılım, dünyada çok hızlı bir şekilde yayılmasına rağmen sadece İran'ın Siemens SCADA sistemleri kullanan nükleer tesislerine zarar vermiştir. Saldırının kompleks yapısı bununla da sınırlı kalmamaktadır. Zararlı yazılım, uranyumun zenginleştirilmesini sağlayan santrifüjlere fiziki hasar verirken, bahse konu olan santrifüjleri kontrol eden ekranlara da sahte veriler yansıtarak, saldırının tespit edilmesini dolayısıyla müdahale edilerek hasarın azaltılmasını da zorlaştırmıştır.[204]

Kosova Krizi'nden günümüze nitelik ve nicelik yönünden gelişim gösteren siber saldırılar hiç şüphesiz devletlerin diplomatik ilişkilerini de etkilemektedir. İran nükleer tesislerine zarar veren STUXNET'in, NSA sızıntısının sorumlusu Edward Snowden tarafından İsrail ve ABD'nin ortak üretimi olduğunun açıklanması[205] ve P 5+1 ülkelerinin İran'la nükleer müzakereleri esnasında bu yazılımın aktif hale gelmesi, bu duruma örnek olarak gösterilebilir. Siber saldırıların doğası gereği sağladığı anonimlik, Snowden sızıntısı gibi içerden bilgi akışı gelmediği sürece devletlerin diplomatik baskılarını devam ettirirken, fiziki olarak çatışma durumuna geçilmeksizin ellerini güçlendirmektedir. Bu durum siber saldırıya uğrayan devlet tarafından uluslararası topluma lanse edilmesine rağmen saldırının menşei devlet, yapılan eylemin devlet ülkesi içindeki alt gruplardan geldiğini ya da saldırının kendi ülke sunucuları üzerinden olsa dahi üçüncü devletler/kişiler tarafından yapıldığını iddia edebilmektedir. 2007 yılında Estonya'ya yapılan siber

[203]Bu konuda ayrıntılı bilgi için bkz. Liam O. Murchu, "Stuxnet Using Three Additional Zero-Day Vulnerabilities", 14.09.2010, http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities (E.T. 10.04.2014).

[204] Bu konuda ayrıntılı bilgi için bkz. Nicolas Falliere, "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems", 06.08.2010, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (E.T. 10.04.2014); Robert McMillan, "Siemens: Stuxnet Worm Hit Industrial Systems", 14.09.2010, http://www.computerworld.com/article/2515570/network-security/siemens--stuxnet-worm-hit-industrial-systems.html (E.T. 10.04.2014).

[205] Thomas Peter, "Snowden Confirms NSA Created Stuxnet with Israeli Aid", 11.07.2013, http://rt.com/news/snowden-nsa-interview-surveillance-831/ (E.T. 10.04.2014); Chenda Ngak, "NSA Leaker Snowden Claimed U.S. and Israel Co-wrote Stuxnet Virus",09.07.2013, http://www.cbsnews.com/news/nsa-leaker-snowden-claimed-us-and-israel-co-wrote-stuxnet-virus/ (E.T. 10.04.2014).

saldırının failinin Estonya hükümet yetkilileri tarafından RF olarak gösterilmesinin ardından, RF'nin açıklamaları bu duruma örnek olarak verilebilir.[206]

Yukarıda genel ve soyut olarak analiz ettiğimiz hususların daha iyi anlaşılabilmesi için çalışmamızın bu kısmında, NATO sunuculara 1999 yılında yapılan siber saldırıdan günümüze değin süregelen siber saldırılar ve bu saldırıların diplomasiye etkisi ele alınacak olup, tarafımızca kırılma noktası oluşturduğu düşünülen bazı saldırılar kronolojik olarak incelenecektir.

2.1. 1999 Kosova Krizi ve NATO Sunucularına Yapılan Saldırılar

1998 yılında Yugoslavya Federal Cumhuriyeti[207] içerisinde başlayan iç savaş sürecinde NATO'nun, Slobadan Miloseviç önderliğindeki Sırp kuvvetlerinin saldırılarına karşı Kosova'yı korumak için 1999 yılında yaptığı operasyon devam ederken, NATO ve NATO'yu oluşturan müttefik kuvvetler ilk defa Sırbistan-Karadağ menşeli siber saldırılara hedef olmuştur. Yapılan bu saldırı ilk ideolojik temelli siber karşı saldırı olarak adlandırılabilir. Saldırının menşei doğrudan Sırbistan-Karadağ yönetimi olmasa da ülke içerisindeki aşırı Sırp milliyetçisi gruplar tarafından yapıldığı daha sonraki süreçte NATO tarafından açıklanmıştır.[208] Zira saldırının yapısı günümüzde yapılan saldırılar karşısında çok basit görünse de 1999 yılında NATO sunucularına gelen birkaç bin mail ve kısıtlı

[206] Bu konuda ayrıntılı bilgi için bkz. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia", 17.05.2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia (E.T. 10.04.2014); "Estonia Hit by 'Moscow Cyber War", 17.05.2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm (E.T. 05.04.2014); Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic", 19.05.2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html (E.T. 10.04.2014).

[207] 1992 yılında Yugoslavya Sosyalist Federal Cumhuriyeti'nin dağılmasının ardından Sırbistan ve Karadağ bölgeleri Yugoslav Federal Cumhuriyeti olarak bağımsızlıklarını ilan ettiler. BM'ye başarısız üyelik girişiminin ardından Sırbistan-Karadağ olarak devletin ismi değiştirilmiştir. Çalışmamızda Yugoslav Federal Cumhuriyeti, Sırbistan-Karadağ olarak kullanılacaktır. Bu konuda ayrıntılı bilgi için bkz. "What is the Former Yugoslavia ?", http://www.icty.org/sid/321 (E.T. 10.04.2014); Barış Özdal, *Avrupa Birliği Siyasi Bir Cüce, Askeri Bir Solucan mı? Ortak Dış Politika ve Güvenlik Politikası ile Ortak Güvenlik ve Savunma Politikası Oluşturma Süreçlerinin Tarihsel Gelişimi*, 1. B., Dora Yayınları, Bursa, 2013. ss. 202-244.

[208] Dan Verton, "Serbs Launch Cyberattack on NATO", 04.04.1999, http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx (E.T. 10.04.2014).

sayıda bilgisayarın yaptığı DDoS atağı, NATO ve müttefiklerinin web sitelerine erişimini geçici olarak engellemeyi başarmıştır.[209]

Kosova Krizi'nde yapılan siber saldırılar karşısında NATO'nun tutumu, siber uzayın geleceğine ilişkin oldukça önemli yaklaşımların oluşturulmasını sağlamıştır. Web sitelerinin ve kurum içi iletişiminin siber saldırılar sonucunda büyük ölçüde işlevsiz hale gelmesine rağmen NATO, söz konusu ülkenin internet çıkışlarını bombalamamıştır. Bu süreçte NATO, Sırbistan Karadağ'ı bir siber laboratuar olarak görmüş ve propanga/karşı propagandasını internet ve diğer medya kanalları üzerinden yapmaya çalışmıştır. Dorothy Denning, bu süreçte NATO'nun siber uzayı kullanarak Sırbistan-Karadağ yönetimine karşı yürüttüğü propagandanın başarısız olduğunu belirtmiştir. Buna rağmen Sırbistan Karadağ yönetimin NATO'ya karşı yürüttüğü propagandaya karşılık NATO'nun yaptığı karşı propagandanın başarılı olduğu tespitinde de bulunmuştur. Bu süreci Denning internetteki ilk savaş olarak isimlendirmiştir.[210]

2.2. 2007 Estonya Saldırısı

2007 yılında Estonya'ya yapılan saldırılar, siber uzayda örgütlü hareket eden ve bir ideoloji etrafında birleşmiş grupların, bir devlet ülkesine siber uzaydan verdikleri en büyük zarar olduğu için önemli bir kırılma noktasıdır. Estonya'ya yapılan siber saldırının ardında 1999 yılında NATO'ya yapılan saldırılara benzer şekilde ideolojik nedenler bulunmaktadır. Zira Estonya'ya yapılan saldırının görünür nedeni SSCB'nin 2. Dünya Savaşı kayıplarını anmak için günümüz Estonya'sının başkenti olan Tallinn'deki bronz asker anıtının yerinin değiştirilmesi olsa da gerçek neden Rus milliyetçiliğidir.

Daha ayrıntılı bir biçimde incelersek Anıtın şehrin dışındaki bir mezarlığa kaldırılmasına RF Başkanı Vladimir Putin oldukça sert tepki göstermiştir ve savaş anıtının yerinin değiştirilmesinin insanlar ve devletler arasında güvensizliğe yol açacağını belirtmiştir.[211] Nisan ayında anıtın yerinin değiştirilmesinin ardından Estonya içindeki Rus

[209] Jason Healey, "Cyber Attacks Against NATO, Then and Now", 06.09.2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now (E.T. 07.04.2014).
[210] Denning, op. cit., pp. 1,9.
[211] Putin'in Estonya hükümetinin tutumu hakkındaki söylemleri için bkz. Andrew E. Kramer, "Putin is Said to Compare U.S. Policies to Third Reich", 10.05.2007, http://www.nytimes.com/2007/05/10/world/europe/10russia.html?_r=0 (E.T. 07.04.2014); Lynn Berry,

azınlığın ve RF yanlılarının fiziki protestosuna paralel olarak siber saldırılar başlamıştır. Saldırı tek bir web sitesini hedeflemekten öte Estonya devlet ülkesi içerisindeki hükümetin kontrolünde olduğunu düşünülen, devleti temsil eden ya da hayatın genel akışını sağlayan tüm web sitelerini hedef almıştır. Estonya'ya yapılan saldırılar kompleks olmaktan çok basit ve kararlı bir tutum izlemiştir. DDoS ataklarının haftalarca sürmesi ve yoğunluğu, Estonya saldırısını daha öncekilerden ayırmıştır.[212] Yapılan saldırılarda Botnetlerin yardımıyla bir milyondan fazla bilgisayarın kullanıldığı düşünülmektedir. Estonya hükümetinin RF merkezli IP'leri engellemesine rağmen dünyanın farklı noktalarından Estonya'ya saldıran Botnetlerden dolayı genel saldırı engellenememiştir.[213] Defense Advanced Research Project Agency (DARPA) başmühendislerinden Prof. James Handler, Estonya'da yaşananları askeri saldırıdan daha çok, siber başkaldırı olarak nitelendirmektedir.[214] Estonya hükümet yetkilileri saldırıların arkasında RF'nin olduğunu belirtse de yapılan çalışmalar bu devletin saldırılara doğrudan destek vermediğini, sadece saldıranların nefretini körükleyici söylemlerde bulunduğunu göstermektedir.[215]

Genel olarak bakıldığında yaklaşık bir ay boyunca Estonya'da insanların hayatı siber saldırıdan etkilense de hiçbir kritik altyapı ya da ağ merkezli yönetim sistemi fiziki hasar görmemiştir. Estonya'da yapılan saldırının oluşturduğu zarar, devlete ait sistemlerin kullanılamaması ve finans sisteminin devre dışı kalmasından kaynaklanan faaliyet zararıdır. Şüphesiz saldırının siber saldırılar içerisinde kırılma noktası oluşturmasının farklı sebepleri bulunmaktadır. Her şeyden önce Estonya'ya yapılan siber saldırı, teknik olarak yeni bir yöntem ortaya koymamasına rağmen, kararlı ve yoğun yapılan saldırıların en basit yöntemle dahi olsa ağlanmış devletlere/toplumlara verebileceği zararı ortaya çıkarmıştır. Bu anlamda saldırının doğurduğu etkinin altında yatan asıl neden, saldırının yapıldığı Estonya devletinin ve toplumunun siber uzaydaki varlığı ile ekonomik açıdan oldukça

---

"Behind Putin's Estonia Complex", 25.05.2007, http://www.themoscowtimes.com/sitemap/paid/2007/5/article/behind-putins-estonia-complex/196806.html (E.T. 07.04.2014).

[212] Estonya saldırısı hakkında teknik bilgi için bkz. Beatrix Toth, "Estonia Under Cyber Attack", http://www.cert.hu/sites/default/files/Estonia_attack2.pdf (E.T. 07.04.2014).

[213] Kertu Ruus, "Cyber War I: Estonia Attacked from Russia", *European Affairs*, http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia (E.T. 07.04.2014).

[214] Shaun Waterman, "Analysis: Who cyber smacked Estonia?", 11.06.2007, http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/ (E.T. 07.04.2014).

[215] Jacob Silverman, "Could hackers devastate the U.S. economy?", http://computer.howstuffworks.com/die-hard-hacker1.htm (E.T. 07.04.2014).

gelişmiş devletlerin siber uzaydaki ağlanmış yapılarının taşıdığı benzerliktir. Finans, iletişim, ulaşım vb. kritik altyapıların kullanımındaki bu benzerlik daha önce yaşanan siber saldırılardan farklı olarak NATO müttefiklerinin ilgisini çekmiştir. Estonya hükümetinin talebiyle bu ülkeye NATO desteği sağlanmış ve ilerleyen süreçte Tallinn'de NATO Siber Savunma Mükemmeliyet Merkezi (CCD COE – Cooperative Cyber Defense Centre of Excellence)[216] kurulmuştur. Bu merkezin, alandaki uzman akademisyenlerin katkısıyla çıkardığı *"The Tallinn Manual on the International Law Applicable to Cyber Warfare"* adlı eser uluslararası hukukta siber savaşın yerini ve NATO müttefiklerinin uygulayabileceği yaklaşımları ortaya koymaktadır. Merkezin yaptığı diğer yayınlar[217] da incelendiğinde Estonya saldırısının kırılma noktası oluşturmasının nedeni daha açık bir şekilde görülmektedir. Asıl neden Estonya'ya verilen zararda değil, ilerde aynı teknik kullanılarak diğer gelişmiş devletlere verilebilecek muhtemel zararı ortaya çıkmış olmasındadır.

2.3. 2008 Gürcistan Saldırısı

8.8.2008 savaşı olarak da bilinen RF – Gürcistan Savaşı öncesinde ve sonrasında yaşanan gelişmeler, bölgesel olarak doğurduğu sonuçlardan daha fazlasına siber uzayda neden olmuştur. Çünkü Güney Osetya üzerindeki anlaşmazlık sonrasında 8 Ağustos'ta konvansiyonel anlamda savaş başlasa da bu anlaşmazlıkla ilgili olarak ilk çatışmalar siber uzayda, konvansiyonel olan çatışmadan önce başlamıştır.

Diğer bir ifade ile belirtirsek, sıcak çatışmanın başlamasından haftalar önce 20 Temmuz'da Gürcistan hükümetine ait web sayfaları, devlet başkanı Mikheil Saakasvili'nin resmi web sayfası, dışişleri bakanlığının web sayfası, haber kuruluşları ve bankacılık sistemine siber saldırılar yapılmıştır. Saakasvili'nin diktatör olduğu göstermek amacıyla internet sayfasına Adolf Hitler ile kıyaslandığı fotoğraflar konulmuştur. 5 Ağustos'ta ise Güney Osetya'ya ait bir web sitesinin ele geçirilmesi ve sonrasında bu siteye Gürcistan Hükümeti yanlısı haberler konulmasının ardından Güney Osetya yetkilileri, bölgede

[216] "About Cyber Defence Centre", https://ccdcoe.org/about-us.html, (E.T. 07.04.2014) ; "Yeni Güvenlik Sorunlarıyla Başa Çıkmak", NATO, p.9, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_new-security-challenges-tu.pdf (E.T. 07.04.2014).
[217] https://ccdcoe.org/publication-library.html (E.T. 07.04.2014).

yaşanan olayların Gürcistan Hükümeti tarafından bu şekilde gizlenmeye çalışıldığını iddia etmişlerdir.[218]

Gürcistan menşeli web sayfalarına düzenlenen saldırıları inceleyen uzmanlar, yapılan saldırıların oldukça eğitimli ve merkezi kontrollü gruplar tarafından gerçekleştirildiğini iddia etmişlerdir. Bu süreçte yalnızca Gürcistan siteleri değil Gürcistan yanlısı yayın yapan RF menşeli sitelerde saldırıya uğramıştır.[219] Gürcistan Hükümeti her ne kadar saldırıların arkasında RF'nin olduğunun iddia etse de RF bu iddiaları reddetmiştir. RF yetkilileri saldırıyı devletin yapmadığını iddia etmekle beraber, ülke içerisindeki aşırı milliyetçi yerel gruplardan gelebileceği varsayımını reddetmemiştir. Washington'daki RF Elçiliği Sözcüsü, Gürcistan'a yapılan saldırıların RF içindeki yapılardan gelip gelmediği sorusu üzerine "*bir konuda aynı fikirde olmayan insanlar var ve onlar fikirlerini ifade etmeye çalışıyorlar*" açıklamasında bulunmuştur.[220] Açıklamanın uluslararası siber suç örgütü *Russian Business Network'ün* saldırıyı üstlenmesi hatta RF içerisinde saldırının temelini oluşturan DDoS ataklarına destek vermek isteyenlere teknik yardım sunmasından sonra gelmesi RF sözcüsünü meşrulaştırmaktadır.[221] Gürcistan ise bu süreçte, Polonya'dan ve bir sene önce siber saldırıya uğrayan Estonya'dan yardım almıştır.[222]

Gürcistan'ın, saldırının kaynağını bulma konusundaki çabası ise siber uzayın doğası gereği sağladığı anonimliğin ilk defa kısıtlı da olsa ortadan kalmasına neden olmuştur. Daha net bir biçimde ifade edersek, RF – Gürcistan Savaşı'nın ardından Gürcistan siber saldırı almaya devam etmiştir. Estonya'da yapılan saldırılardan farklı olarak veri çalınmasına yönelik yapılan daha teknik saldırılar, saldırının kaynağı tespit konusunda Gürcistan'a fırsat tanımıştır. Gürcistan Computer Emergency Response Team

---

[218] "S.Ossetian News Sites Hacked", 05.08.2008, http://www.civil.ge/eng/article.php?id=18896 (E.T. 07.04.2014).

[219] Bu konuda ayrıntılı bilgi için bkz. Travis Wentworth, "How Russia May Have Attacked Georgia's Internet", 23.08.2008, http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111 (E.T. 07.04.2014).

[220] John Markoff, "Before the Gunfire, Cyberattacks", 12.08.2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?em&_r=0 (E.T. 07.04.2014).

[221] "Georgia Cyber Warfare", 09.08.2008, http://rbnexploit.blogspot.com.tr/2008/08/rbn-georgia-cyberwarfare.html (E.T. 07.04.2014).

[222] Noah Shachtman, "Estonia, Google Help 'Cyberlocked' Georgia", 08.11.2008, http://www.wired.com/2008/08/civilge-the-geo/ (E.T. 07.04.2014); Dancho Danchev, "Coordinated Russia vs Georgia Cyber Attack in Progress", 11.08.2008, http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 (E.T. 07.04.2014) ; Jeremy Kirk, "Estonia, Poland Help Georgia Fight Cyber Attacks", 12.08.2008, http://www.pcworld.com/article/149700/cyberattacks.html (E.T. 07.04.2014).

(CERT)'ü saldırganları siber uzayda benzer bir teknik karşı koyuşla ortaya çıkarmıştır. Veri çalma girişiminde bulunulduğunun anlaşılması üzerine "*Georgian-NATO Agreement.zip*" isimli sahte bir dosya ile oluşturdukları *honeypot'un*[223] saldırganlar tarafından çalınması izin verilmiştir. Dosyanın Gürcistan sunucularından çalınmasının ardından dosyanın barındırdığı yazılım, saldırganlar dosyanın asıl amacını fark etmeden aktif hale getirilmiştir. Yazılım ile saldırganın bilgisayarında *back door*[224] oluşturulmuş ve saldırganın bilgisayarının kamerası aktif hale getirilerek fotoğrafı çekilmiştir. Gürcistan CERT'ünün bu karşı saldırısı, fotoğraflarla beraber saldırganların IP'lerinin ve IP'leriyle beraber fiziki adreslerinin, kendi aralarında kurdukları iletişimin ve kaynaklarının kısıtlı da olsa ortaya çıkmasını sağlamıştır.[225] Gürcistan'ın ortaya çıkardığı deliller, saldırının arkasında RF'nin olduğunu doğrular niteliktedir.[226]

Sonuç olarak, Estonya'ya yapılan saldırı ile kıyaslandığında Gürcistan'a yapılan siber saldırıdan (ülkenin çok daha düşük oranda ağlanmış olması nedeniyle) toplum daha az etkilenmiştir. Gürcistan'a yapılan siber saldırının kırılma noktası oluşturmasının en önemli sebebi ise konvansiyonel savaşla içiçe geçmiş olmasıdır. Çünkü ilk defa siber saldırıya paralel olarak fiziki saldırı gerçekleşmiştir. Bu bağlamda Gürcistan saldırısında siber uzay ilk defa askeri stratejinin parçası haline gelmiştir.[227]

---

[223] Türkçede henüz teknik anlamda karşılığı bulunmayan *honeypot* kavramı, veri çalma yada benzeri saldırıda bulunulması durumunda savunma yada karşı saldırı için hazırlanan teknik tuzaklardır. Honeypot'a yerleştirilen dosya ile karşı tarafa virüs bulaştırabileceği gibi saldırıyı değerli sunuculardan uzak tutmak içinde kullanılabilir. Honeypot hakkında detaylı teknik bilgi için bkz. Loras R. Even, "Intrusion Detection FAQ: What is a Honeypot?", 12.07.2000, http://www.sans.org/security-resources/idfaq/honeypot3.php; (E.T. 07.04.2014).

[224] *Back Door* ağa bağlanmış cihaza yetkisiz/izinsiz girişi ve bu sayede cihaz üzerinden veri çalınmasını, cihazda yapılan işlemlerin izlenmesini sağlayan yöntemdir.

[225] Gürcistan CERT'ünün veri çalma girişimi ve sonuçları hakkında hazırladığı ayrıntılı rapor için bkz. "Cyber Espionage Against Georgian Government", Ministry of Justice of Georgia, http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf (E.T. 07.04.2014).

[226] Bu konu hakkında yayınlanan haberler için bkz. John Leyden, "To Russia with Love? Georgia Snaps 'cyber-spy' With His Own Cam", 31.10.2012, http://www.theregister.co.uk/2012/10/31/georgia_russia_counter_intelligence/ (E.T. 07.04.2014); Steve Elwart, "Russian Hackers Beaten at Their Own Game", 11.12.2012, http://www.wnd.com/2012/11/russian-hackers-beaten-at-their-own-game/ (E.T. 07.04.2014); Jeremy Kirk, "Irked by Cyberspying, Georgia Outs Russia-Based Hacker -- With Photos", 30.10.2012, http://www.networkworld.com/news/2012/103012-irked-by-cyberspying-georgia-outs-263790.html (E.T. 07.04.2014).

[227] Markoff, op. cit., passim.

2.4. STUXNET Saldırısı

2010 yılında açığa çıkarılan STUXNET Saldırısı, yıllarca kurgu olarak kalan varsayımları gerçeğe dönüştürerek, siber uzayda önemli bir kırılma oluşturmuştur. Haziran 2010'da Beyaz Rusya menşeli VirusBlokAda firması tarafından ilk defa tespit edilen STUXNET, yazılımının karmaşıklığından dolayı uzun süre çözülememiştir.[228] 500kb'lık bu solucan günümüze değin yapılan siber saldırılar arasında ilk defa dört adet "Zero Day" açık kullanan zararlı yazılımdır. Kullandığı açıkların bir araya geldiğinde gösterdiği hedef, saldırının APT olduğunu ortaya koymaktadır. Bu açıkların ilki olan MS10-046, solucanın sadece ağ üzerinden değil aynı zamanda taşınabilir diskler üzerinden de yayılmasını sağlamaktadır.[229] İkinci açık olan MS10-061 sayesinde ise solucan bir bilgisayardan diğer bir bilgisayara geçiş yapabilmektedir. Bu açık bilgisayarlara uzaktan yetkili olarak erişim imkânı sağlamaktadır.[230] Bu iki açığın dışındaki diğer iki açıksa hak yükseltme açıklarıdır. Bu açıklarla solucan, bulaştığı bilgisayar üzerinde tam kontrol elde edebilmektedir.[231]

STUXNET kullandığı tüm bu açıklara karşın bulaştığı bütün bilgisayarlara zarar vermemiştir. Hedefli yapısı, yazılımın sadece Siemens STEP7 SCADA sistemi kullanan bilgisayarlarda zararlı hale gelmesini sağlamıştır.[232] Sanayi tesislerinin kontrolü için kullanılan bu sistemlere saldırıyla hedeflenen, saldırılan sistemin fiziki olarak devre dışı bırakılmasıdır. Bu amaçla yazılım sadece fiziki hasar verecek komutlar vermekle kalmamış, aynı zamanda hasarın kısa sürede tespit edilmesini engellemek için kontrol ekranlarına sahte veriler yansıtmıştır.[233] Kullanılan zararlı yazılımın aktif hale gelmesi için gerekli tüm isterler sadece İran nükleer tesislerinde bulunduğu için STUXNET yalnızca bu

---

[228] Gregg Keizer, "Is Stuxnet The 'Best' Malware Ever?", *Computer World*, 16.09.2010, http://www.computerworld.com/article/2515757/malware-vulnerabilities/is-stuxnet-the--best--malware-ever-.html (E.T. 07.04.2014).

[229] MS10-046 hakkında ayrıntılı bilgi için bkz. "Microsoft Güvenlik Bülteni MS10-046", 02.08.2010, http://technet.microsoft.com/en-us/security/bulletin/ms10-046 (E.T. 07.04.2014).

[230] MS10-061 hakkında ayrıntılı bilgi için bkz. "Microsoft Güvenlik Bülteni MS10-061", 14.09.2010, http://technet.microsoft.com/en-us/security/bulletin/MS10-061 (E.T. 07.04.2014).

[231] Ryan Naraine, "Stuxnet Attackers Used 4 Windows Zero-Day Exploits" *ZDNET*, 14.09.2010, http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347 (E.T. 07.04.2014).

[232] Symantic'in STUXNET hakkında hazırladığı teknik rapor için bkz. Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier", *Symantec White Paper*, February 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (E.T. 07.04.2014).

[233] David Kushner, "The Real Story of Stuxnet", *IEEE Spectrum*, 26.02.2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (E.T. 07.04.2014).

ülkedeki tesislere fiziki hasar vermiştir. STUXNET Saldırısı ile İran'ın sadece Natanz tesisinde 1000 santrifüjün devre dışı kaldığı düşünülmektedir.[234]

ABD'nin İran'ı nükleer silah üretmekle suçladığı ve yaptırımlar uyguladığı bir zamanda yapılan STUXNET Saldırısı ile verilecek zararın, bu devlete uygulanan uluslararası ambargodan dolayı çok zor telafi edileceği aşikardır. Zararlı yazılımı inceleyen RF merkezli Karspersky Laboratuvarı, STUXNET'in ulus-devlet desteği olmadan geliştirilemeyecek kadar karmaşık olduğunu belirtmiştir. Bunun da ötesinde STUXNET'in pandoranın kutusunu açtığını düşünen laboratuvar yetkilileri, bundan önce de siber suçlular varken bu saldırıyla siber savaş çağının başladığının ilan edildiğini, artık siber teröristler ve siber silahlar olduğunu iddia etmişlerdir.[235]

Karspersky şirketinin kurucu başkanı Eugene Karspersky Münih'te yaptığı konuşmasında STUXNET ve sonrasını "*bu zararlı yazılım para çalmak, spam göndermek ya da kişisel bilgi çalmak için yazılmadı. Bu yazılım tesislere sabotaj düzenlemek endüstriyel sistemlere zarar vermek için oluşturuldu. Korkarım ki bu yeni dünyanın başlangıcı, 1990lar siber vandalların, 2000ler ise siber suçluların on yılıydı. Korkuyorum ki artık siber terörizmin ve siber savaşların başladığı yeni bir çağdayız"* şeklinde ifade etmiştir.[236] NATO CCD COE'nin fonlamasıyla çıkarılan *The Tallinn Manual on the International Law Applicable to Cyber Warfare'in* yazarlarından Michael N. Schmitt ise *Washington Post*'a yaptığı açıklamada STUXNET saldırısının, BM Kurucu Antlaşması'na aykırı olarak güç kullanımı içerdiğini ve bunun uluslararası hukuka aykırı olduğunu belirtmiştir.[237]

---

[234] Instute for Science and International Security'nin STUXNET saldırısının İran'a verdiği zararın boyutuyla ilgili raporuna ulaşmak için bkz. David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment" *ISIS*, 22.12.2010, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (E.T. 07.04.2014).

[235] "Stuxnet – A New Age İn Cyber Warfare Says Eugene Kaspersky", *Info Security, 27.09.2010*, http://www.infosecurity-magazine.com/view/12757/stuxnet-a-new-age-in-cyber-warfare-says-eugene-kaspersky/ (E.T. 07.04.2014).

[236] "Kaspersky Lab Provides İts Insights On Stuxnet Worm", 24.09.2010, http://www.kaspersky.com/news?id=207576183 (E.T. 07.04.2014).

[237] Shaun Waterman, "U.S.-Israeli Cyberattack On Iran Was 'Act Of Force,' NATO Study Found", *The Washington Times*, 24.03.2013, http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all#pagebreak (E.T. 07.04.2014).

İran ise bu süreçte aldığı zarara rağmen uluslararası kamuoyuna, saldırıya başarıyla karşı koyduğuna dair açıklamalarda bulunmuştur. İranlı yetkililer saldırılardan ülkenin nükleer programının etkilenmediğini, iddialarının aksine İran'ın ilk nükleer santrali olan Bushehr Santrali'nin faaliyetlerine devam ettiğini belirmiştir.[238] Saldırının kaynağı olarak İsrail ve ABD'yi suçlayan İran, nükleer santrallerde kullandığı SCADA sisteminin üreticisi olan Almanya menşeli Siemens firmasını da STUXNET'e saldırmasını sağlayacak verileri bu iki devlete vermekle itham etmiştir.[239]

ABD yetkilileri ise bu ithamları reddetmek yerine, ilgili sorulara cevap vermemeyi tercih etmişlerdir.[240] Bu süreçte yapılan araştırmalar saldırının arkasında ABD ve İsrail'in olduğu ihtimalini güçlendirirken, 2012 Haziran'ın da *New York Times* gazetesinde David E. Sanger tarafından yayımlanan raporda, STUXNET'in ABD ve İsrail tarafından yapıldığı ve çok daha büyük bir planın parçası olduğunu iddia edilmiştir. Sanger'e göre eski ABD Başkanı George W. Bush tarafından başlatılan siber silah geliştirme çalışmaları, Barack Obama döneminde devam etmiştir. *Olympic Games* kod adı verilen proje çerçevesinde İran'ın uranyum zenginleştirmesini yavaşlatmak için ABD'nin oluşturduğu yazılımlardan biri olan STUXNET, İran tesislerine zarar vermiştir. Rapora göre ABD yazılımın işlerliğini kontrol edebilmek için İran'da ki santrifüjlerin fiziki kopyasını dahi oluşturmuş ve yazılımı burada denemiştir. İsrail ile işbirliğinin altında yatan temel neden ise bu konuda teknik destek almak ve bununda ötesinde İsrail'in projenin içerisinde tutularak, bu ülkenin tek başına İran'a önleyici saldırı yapmasını engellemektir. Süreçte her ne kadar saldırı başarılı olsa da yazılımın İran dışında hızla dünyaya ve özellikle de dünya ortalamasının üstünde Endonezya'ya yayılması beklenmemiştir. Rapora göre bunun nedeni İsrail'in STUXNET

[238] Thomas Claburn, "Iran Denies Stuxnet Worm Hurt Nuclear Plant", *Information Week*, 27.09.2010, http://www.darkreading.com/vulnerabilities-and-threats/iran-denies-stuxnet-worm-hurt-nuclear-plant/d/d-id/1092812 (E.T. 07.04.2014) ; "Iran Denies Nuclear Setback from Stuxnet Virus" *CBS News*, 23.11.2010, http://www.cbsnews.com/news/iran-denies-nuclear-setback-from-stuxnet-virus/ (E.T. 07.04.2014); "Iran Denies Stuxnet Disrupted İts Nuclear Programme", *BBC News*, 24.11.2010, http://www.bbc.co.uk/news/technology-11821011 (E.T. 07.04.2014); "Iran Denies Bushehr Hit By 'Stuxnet'", *Arab Times*, 21.04.2015, http://www.arabtimesonline.com/NewsDetails/tabid/96/smid/414/ArticleID/159995/reftab/96/Default.aspx (E.T. 07.04.2014).

[239] "Iran Accuses Siemens Over Stuxnet Cyber Attack", *The Telegraph*, 17.04.2013, http://www.telegraph.co.uk/technology/news/8457658/Iran-accuses-Siemens-over-Stuxnet-cyber-attack.html (E.T. 07.04.2014) ; Saeed Kamali Dehghan, "Iran Accuses Siemens Of Helping Launch Stuxnet Cyber-Attack", *The Guardian*, 17.04.2011, http://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack (E.T. 07.04.2014).

[240] Christopher Williams, "Stuxnet Virus: US Refuses To Deny İnvolvement", *The Telegraph*, 27.05.2011, http://www.telegraph.co.uk/technology/news/8541587/Stuxnet-virus-US-refuses-to-deny-involvement.html (E.T. 07.04.2014).

üzerinde yaptıkları değişikliktir.[241] 2013 yılında eski CIA ve NSA çalışını Edward Snowden'ın sızdırdığı belgeler Amerikan istihbarat örgütlerinin siber uzayda gerçekleştirdiği diğer faaliyetleri de ortaya çıkarmıştır. *Der Spiegel'in* Snowden ile yaptığı röportajda Sanger'in raporuna benzer şekilde Snowden STUXNET'i NSA ve İsrail'in beraber oluşturduğunu iddia etmiştir.[242]

STUXNET'in yapısı, yayılması ve sonuçları incelendiğinde, kendisinden önce gelen tüm kırılma noktalarından ayrıldığı görülmektedir. İlk defa bir devletin bir başka devlet ülkesine siber saldırı düzenlediğini kanıtlayacak argümanlar kamuoyuna Sanger ve Snowden'ın katkılarıyla sızmıştır. ABD'nin saldırıyı açık bir şekilde reddetmemesi, İran'da oluşan zararın uluslararası hukuk itibariyle tazminini gündeme getirmektedir.[243]

STUXNET'in asıl yarattığı kırılma ise kendisinden önce sadece olasılık olarak görülen durumları gerçeği dönüştürmesidir. Zira STUXNET'e kadar siber uzayda sadece bilgisayarlara ve diğer ağa bağlanan araçlara yazılımsal zarar vermek söz konusuyken, STUXNET ile ilk defa siber uzay üzerinden fiziki hasar verilmiştir. Endüstriyel kontrol sistemlerinin ele geçirilmesi ile sağlanan bu fiziki hasar, gelecekteki siber savaşlarda yaşanabilecek daha yıkıcı ihtimalleri ortaya çıkarmıştır. Bu nedenle sadece saldırıdan zarar gören İran değil, siber güvenliğini sağlamaya çalışan her devlet hızla bu alanı güvenlikleştiren ve sonucunda siber uzay üzerinde kontrolünü arttıran adımlar atmıştır. Bu adımları atan devletler arasında saldırının faili olduğu iddia edilen ABD de bulunmaktadır. Çünkü siber uzayda en çok ağlanan toplumlar ve dolayısıyla devletler, saldırıya en açık olanlardır.[244]

---

[241] David E. Sanger'in New York Times'ta yayınlanan raporu için bkz. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran" *The New York Times*, 01.07.2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (E.T. 07.04.2014).

[242] "Edward Snowden Interview: The NSA and Its Willing Helpers", *Der Spiegel*, 08.07.2013, http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html (E.T. 07.04.2014).

[243] Shahrooz Shekaraubi, "Iran's Case against Stuxnet", *International Policy Digest*, 18.03.2014, http://www.internationalpolicydigest.org/2014/03/18/irans-case-stuxnet/ (E.T. 07.04.2014).

[244] 31 Mart 2015 tarihinde Türkiye çapında yaşanan elektrik kesintisinin henüz siber saldırı sonucunda olduğuna dair resmi bir beyanat bulunmasa da siber saldırıların kritik altyapılara verebileceği zarar doğrultusunda medya tarafından tartışılmaktadır.

3. Siber Güvenlik ve Kritik Altyapılar

Saldırıya uğraması durumunda devletin güvenliğine büyük boyutta zarar verilebilecek bu yapılar, kritik altyapılar (critical infrastructure) olarak adlandırılmaktadır. Diğer bir deyişle devletten devlete farklılıklar göstermekle beraber temel olarak ulaşım, iletişim, finans, güvenlik, kamu sağlığı ve enerji sektörlerini destekleyen altyapılar, literatürde kritik altyapılar olarak ifade edilmektedir. Siber uzayda her geçen gün saldırıların nicelik ve nitelik olarak arttığı göz önünde bulundurulduğunda, kritik altyapıların siber saldırılara karşı güvenliğinin sağlanması büyük önem kazanmaktadır.

Siber uzayın kullanımının gün geçtikçe artmasıyla ağlanan (networked) toplumlar için fiziki sınırlar her geçen gün önemini kaybetmektedir. Bununla beraber ağlanan toplumlara paralel olarak devletler de temel altyapılarını ağlar üzerinden yönetmektedirler. Ağların kullanılmasıyla altyapıların yönetimi kolaylaşırken, devletlerin siber güvenliklerini sağlamaları ve kendilerine yapılan saldırıların kaynaklarını tespit etmeleri oldukça güçleşmektedir. İran'a yapılan STUXNET Saldırısı kritik altyapılara saldırmanın mümkün olduğunu ve fiziki hasar verilebileceğini kanıtlamıştır.

Çalışmamızın birinci bölümünde belirttiğimiz belli başlı ağlanmış devletler tarafından yayınlanan tüm strateji ve eylem planlarında kritik altyapıların korunmasının devletin güvenliği için oldukça önemli olduğu vurgulanmaktadır. Kritik altyapının tanımı literatürde olmakla beraber, siber uzay bağlamında genel olarak kabul edilen bir tanım bulunmamaktadır. Net bir ifade ile vurgularsak Kritik altyapının tanımı, devletlerin belirledikleri kritik altyapılara ve kritik altyapıları belirlerken korumayı hedefledikleri nesnelere göre değişiklik göstermektedir. Devletten devlete değişmekle beraber temelde vurgu ulusal güvenlik, emniyet, ulusal kamu sağlığı, kamu düzeni, insan ve ekonomi üzerinde yoğunlaşmaktadır.

ABD için kritik altyapı " *…hayati, fiziksel, sanal sistemler ve varlıklar. Öyle ki bu sistemlerin ve varlıkların kapasitesiz bırakılması veya yok edilmesi güvenlik, ulusal ekonomik güvenlik, ulusal kamu sağlığı veya emniyeti veya bütün bu sayılanların bir*

birleşimi üzerinde zayıflatıcı etkiye sahip olacaktır" şeklinde tanımlanmıştır.[245] AB ise kritik altyapıyı "*insanların hayati ve sosyal fonksiyonlarının, güvenliklerinin, sağlıklarının, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları"* şeklinde tanımlamaktadır.[246] Bir diğer ağlanmış topluma sahip devlet olan Japonya ise kritik altyapıyı "*insanların sosyal hayatları ve ekonomik aktiviteler için yeri doldurulamaz servisler sağlayan vazgeçilmez iş birimlerinden oluşmaktadır. Eğer bir altyapının fonksiyonu durdurulur, azaltılır veya erişilmez hale gelirse insanların sosyal hayatları ve ekonomik aktiviteleri alt üst olur"* şeklinde tanımlamıştır.[247] 11 Kasım 2013'te Resmi Gazete'de[248] yayınlanan tebliğde ise Türkiye "*işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran altyapılar*" şeklinde ifade etmiştir.

3.1. Ağlanmış Devletlerde Kritik Altyapıların Kapsamı ve SCADA Sistemleri

ABD, 28 üyesi olan AB, Japonya ve Türkiye gibi ağlanmış devletlerin kritik altyapı tanımlarından anlaşıldığı üzere vurgu, devletten devlete değişmektedir. Örneğin, ABD tarafından ulusal güvenlik, ulusal ekonomik güvenlik gibi devletin korunması öncelikli bir tanımlama yapılmışken Japonya ve AB örneğinde ise insan vurgusu ön plana çıkmaktadır. Genel ve soyut olarak baktığımızda kritik altyapıların tanımı ve kapsamı, tanımlayanın öncelikleri doğrultusunda şekillenmektedir.

[245] Mustafa Ünver, Cafer Canbay, Hüseyin Burhan Özkan, *Kritik Altyapıların Korunması*, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Mayıs 2010, ss. 2-4. http://www.cybersecurity.gov.tr/publications/CIP_Rapor.pdf (E.T. 06.02.2014).

[246] Commission of the European Committees, Critical Infrastructure Protection in The Fight Against Terrorism, 20.10.2014, pp. 3-4. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF (E.T. 06.02.2014).

[247]Information Security Policy Council, *Action Plan on Information Security Measures for Critical Infrastructares*, 13.12.2005, pp. 1-2. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf (E.T. 06.02.2014).

[248] "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ", *Resmi Gazete*, Sayı: 28818, 11 Kasım 2013, s.19. http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (E.T. 06.02.2014).

ABD yapılan tanım doğrultusunda; kimya, iletişim, kritik üretim altyapısı, bankacılık ve finans, tarım ve gıda, ticari tesisler, barajlar, savunma sanayisi, acil servisler, enerji sektörü, hükümet tesisleri, nükleer reaktörler maddeler ve atıklar, bilgi teknolojileri, su ve su sistemleri, ulaşım sistemleri, sağlık hizmetleri ve kamu sağlığı, ulusal anıtlar ve simgeleri kritik altyapı kapsamına almıştır.[249] AB Komisyonu tarafından 2005 yılında yayınlanan öneri mahiyetindeki Green Paper'da[250] ise AB'nin kritik altyapı kapsamına enerji, kamu düzeni ve güvenliği, sivil yönetimler, bilgi ve iletişim, gıda, su, uzay araştırmaları, ulaşım, finans, sağlık ve KRBN (kimyasal, radyoaktif, biyolojik, nükleer) endüstrilerinin dâhil edilmesi tavsiye edilmiştir.[251] Buna karşın AB Resmi Gazetesi'nde 2008 yılında yapılan resmi tanımda enerji başlığı altında elektrik, petrol ve gaz; ulaşım başlığı altında da karayolu, demiryolu, havayolu, su yolu, okyanus ve deniz taşımacılığı sektörleri kritik altyapı olarak ilan edilmiştir.[252] Japonya ise 2005 ve 2009 yıllarında yayınladığı stratejik plan uyarınca telekomünikasyon, finans, sivil havacılık, demiryolları, elektrik, gaz, kamu servisleri, sağlık hizmetleri, su ve lojistik sektörlerini kritik altyapı kapsamına almıştır.[253] Türkiye ise çalışmamızın yapıldığı Temmuz 2015 itibari ile kritik altyapı tanımını deklare etmesine rağmen, tanımın kapsamını oluşturan sektörleri resmi olarak deklare etmemiştir.

Siber uzayda kritik altyapıların güvenliğinin sağlanmasında en önemli hususlardan biri Supervisory Control and Data Acquisition (SCADA) sistemlerinin korunmasıdır. SCADA, veri tabanlı merkezi kontrol ve gözetleme sistemleridir. Devletler tarafından

---

[249] "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection", U.S. Department of Homeland Security, 17. 11. 2013, https://www.dhs.gov/homeland-security-presidential-directive-7#1 (E.T. 06.02.2014); "Presidential Policy Directive -- Critical Infrastructure Security and Resilience – PPD-21", The White House, 12.02.2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (E.T. 06.02.2014).

[250] Green Paper hakkında ayrıntılı bilgi ve AB Hukuku içerisindeki yeri için bkz. Kamuran Reçber, *Avrupa Birliği Hukuku ve Temel Metinleri,* 2. Baskı, Bursa: Dora Yayınları, 2013, pp. 117-120.

[251] "Green Paper On A European Programme For Critical İnfrastructure Protection", *Commission Of The European Communities*, 17.11.2005, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576 (E.T. 06.02.2014).

[252] "Council Directive 2008/114/EC Of 8 December 2008 On The İdentification And Designation Of European Critical Infrastructures And The Assessment Of The Need To İmprove Their Protection" *Official Journal of the European*, L. 345/75, 23.12.2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. (E.T. 06.02.2014).

[253] Bu konuda ayrıntılı bilgi için bkz. "Action Plan on Information Security Measures for Critical Infrastructures", Information Security Policy Council, 13.11.2005, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf (E.T. 06.02.2014); "The First National Strategy on Information Security", Information Security Policy Council, 02.02.2006, http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf (E.T. 06.02.2014).

kritik altyapı kapsamına sokulan sektörlerin çoğu SCADA sistemleri tarafından kontrol edilmektedir. Örneğin elektrik dağıtım, raylı sistemler, su dağıtım, gaz dağıtım ve karayolları gibi sektörlerde SCADA sistemleri kullanılmaktadır.[254] Bu durum kritik altyapıları siber saldırılara açık hale getirmektedir. İran'a 2010 yılında STUXNET ile yapılan siber saldırının hedefi olan SCADA sistemleri temel olarak bilgisayar kontrollü yönetme ve yönlendirme işlemlerini yerine getirmektedir. SCADA sistemlerine siber saldırı ile fiziki zarar verilebileceğinin STUXNET Saldırısı ile kanıtlanması, SCADA sistemlerine gelecekte yapılabilecek daha gelişmiş siber saldırılar ile baraj kapaklarının açılarak şehirlerin sular altında bırakabileceği, devlet ülkesi çapındaki doğalgaz iletim sistemlerine müdahale edilebileceği ya da devlet ülkesi çapında enerji kesintilerine neden olunabileceği ihtimalini ortaya çıkarmıştır.

3.2. Kritik Altyapıların İşletilmesi

Kritik altyapıların hangi süje tarafından işletildiği, güvenliğinin sağlanması için alınması gereken önlemleri farklılaştırabilmektedir. Kritik altyapıların işletilmesi süreci ise devletten devlete değişim göstermektedir. Kritik altyapıların işletilmesi sürecine genel ve soyut olarak bakıldığında üç farklı model ortaya çıkmaktadır. Bu üç modelin isimleri şöyledir:

- Kritik altyapıların devlet kontrolünde işletildiği model,
- Kritik altyapıların devlet-özel sektör ortak işletildiği karma model,
- Kritik altyapıların özel sektör kontrolünde işletildiği model.

Sadece isim olarak belirttiğimiz bu üç model ile siyasal rejimler arasında paralellik kurmak mümkündür. Sosyalist/komünist rejimle yönetilen ülkelerde kritik altyapılar devlet kontrolü altındayken, serbest piyasa ekonomisinin uzun süredir uygulandığı kapitalist/liberal rejimlerde kritik altyapıların kontrolü büyük ölçüde özel sektör kontrolündedir. Türkiye gibi kontrollü serbest piyasa ekonomisi uygulayan ve SSCB'nin dağılmasının ardından serbest piyasa ekonomisine geçen çoğu üçüncü dünya ülkesinde ise devlet-özel sektör karma modeli uygulanmaktadır. Bu model aynı zamanda devlet kontrolünden özel sektör kontrolüne geçişi de temsil eden bir yapı ortaya koymaktadır.

[254] SCADA sistemleri hakkında ayrıntılı bilgi için bkz. "Supervisory control and data acquisition (SCADA)", Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk/advice/cyber/scada/ (E.T. 06.02.2014).

Kritik altyapıların işletilmesinin devlet-özel sektör kontrolünde olduğu karma modelde ve çoğunlukla özel sektör kontrolünde olduğu modelde siber güvenliği sağlayabilmek için bazı kritik hususlar öne çıkmaktadır. Bu hususlar genel ve soyut olarak şu şekilde tespit edilebilir.

- Devlet – özel sektör arasında sürekli bilgi paylaşımı,
- Önleyici regülasyonlar,
- Tehdit algısının oluşturulması,
- Siber tehditlere müdahale altyapısının oluşturulması,
- Toplumsal farkındalığın sağlanması.

Bu noktada ABD yukarıda genel ve soyut olarak verilen hususları sağlayabilmek için Şubat 2014'te "*Framework for Improving Critical Infrastructure Cyber Security"* adıyla çerçeve belgesini yayınlamıştır.[255] Belge kritik altyapıları işleten özel sektörün siber güvenliğini sağlamak üzerine şekillense de bunu sağlamanın çok kolay olmadığı ABD medyası tarafından bilimsel olarak tartışılmaktadır.[256] Tartışmanın asıl konusu gönüllülük temelinde işbirliği yaklaşımının, içerdiği maliyet nedeniyle özel sektör tarafından benimsenmesinin oldukça zor olmasıdır.[257] Bu noktadaki temel tartışma konularından biride özellikle 2013 yılında yayınlanan "*Executive Order*[258] *- Assignment of National Security and Emergency Preparedness Communications Functions"*[259] ve "*Executive*

[255] Çerçeve belgesi hakkında ayrıntılı bilgi için bkz. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cyber Security, Version 1.0, 12.02.2014, passim. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (E.T. 06.02.2014).

[256] ABD medyasının bu konudaki belli başlı haberleri için bkz. William Jackson, "Feds Launch Cyber Security Guidelines For US Infrastructure Providers", *Information Week, 12.02.2014,* http://www.informationweek.com/government/cybersecurity/feds-launch-cyber-security-guidelines-for-us-infrastructure-providers/d/d-id/1113816 (E.T. 06.02.2014); Amitai Etzioni, "Private Sector Neglects Cyber Security", *The National Interest,* 29.11.2011, http://nationalinterest.org/commentary/private-sector-neglects-cyber-security-6196 (E.T. 06.02.2014); Grant Gross, "US Agencies Explore Cybersecurity Incentives For The Private Sector", *PC World*, 06.08.2013, http://www.pcworld.com/article/2046057/us-agencies-explore-cybersecurity-incentives-for-the-private-sector.html (E.T. 06.02.2014).

[257] ABD'nin siber güvenliğini sağlama amacıyla 2013'e kadar çıkardığı kararlar ve bu kararlarla oluşturulmaya çalışılan kamu-özel sektör işbirliği hakkında Jones Day'ın hazırladığı rapor içiz bkz. "The Cybersecurity Debate: Voluntary Versus Mandatory Cooperation Between The Private Sector And The Federal Government", *Jones Day*, July 2013, passim, http://www.jonesday.com/files/Publication/49c491ff-7f05-4932-9287-2c07a131e83d/Presentation/PublicationAttachment/216181fe-3cff-4535-9232-2c603c8bf48b/Cybersecurity%20Debate.pdf (E.T. 06.02.2014).

[258] ABD Başkanı tarafından yürütmenin kolaylaştırılması için kanun hükmünde yayımlanan emirlere Executive Order adı verilmektedir.

[259] Executive order'ın tam metni için bkz. "Executive Order -- Assignment of National Security and Emergency Preparedness Communications Functions", The White House, 06.07.2012, http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness- (E.T. 06.02.2014).

Order – Improving Critical Infrastructure Cyber Security"'nin[260] ABD Başkanı'na verdiği yetkilerdir. Bu kararlar ile ABD Başkanı'nın interneti, ulusal güvenliğin riske girdiği durumlarda tamamen kapatabileceği ve bu durumun yetkilerin tek elde toplanması olduğundan sakıncalı olacağı ABD medyası tarafından tartışılmıştır.[261]

Tehdit algısının oluşturulması ve toplumsal farkındalığın sağlanması ise büyük ölçüde karar alıcıların siber uzayın güvenlikleştirilmesi çabası altında bulundukları söylemlerle başlamıştır. Bu noktada devlet ve hükümet başkanları siber uzayın güvenliğinin kritik öneme sahip, öncelikli ve acil olduğu söyleminde bulunmuşlardır. Söylemlerin arkasından gelen eylem planlarında ise bu bilincin yayılması ve farkındalık oluşturulması için önlemler alınmıştır. Bu konudaki en net adımlar ABD tarafından atılmıştır. ABD İç Güvenlik Bakanlığı (Department of Homeland Security - DHS) ile işbirliği yapan National Cyber Security Alliance (NCSA) tarafından hayata geçirilen ve halka internetin güvenli kullanımını yaymayı amaçlayan Ulusal Siber Güvenlik Farkındalık Ayı (National Cyber Security Awareness Month – NCSAM), bu adımların başında gelmektedir.[262]

Siber tehditlere müdahale yapısının oluşturulması çerçevesinde ise siber güvenlik politikası güden devletlerin büyük çoğunluğunda ulusal Computer Emergency Response Team (CERT)'ler kurulmuştur.[263] Kurulan CERT'lerin[264] amaçları devletten devlete değişiklik gösterebilmekle birlikte görevleri genel olarak vatandaşın ve devletin bilgi güvenliğini korumak, gelen siber saldırılara karşı savunma yapmak, kurumlarda ve

[260] Executive order'ın tam metni için bkz. "Executive Order -- Improving Critical Infrastructure Cybersecurity", The White House, 12.02.2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (E.T. 06.02.2014).

[261] Bu konuda ayrıntılı bilgi için bkz. Marilyn Day, "Obama Signs Executive Order To Allow Shut Down Of All US Communications", *Examiner*, 08.07.2013, http://www.examiner.com/article/obama-signs-executive-order-to-allow-shut-down-of-all-us-communications (E.T. 06.02.2014); Daniel Tencer, "Obama May Get Power To Shut Down Internet Without Court Oversight", *Rawstory*, 24.01.2011, http://www.rawstory.com/rs/2011/01/24/power-shut-internet-court-oversight/ (E.T. 06.02.2014); "Can The President Switch Off The İnternet? Critics Fear New Executive Order Hands Obama Too Much Control Over The Web", *Daily Mail*, 12.07.2012, http://www.dailymail.co.uk/news/article-2172350/Can-president-switch-internet-Critics-fear-new-executive-order-hands-Obama-control-web.html (E.T. 06.02.2014).

[262] National Cyber Security Alliance'ın National Cyber Security Awareness Month etkinliği hakkında ayrıntılı bilgi için bkz. http://www.staysafeonline.org/ncsam/ (E.T. 06.02.2014).

[263] Türkiye'de CERT işlevi gören ve Tübitak tarafından desteklenen Bilgisayar Olaylarına Müdahale Ekibi (BOME) ve 2013 yılında kurulan Siber Olaylara Müdahale Ekibi (SOME) bulunmaktadır.

[264] Bilinen ilk CERT, Carnagie Mellon University tarafından kurulmuştur ve varlığını devam ettirmektedir. Carnagie Mellon University CERT'ü hakkında ayrıntılı bilgi için tıklayınız. http://www.cert.org/index.cfm# (E.T. 31.10.2014).

toplumda siber farkındalık oluşturmak, siber tatbikatlar yapmak şeklinde özetlenebilir. CERT'lerin saldırganın kimliğini tespit etmek ve saldırmasını engellemek için önlem alma görevi varken genellikle misilleme ya da saldırı düzenlemek görevleri arasında bulunmamaktadır.[265]

4. Siber Caydırıcılık Mümkün Mü?

Daha öncede belirttiğimiz üzere devletlerin kritik altyapılarını SCADA sistemleri ile kontrol ettikleri ve ağ merkezli muharebeye geçtikleri günümüz dünyasında, yapılacak bir siber saldırı ile ciddi zararlar verebilmenin mümkün olduğu STUXNET saldırısı ile anlaşılmıştır. Bu nedenle günümüz uluslararası ilişkilerinde II. Dünya Savaşı sonunda oluşan nükleer caydırıcılığa benzer şekilde bir siber caydırıcılığın olup olamayacağı tartışma konusudur. Örneğin ABD Dışişleri Bakanı John Kerry literatürdeki tartışmalar ekseninde bu analojiyi kullanarak siber tehditleri 21. asrın nükleer silahları olarak lanse etmiştir.[266] Çalışmamızın bu başlığında Soğuk Savaş boyunca iki blok arasında dengenin sağlanması noktasında çok önemli bir yer tutan nükleer caydırıcılığın doğurduğu etkiyi, siber uzayda siber caydırıcılığın doğurup doğurmayacağı sorusuna cevap aranacaktır.

Caydırıcılık teorisinde amaç saldırının maliyetini ve sonuçlarını, beklenen yarardan daha fazla hale getirerek saldırının önünü kesmektir. Bu stratejinin yerine getirilebilmesi noktasında da iki önemli unsur vardır. Bu unsurlardan ilki sağlam bir savunma kapasitesine sahip olmaktır. Eğer bir devletin savunması, olası bir saldırıyı son derece zor hale getiriyorsa, saldırma potansiyelini barındıran devlet durmayı seçebilir. Siber uzayda, bu durumu sağlayabilmek, saldırıların büyük bir kısmı için çözüm sunmaktadır. Caydırıcılıkta ikinci önemli unsur ise misillemenin önem kazanmasıdır. Eğer saldırganlar, eylemleri

[265] Avrupa ve Asya-Pasifik bölgesinde bulunan CERT'lerin tam listesi için bkz. http://www.trusted-introducer.org/directory/country_LICSA.html (E.T. 31.10.2014); http://www.apcert.org/about/structure/members.html (E.T. 31.10.2014).

[266] "John Kerry: Cyber threats are 'modern-day nuclear weapons' ", 25 January 2013, http://www.infosecurity-magazine.com/view/30438/john-kerry-cyber-threats-are-modernday-nuclear-weapons (E.T. 31.10.2014); Gerry Smith, "John Kerry: Foreign Hackers Are '21st Century Nuclear Weapons", 24. 01. 2013, http://www.huffingtonpost.com/2013/01/24/john-kerry-hackers_n_2544534.html (E.T. 31.10.2014).

neticesinde misilleme ile yüzleşirse, bu durum diğer saldırganları saldırıdan vazgeçirebilmektedir.[267]

Siber caydırıcılığın, caydırıcılık teorisi çerçevesinde kabul edilip edilmeyeceği ve nükleer caydırıcılığa benzer şekilde etkili olup olamayacağı ise literatürde tartışma konusudur. Bu konuda Martin C. Libicki'nin "*Cyber Deterrence and Cyber War*"[268], Amir Lupovici'nin "*Cyber Warfare and Deterrence: Trends and Challanges in Research*"[269], Joseph Nye'in "*Nuclear Lessons for Cyber Security*"[270] ve "*Cyber Power*"[271], Will Goodman'ın "*Cyber Deterrence Tougher in Theory than in Practice?*"[272], Richard L. Kugler'ın "*Deterrence of Cyber Attacks*"[273] ve Patrick M. Morgan'ın "*Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*"[274] isimli çalışmaları birçok noktada birleşmektedir. Bu bağlamda literatürü oluşturan yazarların görüşlerini ayrıntılı olarak incelemek bizce doğru olacaktır.

Lupovici'ye göre caydırıcılığın başarılı olabilmesi için kapasitenin (defansif kapasite) ve tehdidin gerçekliğinin olması bunun yanında muhtemel rakibe tehdidin başarılı bir şekilde iletilebilmesi gerekmektedir.[275] Caydırıcılığa ilişkin ortaya konulan bu üç ilke ise siber uzaya uygulandığında başarısız olmaktadır.

Bu üç ilkeden ilki olan kapasitenin siber uzaydaki durumunu inceleyecek olursak, siber uzayın asimetrisi, yapılan saldırı sonrasında yüzleşilecek bedelleri etkilemektedir. Bu

---

[267] Supra, pp. 24-30.

[268] Martin C. Libicki, Cyber Deterrence and Cyber War, Rand Corparation, 2009, passim, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (E.T. 31.10.2014).

[269] Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challanges in Research, *Military and Strategic Affairs*, Volume 3, No: 3, December 2011, pp. 49-62, http://www.inss.org.il/uploadimages/Import/%28FILE%291333533336.pdf (E.T. 31.10.2014).

[270] Joseph S. Nye Jr, "Nuclear Lessons for Cyber Security", *Strategic Studies Quarterly*,Winter 2011, pp. 18-38, http://www.au.af.mil/au/ssq/2011/winter/nye.pdf (E.T. 31.10.2014).

[271] Joseph S. Nye Jr, Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, passim, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (E.T. 31.10.2014).

[272] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?", *Strategic Studies Quarterly*,Fall 2010, pp. 102-135, passim, http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf (E.T. 31.10.2014).

[273] Richard Kugler, "Deterrence of Cyber Attacks", Franklin D. Kramer (edt), Stuart H. Starr (edt), Larry Wentz (edt), *Cyber Power and National Security*, National Defence University Press, 2009, pp. 309-342, passim, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf (E.T. 31.10.2014).

[274] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm", *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*, Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council, 2010, pp. 55-76, passim, http://www.nap.edu/openbook.php?record_id=12997&page=55 (E.T. 31.10.2014).

[275] Lupovici, op. cit., p. 49.

noktada sistemdeki göreli olarak küçük devletler, konvansiyonel silahlara yapılan yatırımdan çok daha azıyla siber uzayda önemli bir saldırı kapasitesi oluşturabilmektedir. Oysa ki büyük ve gelişmiş devletler saldırı kapasitelerini geliştirmelerine rağmen, ağlanmış yapılarından dolayı defansif kapasitelerini aynı oranda geliştirememektedirler. Caydırıcılıklarını sağlamak için yapacakları siber misilleme tehdidi ise saldırıyı yapan devletin ağlanmamış olması durumunda önem içermeyecektir. Bu durum, sistemdeki küçük devletlerin alacağı riski arttırmaktayken, büyük devletlerin kapasitelerini sorgulamasına neden olmaktadır.[276]

İkinci olarak siber uzayda tehdidin gerçekliğini ele almak gerekirse, bir strateji olarak caydırıcılıkta Sanayi Devrimi sonrası ve özellikle I. Dünya Savaşı öncesi silah sanayisinde yaşanan gelişmeler kırılma noktası oluşturmuştur. Bu süre boyunca savunmacı devletin saldırgan karşısında üstünlüğü varken yaklaşık bir asır sonra siber uzayda bu üstünlük tekrar savunmacı devletten saldırgan lehine dönmektedir. Bu durum savunmacı devleti misillemeye başvurmaktan dahi vazgeçirebilmektedir. Siber misillemeyle saldırgana verilecek zarar, saldırganı caydırmaya ya da kapasitesini ortadan kaldırmaya yetmeyeceği gibi çatışmayı tırmandırma riskini de ortaya çıkaracaktır. Çatışmanın tırmanması durumunda ise saldırganın yapacağı ikincil ve üçüncül saldırılar, savunmacı devlete misillemeyle saldırgana verdiği zarardan çok daha fazlasını verebilir. Nihai aşamada, savunmacı devletin misilleme sonrası göreceği zararın daha fazla olacağı gerçeği karşısında misillemeden vazgeçme ihtimali ortaya çıkarken, saldırgan ise misillemenin göreli olarak etkisiz olacağını ya da misilleme yapılmayacağını değerlendirerek riski göze alıp, muhtemel hedeflerini gerçekleştirmek için daha saldırgan davranabilir.[277]

Son ilke olan muhtemel rakibe tehdidin başarılı bir şekilde iletilmesini inceleyecek olursak, siber uzayda caydırıcılığı sağlayabilmek için meydan okuyan aktöre tehdidin iletilmesi süreci oldukça zordur. Bu noktada iki alanın netliğe kavuşturulması gerekmektedir:[278]

1. Saldırganın tespiti,
2. Saldırganın kapasitesinin tespiti.

[276] Bu konuda ayrıntılı bilgi için bkz. Ibid., p. 52.
[277] Ibid.
[278] Bu konuda ayrıntılı bilgi için bkz. Ibid., p. 53.

Konvansiyonel ya da nükleer bir saldırıda saldırganın tespiti fiziki takip ya da istihbarat imkanları dahilinde mümkünken, siber uzayın doğası gereği saldırganın tespiti oldukça zordur. Bu noktada saldırganın tespitinde yaşanan zorluğun sebebi sadece saldırganın kendisini siber uzayda anonim tutması değildir. Zira aktörün sadece devletler değil, diğer devlet altı gruplardan bireylere uzanan geniş yelpaze içinden herhangi biri olabilmesi de aynı zamanda etkilidir. Bu doğrultuda tezimizin teorik çerçevesi içerisinde Kopenhag Okulu kapsamında bahsettiğimiz güvenlikleştirme doğrultusunda devletler, siber uzaydaki kontrol yapılarını arttırmaya çalışmaktadırlar.

Saldırganın tespitinin zorluğu ve hatta bazı durumlarda imkânsızlığı, yaşanan saldırının siber suç, siber uzayın terörizm amaçlı kullanımı ya da siber saldırı olup olmadığının tespitini de zorlaştırmaktadır. Saldırının türüne ait bu tespit problemi, verilecek karşılığın ölçülülüğünü sağlamayı da zorlaştırmaktadır. Örneğin saldırı devlet düzeyinden değil birey düzeyinden geliyor ve ekonomik maksatlı bir siber suçsa, hukuk sistemi içerisinde suçlunun cezalandırılmasıyla bu problem çözülebilecekken, aynı saldırının bir başka devletten geldiği varsayımı savaşla sonuçlanacak bir çatışma ihtimalini ortaya çıkarmaktadır. Verilecek karşılığın ölçülülüğün sağlanmasında, işlenen fiil kadar işleyenin kimliği ve saiki de önem kazanmaktadır. Siber saldırı sonrasında siber uzayın sağladığı anonimlik her ne kadar istihbarat imkânları sayesinde bir ölçüye kadar aşılacak olsa da tam olarak tespit/isnat mümkün olmayacaktır. Bu zorluk aynı zamanda saldırganın yeteneklerini/kapasitesini de tahmin etmeyi zorlaştırmaktadır. Caydırıcılık her şeyden önce saldırmaya niyetli tarafın savunmacının kapasitesini bilmesi ve misilleme tehdidinden çekinmesi üzerine kuruluyken, siber uzay bu durumu belirsiz hale getirmektedir.[279]

Mesajın iletilmesinde yaşanan bir diğer zorluk ise Soğuk Savaş'tan farklı olarak aktör sayısında yaşanan artışın meydana getirdiği yeni problemlerdir. Soğuk Savaş boyunca belirli sayıda aktörün sınırlı ve saldırı sonrasında tespit edilebilir kapasitesi, bu aktörlerin birbirlerini caydırmak için ortaya koyduğu pratikleri de belirli bir düzen içerir hale getirmiştir. Siber uzayın getirdiği imkanlarla devletin varlığı için tehdit yaratabilecek aktörlerin çoğalması, bu aktörlerin kimliğinin ve kapasitesinin tespitinde yaşanan zorluklar, Soğuk Savaş ve öncesinde uygulanagelen pratiklerin işlevsiz hale gelmesine neden olmuştur. Siber uzaydaki tehditlerin sayısında ve türünde yaşanan bu artış,

[279] Ibid.

caydırıcılık sağlamak için iletilmesi gereken mesajın kime iletileceği kadar, aktörün kimliğine göre nasıl iletileceği sorusunu da ortaya çıkarmaktadır.[280]

Bu alanda önemli çalışmalar yapan Nye "*Nuclear Lessons for Cyber Security*" isimli makalesinde 1950'li yıllardan başlayarak ABD ve SSCB'nin nükleer silah sahibi olması sonrası bu silahların defansif ve ofansif kullanımı, misilleme ve kontrol altında tutulması gibi alanlarda geliştirdikleri on yıllar alan pratikleri incelemiştir. Bu incelemenin ardından da nükleer alandan alınacak derslerin siber uzayda uygulanıp uygulanamayacağını sorgulamıştır.[281]

Siber uzayın fiziki ve sanal katmanını birbirinden ayıran Nye, diğer yazarların da belirttiği gibi siber uzayın fiziki altyapısını oluşturan parçaların (fiber kablolar, kapalı ağlar, internet altyapısı) klasik egemenlik kurallarına tabi olduğunu belirtmiştir. Bu altyapının üzerinde oluşan sanal yapının ise klasik egemenlik kuralları çerçevesinde kontrol edilmesinin zorluğuna vurgu yapmıştır.[282]

Nye'ın altını çizdiği bir diğer unsur ise siber uzayın maliyet etkinliğidir. Deniz ve hava güçleri ve bu güçlerin alan hâkimiyetlerinin maliyeti oldukça fazladır. Nye ise siber uzayın maliyet etkinliği sayesinde devlet dışı aktörlerin ve göreli olarak küçük devletlerin önemli roller oynayabileceği bir alan olduğunu belirtmektedir. Nye, "*Cyber Power*" isimli çalışmasında deniz ve hava boyutlarıyla benzer karşılaştırmayı yapmasının ardından siber uzay ile kara boyutu arasında üç benzerlik tespit etmektedir. Bu benzerlikler "aktör sayısı", "alana giriş kolaylığı" ve "gizlenme/kamuflaj imkanları"'dır. Deniz, hava ve uzay boyutlarının aksine kara boyutuna benzer şekilde siber uzayın oluşturduğu beşinci boyutta da büyük güçler mutlak bir hâkimiyet kuramayacaklardır. Çalışmamızın kritik altyapılar ve siber saldırı örnekleri kısmında vurguladığımız gibi en çok ağlanan devlet aynı zamanda saldırıya en açık olan devlettir. Bu nedenle büyük güçlerin diğer boyutlarda hâkimiyetlerini destekleyen ağlanmışlıkları, siber uzayda en büyük zaafları haline gelmektedir.[283]

[280] Ibid.
[281] Nye, "Nuclear Lessons…",op. cit., p. 19.
[282] Ibid, pp. 19-20; Nye, "Cyber Power", op. cit., p. 6.
[283] Bu konuda ayrıntılı bilgi için bkz. Nye, "Nuclear Lessons…", op. cit., pp. 19-20; Nye, "Cyber Power", op. cit., pp. 1, 3-4.

Lupovici'nin vurguladığı siber uzayda saldırının, savunma karşısındaki üstünlüğü tezine Nye da katılmaktadır. Büyük güçlerin siber uzayda savunma ve saldırı yapabilmek için geliştirdikleri tüm kapasitelerine rağmen özellikle internetin güvenlik kaygısı duymadan geliştirilen mimarisi, herhangi bir aktörün bulabileceği göreli olarak basit bir sistem açığıyla çok büyük zararlar verme potansiyelini ortaya çıkarmaktadır.[284]

Siber uzayı farklı kılan bir diğer unsur ise saldırganın ortadan kaldırılması sorunudur. Fiziki dünyada silahsızlandırma, düşmanın yok edilmesi ya da işgal edilmesiyle çözülebilecek olan bu sorun, siber uzayda tespit/isnatta yaşanan problemlerden dolayı kolayca çözülememektedir. Tespit / isnat noktasında genellemeye giden Nye, temelde siber uzay kaynaklı tehditleri beş başlıkta ele almaktadır. Sadece rahatsızlık verici yönünden dolayı hacktivizmi bir kenara koyduktan sonra siber suç ve siber terörü devlet dışı aktörlerle ilişkilendirirken, siber savaş/saldırı ve ekonomik amaçlı siber casusluğu ise devletlerle ilişkilendirmektedir. Nye'ın ekonomik amaçlı siber casusluğu devletlerarası düzeyde gerçekleşmesi muhtemel bir tehdit olarak kabul eden bu genellemesi tarafımızca kabul edilmemektedir. Çünkü çalışmamızın önceki bölümlerinde ÇHC-ABD arasındaki ekonomik temelli casusluk faaliyetlerinin varlığı belirtilmiş olsa da çok uluslu şirketlerin değerlerinin ve kontrol ettikleri meblağların üçüncü dünya ülkelerinin ekonomileriyle yarıştığı günümüzde, ekonomik amaçlı siber casusluğun devlet dışı aktörler tarafından yoğun olarak kullanılma potansiyeli içerdiği varsayımında bulunulabilir.[285]

Nye, makalesinin ilerleyen bölümlerinde, çalışmamızın temel inceleme alanları olan siber uzay ve nükleer alanı karşılaştırarak bazı temel farklılıklara vurgu yapmaktadır. Bu farklılıklar genel ve soyut olarak dört başlıkta belirtilebilir:[286]

- Siber saldırı ve nükleer saldırı arasında nitelik farkı bulunmaktadır. Siber saldırı kaynağı belirsiz ve etkisi uzun zaman sonra fark edilebilecek şekilde gerçekleşebilirken, nükleer saldırılar gayet açık, etkisi ve kaynağı belirlenebilecek şekilde olmaktadır.

[284] Bu konuda ayrıntılı bilgi için bkz. Nye, "Nuclear Lessons…", op. cit., p. 21; Nye, "Cyber Power", op. cit., p. 5.
[285] Bu konuda ayrıntılı bilgi için Bu konuda ayrıntılı bilgi için bkz. Nye, "Nuclear Lessons…", op. cit., p. 21; Nye, "Cyber Power", op. cit., p. 5.
[286] Bu konuda ayrıntılı bilgi için bkz. Nye, "Nuclear Lessons…", op. cit., pp. 22-23.

- Siber saldırılar çok büyük meblağlara mal olan ekonomik zarara neden olsa da en fazla insanlığı birkaç on yıl geriye götürebilecek kapasiteyi barındırmaktadır. Oysa nükleer silahlar insanlığı tamamen ortadan kaldırabilir.
- Siber uzay içerisinde askeri yapılar çok az yer tutarken, nükleer alan tamamen askeri kökenlidir.
- Siber uzay ekonomik nedenlerden ötürü tüm aktörlere açıkken, nükleer alan özellikle nükleer terörizm endişesinden ötürü devlet dışındaki aktörlere kapalıdır.

Yukarıda genel ve soyut olarak verilen tüm bu farklılıklara karşın Nye'a göre siber uzay ile nükleer alan arasında siber uzayın kullanımı noktasında yönlendirici benzerlikler bulunmaktadır. Bu benzerlikler dört başlıkta ele alınabilir:[287]

- *"Devam eden teknolojik değişimin stratejideki ilk teşebbüsleri zorlaştırması beklenmektedir,*
- *Yeni bir teknoloji üzerine strateji kurmak yeterli deneysel tecrübeden yoksun kılacaktır,*
- *Yeni teknolojiler sivil-askeri ayrımına yeni konular ilave edecektir,*
- *Siviller tarafından kullanım, ulusal güvenlik stratejisinin işlevselliğini zorlaştıracaktır."*

Bu benzerliklerden ilki olan devam eden teknolojik değişimin stratejideki ilk teşebbüsleri zorlaştırması beklentisine göre nükleer silahların ilk kez kullanılmasından sonra ortaya konan stratejiler, 1950'li yıllarda hidrojen bombasının ve kıtalararası balistik füzelerin icat edilmesiyle işlevsiz hale gelmiştir. Bu noktadan sonra, "sonu olan caydırıcılık yaklaşımı"'nın yerini, "varoluşsal caydırıcılık" almıştır. Yaşanan bu değişim Lupovici'nin de ortaya koyduğu üç ilkeden biri olan tehdidin gerçekliğini ön plana çıkarmıştır. Küba Füze Krizi'nde ABD'nin rakamsal üstünlüğüne rağmen birkaç SSCB bombası iki devletin birbirini karşılıklı olarak tamamen imha etme korkusunu ortaya çıkarmış ve varoluşsal caydırıcılık savaşı önlemiştir.[288]

[287] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 23-29.
[288] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 23-24.

Günümüzde siber uzayda yaşananlara da aynı analoji uygulanabilir. Nükleer silahlanmada hidrojen bombasının yarattığı kırılma, siber uzayın kullanımının son 20 senede yaşadığı artışa ve bu artışın ortaya çıkardığı problemlere benzetilebilir. Bu süre içinde yaşanan artış ve önümüzdeki süreçte bu artışın devam etmesi, siber uzayda verilecek zararların devletler açısından varoluşsal etkileri olmasına yol açacaktır. Bu nedenle geliştirilecek stratejiler teknolojide yaşanacak değişimlere uyumlu olmalıdır.[289]

Nye'ın ikinci olarak belirttiği yeni bir teknoloji üzerine strateji kurmanın yeterli deneysel tecrübeden yoksun kılacağı benzerliğine uygun bir biçimde; 8 Ağustos 1945'te Nagazaki'ye atılan nükleer bombadan sonra dünyada hiçbir güç nükleer bombayı savaşta kullanmamıştır. Elde edilen kısıtlı veriye karşın, stratejistler yeterli deneysel tecrübeden yoksun halde varsayımsal senaryolar üzerinden kaynaklarını boşa kullanmışlardır. Siber uzayda ise saldırganlar, son on yılda yapılan belli başlı saldırılardan gelen veriler neticesinde daha fazla bilgiye sahip olmuşlardır. Bu noktada siber yıkıma ilişkin elde edilen veriler, alanı nükleer deneyimden ayırmaktadır. Bu ayrıma ve eldeki tüm verilere karşın henüz bir siber savaş yaşanmamıştır. Estonya ve Gürcistan'da yaşanan DDOS saldırısı ya da İran'a STUXNET'le yapılan endüstriyel sabotaj sadece gelecekte yaşanabileceklere dair ipuçları vermektedir. Tüm bu ipuçlarına karşın yaşanacak bir siber savaşta hesap edilemeyen zararların neler olacağı ya da Lupovici'nin de vurguladığı ölçülülük ve suçlunun ayrımının savaş hukuku çerçevesinde nasıl yapılacağı bilinmemektedir.[290]

Bu benzerliklerden üçüncüsü olan yeni teknolojik buluşların sivil-askeri ayrımına yeni konular ilave etmesine göre, söz konusu bu teknolojilerin ortaya çıkmasının ardından kullanımı ve kontrolü, devletin farklı mekanizmaları tarafından farklı şekilde algılanmaktadır. Örneğin ABD'de nükleer çağın başlangıcında siyasi karar vericiler nükleer teknolojinin kullanımını ve kontrolünü, Atom Enerjisi Komitesi'ni kurarak sivillere bırakmışlardır.[291] Nükleer silahların kontrolü orduya verilse de oluşturulmaya çalışılan stratejilerle hükümet kontrolü altında tutulmaya çalışılmıştır. Bu bağlamda nükleer çağda yaşanan problemlerin benzeri, siber uzayda da yaşanmaktadır. Siber uzayda

[289] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 24-25.
[290] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 25-26.
[291] Günümüzde BM çatısı altında kurulan uluslararası atom enerjisi kurumu da imzacı devletlerde aynı işlevi yerine getirmektedir. Bu konuda ayrıntılı bilgi için bkz. "The 'Atoms for Peace' Agency", 25 November 2014, http://www.iaea.org/About/about-iaea.html (E.T. 31.10.2014).

yapılacak askeri operasyonlar üzerindeki sivil (hükümet) kontrolünün nasıl sağlanacağı belirsizdir. Belirsizliğin en büyük nedeni ise siber uzayın doğasıdır. Nükleer çağda karar alma süresi kimi durumlarda dakikalara inerken, siber uzayda bu süre saniyelere inmiş durumdadır. Gerçekleşen saldırı karşısında savunmanın nasıl yapılacağı, angajman kuralları çerçevesinde karşılık verilecekse bu karşılığın mahiyeti ya da aktif siber savunmanın hangi sınırdan sonra misilleme veya saldırı şeklini alacağı soruları ve bu sorulara kısıtlı sürede asker ya da sivil hangi kurumun cevap vereceği önem kazanmaktadır.[292]

Nye'ın son olarak ortaya koyduğu varsayıma göre siviller tarafından kullanım, ulusal güvenlik stratejisinin işlevselliğini zorlaştıracaktır. Örneğin Nükleer teknoloji her ne kadar askeri amaçlarla kullanım için keşfedilse de kısa sürede sivil alanda da kullanılabileceği fark edilmiştir. Nükleer santrallerde üretilecek enerjinin göreli olarak ucuz olması nedeniyle dünyayı değiştirebileceğine dair inanç, karar alıcılar tarafından da desteklenmiştir. ABD Başkanı Dwight Eisenhower'ın da desteklediği "Barış İçin Atom"[293] gibi programlar, nükleer enerjinin dünyaya yayılmasını teşvik etmiştir. Her ne kadar ABD Atom Enerjisi Komisyonu nükleer teknolojinin yayılması üzerinde kontrol iddiasıyla kurulsa da alanın ticarileşmesi bu kurumu başarısız kılmıştır. Hindistan nihayetinde nükleer enerji üretecek santrallerde kullanılması amacıyla verilen materyaller ve destek sayesinde 1974'te kendi nükleer silahını geliştirmiştir. Fransa benzer desteği Pakistan'a vermiştir. Almanya ise uranyum zenginleştirme teknolojisini Brezilya'ya vermiştir. Tüm bu süreç boyunca nükleer enerjinin barışçıl amaçlarla kullanılmasını sağlamak gayesiyle kurulan kurumlar ise ticari çıkarı olan devlet ve şirketlerin baskısı altında kalmıştır. Siber uzayda ise sivil sektörün payı nükleer alanla karşılaştırılamayacak kadar fazladır. Çalışmamızın kritik altyapıların güvenliği ile ilgili bölümünde de belirttiğimiz üzere liberal ekonomilere sahip devletlerin ekseri çoğunluğunda kritik altyapılar özel sektör tarafından işletilmektedir.[294] Siber uzayda devletin doğrudan kontrolü altında olan kısım ise oldukça kısıtlıdır. Bu koşullar altında ulusal siber güvenliği sağlamak zorlaşmaktadır. Özel sektör ise çoğu noktada kendi güvenliğini kendi sağlayacağı söylemi altında düzenleyici

[292] Nye, "Nuclear Lessons…", op. cit., pp. 26-27.
[293] Bu konuda ABD Başkanı Dwight Eisenhower'ın 8 Aralık 1953'te yaptığı konuşmanın tam metni için bkz. "Atoms for Peace Speech", 20 October 2014, https://www.iaea.org/about/history/atoms-for-peace-speech (E.T. 31.10.2014).
[294] Supra, pp. 75-81.

regülasyonlara karşı çıkmaktadır. Devletin ortaya koyacağı zorlayıcı regülasyonlar ise özel sektörün hakim olduğu alanda piyasa koşullarını bozma riski taşımaktadır. Devlet-özel sektör işbirliğinin ise ne kadar başarılı olacağı belirsizdir. Orta çıkan bu durum, siber uzayın güvenliğini ve devletlerin ulusal siber güvenliklerini, nükleer alanla karşılaştırılmayacak kadar tehlikeye sokmaktadır.[295]

Nye çalışmasında nükleer alan ve siber uzay arasındaki yukarıda irdelenen tüm benzerlikleri ve farklılıkları ortaya koyduktan sonra nükleer tarihten alınacak tecrübeyle, siber uzayın geleceğine ilişkin çıkarımlarda bulunmaktadır. Nye, nükleer çağın başında bu güce sahip devletlerin kabul etmediği işbirliğini daha sonra kabul etmesine benzer bir sürecin siber uzayda da gerçekleşeceğini savunmaktadır. Bu bağlamda, meydana gelen olayların bu süreci oluşturduğu ve hızlandırdığını örnek gösteren Nye, nükleer alanda II. Berlin Krizi ve Küba Füze Krizi'nin doğurduğu etkiyi siber uzayda Estonya ve Gürcistan'a yapılan DDOS saldırıları ile İran'a yapılan STUXNET saldırısının oluşturacağını düşünmektedir. Yapılan saldırılar ve gelecekte gerçekleşecek saldırılar devletleri işbirliğine itecektir. Bu sürecin ardından gerçekleştirilecek uluslararası işbirliği ve oluşturulacak düzenlemeler siber uzayı daha güvenli bir yer haline getirecektir. Nye, tespit/isnat konusunda ortaya konulan tüm argümanlara rağmen siber caydırıcılığın mümkün olduğunu iddia etmektedir. Savunmanın daha güçlü hale getirilmesi, aktif savunmanın sağlanması, kimliği önemsenmeksizin saldırgana doğrudan karşı saldırı gibi önlemlerle caydırıcılık sağlanabilecektir. Lupovici'ye benzer şekilde Nye da çalışmasında özellikle siber uzayın devlet dışı aktörlere verdiği güce vurgu yapmaktadır. Bu aktörlere karşı caydırıcılığın daha zor sağlanacağı ve böyle durumlarda önleyici tutumun ve insan temelli istihbaratın önemli olacağını belirtmektedir. [296]

Nye, "*Cyber Power*" adlı çalışmasında "*Nuclear Lessons for Cyber Security*" makalesinde kısaca değindiği, siber uzaydaki aktörler ve aktörlerin konumlarını ayrıntılı olarak irdelemektir. Bilindiği üzere 1648 Westphalia Barış Antlaşmaları'yla uluslararası sistemde aktörler yeniden tanımlanmıştır. Westphalian dönemde, feodal lordların, prenslerin, dini otoritenin ve imparatorların gücü paylaştığı uluslararası sistem değişmiş ve merkezi devletlerin yegane aktör olduğu sistem ortaya çıkmıştır. Bu süreçte güç kazanan

[295] Bu konuda ayrıntılı bilgi için bkz. Nye, "Nuclear Lessons…", op. cit., pp. 27-29; Nye, "Cyber Power", op. cit., p. 17.
[296] Bu konuda ayrıntılı bilgi için bkz. Nye, "Nuclear Lessons…", op. cit., pp. 29-36.

merkezi devletler kendi içerisinde bulunan diğer aktörleri ortadan kaldırmışlardır. Ulusal kiliseler kurularak devletin içişlerine müdahale etmek isteyen Katolik Kilisesi engellenmiştir. 1848 Devrimleri diğer adıyla uluslar baharı sonrası ise merkezi devletler/imparatorluklar ulus devletler şeklinde bölünmüştür. I. Dünya Savaşı sonrası genel kabul gören ulusların kendi kaderini tayin hakkı ilkesi ile daha da güç kazanan ulus devletler, günümüzde yaklaşık 200 devletten oluşan uluslararası sistemin temelini teşkil etmektedir.[297]

Siber uzayın ortaya çıkışı sonrası ve özellikle siber uzayın kullanımında son 20 senede yaşanan artış ise ulus devletlerin tek meşru otorite olarak kabul edildiği sistemi tehdit etmektedir. Siber uzayın sanal katmanında sınırların olmayışı ve bu durumdan kaynaklı egemenlik alanlarının belirsizliği, devlet dışı aktörlerin güç kazanmasına neden olmuştur. Bu durumu güç yayılımı (power diffusion) olarak kavramsallaştıran Nye, devletlerin kara, deniz ve hava boyutlarında olduğu gibi siber uzayda da bir güç olarak var olmalarına karşın, siber uzayın doğasının devletlerin tek aktör olarak bu alanda hâkim olmalarına izin vermeyeceğini belirtmiştir.[298] Bu bağlamda siber uzayda güç, büyük devletlerden diğer devletlere ve daha da önemlisi devlet dışı aktörlere yayılmaktadır. Ortaya çıkan yeni sistem ise pre-westphalian sistemin çok aktörlü yapısı ile benzerlik göstermektedir.

Nye'ın ortaya koyduğu bu görüşe katılmakla birlikte her ne kadar siber uzayın doğası, aktör yapısı itibariyle pre-westphalian dönemle benzerlik gösterse de bu alanda aktörlerin birbirleriyle ilişki kurarken dayandığı kapasiteler farklılık göstermektedir. Çalışmamızda daha öncede belirttiğimiz gibi siber uzayda en fazla varlığa sahip olan devletler saldırıya en açık olanlardır. Orta Çağ'da askeri anlamda en güçlü olan aktör, diğer aktörler üzerinde egemenlik kurarken, siber uzayda güçlü olan aktörün diğer aktörler üzerinde egemenlik kurması mümkün değildir. Aksine, siber uzayda güçlü olan devletin siber uzayda varlığı olmayan ama ofansif kabiliyet geliştirmiş bir aktör karşısında

[297] Barış Özdal ve Murat Jane, ""La Der Des"'in Uluslararası Sistemin Yapısına Etkileri", *Gazi Akademik Bakış*, Cilt: 7, Sayı: 14, Yaz 2014, pp. 215-245, pp. 218-226.
[298] Bu konuda ayrıntılı bilgi için bkz. Nye, "Nuclear Lessons…", op. cit., pp. 29-36.

konvansiyonel karşılık vermesi dışında bir seçeneği yokken, ofansif kabiliyet geliştiren aktör, siber uzayda devlete büyük zarar verebilir.[299]

Goodman, *"Cyber Deterrence Tougher Than Theory in Practise"* adlı makalesinde siber caydırıcılık üzerine geliştirilen teorik yaklaşımların işlevselliğini sorgulamaktadır. Bu noktada siber saldırıların fiziksel katmandan bağımsız olmadığını öne süren Goodman, siber uzayda teorinin pratikten yoksun olduğunu belirtmektedir. Siber uzayda caydırıcılığın, teorisyenler tarafından tartışılmasının üç sebebi vardır. Bu sebepler genel ve soyut olarak:[300]

1. Gelecekte yaşanması muhtemel siber savaş riskinin hızla artması,

2. Diğer dört boyutta (kara, hava, deniz, uzay) başarıyla uygulanan caydırıcılığın beşinci boyutta etkili olma ihtimali,

3. Caydırıcılığı sağlamak için yapılacak tüm yatırımların maliyetinin, yaşanacak çatışmada baş gösterecek zarardan göreli olarak daha az olması.

Yukarıda genel ve soyut olarak verilen Goodman'ın ortaya koyduğu sebeplerden dolayı 1994 yılında James Der Derian'ın siber caydırıcılık kavramını kullanmasından bu yana siber uzay ve bu alanda sağlanacak caydırıcılığa yönelik ilgi artmaktadır. Yapılan tüm teorik çalışmaların pratikte test edilmemiş olmasından dolayı, siber uzayda caydırıcılığın etkili olup olmayacağı tartışması ortaya çıkmaktadır.[301]

Goodman çalışmasında caydırıcılığın sağlanabilmesi için sekiz temel unsur ortaya koymaktadır. Bu unsurlar:[302]

1. Menfaat (Korunmak istenen)

2. Caydırıcı deklarasyon

3. Esirgeyici/engelleyici önlemler

[299] Nye, "Cyber Power", passim.
[300] Bu konuda ayrıntılı bilgi için bkz. Goodman, op. cit., pp. 102-104.
[301] Ibid.
[302] Ibid. p. 105.

4. Cezalandırıcı önlemler

5. İnanılırlık

6. Güven verme

7. Korku

8. Kar-zarar hesabı

Yukarıda maddelendirilen bu sekiz unsuru bir bütün halinde açıklamak gerekirse, devletler caydırıcılığı herhangi bir konudaki menfaatlerini korumak için kullanırlar. Bu bağlamda devletlerin yapması gereken, öncelikle menfaatlerini koruyacak ve bu doğrultuda menfaatlerine zarar verecek devletlerin cezalandırılacağını ortaya koyan bir deklarasyonda bulunmalarıdır. Bu deklarasyon doğrultusunda devletler öncelikle menfaatlerine saldırılması durumunda onları koruyacak şekilde defansif, ardından da saldıran devlete bedel ödetmek amacıyla ofansif önlemler almalıdır. Caydırıcılığı asıl işlevsel kılan ise kapasite ile tehdit (deklarasyon) arasındaki paralellik ve ortaya konan kapasitenin menfaatlere zarar verilmesi halinde kullanılacağına dair tarihsel referanslardan beslenen inanılırlıktır. İnanılırlık kadar önemli diğer unsurlar ise menfaatlere zarar verilmemesi halinde rakip devlete zarar verilmeyeceğine dair oluşturulan güven, ödetilecek bedelden kaynaklanan korkudur. Son olarak rakip devletin rasyonel davranacağından hareketle yapılacak kar-zarar hesabı, caydırıcılıkta etkin rol oynamaktadır.[303]

Caydırıcılığın sağlanması noktasında gerekli olan sekiz unsurun yanında, caydırıcılığın siber uzayda işlevsel hale gelebilmesi için özellikle dikkat edilmesi gereken beş başlık ön plana çıkmaktadır. Bu başlıklar Goodman tarafından genel ve soyut olarak şöyle tespit edilmiştir:[304]

> *1. "Devletler, siber çatışma esnasında caydırıcı mesajın oluşturulmasını, iletilmesini ve saldırgan tarafından anlaşılmasını sağlamalıdır.*
> *2. Devletler, ofansif ve defansif kapasitelerinin etkinliğini korumalıdır.*

[303] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 105-107.
[304] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 107-110.

3. Karşı saldırı yapılmadan önce saldırganın kimliği doğru bir şekilde tespit edilmelidir.
4. Devletler ilk saldırı sonrasında karşı saldırı kapasitelerinin varlığının devamını garanti altına almalıdır. Daha da önemlisi savunmacı ve saldırgan devlet arasında jeopolitik simetri olmalıdır.
5. Güvencenin (güven verme) yokluğu siber caydırıcılığın sağlayacağı ilişkiye ket vurabilir."

Teorinin aksine pratikte taraflar arasındaki iletişim kusurlu olabilir. Rasyonel hareket için gerekli olan bilgilerin temin edilememesi ya da karar alıcıların kişiliği gibi etmenler hatalı kararlara yol açabilir. Bu tür yanlış anlaşılmaları engellemek ve mesajın doğru şekilde iletilebilmesini sağlamak için Soğuk Savaş esnasında iki kutup lideri arasında "*kırmızı telefon hattı*" kurulmuştur. Siber uzayda yaşanacak saldırı eylemi halinde de karşı tarafa mesajın doğru şekilde iletilmesi ve saldırgan tarafından mesajın doğru bir şekilde alındığına emin olunması oldukça önemlidir.[305] Bu durum tezimizin teorik çerçevesinde belirttiğimiz Holsti'nin mesajın açık bir şekilde iletiminin önemine örnek olarak gösterilebilir.

Saldırgan devletin saldırı yapmadan önce kar/zarar hesabı yaptığı noktada hesaba kattığı en önemli unsurlardan biri savunmacı devletin defansif ve ofansif kapasitesidir. Bu kapasite saldırgan devlete elde edeceği menfaatten daha fazla zarar verebilir ve saldırgan devleti saldırıdan vazgeçirebilir. Bu bağlamda siber uzayda savunmacı devlet defansif önlem olarak hedefleri çevrimdışı bırakarak saldırmayı imkansız hale getirebilir. Bu tür önlemler saldırganın elde etmek istediği menfaatleri ortadan kaldırabilir. Lakin saldırganı caydıracak asıl önlem ofansif kapasitedir. Defansif önlemler her ne kadar saldırganın elde etmek istediği menfaatlere ulaşmasını engellese de saldırgana büyük boyutlu bir zarar vermez. Oysa ofansif/cezalandırıcı önlemler saldırganın varlığına zarar vereceği için caydırıcılıkta çok daha etkin olacaktır. Sadece defansif önlemler alınması durumunda ise saldırgan menfaatine ulaşmak için etkili bir yol bulana kadar saldırmaya devam edecektir. Bilindiği üzere klasik cezalandırıcı önlemler üç unsuru içermektedir. Bu unsurlar "kesinlik", "şiddet" ve "çabukluktur". Nükleer caydırıcılıkta şiddet ve hız önemliyken, siber caydırıcılıkta kesinlik diğer iki unsurdan daha önemlidir. Bunun en önemli nedeni siber uzayda verilecek zararların nükleer silahlarla verilebilecek zarara kıyasla çok daha az

[305] Ibid., pp. 110.

önemli olmasıdır. Bu noktada saldırının şiddeti ve/veya hızı yerine, saldırganın kimliği tespit edilmeli ve doğru aktöre karşı cezalandırıcı önlemler alınmalıdır.[306]

Lupovici ve Nye'ın siber uzay için önem atfettiği tespit/isnat problemine Goodman da özellikle değinmektedir. Zira fiziksel alana kıyasla siber uzayda saldırganın kimliğinin tespiti oldukça zordur. Bu bağlamda devletler saldırganın kimliğini tespit için uluslararası yardım talep edebilir. Antlaşmalar çerçevesinde yapılacak uluslararası işbirliği, saldırganın kimliğini bulmayı kolaylaştıracağı gibi işbirliği yapmayan devletlere saldırının sorumluluğunu yükleyebilir.[307]

Göz önünde bulundurulması gereken bir diğer önemli unsur da yapılan siber saldırı sonrasında caydırıcılığı sağlayacak kapasite varlığının korunmasıdır. Günümüzde konvansiyonel kapasitelerin kontrolü dahi siber uzaya bağlı komuta-kontrol sistemleri tarafından yapılmaktadır. Bu sistemlere verilecek zarar devletin savunma ve caydırma kapasitesini devre dışı bırakabilir. Bununla beraber savunmacı devlet misilleme yapmadan önce kar/zarar hesabı yapmalıdır. Çünkü siber uzayda başlayan çatışma, konvansiyonel alana sıçrayabilir. Konvansiyonel karşı saldırı olması durumunda alınacak zarar, korunmak istenen menfaatin önüne geçebilir. Bu çerçeveden bakıldığında siber caydırıcılık sağlanmaya çalışılırken savunmacı ve saldırgan devlet arasında jeopolitik simetrinin olmasına dikkat edilmelidir. Son olarak siber caydırıcılığın varlığı güvencenin sağlanmasıyla mümkündür. Goodman'a göre güvence, siber caydırıcılığın sağlanmasında "*kadife eldiven*" işlevi görmektedir. Demirden bir yumruk savunmacı ve cezalandırıcı önlemleri alırken, bu önlemlerin işlevselliği kadife eldiven olarak adlandırılan güvence olmaksızın mümkün değildir. Taraflar birbirlerinin ağında gelecekte zarar vermek için kullanacaklarını açıkları aramaktan vazgeçmeyeceklerdir.[308]

Goodman çalışmasında ortaya koyduğu teorik yaklaşımı iki alan çalışmasıyla somutlaştırmaktadır. Çalışmamızda daha önce ayrıntılı olarak açıklanan 2007 Estonya ve 2008 Gürcistan çatışmalarını inceleyen Goodman, bu iki çatışmada siber caydırıcılığın neden başarısız olduğunu irdelemektedir.

[306] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 107-108.
[307] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 108-109.
[308] Ibid., p. 109.

Bu bağlamda Goodman'a göre 2007 Estonya Saldırısı'nda siber caydırıcılığı sağlamayı zorlaştıran üç unsur ortaya çıkmaktadır. Bu unsurlar siber uzayın doğasının sonuçları olan "anonimlik", "asimetri" ve "aktörlerin aşırı güçlenmesidir" (super empowerment). Estonya Saldırısı sonrası sadece Rus asıllı bir Estonyalının cezalandırılması diğer sorumlularınsa tespit edilememesi anonimliğin sonucudur. Ortaya çıkan asimetri ise Estonya'nın misilleme yapmasını engellemiştir. Bahse konu olan asimetri iki açıdan ele alınmalıdır. Daha öncede belirttiğimiz üzere Estonya, saldırıların sorumlusu olarak kesin kanıtlar sunmasa da RF'yi işaret etmiştir. RF ile Estonya arasındaki ağlanmışlık farkı ise Estonya'nın yapacağı bir siber karşı saldırının/misillemenin RF üzerinde, Estonya üzerinde doğurduğu etkiyi doğurmayacağı gerçeğidir. İkinci olarak göz önünde bulundurulması gereken asimetri ise fiziki katmanda RF ile Estonya arasındaki güç uçurumudur. Estonya'nın RF'ye yapacağı orantısız misilleme sonrasında RF'nin vereceği muhtemel konvansiyonel karşılık, Estonya'ya ağır bedeller ödetme riskini barındırmaktadır.[309]

Goodman iki noktada ise 2007 Estonya Saldırısının siber caydırıcılığın sağlanmasında gelecekte örnek olabilecek olumlu kısmını öne çıkarmaktadır. Bu noktalardan ilki Estonya'nın defansif önlemlerde sağladığı başarıdır. Estonya CERT'i saldırının yoğun olarak geldiği ülkelerin internet çıkışlarını bloklayarak ve yoğun saldırı altında olan Estonya web sayfalarını erişime geçici olarak kapatarak defansif önlemleri başarıyla uygulamıştır. İkinci önemli nokta ise Estonya hükümetinin uluslararası antlaşmalar çerçevesinde RF içerisinde soruşturma talep etmesidir. RF ise uluslararası antlaşma hükümlerine rağmen işbirliği yapmayı reddetmiştir. Bu durum RF'nin Estonya Saldırısındaki sorumluluğunu kanıtlanamamasına rağmen soruşturmayı engellemesi neticesinde RF'nin saldırıdan sorumlu olduğu sonucunun doğmasına neden olmuştur. Zira Estonya Saldırısı, saldırıyı yapan aktörün devlet tarafından gizlenmesi ve savunmacı devlete yardımın reddi gelecekte de yardımı reddeden devletin saldırıdan sorumlu sayılacağı bir yaklaşımı ortaya çıkarmıştır.[310]

2008 Gürcistan Saldırısı ise çalışmamızda daha önce ayrıntılı olarak incelediğimiz üzere RF'nin Gürcistan'a konvansiyonel saldırısı ile birlikte gerçekleşmiştir. Yapılan siber

[309] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 110-112.
[310] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 112-114.

saldırı öncelikle Gürcistan'ın iletişim altyapısını hedef almıştır. Bu sayede Gürcistan'ın dünya ile iletişimi koparılarak yaşanan çatışmayı kendi perspektifinden duyurması engellenmiştir. Estonya saldırısının aksine Gürcistan'a yapılan saldırılar ekonomik etkiye sahiptir. Gürcistan boru hatlarına konvansiyonel saldırı ile eşgüdümlü yapılan siber saldırı, boru hattını işlevsiz bırakmıştır. Boru hattının işlevsiz kalması üzerine RF benzer boru hattı servisini iki katı fiyatına diğer devletlere önermiştir. Bu bağlamda iletişim ve enerji kritik altyapılarına verilen zararlar RF menfaatine sonuçlar doğurmuştur. Estonya'nın aksine Gürcistan saldırıya hazırlıksız yakalanmıştır. Bu hazırlıksızlığa rağmen Gürcistan'a dost devletler yer sağlayıcılık (hosting) hizmeti sunmuş ve özel şirketler saldırılar karşısında savunmaya yardımcı olmuştur.[311]

2008 Gürcistan Saldırısı siber caydırıcılığın sağlanmasında yeni iki problemin tespit edilebilmesini sağlamıştır. Bu problemlerin ilki olan "ölçeklenebilirlik" (scalability), konvansiyonel silahlardaki kullanımı ve etkisi arasındaki ilişkinin siber uzayda farklı olmasından kaynaklanmaktadır. Konvansiyonel silahlar ölçeklenebilir etkiye sahiptir ve bu silahların çoğu zaman ikinci etkileri yoktur. Siber uzayda ise kullanılan silahlar ikinci etkiye sahip olabilmektedir. Bu durum, verilen zararın ölçeklendirilmesini zorlaştırmaktadır. Gürcistan'a yapılan siber saldırıların bir kısmının küçük ölçekli zararlar verdiği düşünülürken, bu saldırılar esnasında hükümet sistemlerine büyük zararlar vermek için zaman ayarlı siber silahların bırakıldığı tespit edilmiştir. Caydırıcılık ise yapılan eyleme değil eylemin doğuracağı muhtemel etkiye verilecek mesajlar üzerinden gerçekleşmektedir. Etki bazlı bu yaklaşım ise siber uzayda etkinin ölçeğinin belirlenmesinde yaşanan zorluktan dolayı çıkmaza girmektedir.[312]

Caydırıcılığın sağlanmasında yaşanan ikinci problem ise "zamansallıktır" (temporality). Diğer dört boyutta kullanılan silahlarla yapılan saldırılar, gelişen teknolojiyle oluşturulan erken uyarı sistemleri sayesinde tespit edilebilmektedir. Siber uzayın doğası ise saldırının önceden tespitine ve tespit kaynaklı engellenmesine izin vermemektedir. Örneğin kara boyutunda bir saldırı için sınıra yığılan tanklar ya da sevk edilen askeri birlikler uydular üzerinden tespit edilebilmekte saldırıyı caydırmak için karşı yığınak ya da farklı eylemlere gidilebilmektedir. Siber uzayda ise saldırı ancak

[311] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 114-116.
[312] Ibid., p. 116.

gerçekleştiği anda tespit edilebilmektedir. Bunun yanında gerçekleşen saldırıyı kimin yaptığı sorusu, caydırıcı önlemler alabilmek için öncelikle çözülmelidir. Diğer boyutların aksine siber saldırılar, saldırganın tespitini sağlayacak imzalar bırakmamaktadır.[313]

Ortaya konan bu iki olumsuzluğa rağmen 2008 Gürcistan Saldırısı siber caydırıcılığın sağlanması noktasında bazı olumlu gelişmelerde ortaya koymuştur. Bu gelişmelerden ilki siber saldırıyla verilecek zararın uzun vadeli anlamsızlığıdır. Diğer boyutların aksine dijital bilgi çok düşük maliyetlere sonsuz kez çoğaltılabilmektedir. Bunun da ötesinde neredeyse maliyetsiz şekilde zarar gören data/veri kurtarılabilmekte ya da programlar işlevsel hale getirilebilmektedir. Bu durum uzun vadede siber saldırıyı anlamsız hale getirmektedir. İkinci olumlu gelişme ise diğer tüm boyutlardan çok daha kolay bir şekilde siber saldırıya uğrayan devlete yardım edilebilmesidir. Bu yardım diğer boyutların aksine kritik öneme sahip olan "zamanın kullanımını" mecbur kılan ve maliyeti olan kuvvet aktarımını gerektirmemektedir. Bu bağlamda Gürcistan, siber saldırıya uğradıktan sonra, hükümete ait web sayfalarını üçüncü ülkelerin yer sağlayıcılığı üzerinden sunmuştur. Bunun yanında Nye'ın siber uzayda aktörler arasındaki güç yayılımı (power diffusion) pratiğe dökülmüş, özel şirketler saldırıya karşı kendi güçlerini kullanarak devlete yardım etmişlerdir. Örneğin Gürcistan Saldırısı'nda Google siber saldırılara karşı devletin savunma yapmasına yardımcı olmuştur. Yaşanan üçüncü olumlu gelişme ise sistemlerin kapalı ağlarla korunabileceğidir. Siber uzayda saldırılar ağa bağlı sistemlerde bulunan açıklar sayesinde yapılmaktadır. Sistemin ağdan koparılması ise saldırının yapıldığı açıkları ortadan kaldırmaktadır. Kapalı ağda çalışan Gürcistan hava savunma sistemleri bu çerçevede siber saldırıdan etkilenmemiştir. Siber saldırılardan etkilenmeyen bu sistemler, görevlerini başarıyla yerine getirerek oldukça gelişmiş RF savaş uçaklarını düşürmeyi başarmıştır.[314]

Goodman'ın ortaya koyduğu ve yukarıda ayrıntılı olarak verilen bu üç olumlu gelişmenin birinci ve üçüncüsü 2008 Gürcistan Saldırısı'nın ardından gerçekleşen diğer saldırılar ve gelişen teknolojiler karşısında geçerliliğini yitirmiştir. Zira 2011 yılında İran'a yapılan STUXNET Saldırısı ile siber saldırı neticesinde ilk kez fiziki hasar verilmiştir. Goodman'ın dijital bilginin çoğaltılması ve kurtarılması sayesinde saldırının

[313] Ibid.
[314] Ibid., p. 117.

anlamsızlaşacağına dair iddiası, siber saldırıyla fiziki hasar verilmesi neticesinde geçerliliğini kaybetmiştir.[315] Benzer biçimde Goodman'ın kapalı ağların güvenli olduğuna dair iddiası da STUXNET Saldırısı ile geçerliliğini yitirmektedir. İran'ın nükleer tesisleri kapalı ağlar üzerinden yönetilmesine rağmen, sisteme hafıza kartı üzerinden sosyal mühendislik ya da fiziki istihbarat yoluyla yazılım bulaştırılmıştır. 2014 yılında düzenlenen Black Hat konferansında ise İsrailli bilimadamları mavi lazer kullanımıyla kapalı ağdaki bir yazıcıdan veri çalmayı başarmış ve aynı yöntemle kapalı ağlara uzun mesafelerden veri aktarmanın mümkün olduğunu iddia etmişlerdir.[316]

Goodman, Gürcistan'a yapılan saldırılar neticesinde siber caydırıcılığın başarısız olmasını ise en temelde jeopolitik faktörlere bağlamaktadır. Gürcistan ile RF arasındaki konvansiyonel güç farkı, Gürcistan'ın misilleme yapmasını engellemiştir. Jeopolitik faktörlerin yanında saldırıyı gerçekleştirenlerin tam olarak kanıtlanamaması ve siber uzayın devlet dışı aktörlere sağladığı aşırı güçlenme (super empowerment) siber caydırıcılığın başarısız olmasında etkili olmuştur. Özellikle RBN'nin Gürcistan'a yaptığı siber saldırılar ve RF'nin bu saldırıların önünü açması, siber caydırıcılığı başarısız kılmıştır.[317]

Richard L. Kugler da "*Deterrence of Cyber Attack*" isimli çalışmasında ABD özelinden hareketle siber caydırıcılığın mümkün olup olmadığını sorgulamaktadır. Kugler çalışmasında siber uzayda yapılan tüm saldırılarda caydırıcılığın mümkün olmadığını, buna karşın zarar verme potansiyeli olan saldırılara karşı caydırıcılığın yeterli olacağını iddia etmektedir. Bu bağlamda çalışmamızda ele aldığımız tüm yazarlara benzer şekilde Kugler da tespit/isnat problemine değinmiştir. Tespit/isnat problemi caydırıcılığın sağlanmasını imkansız kılmamaktadır. İmkanlar dahilinde tespit edilebilen ve/veya saldırganın kimliğini ortaya koyduğu durumlarda caydırıcılık geçerlidir.[318]

[315] Supra, pp. 71-75.
[316] Bu konuda ayrıntılı bilgi için bkz. Pierluigi Paganini, "Hacking air gapped networks by using lasers and drones", 25 October 2014, http://securityaffairs.co/wordpress/29551/hacking/hacking-air-gapped-networks.html (E.T. 15.12.2014); Mathew J. Schwartz, "Black Hat Keynoter: Beware of Air Gap Risks", 16 October 2014, http://www.bankinfosecurity.com/black-hat-europe-beware-air-gaps-a-7442/op-1 (E.T. 15.12.2014)
[317] Goodman, op. cit., pp. 117-118; Supra, pp. 69-71.
[318] Kugler, passim.

Bu bağlamda Kugler'ın altını çizdiği bir diğer önemli konu Soğuk Savaş'ın aksine günümüzde tek bir caydırıcılık stratejisinin işlevsel olmayacağıdır. Soğuk Savaş boyunca tehdit nükleer silah, rakip ise nükleer silaha sahip diğer devletlerdir. Siber uzayda ise tehdit ve rakip farklı düzeylerde ve birden fazladır. Bu nedenden dolayı tek bir caydırıcılık stratejisi yetersizdir, yapılması gereken farklı düzeylerde farklı tehditlere özel caydırıcılık stratejileri oluşturmaktır.[319]

Kugler çalışmasında, ABD ve müttefiklerinin sadece bilgi sistemlerinin değil siber uzaya bağlı tüm kritik altyapılarının saldırıya açık olduğunu belirtmiştir. Bunun da ötesinde siber uzayın kullanımı ve buna bağlı olarak siber uzaya bağımlılığın her geçen gün arttığı küreselleşen dünyada, saldırılacak sistemlerdeki açık sayısı da hızla artmaktadır. Diğer bir deyişle siber uzayın kullanımında yaşanan artış çift taraflı bir tehlikeyi barındırmaktadır. Belirttiğimiz gibi bu artış, saldırılacak sistemlerdeki açık sayısını arttırdığı gibi bu açıklara saldırma potansiyeli olan rakip sayısını da arttırmaktadır. Nye'ın belirttiği farklı aktörlerin siber uzay sayesinde güçlenmesi tezine Kugler da katılmaktadır. Bu bağlamda ortaya çıkan yeni aktörler, tehdidin niteliğini ve niceliği de arttırmaktadır.[320]

Finansal yönden incelenecek olursa küreselleşen dünyada çoğu aktör ekonomik gelişimini siber uzaya borçludur. Ortaya çıkan ekonomik gelişim, yeni aktörlerin küresel politikadaki gücünü arttırmaktadır. Ekonomik açıdan gelişim içindeki bu aktörler siber uzayda çok fazla harcama yapmadan, geliştirdikleri güç ile uluslararası sistemde büyük yatırımlarla diğer dört boyutta güç geliştiren aktörlerle güç mücadelesine girebilir. Bu bağlamda siber uzayın maliyet açısından uygunluğu devletleri ofansif kapasite geliştirmeye teşvik edebilir.[321]

Siber uzayın ortaya koyduğu bu yapıda klasik caydırıcılıkta gerekli olan güçlü bir savunma ve misilleme yapabilmek için etkili bir saldırı kapasitesine ek olarak, saldırganın motivasyonunu ve psikolojisini etkileyecek kapasite geliştirilmesine de ihtiyaç vardır. Bu

[319] Ibid, p. 310.
[320] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 312-314.
[321] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 314-315.

şekilde oluşturulacak bir caydırıcılık stratejisi tüm saldırıları engelleme kapasitesine sahip olmasa da belli başlı saldırıları engelleyebilir.[322]

Patrick M. Morgan " *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*" adlı çalışmasında klasik caydırıcılığın ilkelerini ortaya koyarak, Soğuk Savaş boyunca klasik caydırıcılığın nasıl işlediğini incelemiştir. Ardından bu ilkelerin siber uzaya uygulanması noktasında oluşacak problemleri ortaya koyan Morgan, siber uzayda caydırıcılığı sağlayabilmek için gereken olası girişimleri çalışmasında sıralamıştır.

Morgan caydırıcılığın temel isterleri noktasında Kugler'la birleşmekle beraber "saldırıyı karşılayacak savunma" ve "misillemeyi sağlayacak saldırı" kapasitesinin yanına bu iki eylemi gerçekleştirecek "komuta ve kontrol yapısı"'nı da eklemektedir. Bu noktada Morgan, Soğuk Savaş boyunca uygulanan savunma ve saldırı yönetimiyle, siber uzayda uygulana gelen yapı arasındaki farka dikkat çekmektedir. Soğuk Savaş'ta savunma ve nükleer kapasiteyi de içeren saldırı, merkezi olarak yapılırken; siber uzayda devletlerin sadece saldırı kapasitesi merkezi olarak yönetilmektedir. Savunma kapasitesi ise saldırılan hedefin sahip olduğu lokal savunma mekanizmaları tarafından yapılmaktadır. Soğuk Savaş'ın aksine siber uzayda düşmanın gücü ve verebileceği zararın boyutu bilinmemektedir. Alınacak zararın ne kadardan sonra kabul edilemez olduğu ve ne zaman misillemenin gerekeceği ise savunmanın saldırı kapasitesinin aksine lokal olduğu bu yapıda karar verilmesi zor bir soru haline gelmektedir. Morgan caydırıcılığın işlevsel olabilmesi için siber uzayda savunmanın da merkezileştirilmesinin önemini vurgulamaktadır. Morgan'ın savunmaya verdiği bu önemin bir diğer sebebi ise caydırıcılığı sağlamak için temel ister olarak ortaya koyduğu komuta kontrol yapısına yapılacak siber saldırının, sadece siber kapasiteyi değil devletin tüm saldırı kapasitesini etkileme tehlikesini içermesidir.[323]

Morgan siber uzayda savunmanın ve komuta kontrol yapısının saldırı sonrasında devamlılığını sağlamak adına, yedeklemenin önemli olduğunu vurgulamaktadır. Morgan'ın çalışmasının yayınladığı 2010 yılı itibariyle bu yaklaşım doğru gözükse de 2010 yılında ortaya çıkan ve 2011 yılında etkileri tam olarak anlaşılan STUXNET Saldırısı ile siber

[322] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 317-318.
[323] Bu konuda ayrıntılı bilgi için bkz. Morgan, op. cit., pp. 61-62.

saldırı yaparak fiziki hasar verilebileceği gerçeğinin ortaya çıkması, yedekleme yaklaşımını büyük ölçüde işlevsiz bırakmıştır.[324]

Morgan'a göre klasik caydırıcılıkta önemli olup, siber caydırıcılık sağlanmaya çalışılırken problemli olan unsurlar da bulunmaktadır. Bu unsurlardan biri de mesajın saldırgana iletilmesi sürecidir. Soğuk Savaş'ta nükleer caydırıcılık sağlanırken rakibin kim olduğu ve hangi motivasyonla hareket ettiği gayet açıktır. Siber uzayda ise saldırganın kimliğinin tespiti mümkün olmayabilir. Bu durumda kimliksiz saldırgana mesajın iletilmesi sorunu ortaya çıkmaktadır. Saldırganın kimliği kadar bir diğer önemli hususta saldırganın motivasyonudur. Motivasyonu bilinmeyen saldırgana verilmesi gereken doğru mesajın ne olacağını bilmekte zordur.[325]

Morgan'ın altını çizdiği bir diğer önemli zorlukta inandırıcılıktır. Caydırıcılığın başarılı olabilmesi için yapılacak tehdit inandırıcı olmalıdır. Tehdit inandırıcı olduğu kadar rakip devlette, tehditin gerçekleştirileceğine dair inançta olmalıdır. Siber uzayda ise saldırıyı yapan aktörün kimliği ve motivasyonunun tespiti dahi oldukça zorken yapılan tehdidin inandırıcı olması mümkün değildir. Bunun da ötesinde tespit edilen saldırgana verilecek siber karşılığın zarar verme kapasitesi de bilinmezliğini korumaktadır. Verilecek siber karşılığın saldırgana zarar vermeyeceğine dair oluşan inanç, daha büyük saldırılara neden olabilir.[326]

Morgan'ın öne çıkardığı son unsur ise klasik caydırıcılığın aksine siber uzayda yaşanan istikrar sorunudur. Caydırıcılığın istikrarı sistemin güvenli olmasını ve nihayetinde kontrolünü sağlamaktadır. Caydırıcılıkta devletlerin oluşturduğu inandırıcılık istikrarı destekler. İstikrar inandırıcılık kadar rakiplerin saldırma isteğinin fazlalığıyla da ilişkilidir. Bu bağlamda istikrarı korumak rakip devletin saldırma istediği kuvvetlenmeden müdahale edilmesine bağlıdır. Kriz ne kadar büyürse istikrar o kadar tehlikeye girer. Bu bağlamda caydırıcılığın istikrarı ile rakibin rasyonelliği arasında ters orantı vardır.[327] Siber uzayda ise saldırganın savunmaya karşı kapasitesindeki hızlı değişim istikrarı sarsmaktadır. Nükleer caydırıcılıkta savunmanın zorluğu probleminin üzerinden, misilleme

[324] Ibid., p. 63.
[325] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 64-65.
[326] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 65-69.
[327] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 70-71.

tehdidi ile gelinmiştir. Siber uzayın doğası gereği misilleme üzerinden oluşturulan yaklaşım geçerli değildir. Bu bağlamda devletler siber uzayda inandırıcı tehdide sahip değilken istikrarı sağlamak zorlaşmaktadır. Bu duruma karşın silahların kontrolü istikrarı sağlayabilir. Siber uzayda silahsızlanma ise nükleer silahların aksine mümkün gözükmemektedir. Siber uzayda silahsızlanmanın mümkün olmamasının en temel nedeni geliştirilen silahların nihayetinde dijital bilgi olmasıdır. Dijital bilgiyi ise saklamak kolay, kontrol ise zordur. Yapılacak uluslararası işbirliği ise saldırı halinde alınacak hasarın önüne geçebilir ve caydırıcılığın istikrarına katkı yapabilir.[328]

Morgan çalışmasının sonunda siber caydırıcılığın sağlanması için önerilerde bulunmaktadır. Öncelikle siber uzayda savunma merkezileştirilmeli ve saldırıya derhal ve tüm yönleriyle karşılık verilmelidir. Dijital bilginin korunması noktasında yedekleme oldukça önemlidir. Siber uzayda saldırı kapasitesinin tamamen ortaya konması saldırı kapasitesine zarar verme potansiyelini içerse de caydırıcılığı sağlamak için misilleme kapasitesi yeterince gösterilmelidir. Bir diğer önemli hususta savunmanın yapılabilmesi için yeni teknolojilere yapılacak harcamaların arttırılmasıdır. Son husus ise siber uzayda silahların kontrolüne ilişkin uluslararası mutabakatın sağlanmasıdır.[329]

Libicki'nin "*Cyber Deterrence and Cyber War*" adlı eseri ise siber caydırıcılık çalışmalarında temel kaynaklardan biri olarak kabul edilmektedir. Libicki'ye göre Soğuk Savaş'tan günümüze nükleer caydırıcılığın başarılı olmasının temel sebebi, tekil ve simetrik olmasındandır. Nükleer caydırıcılığın tekilliği, nükleer silaha sahip olan devletlerin gerçekleştirebileceği saldırıların ortaya çıkaracağı olumsuz sonuçlardan kaynaklanmaktadır. Bu sonuçlar nedeniyle diğer devletler nükleer güce sahip devletler ile herhangi bir krizi askeri anlamda tırmandırmaktan kaçınmaktadır. Nükleer güce sahip bir devlete saldırı yapılması durumunda misilleme meydana gelirse, bu durum karşı misillemeyi de içerebilir ve dolayısıyla caydırıcılığın en temel amacı olan menfaati ve nihayetinde öz varlığı koruma durumu zarar görebilir. Bu durum misilleme yapan tarafta dahil olmak üzere her iki tarafı birden ortadan kaldırabilir, geliştirdikleri kapasiteleri ortadan kaldırabilir ya da devletleri güçsüz bırakabilir. Bahse konu olan bu durum konvansiyonel silahların radyasyon hariç benzer kapasiteye ulaştığı günümüzde ağır

[328] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 71-75.
[329] Bu konuda ayrıntılı bilgi için bkz. Ibid., pp. 75-76.

konvansiyonel caydırıcılık için de geçerlidir. Bu duruma 1990'lı yıllar boyunca Türkiye-Yunanistan ilişkileri örnek verilebilir. Kapasitenin bu kadar yüksek olduğu devletler arasında misillemenin ortaya çıkması halinde daha büyük bir savaş riski orta çıkmaktadır. Ortaya çıkacak savaş, taraflardan birinin varlığını tamamen ortadan kaldırabilir.[330]

Nükleer caydırıcılığın aksine siber caydırıcılık tekrarlanabilir olmalıdır. Bunun en büyük nedeni siber misillemenin ne saldırgan devletin kapasitesini ortadan kaldırabilmesi ne saldırgan devletin karar alıcılarının değişmesine yol açabilmesi ne de bu devleti saldırıdan vazgeçirebilecek zararı verebilmesidir. Bu nedenle saldırgan devlet misillemeden zarar görse dahi gelecekte saldırmak için varlığını devam ettirebilir. Ortaya konan yapıdan da görülebileceği gibi siber caydırıcılık simetriktir, dolayısıyla eşitler arasında gerçekleşir. Saldırıya hedef olan devlet (potansiyel misillemeci), saldıran devletten daha üstün bir ahlaki zemine sahip değildir. Ortaya çıkacak çatışma halinde ise herhangi bir tarafın zafer olarak adlandırabilecek boyutta üstün duruma geçebileceğine inanmak için herhangi bir neden bulunmamaktadır. Bu yüzden misilleme yapan devlet daima karşı misillemeye hazır olmalıdır.[331] Libicki'ye göre siber caydırıcılığın nükleer caydırıcılığın aksine simetrik olması ve tekrarlanabilirliği eşsiz değildir. Simetrik ve tekrarlanabilir caydırıcılık genelde bölgesel güçler arasında paylaşılamayan menfaatler nedeniyle sürekli çekişme nedeniyle ve/veya güvenlik ikilemi nedeniyle birbirleri karşısında sürekli savunmada olan iki devlet[332] ya da bazı durumlarda gruplar arasında gerçekleşmektedir. Realizmin ortaya koyduğu anarşik sistem içerisinde, devletlerarasında çatışmanın olağan kabul edildiği böyle durumlarda ise caydırıcılık barışı koruma konusunda yeterli değildir.[333]

Yukarıda teorik olarak incelenen durumu daha somut bir şekilde Libicki'nin örnek olay olarak verdiği ABD üzerinden incelersek, sahip olduğu konvansiyonel güç, Soğuk Savaş'ın hemen sonrasından 2000'li yılların başına kadar bu devletin karşısındaki devletin tepkisini önemsemeden küresel bir polis gibi davranmasına müsaade etmektedir. ABD için konvansiyonel anlamda ortaya çıkan bu durum siber uzayda geçerli değildir. Diğer boyutlarda sağladığı üstünlüğü bu alanda da sağlamak için ABD siber uzayda saldırı

[330] Libicki, op. cit., p.39.
[331] Ibid., p. 31.
[332] Bu duruma 1990'lı yıllar boyunca Türkiye-Yunanistan ilişkileri örnek verilebilir.
[333] Libicki, loc. cit..

kabiliyeti geliştirme noktasında büyük yatırımlarda bulunmaktadır.[334] Bu bağlamda ABD sistemlerinin yazılımları, en iyi mühendisler tarafından yazılmaktadır. Bunun yanında yazılım konusunda ABD dünyanın tek ithalatçısı konumundadır. Bu duruma karşın, ABD siber uzayda saldırıya açıktır. Zira Amerikan toplumunun özellikle de ağ merkezli muharebe yapan ABD ordusunun büyük ölçüde bilgi sistemlerine bağlı olduğu bilinmektedir. Oluşan bu bağlılık daha az gelişen ve daha az demokratik olan ülkelere karşın ABD'yi özel ve kamusal alanda saldırıya daha açık hale getirmektedir. Ayrıca Amerikan kurumları arasında güvenlik politikaları noktasında çok az benzerlik bulunmaktadır. Bu durum toplumu daha güçlü hale getirse de kurumların bağlantılarına zarar vermeyi kolaylaştırmaktadır. ABD ile gireceği çatışmadan konvansiyonel olarak zarar gören taraf eşitliği sağlamak adına siber karşılık verebilir. Diğer bir deyişle ABD, tüm avantajına rağmen karşı misillemeye uğrarsa düşmanlarından daha fazla zarar görecektir.[335] Nye'ın da belirttiği gibi diğer boyutların aksine bu boyutta bir gücün egemenliği siber uzayın doğası gereği mümkün değildir.

Libicki'ye göre uluslararası ilişkiler oyun teorileri çerçevesinden bakıldığında siber caydırıcılık işlevsel bir yöntem olarak görülmektedir. Soğuk Savaş boyunca ABD ile SSCB arasında yaşanan nükleer restleşmenin sağladığı tarihsel veriler siber caydırıcılığın da kullanılabilir olduğunu düşündürmektedir. Oysa ki siber uzayın doğası, bu tarihsel verilere rağmen bu alanda caydırıcılığın sağlanmasının sorgulanmasına neden olmaktadır. Libicki ortaya koyduğu üç temel ve altı destekleyici soru ile siber uzayın nükleer ya da kinetik caydırıcılıktan farkını ortaya koymaktadır. Ortaya konulan sorulara verilen cevaplarda siber uzayın doğası nedeniyle oluşan farklılık, kinetik yada nükleer silahların aksine siber caydırıcılığı sağlamanın problemlerini göstermektedir.[336] Nükleer caydırıcılığın temelini oluşturan ve siber caydırıcılıktan ayıran cevapları sağlayan üç temel soru incelendiğinde:

[334] Bu konuda ayrıntılı bilgi için bkz. Jim Wolf, "US says will boost its cyber arsenal", 7 November 2011, http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107 (E.T. 15.12.2014); Anthony Capaccio, "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion", 10 June 2013, http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html (E.T. 15.12.2014).
[335] Bu konuda ayrıntılı bilgi için bkz. Libicki, op. cit., pp. 31-32.
[336] Ibid., p .39

Libicki öncelikle Lupovici'nin, Nye'ın ve Goodman'ın ortaya koyduğu görüşlere benzer şekilde tespit/isnat problemine değinmek adına "*kimin yaptığını biliyor muyuz*?" sorusunu gündeme getirmektedir. Devletler misilleme yapmadan önce saldırı yapanın kim olduğunu açıkça bilmelidir. Misilleme durumu ortaya çıkmaksızın caydırıcılık işe yarayacaksa, saldırıda bulunacak devlet, caydırıcı devletin kendisine saldıran devletin kimliğinden emin olacağını bilmelidir. Saldırıda bulunan devlet yerine diğer bir devletin yanlış tespit neticesinde saldırıya uğraması sadece caydırıcılığın geçerliliğini ortadan kaldırmayacak aynı zamanda yeni düşmanların ortaya çıkmasına neden olacaktır. Libicki'nin ifadesiyle "*eğer masum olmak umursanmıyorsa neden masum olmalı*?" sorusu bağlamında muhtemel bir siber savaş yerine, kazayla saldırılan devletin de müdahil olmasıyla kendisini savunan devlet iki siber saldırıyla karşı karşıya gelecektir.[337]

Libicki ikinci olarak "*düşmanın varlığı risk altında tutulabilir mi*?" sorusunu ortaya atmaktadır. Goodman'ın özellikle Gürcistan Saldırısı sonrasında ölçeklenebilirlik konusundaki görüşlerine benzer görüşler Libicki'nin cevaplarında da yer bulmaktadır. Savaşta alınan zarar ve bu zararın hesaplanabilmesi çok yönlü bir konudur. Bu noktada siber uzayda saldırı ya da misilleme gerçekleşmeden önce, saldıran da hedef olan da saldırının doğurabileceği sonuçlar konusunda tam anlamıyla fikir sahibi olmayabilir. Saldırı sonrasında dahi saldıran ve özellikle saldırıya hedef olan devlet, hasarın boyutu noktasında emin olamayabilir. Bunun nedeni öncelikle saldıran devlet için olası yan etkilerin hesaplanamaması, saldırıya uğrayan devlet içinse saldırının ölçeklendirilmesinde yaşanan problemdir. Bu bağlamda bir petrol rafinerisini havaya uçurmak ve bu sayede bir yakıt kaynağının kullanılmasını engellemekle, rafineri kontrol sisteminde değişikliklere yol açan ve bu sayede yakıttaki kimyasal oranlarını değiştirerek araçlara zarar veren saldırılar yapmak aynı şey değildir.[338]

Libicki'nin ortaya koyduğu son soru ise "*yapılan saldırı tekrarlanabilir mi?*" şeklindedir. Misilleme her şeyden öte saldıran devlete karşı bir daha saldırı yapmasını engelleyecek bir güç gösterisidir. Eğer yapılan misilleme gelecekte olması muhtemel saldırılara karşı yapılacak misillemeleri engelleyecekse, caydırıcılık istenen sonuçları vermeyebilir. Konvansiyonel ya da nükleer silahlarla sağlanan caydırıcılıkta bu durum

[337] Ibid., p. 41.
[338] Ibid., p. 52.

herhangi bir problem teşkil etmemektedir. Hatta nükleer misilleme o kadar kötü etkiye sahiptir ki hiç kimse bu yönde bir girişimde bulunmazken bazılarında ise yapılan misilleme bir sonraki saldırıyı engellememektedir. Siber uzayda misillemenin tekrar ve tekrar kullanımı gerekli olabilir fakat her kullanım bir sonraki kullanımın beklenen sonuçlarını olumsuz yönde etkileyebilir. Bu durumun en önemli nedeni siber uzayda saldırıların sistemdeki yazılım açıklarına yapılıyor olmasıdır. Yapılan misilleme o ana kadar bilinmeyen bir açığı saldırıya uğrayan devlet açısından açığa çıkartır. Böyle bir durumda ortaya çıkan açık, yazılacak yamalarla hızla ortadan kaldırılabilir. Bu durum aynı yöntemle siber uzayda birden fazla saldırı yapmayı zorlaştırmakta hatta bazı durumlarda imkânsız kılmaktadır.[339]

Üç temel sorunun ardından Libicki ortaya koyduğu "*misilleme caydırıcılığı sağlamasa da silahsızlandırmayı sağlayabilir mi?*" sorusuyla Soğuk Savaş'ın son 20 yılında yaşanan gelişmelere benzer şekilde silahsızlanmanın olup olamayacağını tartışmaktadır. Yapılacak siber misilleme sadece caydırıcılık noktasında etkilidir. Konvansiyonel ve nükleer silahların aksine siber silahlar ise genel olarak saldırganın silahsızlandırılması noktasında etkisizdir. Bu durumda misilleme caydırıcılık etkisi doğuramıyorsa silahlansızlanmayı da sağlamayacağı için herhangi bir anlam taşımamaktadır.[340]

Libicki ikinci destekleyici soruyu "*üçüncü gruplar mücadeleye katılır mı?*" şeklinde oraya koymuştur. Çalışmamızda caydırıcılığın doğasını ayrıntılı olarak incelediğimiz bölümlerde de analiz edildiği üzere caydırıcı kapasite, en temelde saldırgan devlete yaptığı saldırının kendisine beklenmeyen sonuçlar doğurabileceğini gösteren bir mesajdır. Tarafların belli olmaması yani tespit/isnat alanında yaşanan problemler ve verilen ve/veya alınan hasarın tespitinde yaşanan ölçeklendirme sorunu yanlış algılamalara neden olabilmektedir. Saldıran taraf misilleme çekincesiyle siber uzayın olanaklarını kullanarak saldırıyı üçüncü bir aktör üzerinden gelecek şekilde kurgulayabilir. Üçüncü bir devlet içerisindeki devlet altı gruplarda beklenmeyen bir saldırı yaparak iki devlet arasındaki sürece müdahil olabilirler.[341]

[339] Ibid., p. 56.
[340] Ibid., p. 59.
[341] Ibid., p. 62.

"Misilleme tarafımıza doğru mesajı verir mi?" sorusuyla Libicki devlet ülkesi içindeki yapının önemini ortaya koymaktadır. Çalışmamızın kritik altyapılar başlığında incelediğimiz gibi liberal ekonomiye sahip ve gelişmiş devletlerin çoğunluğunda siber saldırılara hedef olan kritik altyapıların mülkiyeti ve işletmesinin bir kısmı devlete aitken bir kısmı da özel sektöre aittir. Özel sektör ve devlet arasında bölüşülmüş olan kritik altyapıların siber saldırılara hedef olması halinde halkın dikkatini çekme potansiyeli oldukça yüksektir. Buna karşın devlete ait gündelik hayata etkisi olmayan web sayfaları ve sistemlere yapılacak saldırılar ise halk için fazla bir önem arz etmemektedir. Daha önce belirttiğimiz gibi özel sektöre ait sistemlerin savunulması genellikle özel sektör tarafından yapılmaktadır. Bu yapılar üzerinde devletin dolaylı olarak uygulamaya koyacağı düzenlemeler ve kanuni zorlamalar dışında, doğrudan etkisi bulunmamaktadır. Özel sektöre ait sistemlerdeki açıkları hükümetler tespit etme şansına sahip değillerken, şirket sahipleri de bunları söyleme konusunda istekli değillerdir.[342]

Libicki'ye göre "saldırıya cevap vermek için bir eşik var mıdır?" sorusu da siber uzayda misilleme için büyük bir öneme sahiptir. Goodman'ın çalışmasında ortaya koyduğu siber uzayda ölçeklendirilebilirlik problemi misilleme için eşik belirlenmesi noktasında da önemli hale gelmektedir. Bu durum misilleme yapacak devlet için hem bir avantaj hem bir dezavantaj haline gelebilir. Örneğin bir devlet düşmanca tutumda bulunan saldırgan devlete karşı siber uzaydaki yeteneklerine zarar verdiği gerekçesiyle (bu durumun objektif olarak değerlendirilmesi oldukça zordur) misillemede bulunabilir. Böylece yetenekleri daha fazla zarar görmeden savunmacı devlet avantajlı konuma geçebilir. Gürcistan Saldırısı'nda olduğu gibi bu durumun aksinin yaşanması yani saldırının gerçekte olduğundan daha az hasara yol açtığının tespit edilmesi ise misillemeyi geciktireceği için dezavantajlı bir durum ortaya çıkarabilir.[343]

"Tırmanmadan kaçınılabilir mi?" sorusuyla Libicki siber caydırıcılıkla diğer enstrümanlarla sağlanan caydırıcılık arasındaki önemli bir farkın altını çizmektedir. İki taraf arasında nükleer caydırıcılığın söz sahibi olduğu bir olasılıkta, stratejistler misilleme durumunda nükleer silahların kullanımının ötesinde ne olacağını hesaplama ihtiyacı hissetmezler. Zira saldırgan devletlerin nükleer silahlarını kullandığı bir çatışmada bundan

[342] Ibid., p. 64.
[343] Ibid., p. 65.

fazla ne olabileceğini tartışmak mantıksızdır. Goodman'ın jeopolitik faktör olarak kavramsallaştırdığı şekilde siber caydırıcılığın kullanılması durumunda, sonrasında ne olacağı hesaplanmalıdır. Siber silahlarla yapılacak misilleme, kinetik hatta nükleer güç kullanarak karşılık verilebilecek bir çatışmaya dönüşebilir. Bu çerçevede ABD ve RF stratejik güvenlik yaklaşımlarında siber saldırıya karşı kinetik ya da farklı herhangi bir yöntemle karşılık verebileceklerini deklare etmişlerdir. Saldırgan devlet gerilimi tırmandırma noktasında eğer:

> *"1- Siber misillemenin hak edildiğine inanmıyorsa,*
>
> *2- İç kamuoyundan sert bir biçimde cevap verilmesi şeklinde baskı görüyorsa,*
>
> *3- Ya da siber misillemeye siber saldırıyla karşılık vermesi durumunda kaybedeceğine inanmıyorsa,"*

farklı enstrümanlarla cevap verebilir.[344] Bu durum siber caydırıcılığın jeopolitik olarak eşit güce sahip devletler arasında anlamlı olacağını aksi halde çok daha büyük çatışmalara yol açacağını göstermektedir.

"Saldırgan devlette vurmaya değer bir şey yoksa ne olur?" biçiminde formüle ettiği son destekleyici sorusuyla Libicki, siber saldırı kapasitesine rağmen, ağlanmışlık oranı düşük bir devletle ağlanmış bir devletin karşı karşıya geleceği bir senaryoyu ortaya koymaktadır. Libicki'nin örnek olarak incelediği ABD'nin karıştığı durumlarda tamamen simetrik bir savaş durumu mümkün değildir. Fakat siber savaş bu durumdan daha da asimetrik olabilir. ABD ekonomisi ve toplumundaki fazlasıyla ağlanmışlık ordusuna da yansımaktadır. Aksine saldırgan devlette ise karşılık olarak saldırılabilecek dijitallikte bir hedef bulunmayabilir, devlet bu ağları yeterince önemsemeyebilir ya da bu hedefler dış dünyaya bağlı olmayabilir. Örneğin Estonya'ya 2007'de yapılan DDOS saldırıları büyük bir şoka neden olmuşken, 2008'de Gürcistan'a yapılan saldırılar o kadar etkili olmamış, 2009'da Kırgızistan'a yapılan saldırılar ise neredeyse fark edilmemiştir.[345] ABD ve RF'nin ayni ile mukabele yerine geliştirdiği bu stratejinin temelinde Libicki'nin de belirttiği gibi nükleer ve konvansiyonel anlamda sağlanan caydırıcılığın, bu alanda tüm yatırım ve çalışmaya rağmen sağlanamaması/sağlanamayacağı gerçeği yatmaktadır.

[344] Ibid., p. 69.
[345] Ibid., p. 70.

Silahlanmanın tüm alanlarında olduğu gibi siber uzayda silahlanma noktasında da savunma yapısını geliştirmek, saldırıdan çok ekonomik güç, teknoloji ve emek gerektirmektedir. Siber saldırı noktasında ise diğer alanların aksine çift yönlü bir farklılık bulunmaktadır. Birinci olarak asgari düzeyde teknik imkânlar, konvansiyonel silahlanmanın aksine belli bir tekel ya da grubun elinde bulunmamaktadır ve edinilen imkânlar diğer devletler tarafından takip edilemeyebilmektedir. İkinci ve daha önemli olan farklılık ise siber uzayda teknolojik olarak en gelişmiş devletin siber saldırıya en müsait devlet olduğu gerçeğidir.

SONUÇ

Tez çalışmamızda ayrıntılı biçimde ele alınan "*nükleer caydırıcılık*" ve siber uzayda varlığı tartışılan "*siber caydırıcılık*" olguları karşılaştırıldığında, bazı farklılıklar ortaya çıkmaktadır. Bu farklılıkları şu başlıklar altında tespit etmek mümkündür:

- Aktör düzeyi,
- Etki kapasitesi,
- Tespit/isnat,
- Uluslararası denetim,
- Caydırıcılığı sağlamak için kapasitenin ifşası.

Bu başlıkları ayrıntılı bir biçimde açıklarsak nükleer caydırıcılığın etkin olarak kullanıldığı Soğuk Savaş boyunca ve sonrasında nükleer silah geliştirmenin maliyeti, geliştirilmesi sürecinde ihtiyaç duyulan disiplinlerarası bilgi, hammadde elde etmenin zorluğu gibi nedenlerle devletler dışında hiçbir aktör nükleer silaha sahip olmamıştır. Sadece kısıtlı sayıda devletin bilimsel ve ekonomik olarak geliştirme kapasitesine sahip olduğu nükleer silahlar, NPT gibi anlaşmaların etkisiyle günümüzde dahi sadece dokuz devletin askeri kapasitesi içerisinde bulunmaktadır. Siber uzayda ise sadece devletler değil, bireylerden çokuluslu şirketlere kadar geniş bir yelpazede aktörler varlık gösterebilmektedir. Siber uzayda kapasite geliştirmek için bu alanda yetişmiş insan gücü ve her bireyin kısıtlama olmaksızın satın alabileceği teknik ekipman dışında herhangi bir ihtiyaç bulunmamaktadır.

Nükleer caydırıcılık ile siber caydırıcılık arasındaki bir diğer temel farklılık da etki kapasitelerindedir. Bilindiği üzere nükleer silahlar, kullanılan birim başına en fazla yıkım kapasitesine sahip olan silahlardır. Hidrojen bombasının üretilmesinin ardından tek nükleer silahla bir şehri haritadan silmek mümkün hale gelmiştir. Siber silahların ise etki kapasitesi her geçen gün büyüse de verilen zarar çoğu zaman ikincil ekonomik kayıplar ve kaybedilen veridir. STUXNET Saldırısı ile siber uzay üzerinden fiziki zarar vermenin önü açılmış olsa da nükleer silahlar ile kıyaslanabilecek bir potansiyel, yakın gelecekte mümkün gözükmemektedir.

Saldırıda bulunan aktörün tespiti/isnati da caydırıcılığı sağlamak adına oldukça önemlidir. Verilen zararın bedelinin ödetilmesi ancak düşmanın kimliğinin bilinmesi ile mümkündür. Sadece dokuz devletin nükleer silaha sahip olduğu ve nükleer silahların geri dönülemeyecek savaşa yol açacak bir krizde kullanılabilecek kadar büyük bir etkiye sahip olduğu göz önünde bulundurulduğunda, failin tespiti oldukça kolaylaşmaktadır. Siber uzayda ise durum nükleer alanla kıyas kabul etmeyecek biçimde farklıdır. Her bireyin siber silah geliştirebilecek bir aktör olabileceği bu boyutta, failin kendini gizlemesi siber uzayın doğasının yardımıyla oldukça kolaydır. Çünkü siber uzayda aktörler gerçek kimlikleri ile değil IP adresleriyle var olmaktadır. IP adreslerini ise gizlemek oldukça kolay olduğu gibi köle bilgisayarlara saldırıyı yaptırarak failin suçu başka bir aktör üzerine atması da mümkündür.

Nükleer alanda enerji üreten tesislerden, enerji üretimi sonrası çıkan radyoaktif atık maddeye, nükleer bomba imalatı için uranyum zenginleştirme çalışmalarından, nükleer bomba geliştirme sürecine kadar ilgili tüm alanlar farklı kurumların uluslararası denetimi altındadır. Nükleer silahların yayılmasını engellemeyi amaçlayan NPT, çalışmamızda değindiğimiz nükleer denemeleri kısıtlayan birçok anlaşma ve nükleer silaha sahip devletlerin SALT I ve SALT II sonrası yaptığı anlaşmalar bu alanda kısıtlamaların ve denetimin oluşmasını sağlamıştır. Günümüzde özellikle BM bünyesinde faaliyet gösteren Uluslararası Atom Enerjisi Ajansı nükleer alandaki faaliyetlerin barışçıl olarak sürdürülmesini sağlamaya çalışmaktadır. Bu konuda aksi yönde görüşler oluşturan Saddam Dönemi Irak ve İran gibi devletlere karşı BM Güvenlik Konseyi yaptırım kararları almaktadır. Siber uzayda ise siber silahların saklanması için askeri tesisler yada füze silolarına ihtiyaç yoktur. Siber silahlar küçük yazılımlar olduğu için denetimini yapmak, uluslararası kontrol mekanizmaları kurarak siber silah geliştirme faaliyetlerini engellemek mümkün değildir. Bilinen en güçlü siber silah olarak kabul edilebilecek STUXNET dahi sadece 500kb gibi küçük bir alan işgal etmektedir.

Son olarak ele alınması gereken temel farklılık ise caydırıcılığı çatışma gerçekleşmeden sağlamak amacıyla (ödetilecek maliyet doğrultusunda) askeri kapasite ve ilişkili yapıların belli bir oranda ifşa edilmesidir. Nükleer alanda bu durumu gerçekleştirmenin en kolay yolu üretilen bir ya da birkaç nükleer silahın kontrollü ortamda denenmesidir. Bu denemelerin yaydığı radyoaktivite ya da sismik dalgalar gibi sonuçlar,

caydırılacak unsura nükleer silaha sahip olunduğu mesajını vermektedir. Nükleer silaha sahip olduğu bilinen devletler ise denemeler dışında etkili bir iletim aracı olan füze kapasitesini cephaneliklerinden çıkararak özel günlerde yapılan geçit törenleri aracılığıyla ifşa etmektedir. Siber uzaya gelindiğinde ise çalışmamızda daha önce de değindiğimiz gibi her siber silah, sistemlerdeki varlığı bilinmeyen yazılımsal açıkları kullanmaktadır. Bu bağlamda siber silahın ifşası aynı zamanda siber silahın hedefi olan sistemlerdeki yazılımsal açıklarında ortaya çıkması anlamına gelmektedir. Ortaya çıkan açıkların yapılacak sürüm yükseltmeleri ve yamalarla kapatılması ise yatırım ve zaman kullanılarak geliştirilen siber silahı bir daha kullanılamayacak hale getirecektir. Bu bağlamda siber kapasitenin caydırıcı olmasının tek yolunun daha önce yapılan siber saldırıların üstlenilmesi yoluyla bu doğrultuda bir kapasite geliştirildiğinin kanıtlanması olduğu iddia edilebilir.

Sonuç olarak, nükleer caydırıcılık üzerinden yapılacak bir analojiyle siber silahlarla sağlanması düşünülen siber caydırıcılığı anlamak mümkün değildir. Bu iki yaklaşım arasında aktör düzeyi, etki düzeyi, denetim düzeyi arasında bulunan büyük farklılıklar kıyaslama yapmayı engellemektedir. Siber uzay ve bunun sonucunda devletlerin sağlamayı hedefledikleri siber caydırıcılık, Soğuk Savaş sonrası dönemin koşulları ve oluşturduğu güç dağılımı içerisinde değerlendirilmelidir. Devletlerin arasında gücün yatay olarak değiştiği sistemde mantıklı ve çözüm odaklı görünen yaklaşımlar, farklı seviyelerde aktörlerin bulunduğu ve gücün hem yatay hem de dikey olarak el değiştirdiği sistemde etkili olmaktan uzaktır. Aktör seviyesinde nükleer silahlarla tek katmanda sağlanan caydırıcılık yerine siber uzayda her aktör seviyesine ve farklı aktör seviyelerinin ortak olarak hareket ettiği melez ara seviyelere karşı, farklı caydırıcılık yaklaşımları gerekmektedir. Bu çok katmanlı yaklaşımların ise her katmanda etkinliği farklı düzeyde olacaktır. Örneğin devletlerarası düzeyde siber uzay üzerinden verilecek caydırıcı bir mesaj, yaşanacak uyuşmazlıkta konvansiyonel ya da nükleer seviyelerde bir caydırıcı mesajla karşılaşması durumunda oldukça etkisiz kalacaktır.

Konu bağlamından vurgulanması gereken son husus ise çalışmanın bitirildiği Temmuz 2015 tarihi itibariyle siber uzayın gelişiminin büyük bir hızla devam etmekte olduğudur. ABD, RF, ÇHC, Fransa, Birleşik Krallık gibi nükleer silah sahibi devletler ise bahse konu olan gelişimin ortaya konmasında başı çekmektedir. Bu devletler nükleer

alandaki üstünlüklerini siber uzay üzerinde de sürdürmeye çalışmakta bu şekilde geleceği şekillendirerek uluslararası sistemdeki güçlü varlıklarını koruma amacını gütmektedirler. İsrail, Hindistan, İran, Estonya gibi devletler ise ekonomik çıkar ya da STUXNET gibi saldırılara karşı güvenliklerini sağlamak amacıyla bu alanda yetişmiş insan gücü oluşturmaktadır.

Günümüzde gücün temelini oluşturan askeri kapasite biyolojik insan gücünden çok teknolojiye dayanmaktadır. Teknoloji geliştirmek içinde devletler yetişmiş insan gücünü ortaya çıkarmalı ve bu gücü ekonomik olarak desteklemelidir. Yukarıda iki grup olarak verilen devletler arasında yaşanan rekabetin temelinde ise güvenlik ihtiyacı kadar bahsedilen bu ekonomik gücün paylaşılması yatmaktadır. Yaşanan rekabet ve ortaya çıkan gelişim üzerinden siber uzayda kapasite geliştiren devletler yeni çözümler üretmeye çalışmaktadır. İçinde bulunduğumuz zamanda gelişen bu süreçte ise beşinci boyut olarak kabul edilen siber uzayın uluslararası ilişkiler içerisinde nasıl konum alacağına dair belirsizlikler bulunmaktadır. Bu alanda devletler arasında ittifak ilişkileri yeni oluşmaya başlamıştır. Örneğin ABD, Asya bölgesinde Singapur, Malezya ve Vietnam'la siber ittifak ilişkileri kurmayı planlamaktadır.[346] ÇHC ve RF ise aralarında imzaladıkları anlaşma ile birbirlerine siber operesyon düzenlememeyi kabul etmektedir.[347] Çalışmamızın sınırları içerisinde bulunmasa da bu alanların incelenmesi sonrasında ortaya çıkacak sonuçlar siber uzayın anlaşılması açısından bizce büyük öneme sahiptir.

[346] "Quadrennial Defense Review 2014", *United States of America Deparment of Defence*, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (E.T. 14.05.2015)
[347] Olga Razumovskaya, "Russia and China Pledge Not to Hack Each Other", *Wall Street Journal*, 8 Mayıs 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/ (E.T. 14.05.2015)

KAYNAKLAR

Kitaplar

AKAD Mehmet Tanju, *Askeri Tarihte Stratejik Düşünce*, 2. Basım, İstanbul: Türkiye İş Bankası Yayınları, Şubat 2014.

AKAD Mehmet Tanju, *Modern Savaşın Temel Kavramları*, 1. Baskı, İstanbul: Kitap Yayınevi, 2011.

ALDRICH Richard, "Intelligence", Saki D. Dockrill and Geraint Hughes(edt.), *Palgrave Advances in Cold War History*, USA: PALGRAVE MACMILLAN, 2006.

ARI Tayyar, *Irak, İran, ABD ve Petrol*, Güncellenmiş 2. Baskı, Bursa: Alfa, 2007.

ARI Tayyar, *Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İşbirliği*, 8. Baskı, Bursa: MKM, 2013.

ARI Tayyar, *Uluslararası İlişkiler ve Dış Politika*, 7 Baskı, Bursa: MKM, 2008.

ARMAOĞLU Fahir, *20. Yüzyıl Siyasi Tarihi 1914-1980*, Ankara: Türkiye İş Bankası Kültür Yayınları, 1983.

ARNESON Richard J. (edt.), *Liberalism Volume I*, Great Britain: Edward Elgar, 1992.

BRIGHT Christopher John, "U2 Incident", James R. Arnold and Roberta Wiener(edt.), *Cold War The Essential Reference Guide*, USA: ABC-CLIO, 2012.

BRODIE Bernard, *Strategy In The Missile Age*, New Jersey: Princeton University Press, 15 January 1959.

BROWN Chris and AINLEY Kirsten, *Understanding International Relations* Third Edition, Palgrave Macmillan, 2005.

BURCHILL Scott et. al., *Uluslararası İlişkiler Teorileri*, çev. Ali Aslan – Muhammed Ali Ağcan, 2. Baskı, İstanbul: Küre Yayınları.

CHAN Steve, *International Relations in Perspective*, Macmillan Publishing Company.

EPLEY William W., *America's First Cold War Army 1945-1950,* The Institute of Land Warfare Association Of The United States Army, 1999, pp. 9-10. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA383639 (E.T. 10.04.2015).

ERHAN Çağrı, "ABD ve NATO'yla İlişkiler", Baskın Oran (ed.), *Türk Dış Politikası, Kurtuluş Savaşından Bugüne Olgular, Belgeler, Yorumlar, Cilt I.,* 13 Baskı, İstanbul: İletişim, 2008.

FREEDMAN Lawrance, *The Cold War*, London: Cassel & Co, 2001.

FREEDMAN Lawrance, *The Evolution of Nuclear Strategy,* Third Edition, New York: Palgrave Macmillan, 2003.

GERGER Haluk, *Soğuk Savaş'tan Yumuşama'ya*, 1. Baskı, Ankara: Işık Yayıncılık, 1980.

GRIFFITHS Martin, ROACH Steven C. vd., *Uluslararası İlişkilerde Temel Düşünürler ve Teoriler,* çev. CESRAN, İkinci Basımdan Çeviri, Ankara: Nobel Yayınevi, 2011.

HERSHBERG James G., "The Cuban Missile Crisis", Melvyn P. Leffler and Odd Arne Wasted(edt.), *The Cambridge History of Cold War, Volume II Crises and Detente*, New York: Cambridge University Press, 2010.

HOBBES Thomas, *Leviathan*, 7. Baskı, İstanbul: Yapı Kredi Yayınları, 2008.

HOLSTI K. J., *International Politics A Framework for Analysis,* Prentice-Hall International, Seventh Edition, 1995.

İŞYAR Göksel, *Karşılaştırmalı Dış Politikalar Yöntemler Modeller Örnekler ve Karşılaştırmalı Türk Dış Politikası*, 1 Baskı, Bursa: Dora Yayınevi, 2009, ss. 605-608.

JACKSON ROBERT and SORENSON Georg, *Introduction to International Relations*, Oxford University Press, 1999.

KARACA R. Kutay, *Çin Halk Cumhuriyeti'nin Orta Doğu ve Orta Asya Politikaları ve Bu Politikaların Türkiye'ye Muhtemel Etkileri*, Ankara: SAREM Yayınları, 2006.

KANT Immanuel, *Ebedi Barış Üzerine Felsefi Deneme,* Çev. Yavuz Abadan – Seha L. Meray, Ankara, 1960.

KUGLER Richard, "Deterrence of Cyber Attacks", Franklin D. Kramer (edt), Stuart H. Starr (edt), Larry Wentz (edt), *Cyber Power and National Security*, National Defence University Press, 2009, pp. 309-342, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf (E.T. 31.10.2014).

LEITENBERG Milton, *Studies of Military R&D and Weapons Development*, Case Study 3 The Origin of MIRV, http://fas.org:8080/man/eprint/leitenberg/index.html

LIBICKI Martin C., *Cyber Deterrence and Cyber War*, Rand Corparation, 2009, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (E.T. 31.10.2014).

LOCKE John, *Two Treaties of Government and A Letter Concerning Toleration*, Ian Shapiro (ed.), New Haven and London: Yale University Press, 2003.

MACHIAVELLI Niccolo, *Hükümdar*, Çeviren: Semih Lim, 1. Baskı, İstanbul: Türkiye İş Bankası Kültür Yayınları, 2008.

MEARSHEIMER J. J., "Structural Realism", Tim Dunne, Milja Kurki, Steve Simith, *International Relations Theories Discipline and Diversity*, Second Edition, Oxford University Press.

MEARSHEIMER John J., *The Tragedy of Great Power Politics*, New York: W. W. Norton & Company, 2003.

MORGENTHAU Hans J., *Politics Among Nations: The Struggle for Power and Peace*, Fifth Edition, Revised, New York: Alfred A. Knopf, 1978.

MORGENTHAU Hans J., *Politics Amongs Nations The Struggle For Power And Peace*, First Edition, New York: Alfred A. Knoph, 1948.

NASH Philip, "Bear Any Burden? John F. Kennedy and Nuclear Weapons", Jonhn Lewis Gaddis Philip Gordon, Enrnest May, Jonathan Rosenberg(edt.), *Cold War Statesman Confront The Bomb Nuclear Diplomacy Since 1945*, New York: Oxford University Press, 1999.

NYE JR Joseph S., *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School , http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (E.T. 31.10.2014).

ODOM William E., *The Collapse of the Soviet Military*, Yale University Press, 1998.

ÖZDAL Barış, *Avrupa Birliği Siyasi Bir Cüce, Askeri Bir Solucan mı? Ortak Dış Politika ve Güvenlik Politikası ile Ortak Güvenlik ve Savunma Politikası Oluşturma Süreçlerinin Tarihsel Gelişimi*, 1. B., Dora Yayınları, Bursa, 2013.

ÖZDEN Nezihi, *Nükleer Çağın İlk 40 yılı*, Cilt 1, İstanbul: İ.T.Ü. Nükleer Enerji Enstitüsü Genel Yayınları No. 17, 1983.

PİRİNÇÇİ Ferhat, *Silahlanma ve Savaş*, 1. Baskı, Bursa: Dora Yayınları.

REÇBER Kamuran, *Avrupa Birliği Hukuku ve Temel Metinleri*, 2. Baskı, Bursa: Dora Yayınları, 2013

REESE Roger R., *The Soviet Military Experience*, Routladge, 2001.

ROBERRA Priscilla, "Cuban Missile Crisis", James R. Arnold and Roberta Wiener(edt.), *Cold War The Essential Reference Guide*, USA: ABC-CLIO, 2012.

ROUSSEAU Jean Jacques, *Discourse on Political Economy and The Social Contract*, New York: Oxford University Press, 1999.

SANDER Oral, *Siyasi Tarih 1918-1994*, 8. Baskı, Ankara: İmge Kitabevi, 2000.

SINGER J. David, *Deterrence, Arms Control, and Disarmament*, Columbus, Ohio University Press, 1962.

SIRICUSA Joseph, *Nuclear Weapons A Very Short Introduction*, Oxford University Press, 2008.

SPALDING Elizabeth Edwards, *The First Cold War Warrior Harry Truman, Containment,and the Remaking of Internationalism*, USA: The University Press of Kentucky, 2006.

STARR Stuart H., "Towards an Evolving Theory of Cyber Power ", *The Virtual Battlefield: Perspectives on Cyber Warfare*, Eds. C. Czosseck and K. Geers, Ios Press, 2009.

STEWERT Richard W. (Gen. Edi.), *American Military History Volume II The United States Army In A Global Era, 1917-2008*, Second Edition, Washington: Center of Military History United States Army, 2010.

TURAN Sibel, USTA Yasin, "Küresel Ve Bölgesel Nükleer Güçlerin Kıskacında Orta Asya", *ISSA II. Uluslararası Sosyal Bilimler Kongresi Kongre Kitabı*, Kocaeli: Kocaeli Üniversitesi Yayını, 2009, pp. 874-892.

UÇAROL Rifat, *Sayasi Tarih [1789-2012]*, Gözden Geçirilmiş ve Genişletilmiş 9. Basım, İstanbul: Der Yayınları, 2013.

VASQUEZ John A., *The Power of Power Politics*, UK: Cambridge University Press, 1998.

VIOTTI Paul R. and KAUPPI Mark V., *International Relations Theory*, Longman, 2010.

WALLACE Robert, MELTON H. Keith, *CIA Kendini Anlatıyor Casusluk*, Çev. Algan Sezgintüredi, 1. Baskı, İstanbul: NTV Yayınları, Aralık 2010.

WILBARKA James H., "Bay of Pigs", James R. Arnold and Roberta Wiener(edit.), *Cold War The Essential Reference Guide*, USA: ABC-CLIO, 2012.

ZUBOK Vladislav M. and HARRISON Hope M., "The Nuclear Education of Nikita Khrushchev", Jonhn Lewis Gaddis Philip Gordon, Enrnest May, Jonathan Rosenberg(edt.), *Cold War Statesman Confront The Bomb Nuclear Diplomacy Since 1945*, New York: Oxford University Press, 1999.

ZUBOK Vladislav M., *A Failed Empire: The Soviet Union In The Cold War From Stalin To Gorbachev*, USA: The University of North Coralina Press, 2007.

Makaleler

AKGÜL-AÇIKMEŞE Sinem, "Algı mı, Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri", *Uluslararası İlişkiler*, Cilt 8, Sayı 30 (Yaz 2011), ss. 43-73.

BAYLIS John, "Uluslararası İlişkilerde Güvenlik Kavramı", çev. Burcu Yavuz, *Uluslararası İlişkiler*, Cilt 5, Sayı 18 (Yaz 2008), s. 70.

BİLGİÇ Ali, ""Güvenlik İkilemi"ni Yeniden Düşünmek: Güvenlik Çalışmalarında Yeni Bir Perspektif", *Uluslararası İlişkiler*, Cilt 8, Sayı 29 (Bahar 2011), ss.123-142.

BUZAN Barry, "Askeri Güvenliğin Değişen Gündemi", *Uluslararası İlişkiler*, Çev. Burcu Yavuz, Cilt 5, Sayı 18 (Yaz 2008), ss. 107-123.

DENNING Dorothy E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", *The Computer Security Journal*, Vol. XVI, No. 3, Summer 2000, pp. 6-7. http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf (E.T. 10.04.2014).

DEVLEN Balkan ve ÖZDAMAR Özgür , "Uluslararası İlişkilerde İngiliz Okulu Kuramı: Kökenleri, Kavramları ve Tartışmaları", *Uluslararası İlişkiler*, Cilt 7, Sayı 25 (Bahar 2010), ss. 43-68.

DULLES John Foster, "Policiy For Security and Peace", *Foreign Affairs*, Vol. 32, April 1954, No. 3., pp. 353-364.

ERHAN Çağrı, "Ortaya Çıkışı ve Uygulanışıyla Marshall Planı", *Ankara Üniversitesi SBF Dergisi*, Cilt: 51, Sayı:1, 1996, ss. 275-287.

GOODMAN Will, "Cyber Deterrence: Tougher in Theory than in Practice?", *Strategic Studies Quarterly*, Fall 2010, pp. 102-135, http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf (E.T. 31.10.2014).

GRAYBAR Lloyd J., " The 1946 Atomic Bomb Test: Atomic Diplomacy or Bureaucratic Infighting?", *The Journal of American History*, Vol. 72, No. 4, March 1986, pp. 888-907.

KARAOSMANOĞLU Ali L., "Nükleer Stratejinin İlk On Yılı", *Ankara Üniversitesi SBF Dergisi*, Cilt: 51, Sayı:1, 1996, ss. 323-345.

KAVUNCU Sibel, "Nükleer Silahsızlanma Yolunda Start Süreci", *Bilge Strateji*, Cilt 5, Sayı 8, Bahar 2013, ss.119-148.

KENNAN(X) George, "The Sources of Soviet Conduct", *Foreign Affairs*, July 1947, Vol. 25, Issue. 14, pp. 566-582, http://www.foreignaffairs.com/articles/23331/x/the-sources-of-soviet-conduct (E.T. 10.04.2015).

LUPOVICI Amir, "Cyber Warfare and Deterrence: Trends and Challanges in Research, *Military and Strategic Affairs*, Volume 3, No: 3, December 2011, pp. 49-62, http://www.inss.org.il/uploadimages/Import/%28FILE%291333533336.pdf (E.T. 31.10.2014).

MORGAN Patrick M., "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm", *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*, Committee on

Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council, 2010, pp. 55-76, http://www.nap.edu/openbook.php?record_id=12997&page=55 (E.T. 31.10.2014).

NITZE Paul H., "Assuring Strategic Stability in on Era of Detanté", *Foreign Affairs*, Vol. 54, January 1976, No. 2., pp. 207-232.

NORRIS Robert S. and KRISTENSEN Hans M., "Global nuclear weapons inventories, 1945–2010", *Bulletin of the Atomic Scientists*, July 2010, Volume 66, Issue 4, pp. 77-83, http://bos.sagepub.com/content/66/4/77.full.pdf+html (E.T. 10.04.2015).

NYE JR Joseph S., "Nuclear Lessons for Cyber Security", *Strategic Studies Quarterly*,Winter 2011, pp. 18-38, http://www.au.af.mil/au/ssq/2011/winter/nye.pdf (E.T. 31.10.2014).

OLEYNIKOV Pavel V., "German Scientists in the Soviet Atomic Project", *The Nonproliferation Review*, Summer 2000, pp. 1-30, http://cns.miis.edu/npr/pdfs/72pavel.pdf (E.T. 10.04.2015)

OPPENHEIMER J. R., "Atomic Weapons", *Proceedings of the American Philosophical Society*, Vol. 90, No. 1, Symposium on Atomic Energy and Its Implications (Jan., 1946), pp. 7-10.

ÖZDAL Barış ve JANE Murat, ""La Der Des"'in Uluslararası Sistemin Yapısına Etkileri", *Gazi Akademik Bakış*, Cilt: 7, Sayı: 14, Yaz 2014, pp. 215-245.

SCHWARTZ Michael I., "The Russian-A(merican) Bomb: The Role of Espionage in the Soviet Atomic Bomb Project", *Journal of Undergraduate Science, Summer 1996, pp. 103-108*, http://www.hcs.harvard.edu/~jus/0302/schwartz.pdf (E.T. 10.04.2015)

VINER Jacob, "The Implications of the Atomic Bomb for International Relations", *Proceedings of the American Philosophical Society*, Vol. 90, No. 1, Symposium on Atomic Energy and Its Implications (Jan. 1946), pp. 53-58.

WAEVER Ole, "Toplumsal Güvenliğin Değişen Gündemi", *Uluslararası İlişkiler*, Çev. Birgül Demirtaş Coşkun, Cilt 5, Sayı 18 (Yaz 2008), s. 151-178.

WOHLSTETTER Albert, "The Delicate Balance of Terror", *Foreign Affairs*, Vol. 37, January 1959, No. 2., pp. 211-234, http://www.rand.org/about/history/wohlstetter/P1472/P1472.html (E.T. 10.04.2015).

Diğer Kaynaklar

"A short history of NATO", http://www.nato.int/history/nato-history.html (E.T. 10.04.2015).

"ABM Treaty Fact Sheet", White House Press Secretary, http://2001-2009.state.gov/t/ac/rls/fs/2001/6848.htm (E.T. 10.04.2015).

"About Cyber Defence Centre", https://ccdcoe.org/about-us.html, (E.T. 07.04.2014).

"Action Plan on Information Security Measures for Critical Infrastructures", Information Security Policy Council, 13.11.2005, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf (E.T. 06.02.2014).

"Address To The Nation On Defense And National Security", http://www.atomicarchive.com/Docs/Missile/Starwars.shtml (E.T. 10.04.2015).

"Advanced Persistent Threats: A Brief Description", https://www.damballa.com/advanced-persistent-threats-a-brief-description/ (E.T. 10.04.2014).

"Advanced Persistent Threats: A Symantec Perspective Preparing the Right Defense for the New Threat Landscape", Symantec Report, http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (E.T. 10.04.2014).

"Atoms for Peace Speech", 20 October 2014, https://www.iaea.org/about/history/atoms-for-peace-speech (E.T. 31.10.2014).

"B-47 Stratojet", http://www.boeing.com/boeing/history/boeing/b47.page (E.T. 10.04.2015).

"B-50 Bomber", http://www.boeing.com/boeing/history/boeing/b50.page (E.T. 10.04.2015).

"Ballistic Missile Basics", Federation of American Scientist, http://fas.org/nuke/intro/missile/basics.htm (E.T. 10.04.2015).

"Bilgisayar virüsü nedir?", http://www.microsoft.com/tr-tr/security/pc-security/virus-whatis.aspx (E.T. 10.04.2014).

"Botnet nedir?", http://www.microsoft.com/tr-tr/security/resources/botnet-whatis.aspx (E.T. 10.04.2014).

"Can The President Switch Off The İnternet? Critics Fear New Executive Order Hands Obama Too Much Control Over The Web", *Daily Mail*, 12.07.2012, http://www.dailymail.co.uk/news/article-2172350/Can-president-switch-internet-Critics-fear-new-executive-order-hands-Obama-control-web.html (E.T. 06.02.2014).

"Cisco, 2014 Annual Security Report", Cisco, p. 21. "https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf (E.T. 10.04.2014).

"Computer Virus Information", http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses (E.T. 10.04.2014).

"Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space", *NATO Cooperative Cyber Defence Centre of Excellence*, http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf (E.T. 06.02.2014).

"Convention of International Information Security (Consept), *MFA of Russia*, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument (E.T. 06.02.2014).

"Council Directive 2008/114/EC Of 8 December 2008 On The Identification And Designation Of European Critical Infrastructures And The Assessment Of The Need To Improve Their Protection".

"Creatıon Of Nuclear Center, Arzamas-16", http://www.sarovlabs.com/history_sarov_nc/ (E.T. 10.04.2015).

"Cruise Missiles", Federation of American Scientist, http://fas.org/nuke/intro/cm/index.html (E.T. 10.04.2015).

"Cyber Espionage Against Georgian Government", Ministry of Justice of Georgia, http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf (E.T. 07.04.2014).

"Cyber Security Strategy for Germany", *Federal Ministry of the Interior*, February 2011, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (E.T. 06.02.2014).

"Cyber Security Strategy of the United Kingdom Safety, Security and Resilience in Cyber Space", *Cabinet Office*, June 2009, http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (E.T. 06.02.2014).

"Edward Snowden Interview: The NSA and Its Willing Helpers", *Der Spiegel*, 08.07.2013, http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html (E.T. 07.04.2014).

"Enrico Fermi – Biographical", http://www.nobelprize.org/nobel_prizes/physics/laureates/1938/fermi-bio.html (E.T. 10.04.2015).

"Enrico Fermi (1901 - 1954)", http://www.atomicarchive.com/Bios/Fermi.shtml (E.T. 10.04.2015).

"Enrico Fermi and the First Self-Sustaining Nuclear Chain Reaction", Research and Development of the U. S. Depertment of Energy, http://www.osti.gov/accomplishments/fermi.html (E.T. 10.04.2015).

"Ernest Rutherford – Biographical", http://www.nobelprize.org/nobel_prizes/chemistry/laureates/1908/rutherford-bio.html (E.T. 10.04.2015).

"Espionage And The Manhattan Project (1940-1945)", U. S. Department of Energy- Office of History and Heritage Resources, https://www.osti.gov/manhattan-project-history/Events/1942-1945/espionage.htm (E.T. 10.04.2015).

"Estonia Hit by 'Moscow Cyber War", 17.05.2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm (E.T. 05.04.2014).

"Executive Order -- Assignment of National Security and Emergency Preparedness Communications Functions", The White House, 06.07.2012, http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness- (E.T. 06.02.2014).

"Executive Order -- Improving Critical Infrastructure Cybersecurity", The White House, 12.02.2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (E.T. 06.02.2014).

"Exposing One of China's Cyber Espionage Units", Mandiant Report, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (E.T. 10.04.2014).

"Farm Hall Transcripts", 6 Ağustos 1945, http://www.aip.org/history/heisenberg/p11a.htm (E.T. 10.04.2015).

"FireEye Advanced Threat Report: 2013", FireEye, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf (E.T. 10.04.2014).

"GBU-43/B 'Mother of All Bombs' MOAB- Massive Ordnance Ait Blast Bomb", 07. 07. 2011, http://www.globalsecurity.org/military/systems/munitions/moab.htm (E.T. 15.12.2014).

"Georgia Cyber Warfare", 09.08.2008, http://rbnexploit.blogspot.com.tr/2008/08/rbn-georgia-cyberwarfare.html (E.T. 07.04.2014).

"Green Paper On A European Programme For Critical İnfrastructure Protection", *Commission Of The European Communities,* 17.11.2005, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576 (E.T. 06.02.2014).

"Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection", U.S. Department of Homeland Security, 17. 11. 2013, https://www.dhs.gov/homeland-security-presidential-directive-7#1 (E.T. 06.02.2014).

"How Are Email Viruses Still So Effective?: Lessons We Can Learn from the "Here you have" Worm", 16.09.2010, http://www.pctools.com/security-news/email-viruses-here-you-have-worm/ (E.T. 10.04.2014).

"Information Security Doctrine of the Russian Federation", *MFA of Russia*, 29.12.2008, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument (E.T. 06.02.2014).

"Information Security Strategy for Protecting the Nation", *National Center of Incident Readiness and Strategy for Cyber Securtiy*, 11 May 2010, http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf (E.T. 06.02.2014).

"Information Systems Defence Security France's Strategy", *Premier Ministre Agence Nationale de la Sécurité des Systémes d'Information*, February 2011, http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (E.T. 06.02.2014).

"Interim Agreement Between The United States Of America And The Union Of Soviet Socialist Republics On Certain Measures With Respect To The Limitation Of Strategic Offensive Arms", 26 May 1972, http://fas.org/nuke/control/salt1/text/salt1.htm (E.T. 10.04.2015).

"International Strategy For Cyberspace Prosperity, Security, and Openness in a Networked World", *The White House*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (E.T. 06.02.2014).

"Internet Growth Statistics", http://www.internetworldstats.com/emarketing.htm (E.T. 20.03.2014).

"Iran Accuses Siemens Over Stuxnet Cyber Attack", *The Telegraph*, 17.04.2013, http://www.telegraph.co.uk/technology/news/8457658/Iran-accuses-Siemens-over-Stuxnet-cyber-attack.html (E.T. 07.04.2014).

"Iran Denies Bushehr Hit By 'Stuxnet'", *Arab Times*, 21.04.2015, http://www.arabtimesonline.com/NewsDetails/tabid/96/smid/414/ArticleID/159995/reftab/96/Default.aspx (E.T. 07.04.2014).

"Iran Denies Nuclear Setback from Stuxnet Virus" *CBS News*, 23.11.2010, http://www.cbsnews.com/news/iran-denies-nuclear-setback-from-stuxnet-virus/ (E.T. 07.04.2014).

"Iran Denies Stuxnet Disrupted İts Nuclear Programme", *BBC News*, 24.11.2010, http://www.bbc.co.uk/news/technology-11821011 (E.T. 07.04.2014).

"John Kerry: Cyber threats are 'modern-day nuclear weapons' ", 25 January 2013, http://www.infosecurity-magazine.com/view/30438/john-kerry-cyber-threats-are-modernday-nuclear-weapons (E.T. 31.10.2014).

"Kaspersky Lab Provides İts Insights On Stuxnet Worm", 24.09.2010, http://www.kaspersky.com/news?id=207576183 (E.T. 07.04.2014).

"Kennan and Containment, 1947", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/kennan (E.T. 10.04.2015).

"Marshall Plan, 1948", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/marshall-plan (E.T. 10.04.2015).

"Microsoft Güvenlik Bülteni MS10-046", 02.08.2010, http://technet.microsoft.com/en-us/security/bulletin/ms10-046 (E.T. 07.04.2014).

"Microsoft Güvenlik Bülteni MS10-061", 14.09.2010, http://technet.microsoft.com/en-us/security/bulletin/MS10-061 (E.T. 07.04.2014).

"National Cyber Security Strategies in the World", *European Union Agency for Network and Information Security*, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (E.T. 06.02.2014).

"National Security Act of 1947", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/national-security-act (E.T. 10.04.2015).

"NSC 162/2: A Report to National Securtiy Council", http://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf (E.T. 10.04.2015).

"NSC-68, 1950", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/NSC68 (E.T. 10.04.2015).

"Otto Hahn" Atomic Heritage Foundation, http://www.atomicheritage.org/profile/otto-hahn (E.T. 10.04.2015).

"Partial Bibliography of the Internet/Arpanet", http://www.darpa.mil/About/History/PARTIAL_BIBLIOGRAPHY_OF_THE_INTERNETARPANET.aspx (E.T. 20.10.2014).

"Presidential Policy Directive -- Critical Infrastructure Security and Resilience – PPD-21", The White House, 12.02.2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (E.T. 06.02.2014).

"Protocol To The Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Limitation Of Anti-Ballistic Missile Systems", 3 July 1974, http://fas.org/nuke/control/abmt/text/abmprot1.htm (E.T. 10.04.2015).

"Quadrennial Defense Review 2014", *United States of America Deparment of Defence*, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (E.T. 14.05.2015)

"S.Ossetian News Sites Hacked", 05.08.2008, http://www.civil.ge/eng/article.php?id=18896 (E.T. 07.04.2014).

"Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ", *Resmi Gazete*, Sayı: 28818, 11 Kasım 2013, s.19. http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (E.T. 06.02.2014).

"Status of World Nuclear Forces", *Fedaration of American Scientist*, http://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/ (E.T. 10.04.2015).

"Stuxnet – A New Age İn Cyber Warfare Says Eugene Kaspersky", *Info Security, 27.09.2010,* http://www.infosecurity-magazine.com/view/12757/stuxnet-a-new-age-in-cyber-warfare-says-eugene-kaspersky/ (E.T. 07.04.2014).

"Supervisory control and data acquisition (SCADA)", Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk/advice/cyber/scada/ (E.T. 06.02.2014).

"The 'Atoms for Peace' Agency", 25 November 2014, http://www.iaea.org/About/about-iaea.html (E.T. 31.10.2014).

"The Acheson-Lilienthal & Baruch Plans, 1946", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/baruch-plans (E.T. 10.04.2015).

"The Charge in the Soviet Union to the Secretary of State" adıyla gönderilen telgrafın tam metni için bkz. http://nsarchive.gwu.edu/coldwar/documents/episode-1/kennan.htm (E.T. 10.04.2015).

"The Cybersecurity Debate: Voluntary Versus Mandatory Cooperation Between The Private Sector And The Federal Government", *Jones Day,* July 2013, http://www.jonesday.com/files/Publication/49c491ff-7f05-4932-9287-2c07a131e83d/Presentation/PublicationAttachment/216181fe-3cff-4535-9232-2c603c8bf48b/Cybersecurity%20Debate.pdf (E.T. 06.02.2014).

"The Department of Space Cyber Strategy", *United States of America Department of Defence*, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (E.T. 14.05.2015)

"The Discovery of Radioactivity", Berkeley Lab., U. S. Deparment of Energy, http://www2.lbl.gov/abc/wallchart/chapters/03/4.html (E.T. 10.04.2015).

"The First National Strategy on Information Security", Information Security Policy Council, 02.02.2006, http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf (E.T. 06.02.2014).

"The Internet Users (per 100 people)", http://data.worldbank.org/indicator/IT.NET.USER.P2/countries?display=graph (E.T. 06.02.2014).

"The Soviet Nuclear Weapons Program", http://nuclearweaponarchive.org/Russia/Sovwpnprog.html (E.T. 10.04.2015)

"The Truman Doctrine, 1947", U.S. Deparment of State Office of the Historian, http://history.state.gov/milestones/1945-1952/truman-doctrine (E.T. 10.04.2015).

"The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World", *Cabinet Office*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (E.T. 06.02.2014).

"Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Limitation Of Anti-Ballistic Missile Systems", 26 May 1972, http://www.state.gov/www/global/arms/treaties/abm/abm2.html (E.T. 10.04.2015).

"Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Limitation Of Strategic Offensive Arms, Together Wıth Agreed Statements And Common Understandings Regarding The Treaty" 18 June 1979, http://fas.org/nuke/control/salt2/index.html (E.T. 10.04.2015).

"Trojan Horse", http://www.sans.org/security-resources/glossary-of-terms/?pass=t (E.T. 10.04.2014).

"Types of DDoS Attacks", http://web.archive.org/web/20100808153343/http://www.anml.iu.edu/ddos/types.html (E.T. 10.04.2014).

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", *Resmi Gazete*, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf (E.T. 06.02.2014).

"What is a Computer Worm?", http://www.pctools.com/security-news/what-is-a-computer-worm/ (E.T. 10.04.2014).

"What is a DDoS Attack?", http://www.digitalattackmap.com/understanding-ddos/ (E.T. 10.04.2014).

"What is a DDoS Attack?", http://www.verisigninc.com/tr_TR/website-availability/ddos-protection/what-is-a-ddos-attack/index.xhtml#infograph (E.T. 10.04.2014).

"What is a Trojan Virus?", http://usa.kaspersky.com/internet-security-center/threats/trojans#.VJlxI_8NQCM (E.T. 10.04.2014).

"What is a Trojan Virus?", http://www.pctools.com/security-news/what-is-a-trojan-virus/ (E.T. 10.04.2014).

"What is the Former Yugoslavia ?", http://www.icty.org/sid/321 (E.T. 10.04.2014).

"World War II: Operation EPSILON Detention of German Nuclear Scientists British Intelligence Files", http://www.paperlessarchives.com/wwii-operation-epsilon.html (E.T. 10.04.2015).

"Worm", http://www.sans.org/security-resources/glossary-of-terms/?pass=w (E.T. 10.04.2014).

"Yeni Güvenlik Sorunlarıyla Başa Çıkmak", NATO, p.9, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_new-security-challenges-tu.pdf (E.T. 07.04.2014).

ALBRIGHT David, BRANNAN Paul, and WALROND Christina, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment" *ISIS*, 22.12.2010, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (E.T. 07.04.2014).

B-29 Superfortress", http://www.boeing.com/boeing/history/boeing/b29.page (E.T. 10.04.2015).

BÂKIR Emre, "5. Boyutta Savaş: Siber Savaşlar – I", 20.12.2012, https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html (E.T. 10.04.2014).

BARWISE Mike, "What is an Internet Worm?", 09.09.2010, http://www.bbc.co.uk/webwise/guides/internet-worms (E.T. 10.04.2014).

BEAL Vangie, "Computer Virus (virus)", http://www.webopedia.com/TERM/V/virus.html (E.T. 10.04.2014).

BEAL Vangie, "The Difference Between a Computer Virus, Worm and Trojan Horse", 12.03.2014, http://www.webopedia.com/DidYouKnow/Internet/virus.asp (E.T. 10.04.2014).

BERRY Lynn, "Behind Putin's Estonia Complex", 25.05.2007, http://www.themoscowtimes.com/sitemap/paid/2007/5/article/behind-putins-estonia-complex/196806.html (E.T. 07.04.2014).

BEST JR Richard A., *The National Security Council: An Organizational Assessment*, Congressional Research Service, 28 Aralık 2011, https://fas.org/sgp/crs/natsec/RL30840.pdf (E.T. 10.04.2015).

BÖLÜKBAŞ Candan , "Yeni Nesil Teknolojik Silahlar: DoS/DDoS", 22.12.2014, http://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/ (E.T. 10.01.2015).

BRADLEY Tony, “Zero Day Exploits”, http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm (E.T. 05.04.2014).

CAPACCIO Anthony, “Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion”, 10 June 2013, http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html (E.T. 15.12.2014).

CENCİOTTİ David, “Sixty F-16s Taxiing at Kunsan Air Base in One of the Greatest Show of Force Ever: That’s a Record-Breaking Elephant Walk”, *The Aviationist*, 6 March 2012, http://theaviationist.com/2012/03/06/elephant-walk/ (E.T. 20.03.2014).

China’s Military Strategy, The State Council Information Office of the People’s Republic of China, Beijing, May 2015, http://cryptome.org/2015/05/prc-military-strategy-cctv-america-15-0526.pdf (E.T. 02.07.2015).

CLABURN Thomas, “Iran Denies Stuxnet Worm Hurt Nuclear Plant”, *Information Week*, 27.09.2010, http://www.darkreading.com/vulnerabilities-and-threats/iran-denies-stuxnet-worm-hurt-nuclear-plant/d/d-id/1092812 (E.T. 07.04.2014).

CLULEY Graham, “Zero-day exploit in Apple’s iOS operating system "sold for $500,000"”, http://grahamcluley.com/2013/07/zero-day-ios-exploit/ (E.T. 05.04.2014).

Commission of the European Committees, Critical Infrastructure Protection in The Fight Against Terrorism, 20.10.2014, pp. 3-4. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF (E.T. 06.02.2014).

DANCHEV Dancho, “Coordinated Russia vs Georgia Cyber Attack in Progress”, 11.08.2008, http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 (E.T. 07.04.2014).

DAY Marilyn, “Obama Signs Executive Order To Allow Shut Down Of All US Communications”, *Examiner*, 08.07.2013, http://www.examiner.com/article/obama-signs-executive-order-to-allow-shut-down-of-all-us-communications (E.T. 06.02.2014).

DEHGHAN Saeed Kamali, “Iran Accuses Siemens Of Helping Launch Stuxnet Cyber-Attack”, *The Guardian*, 17.04.2011, http://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack (E.T. 07.04.2014).

ELWART Steve, “Russian Hackers Beaten at Their Own Game”, 11.12.2012, http://www.wnd.com/2012/11/russian-hackers-beaten-at-their-own-game/ (E.T. 07.04.2014).

ETZİONİ Amitai, “Private Sector Neglects Cyber Security”, *The National Interest,* 29.11.2011, http://nationalinterest.org/commentary/private-sector-neglects-cyber-security-6196 (E.T. 06.02.2014).

EVEN Loras R., “Intrusion Detection FAQ: What is a Honeypot?”, 12.07.2000, http://www.sans.org/security-resources/idfaq/honeypot3.php; (E.T. 07.04.2014).

FALLIERE Nicolas, “Stuxnet Introduces the First Known Rootkit for Industrial Control Systems”, 06.08.2010, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (E.T. 10.04.2014).

FALLIERE Nicolas, MURCHU Liam O. and CHIEN Eric, “W32.Stuxnet Dossier”, *Symantec White Paper*, February 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (E.T. 07.04.2014).

FINN Peter, “Cyber Assaults on Estonia Typify a New Battle Tactic”, 19.05.2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html (E.T. 10.04.2014).

FORD Daniel, “B-36: Bomber at the Crossroads”, *Air&Space Magazine,* April 1996, http://www.airspacemag.com/history-of-flight/b-36-bomber-at-the-crossroads-134062323/?no-ist (E.T. 10.04.2015).

GILES Keir, “Russia’s Public Stance on Cyberspace Issues”, *NATO Cooperative Cyber Defence Centre of Excellence*, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf (E.T. 07.02.2014).

GLEICK James, After The Bomb, A Mushroom Cloud Of Metaphors, *The New York Times,* 21 Mayıs 1989, http://www.nytimes.com/1989/05/21/books/after-the-bomb-a-mushroom-cloud-of-metaphors.html (E.T. 10.04.2015).

GONSALVES Antone, “US commission fingers China as biggest cyberthreat”, *CSO,* 8 November 2012, http://www.csoonline.com/article/721032/u.s.-commission-fingers-china-as-biggest-cyberthreat (E.T. 07.02.2014).

GORMAN Siobhan and BARNES Julian E., “Cyber Combat: Act of War”, *The Wall Street Journal*, 31 May 2011, http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304563104576355623135782718.html (E.T. 07.02.2014).

GROSS Grant, “US Agencies Explore Cybersecurity Incentives For The Private Sector”, *PC World,* 06.08.2013, http://www.pcworld.com/article/2046057/us-agencies-explore-cybersecurity-incentives-for-the-private-sector.html (E.T. 06.02.2014).

HEALEY Jason, “Cyber Attacks Against NATO, Then and Now”, 06.09.2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now (E.T. 07.04.2014).

HOLMES Marian Smith, “Spies Who Spilled Atomic Bomb Secrets”, 19 Nisan 2009, http://www.smithsonianmag.com/history/spies-who-spilled-atomic-bomb-secrets-127922660/?all (E.T. 10.04.2015)

HOYLE Craig, “USAF, South Korean F-16s walk the walk”, *Flightglobal*, 9 March 2012, http://www.flightglobal.com/blogs/the-dewline/2012/03/usaf-south-korean-f-16s-walk-t/ (E.T. 20.03.2014).

http://home.mcafee.com/virusinfo/anti-virus-tips?ctst=1 (E.T. 10.04.2014).

http://research.archives.gov/description/593374 (E.T. 10.04.2015).

http://trumanlibrary.org/publicpapers/index.php?pid=642&st=&st1 (E.T. 10.04.2015).

http://www.apcert.org/about/structure/members.html (E.T. 31.10.2014).

http://www.cert.org/index.cfm# (E.T. 31.10.2014).

http://www.staysafeonline.org/ncsam/ (E.T. 06.02.2014).

http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.55355d01abed21.36704295 (E.T. 07.02.2014).

http://www.trusted-introducer.org/directory/country_LICSA.html (E.T. 31.10.2014).

https://ccdcoe.org/publication-library.html (E.T. 07.04.2014).

Information Security Policy Council, *Action Plan on Information Security Measures for Critical Infrastructares*, 13.12.2005, pp. 1-2. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf (E.T. 06.02.2014).

JACKSON William, “Feds Launch Cyber Security Guidelines For US Infrastructure Providers”, *Information Week, 12.02.2014,* http://www.informationweek.com/government/cybersecurity/feds-launch-cyber-security-guidelines-for-us-infrastructure-providers/d/d-id/1113816 (E.T. 06.02.2014).

KEIZER Gregg, “Is Stuxnet The ’Best’ Malware Ever?”, *Computer World*, 16.09.2010, http://www.computerworld.com/article/2515757/malware-vulnerabilities/is-stuxnet-the--best--malware-ever-.html (E.T. 07.04.2014).

Khrushchev and Eisenhower: Summit Statements, 16 Mayıs 1960, http://legacy.fordham.edu/halsall/mod/1960summit-statements1.asp (E.T. 10.04.2015).

KIRK Jeremy, “Estonia, Poland Help Georgia Fight Cyber Attacks”, 12.08.2008, http://www.pcworld.com/article/149700/cyberattacks.html (E.T. 07.04.2014).

KIRK Jeremy, “Irked by Cyberspying, Georgia Outs Russia-Based Hacker -- With Photos”, 30.10.2012, http://www.networkworld.com/news/2012/103012-irked-by-cyberspying-georgia-outs-263790.html (E.T. 07.04.2014).

KLINGOVA Katerina, “Securitization of Cyber Space in the United States of America, The Russian Fedaration and Estonia”, Yayımlanmamış Yüksek Lisans Tezi, Danışman: Paul Roe, Central European University Department of Political Science, 2013.

KRAMER Andrew E., “Putin is Said to Compare U.S. Policies to Third Reich”, 10.05.2007, http://www.nytimes.com/2007/05/10/world/europe/10russia.html?_r=0 (E.T. 07.04.2014)

KUSHNER David, “The Real Story of Stuxnet”, *IEEE Spectrum*, 26.02.2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (E.T. 07.04.2014).

LEYDEN John, “To Russia with Love? Georgia Snaps ’cyber-spy’ With His Own Cam”, 31.10.2012, http://www.theregister.co.uk/2012/10/31/georgia_russia_counter_intelligence/ (E.T. 07.04.2014).

MADSEN Michael, “Pioneering Nuclear Science: The Discovery of Nuclear Fission”, International Atomic Energy Agency, https://www.iaea.org/newscenter/news/pioneering-nuclear-science-discovery-nuclear-fission (E.T. 10.04.2015).

MALKIN Gary Scott and PARKER Tracy LaQuey, “Internet User’s Glossary”, January 1993, http://tools.ietf.org/html/rfc1392#appendix-H (E.T. 05.04.2014).

MARKOFF John, “Before the Gunfire, Cyberattacks”, 12.08.2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?em&_r=0 (E.T. 07.04.2014).

MCDOWELL Mindi, “Understanding Denial-of-Service Attacks”, 06.02.2013, https://www.us-cert.gov/ncas/tips/ST04-015 (E.T. 10.04.2014).

MCMILLAN Robert, “Siemens: Stuxnet Worm Hit Industrial Systems”, 14.09.2010, http://www.computerworld.com/article/2515570/network-security/siemens--stuxnet-worm-hit-industrial-systems.html (E.T. 10.04.2014).

MINNICK Wendell, “Experts: Chinese Cyber to US is Growing”, *Defence News*, 9 July 2013, http://www.defensenews.com/article/20130709/DEFREG03/307090009/Experts-Chinese-Cyber-Threat-US-Growing (E.T. 07.02.2014).

MITCHELL Bradley, “Worm - Computer Worm”, http://compnetworking.about.com/cs/worldwideweb/g/bldef_worm.htm (E.T. 10.04.2014).

MURCHU Liam O., “Stuxnet Using Three Additional Zero-Day Vulnerabilities”, 14.09.2010, http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities (E.T. 10.04.2014).

NARAINE Ryan, “Stuxnet Attackers Used 4 Windows Zero-Day Exploits” *ZDNET*, 14.09.2010, http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347 (E.T. 07.04.2014).

National Cyber Security Policy, Department of Eloctronics and Information Technology, 2013, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf (E.T. 02.07.2015).

National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cyber Security, Version 1.0, 12.02.2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (E.T. 06.02.2014).

NGAK Chenda, “NSA Leaker Snowden Claimed U.S. and Israel Co-wrote Stuxnet Virus”,09.07.2013, http://www.cbsnews.com/news/nsa-leaker-snowden-claimed-us-and-israel-co-wrote-stuxnet-virus/ (E.T. 10.04.2014).

NSC 68: United States Objectives and Programs for National Security, Washington, 7 Nisan 1950, http://fas.org/irp/offdocs/nsc-hst/nsc-68.htm (E.T. 10.04.2015).

NUTTALL Chris, “Sci/TechKosovo Info Warfare Spreads”, 01.04.1999, http://news.bbc.co.uk/2/hi/science/nature/308788.stm (E.T. 10.04.2014).

Official Journal of the European, L. 345/75, 23.12.2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. (E.T. 06.02.2014).

PAGANINI Pierluigi, “Hacking air gapped networks by using lasers and drones”, 25 October 2014, http://securityaffairs.co/wordpress/29551/hacking/hacking-air-gapped-networks.html (E.T. 15.12.2014).

PERRIN Chad, “Hacker vs. cracker”, 17 April 2009, http://www.techrepublic.com/blog/it-security/hacker-vs-cracker/ (E.T. 05.04.2014)

PETER Thomas, “Snowden Confirms NSA Created Stuxnet with Israeli Aid”, 11.07.2013, http://rt.com/news/snowden-nsa-interview-surveillance-831/ (E.T. 10.04.2014).

PURI Ramneek, “Bots &; Botnet: An Overview”, SANS Institute InfoSec Reading Room, 08.07.2003, http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299 (E.T. 10.04.2014).

Resolution 84, UN Security Council, 7 Haziran 1950, http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3b00f1e85c (E.T. 10.04.2015).

RAZUMOVSKAYA Olga, "Russia and China Pledge Not to Hack Each Other", Wall Street Journal, 8 Mayıs 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/ (E.T. 14.05.2015)

ROUSE Margaret, "Advanced Persistent Threat (APT)", http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT (E.T. 10.04.2014).

ROUSE Margaret, "Trojan Horse", July 2006, http://searchsecurity.techtarget.com/definition/Trojan-horse (E.T. 10.04.2014).

RUCKER Philip, "Obama warns Xi that continued cybertheft would damage relations, US officials said", *The Washington Post*, 8 June 2013, http://www.washingtonpost.com/politics/obama-warns-xi-that-continued-cybertheft-would-damage-relations-us-officials-said/2013/06/08/04843edc-d075-11e2-8845-d970ccb04497_story.html (E.T. 07.02.2014).

RUUS Kertu, "Cyber War I: Estonia Attacked from Russia", *European Affairs*, http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia (E.T. 07.04.2014).

SAGAN Carl, "How to Reduce the Risk of Nuclear Warfare: Carl Sagan on Space Exploration", https://www.youtube.com/watch?v=fVUk30GFsL4 (E.T. 10.04.2015).

SANGER David E., "Obama Order Sped Up Wave of Cyberattacks Against Iran" *The New York Times*, 01.07.2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (E.T. 07.04.2014).

SCHWARTZ Mathew J., "Black Hat Keynoter: Beware of Air Gap Risks", 16 October 2014, http://www.bankinfosecurity.com/black-hat-europe-beware-air-gaps-a-7442/op-1 (E.T. 15.12.2014).

SHACHTMAN Noah, "Estonia, Google Help 'Cyberlocked' Georgia", 08.11.2008, http://www.wired.com/2008/08/civilge-the-geo/ (E.T. 07.04.2014).

SHEKARAUBI Shahrooz, "Iran's Case against Stuxnet", *International Policy Digest*, 18.03.2014, http://www.internationalpolicydigest.org/2014/03/18/irans-case-stuxnet/ (E.T. 07.04.2014).

SILVERMAN Jacob, "Could hackers devastate the U.S. economy?", http://computer.howstuffworks.com/die-hard-hacker1.htm (E.T. 07.04.2014).

SMITH David J., "Russian Cyber Capabilities, Policy and Practice", *The Jewish Policy and Practice*, http://www.jewishpolicycenter.org/4924/russian-cyber-capabilities (E.T. 07.02.2014)

SMITH Gerry, “John Kerry: Foreign Hackers Are ‘21st Century Nuclear Weapons”, 24. 01. 2013, http://www.huffingtonpost.com/2013/01/24/john-kerry-hackers_n_2544534.html (E.T. 31.10.2014).

TENCER Daniel, “Obama May Get Power To Shut Down Internet Without Court Oversight”, *Rawstory*, 24.01.2011, http://www.rawstory.com/rs/2011/01/24/power-shut-internet-court-oversight/ (E.T. 06.02.2014).

TOTH Beatrix, “Estonia Under Cyber Attack”, http://www.cert.hu/sites/default/files/Estonia_attack2.pdf (E.T. 07.04.2014).

TRAYNOR Ian, “Russia Accused of Unleashing Cyberwar to Disable Estonia”, 17.05.2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia (E.T. 10.04.2014).

UNVER Mustafa, CANBAY Cafer, ÖZKAN Hüseyin Burhan, *Kritik Altyapıların Korunması*, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Mayıs 2010. http://www.cybersecurity.gov.tr/publications/CIP_Rapor.pdf (E.T. 06.02.2014).

VERTON Dan, “Serbs Launch Cyberattack on NATO”, 04.04.1999, http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx (E.T. 10.04.2014).

WATERMAN Shaun, “Analysis: Who cyber smacked Estonia?”, 11.06.2007, http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/ (E.T. 07.04.2014).

WATERMAN Shaun, “U.S.-Israeli Cyberattack On Iran Was ‘Act Of Force,’ NATO Study Found”, *The Washington Times*, 24.03.2013, http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all#pagebreak (E.T. 07.04.2014).

WEITZ Richard, “The Historical Context”, Tom Nichols, Douglas Stuart, Jeffrey D. McCausland(edt.), *Tactical Nuclear Wepons and Nato*, US Army War College, Strategic Studies Institute, April 2012, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1103.pdf (E.T. 10.04.2015).

WENTWORTH Travis, “How Russia May Have Attacked Georgia’s Internet”, 23.08.2008, http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111 (E.T. 07.04.2014).

WILLIAMS Christopher, “Stuxnet Virus: US Refuses To Deny İnvolvement”, *The Telegraph*, 27.05.2011, http://www.telegraph.co.uk/technology/news/8541587/Stuxnet-virus-US-refuses-to-deny-involvement.html (E.T. 07.04.2014).

WOLF Jim, “US says will boost its cyber arsenal”, 7 November 2011, http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107 (E.T. 15.12.2014).

ÖZGEÇMİŞ			
Adı, Soyadı	Uğur		Ermiş
Doğum Yeri ve Yılı	İstanbul		1990
Bildiği Yabancı Diller	İngilizce		İleri Düzey
ve Düzeyi			
Eğitim Durumu	**Başlama - Bitirme Yılı**		**Kurum Adı**
Lise	2003	2007	Rıfat Canayakın Lisesi
Lisans	2007	2011	Uludağ Üniversitesi
Yüksek Lisans	2012	2015	Uludağ Üniversitesi
Doktora			
Çalıştığı Kurum (lar)	**Başlama - Ayrılma Yılı**		**Çalışılan Kurumun Adı**
1.	2013	-	Uludağ Üniversitesi
2.			
3.			
Üye Olduğu Bilimsel ve Mesleki Kuruluşlar			
Katıldığı Proje ve Toplantılar			
Yayınlar:			
Diğer:			
İletişim (e-posta):	ugurermis@outlook.com		
		Tarih **İmza** **Adı Soyadı**	

ULUDAĞ ÜNİVERSİTESİ

TEZ ÇOĞALTMA VE ELEKTRONİK YAYIMLAMA İZİN FORMU

Yazar Adı Soyadı	Uğur Ermiş
Tez Adı	Siber Caydırıcılık Kavramının Nükleer Caydırıcılık Olgusu İle Karşılaştırmalı Analizi
Enstitü	Sosyal Bilimler Enstitüsü
Anabilim Dalı	Uluslararası İlişkiler
Tez Türü	Yüksek Lisans
Tez Danışman(lar)ı	Doç. 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 :

İmza :