

**T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ
EĞİTİM ENSTİTÜSÜ**

**SİBER TEHDİTLERE KARŞI CAYDIRICILIK STRATEJİSİNİN
NEOKLASİK REALİZM ÇERÇEVESİNDE ANALİZİ:
OBAMA VE TRUMP DÖNEMLERİNİN KARŞILAŞTIRILMASI**

Emre İNAN

DOKTORA TEZİ

**STRATEJİ VE GÜVENLİK ARAŞTIRMALARI ANA BİLİM DALI
GÜVENLİK ARAŞTIRMALARI DOKTORA PROGRAMI**

Tez Danışmanı:

Prof. Dr. Haldun YALÇINKAYA

Haziran 2025

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ
EĞİTİM ENSTİTÜSÜ

SİBER TEHDİTLERE KARŞI CAYDIRICILIK STRATEJİSİNİN
NEOKLASİK REALİZM ÇERÇEVESİNDE ANALİZİ:

OBAMA VE TRUMP DÖNEMLERİNİN KARŞILAŞTIRILMASI

Emre İNAN tarafından hazırlanan tez çalışması 03.06.2025 tarihinde aşağıdaki jüri tarafından Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar Enstitüsü, Strateji ve Güvenlik Araştırmaları Ana Bilim Dalı, Güvenlik Araştırmaları Programı **DOKTORA TEZİ** olarak kabul edilmiştir.

Prof. Dr. Haldun YALÇINKAYA
TOBB ETU Üniversitesi
Tez Danışmanı

Jüri Üyeleri

Prof. Dr. Haldun YALÇINKAYA, Tez Danışmanı
TOBB ETU Üniversitesi

Prof. Dr. Mitat ÇELİKPALA, Üye
Kadir HAS Üniversitesi

Prof. Dr. Burak Samih GÜLBOY, Üye
İstanbul Üniversitesi

Doç. Dr. Güngör ŞAHİN, Üye
Milli Savunma Üniversitesi

Doç. Dr. Öner AKGÜL, Üye
Milli Savunma Üniversitesi

Danışmanım Prof. Dr. Haldun YALÇINKAYA sorumluluğunda tarafımda hazırlanan “Siber Tehditlere Karşı Caydırıcılık Stratejisinin Neoklasik Realizm Çerçevesinde Analizi: Obama ve Trump Dönemlerinin Karşılaştırılması” başlıklı çalışmada veri toplama ve kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Emre İNAN

*Eşime ve
Oğluma*



TEŞEKKÜR

2019 yılında başladığım doktora eğitimimi yazmış olduğum tez çalışmam ile sonlandırıyorum. Eğitim sürecimin başından bu yana farklılaşan güvenlik ve tehdit ortamında Türk Silahlı Kuvvetlerinin de en önemli görevlerinden biri olan ‘‘caydırıcılık’’ kavramının nasıl sağlanacağı konusu ilgimi çekmiş bulunmaktaydı. Yapmış olduğum çalışma ile bu konuya naçizane bir katkı olmasını umuyor ve gelecek çalışmalara yol göstermesini temenni ediyorum. Bu çalışmanın en başından bu yana bana destek olan, değerli fikirleri ile ışık tutan, akademik ve sosyal anlamda bana örnek olan çok değerli tez danışmanım Prof.Dr. Haldun Yalçinkaya’ya şükranlarımı sunuyorum. Tez izleme komitemde bulunarak beni onurlandıran ve yazım aşamalarında bana yol gösteren Prof.Dr. Mitat Çelikpala’ya ve Per.Alb.Doç.Dr. Güngör Şahin’e teşekkürü bir borç biliyorum. Tezimin kavramsal ve kuramsal açıdan olgunluk kazanmasında bana değerli fikirleri ile katkı sağlayan değerli hocalarım Prof.Dr. Şaban Kardaş, Prof.Dr. Mehmet Ali Tuğtan ve Prof.Dr. Ertan Kardeş’e teşekkür ediyorum. Tezimden üretmiş olduğum makalenin olgunluğa erişmesinde bana yardımcı olan ve makale yazım teknikleri hakkında beni aydınlatan Doç.Dr. Klevis Kolasi’ye teşekkür ediyorum. Gerek doktora eğitimi ders sürecinde, gerek Komuta ve Kurmay Eğitiminde, gerekse tez jürisi sürecinde güvenlik konusunun çeşitli boyutları ile beni düşünmeye sevk eden ve analitik düşünme becerimi geliştiren Prof.Dr. Burak Samih Gülboy’a teşekkürlerimi sunuyorum. Son olarak tez jürimde yer alarak tezimi titizlikle inceleyen ve değerli geri bildirimleri ile çalışmamın nihai olgunluğa erişmesine katkı sağlayan Doç.Dr. Öner Akgül’e teşekkür ediyorum.

Ayrıca eğitim hayatımın başından beri beni destekleyip yanımda olan anneme, babama ve kardeşime ne kadar teşekkür etsem azdır. Son olarak yoğun mesai programımdan dolayı kendisine yeterli vakti ayıramama rağmen beni daima kendisinden önde tutan, yorulduğum ve karamsarlığa düştüğüm zamanlarda beni cesaretlendiren sevgili eşim Neslihan teşekkürlerin en büyüğünü hak etmektedir. Sen olmasan hiçbir şey mümkün olmazdı. Eylül ayında aramıza katılacak olan oğlumuz bu son dönemin bizlere en büyük müjdesi oldu. Çalışmamı canım oğlum Mete’ye armağan ediyorum. *Emre İNAN*

İÇİNDEKİLER

İÇİNDEKİLER	vii
TABLolar LİSTESİ	ix
ŞEKİLLER LİSTESİ	xi
KISALTMALAR	xiii
ÖZET	xv
ABSTRACT	xvii
GİRİŞ	1
1. AKADEMİK YAZINDA CAYDIRICILIK STRATEJİSİ	13
1.1. Caydırıcılığın Tarihsel Gelişimi	14
1.2. Caydırıcılığın Dört Dalgası	15
1.2.1. Birinci ve İkinci Dalgalar:	18
1.2.2. Üçüncü Dalga	27
1.2.3. Dördüncü Dalga	31
1.3. Caydırıcılık Yazınında Kabiliyet Bileşeni Sorunu ve Siber Tehditlere Yansıması	36
1.4. Caydırıcılık Metotları	39
1.4.1. Ceza Yoluyla Caydırıcılık	39
1.4.2. İkna Yoluyla Caydırıcılık	40
1.4.3. Dayanıklılık Yoluyla Caydırıcılık	41
1.4.4. Normlar Yoluyla Caydırıcılık	42
2. KURAMSAL ÇERÇEVE: NEOKLASİK REALİZM	45
2.1. Analiz Düzeyleri ve Neoklasik Realizm	46
2.2. Neoklasik Realizmin Araştırma Metodolojisinde Bağımsız Değişken: Yapı-Aktör Etkileşimi	50
2.2.1. Yapısal Dönüştürücüler	53
2.2.2. Siber Kavramı ve Bir Yapısal Dönüştürücü Olarak Siber Uzay	53
2.2.3. Açıklık ve Stratejik Çevre	67
2.3. İç Değişkenler	69
3. VAKA ANALİZİ: ABD SİBER CAYDIRICILIK POLİTİKALARINDA YAPISAL VE İÇ DEĞİŞKEN ETKİLERİNİN İNCELENMESİ	77
3.1. Yapısal Faktörlerin Etkileri: ABD'nin Küresel Güç Dağılımındaki Yeri ve Tehdit Algılaması	77
3.2. Farklılaşan Caydırıcılık Stratejileri: Obama ve Trump Dönemleri Siber Güvenlik Politikalarının Karşılaştırılması	79
3.2.1. Barack Obama Dönemi (2009-2016)	80

3.2.2. Donald Trump Dönemi (2017-2021).....	118
3.2.3. Obama ve Trump Dönemi Siber Güvenlik Politikalarının Caydırıcılık Metotları Bakımından Değerlendirilmesi.....	143
3.3. İç Değişkenlerin Etkileri: İki Başkan Döneminde Farklılık Gösteren Siber Güvenlik Politikalarının Nedenleri	146
3.3.1. Lider Değişkeni – Alternatif Açıklamalar	148
3.3.2. Güvenlik Politikalarına Etki Eden bir Bileşen olarak Dış Politika Gelenekleri	152
3.3.3. Obama ve Trump Dönemlerinde Takip Edilen Stratejik Kültürün Farklı Dış Politika Kararları Üzerinden İncelenmesi	161
3.3.4. Jeffersoncu ve Jacksoncu Dış Politika Geleneklerinin Siber Caydırıcılık Politikalarına Etkileri	164
3.3.5. Kongre Değişkeni.....	175
SONUÇ	199
KAYNAKÇA.....	205
VERİ ANALİZİNDE BAŞVURULAN RESMİ GÜVENLİK BELGELERİ....	227
TEZDEN ÜRETİLMİŞ YAYINLAR.....	229

TABLÖLAR LİSTESİ

Tablo 1: Başkanlık Dönemlerine İlişkin Analiz Edilen Veri Tablosu.....	9
Tablo 2: Caydırıcılık Alanyazınında Öne Çıkan Akademik Çalışmalar	18
Tablo 3: Eylemlerin Gerçekleştiği Safhaya Yönelik Caydırıcılık Metotları	42
Tablo 4: Tehdit Ortamları ve Karakteristik Özellikleri	64
Tablo 5: Neoklasik Realizm Kuramsal Çalışmalarında Ara Değişkenlerin Kullanım Biçimleri.....	71
Tablo 6: ABD'nin ve Rusya Ulusal Kabiliyet Bileşik Endeks Puanları	78
Tablo 7: 13636 Sayılı Başkanlık İcra Emrinde Tanımlanan Kritik Altyapı Tesisleri	99
Tablo 8: 41. Başkanlık Siyaset Direktifi Kapsamında Federal Kurumlara Verilen Sorumluluklar	112
Tablo 9: İş Birliği-Bürokrasi ve Çatışmaya Yönelik Tavrı Bileşenleri Kapsamında Obama ve Trump Karakteristikleri	165
Tablo 10: İki Başkan Dönemindeki Kongre Temsilîyet Durumları	180

ŞEKİLLER LİSTESİ

Şekil 1: Kahn'ın Tırmanma Merdiveni	23
Şekil 2: Yapı-Dış Politika İlişkisi - Neorealizm vs. Neoklasik Realizm	51
Şekil 3: Stratejik Kültür - Caydırıcılık Metodu İlişkisinin Nedensellik Analizinde Süreç Takibi Aşamaları	148
Şekil 4: İş Birliği ve Bürokrasiye Bakış Açısından Jeffersoncu/Jacksoncu Gelenek	160
Şekil 5: Çatışmaya Yönelik Tavır Açısından Jeffersoncu/Jacksoncu Gelenek	161





KISALTMALAR

CIA	: Merkezi İstihbarat Teşkilatı (Central Intelligence Agency)
CISA	: Kritik Altyapı Güvenliği Teşkilatı (Critical Infrastructure Security Agency)
CSC	: Siber Solaryum Komitesi (Cyber Solarium Commission)
CTIIC	: Siber Tehdit İstihbaratı Entegrasyon Merkezi (Cyber Threat Intelligence Integration Center)
DDOS	: Dağıtık Hizmet Engelleme (Distributed Denial of Service)
EO	: İcra Emri (Executive Order)
FBI	: Federal Soruşturma Bürosu (Federal Bureau of Investigation)
HR	: Temsilciler Meclisi (House of Representatives)
IAAS	: Servis olarak Altyapı (Infrastructure as a Service)
JP	: Müşterek Yayın (Joint Publication)
NDAA	: Ulusal Savunma Yetkilendirme Yasası (National Defense Authorization Act)
NPT	: Nükleer Silahların Azaltılması Antlaşması (Nuclear Proliferation Treaty)
NSPM	: Ulusal Güvenlik Başkanlık Memorandumu (National Security Presidential Memorandum)
PPD	: Başkanlık Siyaset Direktifi (Presidential Policy Directive)
SCADA	: Denetleyici Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition)
UNGGE	: Birleşmiş Milletler Devlet Uzmanları Grubu (United Nations Group of Governmental Experts)



SİBER TEHDİTLERE KARŞI CAYDIRICILIK STRATEJİSİNİN NEOKLASİK REALİZM ÇERÇEVESİNDE ANALİZİ:

OBAMA VE TRUMP DÖNEMLERİNİN KARŞILAŞTIRILMASI

Emre İNAN

Strateji ve Güvenlik Araştırmaları Ana Bilim Dalı

Güvenlik Araştırmaları Doktora Programı

Doktora Tezi

Tez Danışmanı: Prof.Dr. Haldun YALÇINKAYA

Caydırıcılık stratejisi üzerine akademik çalışmalar, Soğuk Savaş döneminin nükleer silah ve güç dengesi faktörlerinden önemli ölçüde etkilenmiştir. Bununla birlikte yakın dönemde ortaya çıkan siber tehditlere karşı uygulanan caydırıcılık stratejilerini anlamak için yapısal faktörlerin yanında devlete ait iç değişkenlerin analize dahil edilmesi gerekmektedir. Bu çalışmada; siber tehditlere karşı yürütülen caydırıcılık stratejisinde stratejik kültür ve kurum etkisi araştırılmıştır. Neoklasik realizm kuramsal çerçevesine başvurulmuş çalışmada, vaka analizi ve süreç takibi yöntemleri uygulanmıştır. Örnek vaka olarak Amerika Birleşik Devletleri (ABD) siber caydırıcılık politikaları ele alınmış ve Barack Obama ile Donald Trump dönemleri karşılaştırılmıştır. Analiz sonucunda; güç dağılımı ve tehdit algılaması gibi yapısal faktörlerin, güvenlik politikalarına belirli bir yön verdiği ancak stratejik kültür ve kurum değişkenlerinin aynı bağlamsal koşullar altında farklı caydırıcılık uygulamalarını doğurduğu bulgusuna varılmıştır. Elde edilen bulgular, dış politika analizinde yapısal faktörler ile birlikte iç değişkenlerin kullanımına örnek teşkil eden kuramsal bir katkı sunmaktadır.

Anahtar Kelimeler: Neoklasik Realizm, Caydırıcılık, Siber Tehditler, Dış Politika Gelenekleri, Kongre



THE ANALYSIS OF DETERRENCE STRATEGY AGAINST CYBER THREATS UNDER THE FRAMEWORK OF NEOCLASSICAL REALISM: COMPARISON OF OBAMA AND TRUMP TERMS

Emre İNAN

Department of Security and Strategy Studies

Doctoral Dissertation

Supervisor: Prof.Dr. Haldun YALÇINKAYA

Academic studies on deterrence strategy are significantly influenced by the defining factors of the Cold War era - nuclear weapons and balance of power. However, in order to understand the deterrence strategy against recent cyber threats, it is crucial that internal variables be included in the foreign policy analysis. This study examines the strategic culture and institution effects in deterrence strategy applied against cyber threats. The theoretical framework is neoclassical realism and the methods applied are case analysis and process tracing. Cyber deterrence policies of the United States of America is selected as a case whereby the cyber implementations of Barack Obama and Donald Trump presidencies are compared. The analysis reveals that whereas structural factors such as distribution of power and threat perception lead the state to a certain way of security posture; strategic culture and institution variables yield to different deterrence strategies under similar contexts. The findings of the study exemplifies the combined application of internal factors and the structural factors in the foreign policy analysis. Thus it makes a theoretical contribution to the field.

Keywords: Neoclassical Realism, Deterrence, Cyber Threats, Foreign Policy Traditions, Congress



Soğuk Savaş döneminin devletler arası güç ilişkilerinde caydırıcılık stratejisi önemli bir yere sahip olmuştur. Nükleer silahlar etkisinde şekillenen çift kutuplu güç dengesi ve bu koşullar bağlamında takip edilen caydırıcılık stratejisi, döneme dair dış politika analizlerinde belirleyicidir. Caydırıcılık stratejisinin nükleer tehdit koşullarındaki başarısı, bu stratejinin konvansiyonel ve hibrit tehditler karşısında kullanımına aracılık etmiştir. Bu doğrultuda, siber tehditler karşısında caydırıcılık stratejisinin uygulanabilirliği son yıllarda akademik yazında ilgi gören bir konudur. Ancak bu çalışmaların siber tehditlerin kapasite boyutunu verili olarak ele aldığı ve doğrudan caydırıcılığın inandırıcılık bileşenine odaklandığı görülmektedir. Oysaki caydırıcılık stratejisinde kullanılacak olan siber kapasite, devletlerin iç değişkenlerinin de dahil olduğu bir inşa süreci geçirmektedir. Dolayısıyla güç dağılımı ve tehdit algılaması gibi yapısal faktörlere ilaveten iç değişkenlerin etkisi de dış politika analizine dahil edilmelidir. Bu doğrultuda çalışmanın cevaplamak amacıyla olduğu sorun farklılaşan caydırıcılık stratejilerinde iç bileşenlerin etkin olup olmadığıdır.

Genel olarak çalışmada; dış politika inşa sürecinde, ulusal ve uluslararası düzeydeki farklı değişkenlerin birlikte etkin olduğunu savunan Neoklasik Realizmin geçerliliği tartışılmaktadır. Özelde ise; stratejik kültür ve kurum gibi değişkenlerin dış politika analizine nasıl dahil edileceği ortaya konulmaktadır. Zira iç değişkenlerin gelişigüzel bir şekilde seçildiği ve belirli bir analiz metodunu izlemediği görüşleri Neoklasik Realizm teorisine sıklıkla yöneltilen eleştiriler arasındadır.

Caydırıcılık, belli bir askeri kabiliyetin kullanımına dair karşı tarafın zihninde inandırıcılık oluşturarak onu olası bir istenmeyen eylemden alıkoyma davranışıdır. Zorlayıcı diplomasinin bir ürünü olan caydırıcılık stratejisinin başarı koşulları ve uygulama biçimleri Soğuk Savaş'ın başlangıcından günümüze dört dalga altında sınıflandırılabilir çok sayıda çalışmaya konu olmuştur. Bu kapsamda ilk iki dalgada nükleer silahların güvenlik stratejisinde nasıl konumlandırılacağını esas alan öğretici çalışmalar ön plandayken, üçüncü dalga ile birlikte konvansiyonel kabiliyetleri de analiz kapsamına dahil eden ve ampirik bir yaklaşım benimseyen çalışmaların ağırlık kazandığı görülmektedir. Dördüncü dalga çalışmalarında ise caydırıcılık stratejisinin tehdit aktörü ve tehdit cinsindeki niteliksel ve niceliksel farklılaşmalar karşısındaki durumu irdelenmektedir. Nitekim farklılaşan tehdit ortamı örneklerinden biri olan siber

tehditler bu çalışmanın vaka konusudur. Dolayısıyla bu çalışma caydırıcılık alan yazınında dördüncü dalga çalışmalarına girmektedir.

Caydırıcılık çalışmaları, takip kolaylığı açısından her ne kadar dört dalga halinde sınıflandırılrsa da bütün bu dalgaların ortak noktası başarılı bir caydırıcılık stratejisi için üç temel bileşenin (kabiliyet, inandırıcılık ve iletişim) vazgeçilmez olduğudur. Zira başarılı bir caydırıcılık için etkin bir zorlayıcı kabiliyet, bu kabiliyetin gerektiğinde kullanılabileceğine dair inandırıcılık ve hangi istenmeyen davranış sonucunda bu kabiliyete maruz kalınacağına dair karşı tarafa net mesajlar veren etkin bir iletişim gereklidir. Bununla birlikte inandırıcılık bileşeninin ikinci caydırıcılık dalgası çalışmalarından itibaren araştırmacıların dikkatini diğer bileşenlerden daha fazla çektiği ifade edilebilir. Söz konusu durumun iki nedenden kaynaklandığı değerlendirilmektedir. Birincisi, inandırıcılığın vaka sınırlarını aşan tarihsel ve psikolojik uzantılarının bulunmasıdır.¹ Devletlerin bir vakaya karşı benimseyeceği caydırıcılık stratejileri, önceki benzer vaka örneklerine ve geçmiş tutumlarıyla ilişkili psikolojik tutumlarına bağlı olarak değişebilmektedir. Daryl Press'e göre 1938 Münih Konferansı'nda ortaya konulan başarısız inandırıcılık örneği takip eden süreçte ABD dış politikasını etkilemiş ve bu doğrultuda Soğuk Savaş sürecinde Kore, Küba ve Vietnam gibi kriz noktalarında geri adım atmayan bir ABD stratejisinin tetikleyicisi olmuştur.² Dolayısıyla inandırıcılık bileşeni farklı vakaların birarada değerlendirilmesini gerekli kılan geniş bir çalışma alanı sunmaktadır.

İkincisi Realizmin temel argümanlarından biri olan rasyonel aktör kavramının nükleer silahlar ile ilişkilendirme sorunudur. "Alışılmadık derecede şiddetli ve yıkıcı"³ bir silahın kullanımının temelde irrasyonel olmasına rağmen zorlayıcı diplomasiye eklemlenmesi tartışmaya açık bir araştırma alanı olarak ortaya çıkmıştır. Böylece inandırıcılık kavramı, eldeki sert güç kapasitesinden diplomasi yoluyla nasıl azami fayda sağlanacağı sorusuna yanıt arayan araştırmacılar için genel bir çerçeve sunmuştur. Schelling ve Kahn'ın Oyun Teorisi katkılarıyla kapısı aralanan bu alan, takip eden

¹ Shping Tang, "Reputation, Cult of Reputation and International Conflict", *Security Studies* 14, sayı: 1 (2005): 38.

² Daryl G. Press, "The Credibility of Power: Assessing Threats during the 'Appeasement' Crises of the 1930s", *International Security* 29, sayı: 3 (2005): 136-38.

³ Morgan, "The State of Deterrence in International Politics Today", 86.

süreçte hesaplama, rasyonelite, psikoloji ve karar alma gibi pek çok alt konuyu yelpazesine dahil etmiştir.⁴

Diğer taraftan kabiliyet değişkeninin ise daha çok verili kabul edildiği ve inandırıcılığa kıyasla alan yazında daha sınırlı bir yer teşkil ettiği ifade edilebilir. Kabiliyet değişkenine olan sınırlı ilginin sebebinin bu silahların şüpheyi yer bırakmayan devasa yıkım özelliklerinden kaynaklandığı muhtemeldir. Kullanılmaları durumunda uluslararası toplumu nükleer bir felaket senaryosu ile baş başa bırakacak olan söz konusu silahların etkileri ve doktrinsel konumlandırılmaları akademik yazında daha az ele alınmıştır. Bir bağımsız değişkenden ziyade ara değişken rolünde sunulan kabiliyetlerin geri plandaki bu durumu nükleer silahların şüpheyi götürmeyen yıkım kapasiteleri nedeniyle akademik alanda bir eksiklik olarak görülmeyebilir. Bununla birlikte son dönem farklılaşan tehdit algılamaları çerçevesinde caydırıcılığı oluşturacak kabiliyetlerin nasıl oluşturulacağı ve nasıl konumlandırılacağı önem arz etmektedir.

Bu noktada çalışma akademik yazına katkı sağlamayı hedeflemektedir. Siber uzayda geliştirilecek caydırıcılık stratejisinde nükleer silahlar gibi verili kabiliyetler mevcut değildir. Söz konusu kabiliyetler yazılım ve donanım aygıtlarının geliştirilmesi, bilişim altyapısını kullanan aktörler arasında ortak davranış şekilleri ve tedbir mekanizmalarının geliştirilmesi ve agresif yöntemlerle bilişim farklı internet tabanlı ağlarda sızma, ele geçirme, bilgi elde etme ve zarar verme uygulamaları gibi örnekleri kapsamaktadır. Karşılaşılan tehditlerin henüz yeni olması ve etkilerinin halen keşfedilmekte olması takip edilecek örnek başarılı modellerin yokluğu anlamına gelmektedir. Burada Neorealizmin benzer davranış modellerine gerekçe olarak öne sürdüğü “rekabet” ve “taklit” etkileşimlerinin işlevsiz olduğu görülmektedir. Hangi tür kabiliyetin ne derece etkin olduğu halen denenmekte olduğundan dolayı bu doğrultuda izlenecek politikaların belirlenmesinde lider, kurum, stratejik kültür gibi iç değişkenlerin etkileri kabiliyet inşasında daha belirleyici olmaktadır.

Sonuç olarak bu çalışma caydırıcılık yazınına dair kavramsal ve kuramsal iki boyutta görülen iki eksikliğe cevap verecektir. Bunların ilki caydırıcılığın birinci dalga

⁴ Press, “The Credibility of Power: Assessing Threats during the ‘Appeasement’ Crises of the 1930s”; Snyder, *Deterrence and Defense. Toward a theory of national security.*; Jervis, *Perception and Misperception in International Politics*; Frank C. Zagare ve Stephen L. Quackenbush, “Modern Deterrence Theory: Research Trends, Policy Debates, and Methodological Controversies”; Tang, “Reputation, Cult of Reputation and International Conflict”.

çalışmalarından bu yana tespit edilen iç değişken kullanımı eksikliğidir. Çalışmada, Neoklasik Realizm kuramsal çerçevesinde, güç dengesi ve tehdit algılaması gibi yapısal faktörlerin yanı sıra kurum ve stratejik kültür iç değişkenleri dış politika analizine dahil edilmiştir. Söz konusu değişkenlerin kullanılması ile elde edilen açıklayabilme özelliği tespit edilen ikinci alan yazın eksikliği için önemlidir. Zira caydırıcılığın pratikte hangi yönetsel ve araçsal kabiliyetler ile sürdürüldüğü akademik çalışmalarda yetersiz bir şekilde ele alınan bir konudur. Söz konusu kabiliyet inşasının belirlenmesinde yapısal faktörler ve iç değişkenlerin birlikte ele alınması, farklı uygulama biçimlerini ortaya koyma ve açıklama noktasında değerli katkılar sunacaktır.

Çalışmada örnek vaka olarak; 2009-2021 yılları arasında ABD tarafından yürütülen siber caydırıcılık stratejisi ele alınmıştır. Vaka çerçevesinde siber tehditlerin kullanılmasının sebebi; bu tehditlerin anarşiye dair klasik güç dengesi koşulları dışında güvenlik ilişkileri meydana getirmesi ve güvenlik stratejisi üretiminde aktör odaklı iç değişkenlere alan açmasıdır.

Çalışmanın hipotezi benzer yapısal koşullar altında devletlerin dış politika tercihlerinin stratejik kültür ve kurum değişkenleri doğrultusunda farklılık gösterebildiğidir. Çalışmanın modeli, hipotezin doğruluğunu test etmek amacıyla sırayla yöneltilen üç alt sorudan oluşmaktadır. Bu sorular sırasıyla şu şekildedir:

1. Güç dağılımı ve tehdit algılaması koşullarının siber tehditlere karşı caydırıcılık stratejisinin benimsenmesinde etkileri nelerdir?
2. Benzer yapısal koşullar altında devletlerin siber caydırıcılık stratejileri farklılık gösterir mi? Eğer gösterir ise;
3. Caydırıcılık stratejileri arasındaki farkların oluşumunda stratejik kültür ve kurum değişkenlerinin etkileri nelerdir?

Hipotezin testinde yöneltilen her soru, farklı bir değişkeni analiz etmek için tasarlanmıştır. Şöyle ki, güç dağılımı etkilerini sorgulayan ilk soru hipotezin bağımsız değişkeni olan yapısal faktörlere eğilirken ikinci soruda bağımlı değişken olan caydırıcılık stratejisi farklılaşması sorgulanmaktadır. Son sorunun ele alındığı bölümde ise bağımlı değişken farklılaşmasının nedenleri stratejik kültür ve kurum ara değişkenlerinde aranmaktadır.

Araştırmada nitel araştırma yöntemlerinden karşılaştırmalı vaka analizi yöntemi ve Stuart Mill'in "En Benzer Sistemler Tasarımı" kullanılmıştır. Çalışmada vaka analizi yönteminin seçilmesinin önemli bir nedeni Neoklasik Realizmin, kapsam ve sınırlılıkları itibariyle halen gelişmekte olan bir teori olmasıdır. Bu araştırmada başvuru vakaların teorisinin geçerlilik iddiasına önemli katkılarda bulunacağı değerlendirilmektedir. Nitekim "*Uluslararası Siyasetin Neoklasik Realist Teorisi*" adlı çalışmada Lobell, Ripsman ve Taliaferro teori çerçevesi kullanarak yapılacak farklı vaka analizlerinin teoriye önemli katkılar sunacağını ifade etmektedir.⁵

George ve Bennett teori oluşturma ve test etmede vaka analizi yönteminin nicel araştırmalara olan üstünlüğüne dikkat çekerek yöntemin avantajlarını şu şekilde sıralamaktadır:⁶

1. Yüksek kavramsal geçerliliğe ulaşma potansiyeli,
2. Yeni hipotezler üretebilmek için güçlü yaklaşımlar ihtiva etme,
3. Hipoteze konu olan nedensellik bağının farklı vaka bağlamlarına oturtulabilmesi,
4. Açıklanması karmaşık nedensellik bağlarına ışık tutabilmesi.

Görüldüğü gibi vaka analizi yönteminde diğer yöntemlere kıyasla öne çıkan husus nedensellik bağının test edilmesidir. Yöntemin sağlamış olduğu bu fayda iç değişkenlerin etkilerinin analiz edilebilmesi açısından kullanışlı bir çerçeve sunmaktadır. Bu doğrultuda seçilen vakalarda bağımsız değişken ve kontrol değişkenlerinin benzerlik oranının yüksek olması hedeflenmiş ve böylece ara değişken ile bağımlı değişken arasındaki ilişki derinlemesine incelenmiştir.

Çalışmada etkileri test edilen ara değişkenler stratejik kültür ve kurumlardır. Bu değişkenlerin caydırıcılık stratejisi üzerindeki etkilerini test etmek için ABD siber güvenlik politikaları analiz birimi olarak kabul edilmiştir. Dış politika kararlarının alınmasında Neoklasik Realizm karar alıcı yaklaşımlarının dış politika tercihlerinde farklılık yaratabildiğini öne sürmektedir. Bu açıdan bakıldığında ABD siyasetinde birçok bakımdan farklı bir çizgiye sahip olan Donald Trump başkanlığının ABD

⁵ Ripsman, Taliaferro, ve Lobell, 181.

⁶ Alexander L. George ve Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge: MIT Press, 2005), 40.

caydırıcılık stratejisinde meydana getirdiği farkları test edebilmek Neoklasik Realizm için kritik bir vaka niteliği taşımaktadır. Bahse konu olan farkların test edilebilmesi için ABD siber güvenlik politikalarını kapsayan caydırıcılık stratejisi oluşturma süreçleri irdelenmiştir. Kontrollü karşılaştırma yönteminde boylamsal analiz ilgili vakaya dair gelişmeleri zamansal olarak bölmekte ve “öncesi-sonrası” karşılaştırmasını mümkün kılmaktadır.⁷ Bu doğrultuda ABD siber caydırıcılık stratejisinin gelişimi Obama dönemi (2009-2016) ve Trump dönemi (2017-2021) olmak üzere iki ayrı zaman dilimine ayrılmış ve karşılaştırmaya tabi tutulmuştur.

Vaka analizinin ilk bölümü olan yapısal değişkenler bölümünde yukarıda sunulan soruya - Güç dağılımı ve tehdit algılaması koşullarının siber tehditlere karşı caydırıcılık stratejisinin benimsenmesinde etkileri nelerdir? – cevap aranmıştır. Bu kapsamda hipotezin bağımsız değişkeni olan güç dağılımı ve tehdit algılamasının caydırıcılık stratejisindeki etkisi incelenmiştir. ABD’nin içinde bulunduğu uluslararası bağlamın ortaya konulması, güvenlik stratejilerine yön veren ana çerçevenin belirlenmesi açısından önemlidir. Bu doğrultuda küresel güç dağılımında ABD’nin farklılaşan konumu ve farklılaşan tehdit algılaması strateji belgeleri ve siber saldırı veri tabanları aracılığıyla ortaya konulmuştur.

Bir sonraki bölümde yanıt aranan soru benzer yapısal koşullar altında devletlerin siber caydırıcılık stratejilerinin farklılık gösterip göstermediğidir. Bağımlı değişkende bir farklılaşma olup olmadığını ortaya koymak maksadıyla öncelikle bu değişkenin aldığı değerler (ikna/dayanıklılık yoluyla caydırıcılık ve ceza yoluyla caydırıcılık metodu) ortaya çıkarılmıştır. Zira uygulanan caydırıcılık stratejileri verili olmayıp, incelemeye konu olan siber güvenlik politikalarının caydırıcılık çerçevesinde yorumlanması sonucu ortaya çıkmaktadır. Bu kapsamda; 2009-2021 yılları arasında yayımlanan ABD ulusal güvenlik belgeleri, siber güvenlik belgeleri ve Başkanlık İcra Emirleri gibi siber güvenlik ile ilgili 25 adet birincil kaynak analiz edilmiştir. Elde edilen bulgular caydırıcılık stratejisi kapsamında yorumlanmış ve izlenen metot ortaya çıkarılmıştır. Bağımlı değişken olan caydırıcılık stratejisi iki ayrı nominal değer ile ölçeklendirilmiştir: İkna/dayanıklılık yoluyla caydırıcılık metodu ve ceza yoluyla caydırıcılık metodu.

⁷ George ve Bennett, 210-11.

Analizin son bölümü olan iç değişkenler bölümünde- Caydırıcılık stratejileri arasındaki farkların oluşumunda stratejik kültür ve kurum değişkenlerinin etkileri nelerdir? – sorusuna yanıt aranmıştır. Bu doğrultuda iki dönemde görülen farklı caydırıcılık metotları ile stratejik kültür ve kongre değişkenleri arasındaki nedensellik bağı incelenmiştir. Bu bölümde süreç takibi metoduna başvurulmuştur. Süreç takibi metodu, Stuart Mill’in analiz tasarımları ile ortaya konulan ve nedensel ilişkilerin değerlendirilmesini sağlayan etkin bir araçtır.⁸ İncelemeye konu nedensel ilişkiyi tespit etmek için sebepten sonuca giden sürecin açığa çıkarılması gerekmektedir.⁹

Veri analizi sonucunda, ilgili başkanlık dönemine dair saptanan caydırıcılık stratejisi metodunu mümkün kılan resmî belgenin bizzat başkanlık makamı tarafından yayımlanması caydırıcılık stratejisi ve başkan arasında eylemsel bir ilişkiyi ortaya koymaktadır. Bu bulgu, hipotezin geçerliliği için gerekli bir şarttır. Bununla birlikte tek başına bu ilişki caydırıcılık stratejisi üzerindeki stratejik kültür etkenini ispatlamak için yeterli değildir. Zira başkan söz konusu belgeyi kurumlar, muhalefet baskısı veya anlık bir dış tehdit gibi farklı bağlamsal koşullar altında yayımlamış olabilir. Başkanın benimsemiş olduğu stratejik kültürün söz konusu başkanlık belgesi ve caydırıcılık stratejisi ile uyumlu olduğunu ortaya koymak, ara değişken ve bağımlı değişken arasındaki nedensellik bağına güçlendirecek bir yeter şarttır. Burada liderin benimsediği stratejik kültür çerçevesi olarak Mead’in dış politika gelenekleri kavramından faydalanılmıştır. Söz konusu geleneklerden Jeffersoncılık Başkan Obama ile, Jacksoncılık ise Trump ile ilişkilendirilmiş ve bu geleneklerin temsil ettiği düşünce kalıpları sunulmuştur. Daha sonra söz konusu geleneklerin karakteristik özellikleri bağlamında caydırıcılık stratejilerinde farklılığa yol açan ana belgeler incelenmiştir. Son olarak, bu belgelerde tespit edilen yaklaşımlar başkanların diğer ofansif kabiliyet kullanımı öngören dış politika kararları ile karşılaştırılarak birbirleri ile uyumluluğu incelenmiştir.

Kurum değişkeninin incelendiği son bölümde ise ABD Kongresinin siber güvenlikle ilgili yasama ve denetim faaliyetleri incelenmiştir. ABD siyasal sistemi, yürütme-yasama ve yargı sistemlerinin birbirini etkin bir şekilde kontrolüne ve güçler dağılımına

⁸ George ve Bennett, 268.

⁹ David Collier, “Understanding Process Tracing”, *PS: Political Science & Politics* 44, sayı: 04 (Ekim 2011): 824, <https://doi.org/10.1017/S1049096511001429>.

dayanmaktadır. Özellikle dış politika uygulamalarında yürütme organı tarafından takip edilecek siyasete temel teşkil edecek yasama faaliyetleri önemli rol oynamaktadır. Bu yüzden başarılı bir dış politika için Başkan ve Kongrenin uyumlu çalışmasının gerekli olduğu ifade edilebilir. Çalışmanın bu bölümünde Kongrenin yapısı, çalışmaları, başkanla olan ilişkileri ve başkanın tek taraflı uygulamaları incelenerek Kongrenin farklılık yaratan caydırıcılık stratejilerindeki rolü sorgulanmıştır.

Karşılaştırmalı vaka analizinde caydırıcılık stratejilerindeki farklılıkları ortaya koyabilmek için Obama ve Trump dönemindeki Siber Güvenlik Belgeleri analiz edilmiştir. Caydırıcılık stratejisinin doğrudan somut sonuçlar barındırmayan subjektif yapısı analiz edilen stratejilerin farklı şekilde yorumlanabilmesi sonucunu doğurabilmektedir. Bu sınırlılığı aşmak için karşılaştırmada birincil kaynaklara yer verilmiştir. Bu kaynaklar güvenlik strateji belgeleri, siber güvenlik belgeleri ve icra emirleridir. Yalnızca Trump döneminde yapılmış olan 13. Ulusal Güvenlik Başkanlık Memorandumu (NSPM-13) halen gizli belge statüsünde olmasından dolayı bu veriye yönelik ikincil kaynaklara başvurulmuştur. Belgelere ilaveten söz konusu dönemlerin siber güvenlik politikalarına etki eden siber saldırı, kurum inşası, yetkilendirme gibi birtakım önemli gelişmelere de aynı esaslar dahilinde yer verilmiştir.

	BARACK OBAMA DÖNEMİ	DONALD TRUMP DÖNEMİ
Güvenlik Strateji Belgeleri	Ulusal Güvenlik Stratejisi (2010) Ulusal Güvenlik Stratejisi (2015)	Ulusal Güvenlik Stratejisi (2017)
Savunma Bakanlığı / İç Güvenlik Bakanlığı Siber Strateji Belgeleri	Siber Uzayda Harekât Strateji Belgesi (2011) Siber Uzay Politika Raporu (2011) Savunma Bilimi Kurulu Raporu – Dayanıklı Askeri Sistemler ve Gelişmiş Siber Tehdit Raporu (2013) Savunma Bakanlığı Siber Stratejisi (2015)	Savunma Bakanlığı Siber Stratejisi (2018) İç Güvenlik ve Ticaret Bakanlıkları Raporu: Botnet ve Diğer Otomatik Dağıtık Tehditlere Karşı İnternet ve İletişim Ekosisteminin Dayanıklılığını Artırmak (2018)
Başkanlık İcra Emirleri	İcra Emri 13636 (2013) İcra Emri 13687 (2015) İcra Emri 13691 (2015) İcra Emri 13694 (2015) İcra Emri 13718 (2016) İcra Emri 13757 (2016)	İcra Emri 13800 (2017) İcra Emri 13870 (2019) İcra Emri 13873 (2019) İcra Emri 13942 (2019) İcra Emri 13943 (2019) İcra Emri 13984 (2021)
Başkanlık Siber Güvenlik Belgeleri	Siber Uzay Politika Değerlendirmesi (2009) Siber Uzay Uluslararası Stratejisi (2011) Siber Uzayda Güvenilir Kimlikler için Strateji (2011)	Ulusal Siber Strateji (2018)
Başkanlık Siyaset Direktifleri	Başkanlık Siyaset Direktifi-20 (2012) Başkanlık Siyaset Direktifi-21 (2013) Başkanlık Siyaset Direktifi-41 (2016)	Başkanlık Siyaset Direktifi-20 Revizyonu: Ulusal Güvenlik Başkanlık Memorandumu-13 (2018)
Önemli Olaylar	Stuxnet Saldırısı (2009) Siber Komutanlığın Kurulması (2009) İran, Kuzey Kore, Çin ve Rusya tarafından Gerçekleştirilen Siber Saldırıları (2012-2016)	Beyaz Saray Siber Güvenlik Koordinatörü Kadrosunun İptal Edilmesi (2018)

Tablo 1: Başkanlık Dönemlerine İlişkin Analiz Edilen Veri Tablosu

Siber saldırıları gerçekleştiren aktörler genel olarak sorumluluğu kabul etmemekte, saldırılar devlet harici terör örgütü, hacker grupları gibi farklı aktörler tarafından gerçekleştirilmekte ve devletlerin yapılan saldırıyı tespit edemediği durumlar ile karşılaşmaktadır. Bahse konu olan mevcut durum doğrultusunda, araştırmada spesifik bir aktöre yönelik caydırıcılık stratejisinden ziyade caydırıcılık kavramı genel bir dış politika stratejisi olarak ele alınmıştır.

Yukarıda bahsedilen sınırlılığa paralel olarak, kuramsal açıdan ele alındığında, araştırmada caydırıcılık stratejisi ikinci tip Neoklasik Realizm çerçevesinde değerlendirmektedir. Şöyle ki teorinin gelişim evresine bakıldığında; Neorealizmin açıklamakta sınırlı kaldığı dış politika tercihlerini analiz eden çalışmalar birinci tip, devletlerin tüm dış politika tercihlerini açıklama iddiasında olan çalışmalar ikinci tip, dış politikadan yola çıkarak tümevarımsal bir şekilde yapıyı açıklama hedefi olan

alışmalar ise üçüncü tip Neoklasik Realizm yaklaşımı olarak ifade edilmektedir.¹⁰ Bu doğrultuda araştırmada ele alınan bağımlı deęişken ne bir Neorealizm anomalisi, ne de yapısal bir uluslararası ilişkiler teorisidir. Analizde incelenen caydırıcılık metotları, ikinci tip yaklaşımı esas alan dış politika stratejisinin bir ürünüdür.

Çalışmanın esas ağırlık noktası Neoklasik Realizmin caydırıcılık stratejisindeki uygulamasını test ederek kuramsal bir katkı sağlamaktır. Bu doğrultuda liderlerin politik psikolojilerine yer verilmemiştir. Zira algı ve psikolojileri ön plana çıkaran alternatif bir yaklaşım çalışmanın kuramsal çerçevesini Klasik Realizme yaklaştıracaktır. Diğer taraftan benzer hassasiyetle stratejik kültür bileşeni dar bir kapsamda ele alınmıştır. Stratejik kültür kavramının farklı boyutlarını ele alan zengin bir alan yazının bulunduğu aşıkardır. Bununla birlikte söz konusu geniş çerçeveye başvurmak çalışmanın esas amacı olan kuram testini geri planda bırakacaktır. Dolayısıyla kuramsal katkının daha belirgin bir şekilde ortaya konması maksadıyla stratejik kültür kavramı Mead'ın Dış Politika Gelenekleri çerçevesinde kullanılmıştır.

Bahsedilen kapsam ve sınırlılıklara ilaveten bir diğer sınırlılık da bağımlı deęişken olan caydırıcılık stratejilerinin tipolojik olarak yorumlanması ve başarı durumunun kapsam dışı bırakılmasıdır. Diğer bir deyişle, söz konusu caydırıcılık stratejilerinin siber saldırılar karşısında başarı veya başarısızlığı çalışmanın konusu deęildir. Ele alınan konu başvuru farklı caydırıcılık metotlarıdır.

Elde edilen verilen analizinde içerik analiz yöntemine başvurulmuştur. Bu doğrultuda ABD'nin siber uzaya ilişkin dış politikasına yön veren resmî belgelerinin her biri şu ara başlıklar altında incelenmiştir:

- Belgenin tanımı
- Tehdit algılaması
- Ağırlık noktaları
- Amaçları
- Araçları
- Caydırıcılık metodu

¹⁰ Ripsman, Taliaferro, ve Lobell, *Neoclassical Realist Theory of International Politics*, 80-91.

Belirlenen altı ara başlık aracılığıyla farklı kaynak ve içeriklere sahip olan resmî belgelerin mümkün olduğunca standart bir şekilde analiz edilmesi ve analiz sonucu her bir belgeye ilişkin caydırıcılık metodu elde edilmesi hedeflenmiştir. Belgede geçen caydırıcılık metodunun tespitinde ceza yoluyla caydırıcılık için cezai yaptırımları ihtiva eden ofansif araçların izi sürülmüştür. Diğer metotlar için aşağıda sunulan teorik tanımlamalar kullanılmıştır.

İkna yoluyla caydırıcılık metodunda, rakibin amacına ulaşma ve fayda elde etme kabiliyetini fiziksel olarak imkânsız hale getirmek hedeflenir.¹¹ Rakibe verilen mesaj, istenmeyen davranışı uygulaması durumunda vermiş olduğu kararın kendine büyük maliyetler/zararlar doğuracağıdır.¹² Dayanıklılık, maruz kalınan bir saldırı sonrasında iyileşebilme ve mevcut koşullara adapte olarak gelecek muhtemel tehditlerin zararlarından kaçınma becerisidir.¹³ Amaç, saldırının öngörülen etkileri doğurmadığını rakibe gösterip bir sonraki eyleme dair öngörülen faydaların gerçekleşmeyeceği algısını yaratmaktır. Reaktif bir tutum benimsemeleri ve savunma tedbirlerini içermeleri bakımından ikna ve dayanıklılık yoluyla caydırıcılık stratejileri tek bir metot olarak ele alınmıştır. İncelemede siber güvenlik platformlarının donanım ve yazılımsal güncelleştirilmeleri, siber iş gücü nitelik ve niceliğinin artırılması, kritik altyapı savunmasında güvenlik artırıcı idari tedbir ve sorumluluk tahsisleri, kamu-özel sektör iş birliğinin artırılması gibi adımlar savunma düzeyini artıran adımlardır. Bu adımların etkinliği rakibin saldırgan davranışlarının başarıya ulaşma şansını azalttığından ve bir resmî güvenlik belgesi vasıtasıyla rakibe dolaylı olarak iletildiğinden ötürü ikna ve dayanıklılık yoluyla caydırıcılık stratejisi kapsamında değerlendirilmiştir. Öte yandan analiz edilen belgelerde geçen; rakibe bedel ödetme anlayışına dayanan ofansif tedbirler ise ceza yoluyla caydırıcılık metodu olarak yorumlanmıştır.

Stratejik kültür ve kurum bileşenlerinin etkilerinin analizi sonucunda elde edilen bulgular, siber güvenlik uygulamalarının başkanların benimsemiş olduğu stratejik kültürlerin doğal bir uzantısı olduğunu ve farklılaşan caydırıcılık stratejilerinde doğrudan belirleyici olduğunu göstermektedir. Kongrenin ise yasama ve denetim

¹¹ Snyder, *Deterrence by Denial and Punishment*, 38.

¹² Schelling, *Arms and Influence*, 78-79.

¹³ Lasconjarias, "Deterrence Through Resilience: NATO, the Nations and the Challenges of Being Prepared", 2.

yoluyla caydırıcılık stratejisine katkıda bulunma ve yön verebilme kapasitesinin bulunduğu, ancak söz konusu gücü partizanlık engelinin aşıldığı koşullarda ortaya koyabildiği görülmektedir.



AKADEMİK YAZINDA CAYDIRICILIK STRATEJİSİ

Caydırıcılık, bir aktörün belirli bir davranış biçimini benimsemesi halinde maliyetlerle karşılaşacağına dair bir beklenti oluşturarak bu davranışın engellenmesini amaçlayan stratejik bir yaklaşımdır.¹⁴ Bu strateji, özellikle II. Dünya Savaşı sonrasında nükleer silahların ortaya çıkmasıyla birlikte uluslararası ilişkilerde merkezi bir konuma yerleşmiş ve bu silahların kullanım tehdidi üzerinden şekillenen zorlayıcı diplomasi türü olarak kavramsallaşmıştır.

Siber caydırıcılık ise, dijital altyapılara yönelik kötü niyetli faaliyetlerin önlenmesini hedefler ve bu faaliyetleri yürüten aktörlerin geniş bir yelpazeye yayılması nedeniyle klasik caydırıcılıktan önemli farklılıklar taşır.¹⁵ Bu çalışmada siber tehditler; devletin stratejik çıkarlarına zarar verebilecek, askeri veya sivil altyapılara yönelen saldırılar olarak ele alınmaktadır. Siber saldırılar; düşük maliyetli, yüksek erişimli ve anonim karakterleri nedeniyle karşılıklı şeffaflık ve hesap verebilirlik ilkelerini ihlal etmektedir. Bu yönüyle siber caydırıcılık, nükleer caydırıcılığın topyekûn engelleme mantığından ayrılarak, tehditlerin yoğunluğunu ve sıklığını azaltmaya odaklanan bir stratejiye evrilmiştir.¹⁶

Çalışmanın amacı caydırıcılık stratejisi uygulamalarındaki iç bileşen etkisini ortaya koymaktır. Bunun için söz konusu probleme dair akademik yazın eksikliğini saptamak ve problemin çözümünde başvurulacak kavramları açıklamak önem arz etmektedir. Bu doğrultuda caydırıcılık stratejisinin bir akademik araştırma alanı olarak doğuşundan günümüze kadar olan gelişimi sunulmuştur. Söz konusu süreç farklı karakteristik özellikleri barındıran dört dalga aracılığıyla izah edilmiştir.

¹⁴ Thazha V. Paul vd., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, 2009)

¹⁵ Eugenio Lilli, “Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence”, *Contemporary Security Policy*, Sayı: 42 (2) (2021):163.

¹⁶ A.g.e.

1.1. Caydırıcılığın Tarihsel Gelişimi

“Si Vis Pacem, Para Bellum”

(Barış istiyorsan savaşa hazır ol!)

Antik yazar *Flavius Vegetius Renatus*’a ait bu söz, Caydırıcılık stratejisi pratiklerinin ilk çağlardan bu yana varlığını sürdürmekte olduğuna işaret etmektedir.¹⁷ Devletlerin varlıklarını korumak ve elde bulundurduğu askeri kabiliyetler vasıtasıyla rakiplerinin kararlarına yön verebilme gayreti tarih boyunca var olmuştur. Bununla birlikte, söz konusu davranışın kavramsallaştırılması, yeni bir askeri kabiliyetin ortaya çıkması ile mümkün olmuştur. İkinci Dünya Savaşı’nın sonu itibariyle sahne alan nükleer silahlar salt bir askeri kabiliyetten öte, güç ilişkilerini doğrudan etkileyerek Soğuk Savaşın ayrılmaz bir parçası haline gelmiştir. Caydırıcılığın halen “nükleer” kelimesi ile özdeşleşmiş durumda olmasının sebebi, kavramın dönemin düşünürleri tarafından nükleer silahlar ekseninde teorileştirilmesi ve bu silahların varlığından azami fayda sağlamak maksadıyla stratejiler üretilmesidir. Teorinin önemli araştırmacılarından Thomas Schelling’in şu ifadesi dönemin düşünürlerinin nükleer silahlara ve onların etkisiyle ortaya çıkan yeni koşullara bakış açısını yansıtmaktadır:

“Nükleer silahlar savaşları daha az askeri, zaferleri ise daha az değerli hale getirmiştir. Düşmana zarar vermek için zafer kazanmak şartını ortadan kaldıran bu kabiliyetler şüphesiz savaşın doğasını da değiştirmiştir.”¹⁸

Caydırıcılık kavramı aynı anda teori ve stratejiye karşılık gelen bir varsayım, söylem ve uygulama bütünü olarak karşımıza çıkmaktadır. Kavramın teorik gelişimine

¹⁷ Caydırıcılığın modern döneme ait bir strateji olmaktan öte antik çağa kadar uzanan köklü bir strateji olduğunu savunan en önemli çalışmalardan biri Richard Ned Lebow’un “Thucydides and Deterrence” adlı çalışmasıdır. Thucydides’in Peloponnes Savaşı aktarımlarını veri tabanı olarak kullanan Lebow, modern dönem Caydırıcılık teorisi ile M.Ö. 5’nci yüzyıl güç politikaları arasında önemli benzerlikler olduğunu öne sürmektedir. Atinalıların güç rekabetinde nispeten üstün durumlarından yola çıkarak söz konusu üstünlüklerini hedefleri doğrultusunda kullanma kararlılıklarının modern dönem Caydırıcılık teorisyenlerinden Thomas Schelling’in tespitleri ile aynı düzlemde olduğunu ifade eden Lebow, caydırıcılığın başarısız olmasındaki “insani” faktörlerin önemine dikkat çekmiştir. Richard Ned Lebow, “Thucydides and Deterrence”, *Security Studies* 16, sayı 2 (2007): 163-88, <https://doi.org/10.1080/09636410701399440>.

¹⁸ Thomas C. Schelling, *Arms and Influence*, 2008 Edition (Londra: Yale University Press, 1966), 22.

bakıldığında konjonktürel olarak iki koşuldan¹⁹ önemli derecede etkilendiği ve bu doğrultuda şekillendiği görülmektedir:

1. Nükleer Silahların Etkisi
2. Çift Kutuplu Dünya Düzeni

Bu eğilimin nedenlerini şu şekilde açıklamak mümkündür: Öncelikle teorisyenler nükleer silahların devasa yıkım kapasitelerinden oldukça etkilenmişler ve bunun farklı kavramlarla açıklanması gereken yeni bir dönemin habercisi olduğunu savunmuşlardır. Caydırıcılık teorisinin fikir babası olarak kabul edilen Bernard Brodie'nin, bahse konu olan bu yeni askeri kabiliyete yönelik olarak şu ifadeleri dikkat çekicidir:

“Şimdiye kadar askeri yapılanmamızın temel amacı savaşları kazanmak olmuştur. Bundan sonra ise asıl amacımız savaşları önlemek olacaktır.”²⁰

Bu ifade ile Brodie, bir taraftan yeni savaşların altından kalkılamayacak muhtemel tahribatına dikkat çekerken diğer taraftan bu silahları etkin bir şekilde araçsallaştırmanın yolunun onları kullanmaktan ziyade sahip olmak olduğuna işaret etmektedir. Caydırıcılığın ana fikri olan askeri kabiliyetler üzerinden tehditler yaratarak rakibin karar alma mekanizmalarına etki edebilme düşüncesi, Brodie'nin bu eserinden yola çıkarak kavramsallaşmıştır.

1.2. Caydırıcılığın Dört Dalgası

Caydırıcılığın kavramsal ve metodolojik gelişimini takip etmede Robert Jervis'in 1979 yılında yayımladığı *Deterrence Theory Revisited*²¹ adlı makalesi kullanışlı bir çerçeve sunmaktadır. Adı geçen çalışmada Jervis, nükleer silahların ortaya çıkışından bu tarihe kadar yapılan akademik çalışmaları amaç, kapsam ve metotlar bağlamında üç dalga halinde sınıflandırmıştır. Söz konusu sınıflandırma, kendinden sonra gelen

¹⁹ Kenneth N. Waltz, “Emerging Structure of International Politics”, *International Security* 18, sayı:2 (1993): 44.

²⁰ Bernard Brodie, *The Absolute Weapon: Atomic Power and World Order* (New York: Yale University Institute of International Studies, 1946), 62.

²¹ Robert Jervis, “Deterrence Theory Revisited”, *World Politics* 31, sayı:2 (1979): 289-324, <https://doi.org/doi:10.2307/2009945>.

araştırmacılar²² tarafından sıklıkla kullanılarak literatür takibi açısından anlaşılır bir zemini oluşturmuştur. Jervis'e göre nükleer silahların ortaya çıkışı ile başlayan birinci dalga, bu yeni kabiliyeti anlamlandırma ve uluslararası güvenlikteki yerini konumlandırmaya yönelik ilk adımları teşkil etmektedir. Albert Wohlstetter ve Bernard Brodie gibi araştırmacılar tarafından temsil edilen akımı Jervis, takip eden çalışmalar için bir hazırlık ve geçiş süreci olarak tanımlamıştır.²³ Jervis'in çalışmasında ikinci dalga üzerinde önemle durduğu görülmektedir. Jervis'e göre teori ve buna bağlı bir ulusal strateji geliştirilmesi söz konusu dönemde paralellik kazanmış, oyun teorisi, rasyonalite, inanılabilirlik ve manipülasyon gibi kavramların caydırıcılıktaki yeri irdelenmiştir.²⁴

Teoride üçüncü dalganın habercisi ise Alexander George ve Richard Smoke'un ses getiren *Deterrence in the American Foreign Policy*²⁵ adlı kitabıdır. Bu çalışma birinci ve ikinci dalga araştırmalarına yöneltilen test edilme, ispatlama ve genelleme gibi bilimsel araştırma özelliklerinden yoksunluk eleştirilerini dikkate alan ilk çalışmadır. George ve Smoke, Amerikan zorlayıcı diplomasisi çerçevesinde giriştikleri vaka analizlerinde caydırıcılığın başarı ihtimalindeki adanmışlık ve risk analizi değişkenlerini

²² Lawrence Freedman, "Deterrence: A Reply", *Journal of Strategic Studies* 28, sayı:5 (2005): 789-801, <https://doi.org/10.1080/01402390500393944>;

Amir Lupovici, "The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda", *International Studies Quarterly* 54 (2010): 705-32;

Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research", *Contemporary Security Policy* 31, sayı: 1 (2010): 1-33, <https://doi.org/10.1080/13523261003640819>;

Reuben Steff, *Strategic Thinking, Deterrence and the US Ballistic Missile Defense Project: From Truman to Obama* (Surrey: Ashgate Publishing Limited, 2013).

²³ Jervis, "Deterrence Theory Revisited", 291.

²⁴ Jervis, 292-93;

Schelling, *Arms and Influence*;

Herman Kahn, *Thinking about the Unthinkable* (New York: Avon Books, 1962);

Glenn Snyder, "The Balance of Power and the Balance of Terror", içinde *The Balance of Power*, ed. Paul Seabury (San Fransisco: Chandler Books, 1965);

Glenn Snyder, *Deterrence and Defense. Toward a theory of national security*. (New Jersey: Princeton University Press, 1961).

²⁵ Alexander George ve Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia Universtiy Press, 1974).

inceleyerek sebep-sonuç ilişkilerini ortaya koymuşlardır. Böylece, bu çalışma ile o tarihe dek soyut biçimde ele alınan bir tür reçeteler bütünü olarak betimlenebilecek olan akademik çalışmalara bilimsel bir boyut kazandırmıştır. Dolayısıyla bu çalışma takip eden dönemde yapılan çalışmalara yön vermiştir.²⁶ Takip eden süreçte Knopf, Soğuk Savaşın sona ermesi ile birlikte yeni oluşan düzlemde ortaya çıkan kabiliyet ve tehdit algılamalarındaki farklılaşmaları dördüncü dalga olarak adlandırmış ve günümüze kadar gelen son dönem caydırıcılık çalışmalarını bu sınıfa dahil etmiştir.²⁷

Bu kapsamda; akademik yazında görülen son dönem akademik çalışmalar, caydırıcılık aktörlerine devlet dışı aktörleri ilave ederken, kullanılan kabiliyetleri salt nükleer ve konvansiyonel silahlardan öte terörizm, savaş dışı çatışmalar ve de siber araçlar olarak incelemektedir.²⁸ Görüldüğü gibi en başta belirli güç dengesi koşullarında indirgemeci ve doktrinel bir görünüm sunan caydırıcılık çalışmaları ilerleyen süreçte farklı aktörleri ve kabiliyetleri çalışma kapsamına dahil etmiştir. Bununla birlikte söz konusu analizlerdeki iç değişken eksikliğinin dört dalga boyunca varlığını sürdürdüğü görülmektedir. Aşağıdaki bölümde söz konusu dalgalara ait çalışmalara daha geniş yer verilerek katkıda bulunulması amaçlanan akademik yazın eksikliği aktarılmıştır.

²⁶ Paul Huth ve Bruce Russett, “What Makes Deterrence Work? Cases from 1900 to 1980”, *World Politics* 36, sayı: 4 (1984): 496-526;

Vesna Danilovic, *When Stakes are High* (Michigan: The University of Michigan Press, 2002); Vipin Narang, *Nuclear Strategy in the Modern Era* (Oxford: Princeton University Press, 2014);

Frank C. Zagare ve Mark D. Kilgour, *Perfect Deterrence* (New York: Cambridge University Press, 2004);

Stephen L. Quackenbush, *Understanding General Deterrence* (New York: Palgrave Macmillan, 2011).

²⁷ Knopf, “The Fourth Wave in Deterrence Research”.

²⁸ Van Jackson, “Beyond Tailoring: North Korea and the Promise of Managed Deterrence”, *Contemporary Security Policy* 33, sayı: 2 (2012): 289-310, <https://doi.org/10.1080/13523260.2012.693795>;

Emilio Iasiello, “Is Cyber Deterrence an Illusory Course of Action?”, *Journal of Strategic Security* 7, sayı: 1 (2014): 54-67;

Frank C. Zagare ve Stephen L. Quackenbush, “Modern Deterrence Theory: Research Trends, Policy Debates, and Methodological Controversies”, *Oxford Handbooks Online*, 2016

Alex Wilner, “US cyber deterrence: Practice guiding theory”, *Journal of Strategic Studies*, 2020, <https://doi.org/10.1080/01402390.2018.1563779>;

Lupovici, “The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda”; Doron Almog, “Cumulative Deterrence and the War on Terrorism”, *Parameters* 34, sayı: 3 (2004): 4-19.

CAYDIRICILIK STRATEJİSİNE İLİŞKİN AKADEMİK ÇALIŞMALAR						
Araştırmacılar	Tehdit Cinsi	Caydırıcılık Bileşeni	Temel Argüman	Çalışma Bulguları	Araştırma Sorunsalı	Temsil Ettiği Yaklaşım
Bernard Brodie, Albert Wohlstetter	Nükleer	Kapasite İnandırıcılık	Nükleer silahlar ile birlikte savaşları kazanmak değil, misilleme kabiliyeti edinmek önemli hale gelmiştir.	Teorik	Caydırıcılığın Başarı Durumu	1. Dalga
Thomas Schelling, Herman Kahn	Nükleer	İnandırıcılık İletişim	Nükleer silahı kullanma kararlılığını rakibe daha etkin şekilde gösteren taraf caydırıcılıkta başarılı olur.	Teorik	Caydırıcılığın Başarı Durumu	2. Dalga
John Mearsheimer	Nükleer Konvansiyonel	Kapasite İnandırıcılık İletişim	Nükleer silahların imha kapasitesi arttıkça elde bulunduran tarafın caydırıcılık ihtimali artar. Konvansiyonel ortamda ise elde bulundurduğu silahlı kapasiteyi bir çabuk zafere dönüştürebilen ve bu tehdidin geçerliliğini karşı tarafa kabul ettiren taraf caydırıcılık sağlar.	Teorik	Caydırıcılığın Başarı Durumu	2. Dalga
Alexander George, Richard Smoke	Konvansiyonel	İnandırıcılık İletişim	Caydırıcılığın başarısı, askeri tehditlerin ötesinde, bağlamsal koşullara, diplomatik süreçlere ve rakiplerin risk alma yatınlığına bağlıdır.	Ampirik	Caydırıcılığın Başarı Durumu	3. Dalga
Frank Zagare, Mark Kilgour	Nükleer Konvansiyonel	İnandırıcılık	Tehditlerin imha kapasitesi ile caydırıcılık başarısı doğru orantılı değildir. Tehditler uygulanabilir olduğu sürece inandırıcı olur ve caydırıcılığı mümkün kılar.	Teorik	Caydırıcılığın Başarı Durumu	2. Dalga
Emilio Iasiello	Siber	Kapasite	Siber uzayda aktörlerin kar/zarar rasyonalitesi öngörülemez. Bu nedenle ceza yoluyla caydırıcılık etkin bir şekilde uygulanamaz. Bunun yerine savunma tedbirlerine dayanan ikna yoluyla caydırıcılık daha ön plandadır.	Teorik	Caydırıcılığın Başarı Durumu ve Caydırıcılık Metodu	4. Dalga
Maurizio Martellini	Siber	Kapasite	Saldırgan aktörün tespitindeki güçlük ve tüm tehditleri bertaraf etmenin neredeyse imkansız olması sebebiyle klasik caydırıcılık anlayışı yerine çok katmanlı ve dayanıklılık esaslı caydırıcılık tatbik edilmelidir.	Teorik	Caydırıcılık Metodu	4. Dalga
Alex Wilner	Siber	Kapasite	Gelişen teknolojiler, saldırgan tespitindeki güçlüğü ortadan kaldırmaktadır. Böylece ceza yoluyla caydırıcılık siber uzayda etkili bir yöntem haline gelmektedir.	Teorik Ampirik	Caydırıcılık Metodu	4. Dalga
Eugenio Lilli	Siber	Kapasite	Caydırıcılık stratejisi, siber uzaydaki bütün tehditlere karşı başarılı olamaz. Ancak sınırları ve çerçevesi belirli siber tehditlere karşı kullanıldığında başarılı olabilir. Bunun da en önemli şartı özel sektörün planlama ve uygulamada somut katkı sağlamasıdır.	Teorik	Caydırıcılığın Başarı Durumu	4. Dalga

Tablo 1: Caydırıcılık Alanyazınında Öne Çıkan Akademik Çalışmalar

1.2.1. Birinci ve İkinci Dalgalar:

Caydırıcılığın bir dış politika stratejisi olarak ilk kez kavramsallaşmaya başladığı bu dönemde araştırmacıların ve dış politika uygulayıcılarının kayda değer bir etkileşim halinde olduğu görülmektedir. Nükleer silahların etkilerinin henüz tam anlamıyla bilinmediği, stratejik dengenin yeni oluşmaya başladığı bu dönemde teorisyenler karar alıcılara yol gösterme arayışında olmuştur. Diğer taraftan nükleer silahlanma yarışından önemli derecede etkilenmişlerdir. Bu kapsamda Sovyetler Birliği'nin ABD nükleer monopolisini ortadan kaldırması ve 1957 yılında Sputnik uydusunu başarıyla yörüngeye oturtması ABD'nin kendi topraklarında bir nükleer saldırıya uğrama ihtimalini ortaya koymuştur. Böylece stratejiye dair akademik çalışmalar farklı bir yöne evrilmiştir. Söz konusu gelişmeye işaret eden Albert Wohlstetter, nükleer silahlara sahip olmanın

caydırıcılık için yeterli olmadığını, etkin bir caydırıcılık tesis etmek için muhtemel bir saldırıdan sağ kurtularak karşı tarafa misilleme yapabilme kabiliyeti gerekliliğinin altını çizmiştir.²⁹

Wohlstetter'in bu tespitini izleyen süreçte Caydırıcılık stratejisi akademik yazında ceza yoluyla caydırıcılık olarak anlaşılmıştır. Ceza Yoluyla Caydırıcılık, rakibe istenmeyen bir davranışta bulunması durumunda katlanmak istemeyeceği bir misillemeye maruz kalacağı iletilmesi ve bu yolla statükonun korunmasıdır. ABD Başkanı Kennedy'nin *Minuteman* ve *Polaris* füzelerinden oluşan Stratejik Taarruz Kuvveti'nin (*Strategic Offensive Forces*) ismini Stratejik Misilleme Kuvveti (*Strategic Retaliation Forces*) olarak değiştirmesi Ceza Yoluyla Caydırıcılığın bu dönemde ne kadar ön planda olduğunu göstermektedir.³⁰ Bu durumun akademik yazındaki tezahürünü Kenneth Waltz'un çalışmalarında görmek mümkündür. Waltz, yalnızca savunma yönü olan kuvvetlerin caydırıcılık değeri taşımadığını, etkin bir savunmaya sahip olunmasa bile cezalandırma yeteneği olan ikinci taarruz kuvvetlerinin başarılı bir caydırıcılık için elzem olduğunun altını çizmektedir.³¹

Soğuk Savaş döneminin en belirgin özellikleri olan güç dengesi koşulları ve nükleer silahlar caydırıcılık stratejisini güçlü bir biçimde etkileyerek Yapısal Caydırıcılığın ortaya atılmasına yol açmıştır. Waltz'a göre nükleer bir savaşta meydana gelecek yıkım ihtimali bu savaşları anlamsız kılmış, böylece uluslararası düzeni barışçıl kılan otomatik bir caydırıcılık sağlamıştır.³² Rasyonel aktörler olarak tanımlanan karar alıcılar söz konusu konjonktürde devasa maliyetlere neden olmamak için savaşı göze alamayacaklardır. Waltz, nükleer silahların yayılmasının engellenmemesi gerektiğini, daha fazla nükleer aktörün barış için gerekli olan kuvvet dengelerini sağlayacağını ve bu silahlara sahip olan devletlerin daha sorumlu davranacağını iddia etmiştir.³³

²⁹ Albert Wohlstetter, "The Delicate Balance of Terror", *Survival: Global Politics and Strategy*, sayı: 1 (1959): 8-9.

³⁰ Robert Zarate ve Henry Sokolski, *Nuclear Heuristics: Selected Writings of Albert and Roberta Wohlstetter* (Carlisle: Strategic Studies Institute, 2009), 170.

³¹ Kenneth N. Waltz, "The Spread of Nuclear Weapons: More May Be Better", *Adelphi Papers*, sayı: 171 (1981): 5.

³² Kenneth N. Waltz, "Nuclear Myths and Political Realities", *American Political Science Review* 84, sayı: 3 (Eylül 1990): 734.

³³ Waltz, "The Spread of Nuclear Weapons: More May Be Better".

Soğuk Savaşın sona ermesi sonrası Avrupa güç dengelerine dair öngörülerde bulunan Mearsheimer, Yapısal Caydırıcılığın önemli savunucularından biri olmuştur. “Uzun barışın”³⁴ ortaya çıkmasındaki en önemli gerekçeler olarak çift kutuplu stratejik denge ve nükleer silahların varlığını öne süren Mearsheimer, Soğuk Savaş dönemi Avrupa güvenlik konjonktüründeki barış ortamının ancak Nükleer bir Almanya ile mümkün olabileceğini iddia etmiştir.³⁵ Yazarların söz konusu yaklaşımlarının Yapısal Realizmden fazlasıyla etkilendiği görülmektedir. Zira başarılı bir caydırıcılık için güç dağılımı ve tehdit algılaması gibi faktörler ele alınmaktadır. Örneğin Mearsheimer’ın ileri sürdüğü üzere, nükleer silahların farklı devletler tarafından elde bulundurulduğu bir güç dağılımı senaryosunda bir “hayatta kalma” aracı olarak başvurulabilecek nükleer kabiliyetlerin beraberinde getirdiği katlanılamaz maliyetler ve nihayetinde oluşan “dehşet dengesi” (*mutual assured destruction*) statüko bozucu adımları rasyonel olmaktan çıkarak kendiliğinden bir caydırıcılık sağlanacaktır.³⁶

Özellikle ikinci dalga çalışmaları ile birlikte Rasyonel Caydırıcılık Teorisinin temelleri atılmıştır. Bu yaklaşım, aktörlerin kararlarını rasyonel fayda-maliyet analizine göre verdikleri varsayımına dayanır. Rasyonel aktörler olarak tanımlanan devletlerin yapısal faktörler karşısında benzer davranışlar göstereceği varsayılmaktadır. Diğer taraftan devlet içi değişkenlerin analize dahil edilmediği görülmektedir. Bu kısıtlılığa işaret eden Sagan’ın eleştirileri dikkat çekicidir. Sagan’a göre, devlet politikaları tek bir karar alıcının rasyonalitesine bağlı kalmaktan öte farklı iç mekanizmalar ekseninde şekillenmektedir. Sagan’ın ortaya koymuş olduğu Organizasyon Teorisine göre, güvenlik politikaları askeri kararlardır ve devlet liderlerinden ziyade askeri bürokrasinin ürünüdür. Söz konusu kararlar sınırlı rasyonalitenin egemen olduğu örgütsel bir mekanizmanın çıktısı olarak ortaya konmaktadır.³⁷ Sagan alınan kararların yanlış

³⁴ Soğuk Savaşa atfen kullanılan “Uzun Savaş” deyimi ilk kez John Lewis Gaddis tarafından kullanılmış ve sonrasında yaygınca benimsenmiştir. Gaddis, 1986 yılındaki makalesinde yapısal caydırıcılık teorisine paralel olarak nükleer silahların liderleri daha temkinli davranmaya davet eden istikrar yaratıcı etken olduğunu savunmuştur.

John L. Gaddis, “Long Peace: Elements of Stability in the Postwar International System”, *International Security* 10, sayı: 4 (1986): 99-142.

³⁵ John J. Mearsheimer, “Back to the Future: Instability in Europe after the Cold War”, *International Security* 15, sayı: 1 (1990): 53.

³⁶ Age, 21

³⁷ Scott D. Sagan, “The Perils of Proliferation: Organization Theory, Deterrence Theory and the Spread of Nuclear Weapons”, *International Security* 18, sayı: 4 (1994): 68.

hesaplama, koordinasyon eksikliği ve basitleştirici süreçler yüzünden nükleer düzenin belirsizlikleri karşısında her zaman optimal çıktıyı yaratamayacağını ifade etmektedir. Bu yönüyle Sagan, Waltz'un rasyonalite kavramına önemli bir eleştiri getirmektedir. Bu noktada Graham Allison'ın ünlü çalışması *Essence of Decision*, Sagan'ın argümanlarını doğrular niteliktedir. Allison devletin iç yapısındaki farklı karar mekanizmalarının alternatif rasyonaliteler yaratabileceğini savunmaktadır.³⁸

Caydırıcılık stratejisine dair kavramsal altyapının ağırlıkla birinci ve ikinci dalga akademik çalışmalar doğrultusunda inşa edildiği ifade edilebilir. Bu çalışmalarda, stratejiye ilişkin analizlerde önemli yer tutan inandırıcılık (*credibility*) kavramının çok çeşitli yönleriyle birlikte ele alındığı görülmektedir. Bununla birlikte söz konusu dönemde akademik çalışmalara yön veren William Kaufmann, Herman Kahn, Glenn Snyder ve Thomas Schelling gibi yazarlar inandırıcılık bileşenini nükleer silahlanma yarışı gölgesi ötesine götürememiştir.³⁹ Takip eden paragraflarda görüleceği üzere, bahse konu olan çalışmalarda caydırıcılığın tesisine dair önemli çıkarımlar ortaya atılmış olsa da bu çalışmalarda güç dengesi koşulları esas belirleyici etken olarak yerini korumuştur. Benzer ve homojen birer birim olarak ele alınan devletlerin uyguladığı caydırıcılık stratejisinin başarısı manipülasyon, tırmandırma ve oyun teorisi kavramları üzerinden açıklanma yoluna gidilmiştir.

Caydırıcılığın oluşumu için iki bileşenin gerekli olduğunu belirten Kaufmann, bu bileşenleri şu şekilde ifade etmiştir: Belirli bir faydayı savunmak için açıklanmış irade ve söz konusu iradeyi destekleyecek askeri kabiliyet.⁴⁰ Herman Kahn ise bu iki bileşene inandırıcılık kavramını eklerken karşılıklı caydırıcılık ilişkisinde algılamaların önemine işaret etmiştir. Kahn, ABD nükleer kabiliyetlerinin Sovyet karar alıcılarda nasıl bir algı yarattığı üzerinde varsayımlarda bulunarak caydırıcılığın çift taraflı doğasına dikkat çekmiştir. Etkin bir caydırıcılık için İkinci Taarruz Kabiliyeti (*Second Strike Capability*)

³⁸ Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown and Company, 1971).

³⁹ William Kaufmann, *Requirements of Deterrence* (Princeton: Princeton University Press, 1954)

Herman Kahn, *Thinking About the Unthinkable* (New York: Avon Books, 1962)

Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961)

Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966)

⁴⁰ William Kaufmann, *Requirements of Deterrence* (New York: Princeton University Press, 1954), 2.

ve Karşılıklı Teyit Edilmiş İmha (*Mutual Assured Destruction*) durumunun önemine işaret eden Kahn, ABD Stratejik Misilleme Kuvvetinin bu kabiliyete erişememesinin bir güvenlik ikilemi oluşturacağını altını çizmiştir. Bu noktada söz konusu seviyenin altında kalan nükleer kabiliyetin bir zayıflık algısı yaratacağı ve bu algıyı ortadan kaldırmak adına önleyici bir taarruzun elzem hale geleceğini ifade etmiştir.⁴¹ Söz konusu durumun her iki tarafı da önleyici bir saldırıya teşvik edeceğini ifade eden Kahn, yanlış algılara sebep olmamak için Teyit Edilmiş Caydırıcılığın gerekli olduğunu dile getirmiştir.

Bu noktada Patrick Morgan, Kahn’a önemli eleştiriler getirmektedir. Morgan’a göre nükleer silahların yok etme boyutları göz önüne alındığında, bu silahların etkilerini caydırıcı bir tehdit olarak sunmak kendi amacını aştığından dolayı anlamsızdır.⁴² Dahası bu durumun farkında olan rakip kendisine yöneltilen tehditleri bir blöf olarak görebilmektedir. Aslında söz konusu sıkıntı Kitlesele Caydırıcılık Stratejisinin ilanından sonra fark edilmiş ve Wohlstetter tarafından “Dereceli Caydırıcılık” (*Graduated Deterrence*) Stratejisi ortaya atılmıştır. Buna göre, gelişen tehdidin boyutu ile orantılı olarak nükleer silahların bir şekilde taktik kullanımı öngörülmektedir. Fakat söz konusu durum Sovyetlerin kendi taktik nükleer kabiliyetlerini geliştireceğinden ötürü fazla benimsenmemiştir.⁴³ Dolayısıyla nükleer silahların gerektiğinde kullanılabilme iradesi kuşku ile karşılanmaya devam edilmiştir. Morgan, “kullanılması muhtemel olmayan” silahlar üzerinden kurulan caydırıcılık anlayışını kesinlikle reddetmektedir. Morgan, gerçekleştirilemeyecek tehditler üzerine kurulu bir caydırıcılığın başarısız olacağını ve rakibi saldırmaktan alıkoymayacağını ifade etmektedir.⁴⁴ Saldırının niteliği konusunda açıklama yapmaması ise iki farklı yoruma sebebiyet vermektedir. Birincisi, eğer kastettiği nükleer bir saldırı ise kendi ile çeliştiği bir durum söz konusudur. Şöyle ki eğer nükleer silahların herhangi bir şekilde kullanılması amacını aşıyor ve bu doğrultuda etkin bir caydırıcılık sağlamıyorsa aynı durum söz konusu tarafların ilk taarruzu için de bir kısıtlama yaratmalıdır. Dolayısıyla “saldırı düşüncesindeki tarafı

⁴¹ Herman Kahn, *On Thermonuclear War* (Londra: Transaction Publishers, 2007), 158-59.

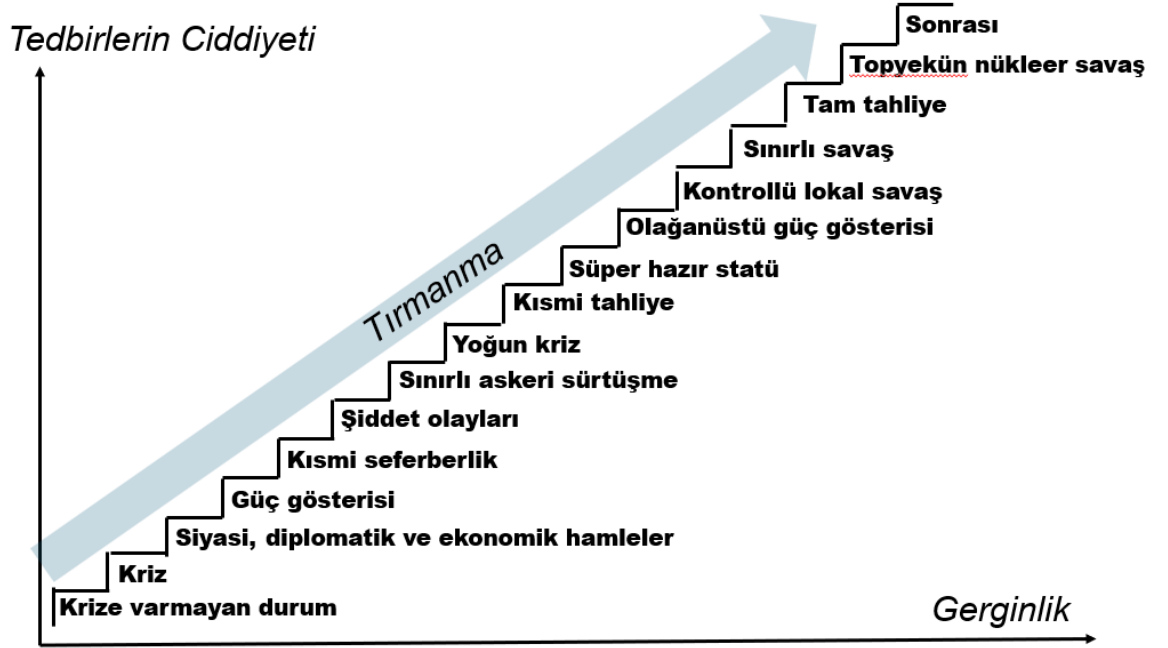
⁴² Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Londra: SAGE Publications, 1977), 94.

⁴³ Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, 31-32.

⁴⁴ Morgan, *Deterrence: A Conceptual Analysis*, 94.

vazgeçirecek bir durum ortada yoktur”⁴⁵ tespiti yerinde değildir. Bununla birlikte eğer Morgan’ın kastettiği saldırı türü konvansiyonel ise bu tespit o zamana kadar sınırlı savaşların nükleer kabiliyetlerle önlenmesi mantığını çürüten ve konvansiyonel caydırıcılığın gerekliliğine işaret eden önemli bir argümandır.

Söz konusu argüman aslında çok önceden Glenn Snyder tarafından “istikrar-istikrarsızlık paradoksu” adı altında tespit edilmiştir. Snyder’e göre “güç dengesi topyekûn nükleer harp riski karşısında ne kadar istikrarlı ise sistem daha alt şiddet seviyelerini barındıran saldırganlık karşısında o derecede istikrarsızdır”.⁴⁶ Snyder, nükleer silahların bir caydırıcı kabiliyet olarak kullanımına ilişkin olarak söz konusu silahların simetrik olarak birbirlerini dengelemekten ötede bir fayda sunamayacağını dile getirmektedir. Bu silahların kullanılması önündeki rasyonel engellere gönderme yaparak konvansiyonel tehditlere karşı asimetrik bir caydırıcılık sağlanamayacağını altını çizmiştir. Caydırıcılık stratejisindeki nükleer-konvansiyonel tehdit asimetrisi tartışmalarına dahil olan Kahn “tırmanma merdiveni” metaforunu ortaya atmıştır.



Şekil 1: Kahn'ın Tırmanma Merdiveni⁴⁷

⁴⁵ Morgan, 94.

⁴⁶ Snyder, “The Balance of Power and the Balance of Terror”, 30.

⁴⁷ Kahn, *Thinking about the Unthinkable*, 194-95.

Modele göre, nükleer güçler arasında cereyan eden sürtüşmeler bağlamsal olarak ele alınmaktadır. Karşılaşılan tehdidinin niteliği ile karşı aktörün adımları hesaba katılmalı, farklı yoğunluk seviyesindeki diplomatik ve askeri yaptırımlar takip edilmelidir. Amaç söz konusu çatışma durumlarını nükleer düzeye tırmanmadan engellemek, bu doğrultuda gerektiğinde konvansiyonel kabiliyetlerden faydalanmaktır. Müteakiben Kahn, ortaya koymuş olduğu merdiven modelinden yola çıkarak “tırmanma hâkimiyeti” terimini öne sürmüştür. Buna göre, olası bir kriz durumunda söz konusu merdivenin basamaklarını rakibe kıyasla daha kolay tırmanabilen ya da başka bir deyişle krizin boyutunu ve kullanılacak askeri kabiliyetin niteliğini artırmaktan çekinmeyen taraf rakip üzerinde caydırıcılık sağlayacaktır. Bahse konu olan argümanı destekleyen Schelling, rakibi boyun eğmeye iten esas faktörün şiddeti artarak devam eden zarar verebilme yeteneğinde saklı olduğunu ifade etmiştir.⁴⁸ Kahn’ın ortaya koymuş olduğu tırmanma merdiveni ve tırmanma hakimiyeti modelleri halen modern caydırıcılık teorisinde geçerliliğini korumaktadır.

Snyder ve Kahn’ın çalışmalarına konu olan tehdit asimetrisi sorunu ABD Caydırıcılık Stratejisinin 1954 yılından beri ana doktrini olan “Kitlel Misilleme” (*Massive Retaliation*) doktrininin yerini 1961 yılında “Esnek Karşılık” (*Flexible Response*) doktrinine bırakması ile yansıma bulmuştur. Kahn, Esnek Karşılığı şu şekilde tanımlamaktadır: Ciddi bir provokasyon karşısında karşı tarafça değerli olan bir şehir veya kaynağın sınırlı bir nükleer saldırı sonucu imha edilmesi.⁴⁹ Kahn’ın bu tanımıyla Ceza Yoluyla Caydırıcılık yöntemine hedef olarak şehirleri göstermesi Soğuk Savaş döneminin bakış açısını göstermesi bakımından dikkat çekicidir. Adil Savaş kavramının göz ardı edildiği bu dönemde şehirlerin hedef alınması çoğunlukla tehditlerin inandırıcılığı açısından irdelenmiştir.

Söz konusu dönemde caydırıcı tehditlerin inandırıcı özelliklerinin vurgulanması için oyun teorisine sıklıkla başvurulduğu görülmektedir.⁵⁰ Bu kapsamda; yardımlaşmasız

⁴⁸ Schelling, *Arms and Influence*, 3.

⁴⁹ Kahn, *Thinking about the Unthinkable*, 112.

⁵⁰ Örn: Robert Jervis, “Cooperation Under the Security Dilemma”, *World Politics* 30, sayı: 2 (1978): 177-79.

çift taraflı oyun modellerinden Tavuk Oyunu⁵¹ analogisi ön plana çıkmıştır. Oyunda nükleer denge koşullarında tehdit inandırıcılığını başarılı şekilde gerçekleştiren tarafın karşı tarafa üstünlük sağlayacağı varsayılmaktadır. Bu modelde nükleer savaş anlamına gelen çarpışma senaryosuna karşı her türlü riski göze alabildiğine dair karşı tarafı inandıran taraf kazançlı çıkmaktadır.⁵² Kahn, tavuk oyununun anlaşılabilirlik, simetri ve sıfır toplamli rekabet koşulları açısından stratejik dengeyi açıklamada önemli olduğunu dile getirmiştir.⁵³

Rakibe yöneltilen tehdidin inandırıcılığı hakkında tespitlerde bulunan yalnızca Kahn değildir. Bu doğrultuda Schelling'in öne sürdüğü "irrasyonelitenin rasyonelitesi" ve "bazı şeyleri şansa bırakmak" gibi tespitler caydırıcılık teorisinde "rasyonelite" ve "belirsizlik" olgularının girişini sağlamıştır. Schelling, nükleer silahların doğası gereği ortaya çıkan dehşet dengesinde tehdit inandırıcılığını sağlamanın en etkili yolunun karşı tarafa karar alıcının rasyonel olmadığı, en riskli kararları almaktan çekinmeyeceği izlenimini vermekten geçtiğini savunmuştur.⁵⁴ Bu noktada "köprüleri yakmak" (*burning the bridge*) metaforunu kullanan Schelling, nükleer silahlar söz konusu olduğunda ancak geri adım atamayacak durumda olan ve bunu karşı tarafa etkili bir şekilde aktarabilen tarafın caydırıcılığından söz edilebileceğini vurgulamaktadır.⁵⁵ Schelling'e göre zaman zaman belirli etmenleri kontrol altında bulundurmamak, fevri görünmek ve spontane kararlar almak karar vericilerin inandırıcılığına pozitif etki sağlayan hamlelerdir. Örneğin; nükleer silahların kontrolünü bir saha komutanına devrederek sivil bürokrasinin hantallığını askeri cüret ile değiştirmek, rakibi göze alınabilecek

⁵¹ İki rakip arasındaki çatışma ve tırmandırma ilişkisini barındıran tavuk oyunu modeli nükleer rekabetteki dehşet dengesi güç ilişkilerini tasvir etmek için kullanılmaktadır. Analoji, tek şeritli bir yolda birbirine doğru hızla araç süren sürücüler üzerinden kurulmuştur. Buna göre iki taraf için kayıp olacak çarpışma senaryosunun yaşanmaması için taraflardan birinin boyun eğerek direksiyonu çevirmesi ve şeritten çıkması gerekmektedir. Ancak bu durum kişisel gurur ve aşağılanma davranışı ile özdeşleştirilerek geri adım atan tarafın "tavuk" olarak nitelendirilmesine yol açacaktır. Rakipler bir taraftan tavuk durumuna düşmemek, diğer taraftan da çarpışmaya maruz kalmamak için birbirlerine ne kadar kararlı olduklarını aktarma amacı gütmektedir. Zira rakiplerin rasyonel olduğu varsayımında oyunculardan biri mutlak zarar olan çarpışma senaryosundan kaçınmak için şerit değiştirecektir. İşte bu durumda çarpışma senaryosu daih her türlü riski kabul ettiğine dair karşı tarafı inandıran taraf caydırıcılıkta başarılı olacaktır.

⁵² Jervis, "Cooperation Under the Security Dilemma", 178.

⁵³ Kahn, *Thinking about the Unthinkable*, 196-98.

⁵⁴ Schelling, *Arms and Influence*, 38.

⁵⁵ Schelling, 43

riskler karşısında daha temkinli olmaya davet edebilecektir.⁵⁶ Bunun karşısında birçok yazar rasyonel olmayan davranışların caydırıcılıkta yalnızca kısa vadede başarı sağlayacağını, uzun vadede ise benzer şekilde davranan aktörler karşısında etkinliğini yitireceğini savunarak Schelling'i eleştirmektedir.⁵⁷

Schelling'in caydırıcılık literatürüne sağladığı diğer bir önemli katkı aktörler arası karşılıklı iletişimin rolüdür. Schelling'e göre, kabiliyet ve inandırıcılığın yanı sıra rakibe hangi davranıştan kaçınması gerektiği kuşku bırakmayacak bir şekilde aktarılması sağlanmalıdır. Hangi hedefin aktör için ne derecede önemli olduğunun karşı tarafa iletilmesi caydırıcılığın başarısı için önemli bir faktördür. Schelling bu tespiti Soğuk Savaş dönemindeki Macaristan vakası üzerinden ifade etmektedir. 1956 yılında Sovyet ordusunun Macar isyancıları sert bir şekilde bastırması, ABD'nin muhtemel bir karşı müdahaleden caydırılarak statükonun Sovyetler Birliği lehinde devam etmesi Schelling'e göre bir iletişim ve inandırıcılık başarısıdır. Bu doğrultuda Schelling, Sovyetlerin ABD'den askeri olarak daha güçlü olduğundan dolayı değil, Macaristan'ın kendileri için büyük önem teşkil ettiği ve statükonun korunması için her türlü adımı atabileceğine dair karşı tarafı ikna ettiği için başarılı olduğunu savunmaktadır.⁵⁸

Yukarıda gösterildiği üzere, Soğuk Savaş sürecinde caydırıcılığa ilişkin çalışmalar dönemin yapısal koşullarından doğrudan etkilenmiştir. Bu çalışmalarda ana temanın nükleer silahların bir tehdit aracı olarak güvenlik stratejilerinde konumlandırılması olduğu görülmektedir. İzlenmesi öngörülen stratejiye dair bir yol gösterme gayretinde olan bu çalışmalar, uygulanması tavsiye edilen manipülatif eylemleri ve angajman şekillerini barındırmaktadır. Dolayısıyla bu çalışmaların metotsal olarak bilimsel bir yaklaşım sunmadığını, kuramsal açıdan ise devletler arası farkları hesaba katmaksızın güç dengesi koşulları gölgesinde kaldığını ifade etmek mümkündür. Diğer bir deyişle dönemin Uluslararası İlişkiler Disiplinine hakim olan Neorealizm Kuramının caydırıcılık çalışmalarında esas kuramsal çerçeve olarak benimsendiği görülmektedir. Devletleri birer rasyonel aktör olarak kabul eden bu çalışmalar, stratejik kültür, kurum

⁵⁶ Schelling, 38.

⁵⁷ Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Londra: Cornell University Press, 1989), 246.

⁵⁸ Schelling, *Arms and Influence*, 36-37.

ve toplum gibi iç bileşenleri göz ardı ederek yapısal faktörlerin tamamen belirleyici olduğu bir analiz ortaya koymuştur.

1.2.2. Üçüncü Dalga

Wohlstetter, Kahn, Schelling gibi araştırmacılar Caydırıcılık teorisinin gelişiminde literatüre önemli katkılar sağlamıştır. Bununla birlikte söz konusu araştırmacılar tarafından ortaya atılan tespit ve varsayımlar bütünü fazlasıyla soyut, kuralcı ve normatif bulunduğu için eleştirilmiştir.⁵⁹ Diğer bir deyişle bu çalışmalar, mevcut durumdan ziyade olması gereken durumu ele alarak dış politika yapımına yön vermeyi amaçlamıştır. Takip eden dönemde Uluslararası İlişkiler disiplininde hakim olan davranışsalcı akımın etkisiyle Alexander George ve Richard Smoke genellenebilir, test edilebilir ve ampirik bir yöntem izleyerek çalışmalara bilimsel bir nitelik kazandırmıştır. Oyun teorisinin aşırı indirgemeci çerçevesini eleştiren George ve Smoke Amerikan Caydırıcılık stratejisini vaka analizi üzerinden test ederek birey, grup ve örgütsel davranış gibi etmenlerin caydırıcılık başarısındaki etkilerini ortaya koymuştur.⁶⁰ Caydırılmak istenen rakibin algısının yanında hesaplanabilir ve kontrol edilebilir risklerin önemine vurgu yapan yazarlar üç çeşit başarısız caydırıcılık kalıbı öne sürmüşlerdir.⁶¹

1. Oldu-bitti (*Fait Accompli*): Kuvvetli bir rakibin koruma taahhüdünün azaldığı anda ani saldırı
2. Sınırlı müdahale (*Limited Probe*): Rakibin şüpheli durumdaki taahhüdünü test etmek için yaratılan sınırlı kriz
3. Kontrollü baskı (*Controlled Pressure*): Kuvvet kullanma eşiği konusunda rakibi kararsızlıkta bırakacak şekilde sert güç dışı kriz durumları

George ve Smoke ile başlayan deneysel yaklaşımın kısa sürede diğer araştırmacılara ön ayak olduğu görülmektedir. Bu akımın en önemli ikinci çalışması olarak Paul Huth ve

⁵⁹ Morgan, *Deterrence: A Conceptual Analysis*.

Janice Stein Gross, "Deterrence and Reassurance", içinde *Behavior, Society and Nuclear Weapons*, ed. Philip E. Tetlock vd. (New York: Oxford University Press, 1991), 19.

Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, 635-636.

⁶⁰ Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, 511-12.

⁶¹ Smoke, 536-46.

Bruce Russett'ın *What makes Deterrence Work* adlı makalesinden bahsetmek mümkündür.⁶² Araştırmalarında 54 adet ani caydırıcılık⁶³ (*Immediate Deterrence*) vakasını inceleyen Huth ve Russett daha önce verili olarak kabul edilen bazı varsayımları çürüten birtakım bulguları belirlemiştir. Bunlardan bazıları; uzatılmış caydırıcılıkta koruyan ve korunan devlet arasındaki iş birliğinin önemi, toplam askeri kabiliyetlerden ziyade muhtemel çatışma bölgesindeki askeri üstünlüğün caydırıcılığı desteklediği, resmî askerî ittifakların caydırıcılıkta daha çok olumsuz sonuçlar doğurduğu ve nükleer silahların varlığının caydırıcılığa önemli bir etkisinin bulunmadığıdır.⁶⁴ Araştırmanın sonuçları nükleer silahların doğrudan caydırıcılık sağladığı varsayımını sorgulaması açısından önemlidir. Sonuçta 1980'lerden itibaren konvansiyonel kabiliyetlerin caydırıcılıktaki yerini ele alan araştırmalar, teorinin nükleer silahlar hakimiyetinden kısıtlı da olsa uzaklaşmasını mümkün kılmıştır.

Akdemik yazında her ne kadar nükleer savaş riskine varmayan kriz durumlarında konvansiyonel kabiliyetlere başvurulabileceği dile getirilmiş olsa da nükleer silahların caydırıcılık stratejisindeki mutlak ağırlığı Mearsheimer'in *Konvansiyonel Caydırıcılık* adlı eseri ile sarsılmıştır. Schelling'in nükleer silahlar ile birlikte savaşın ve caydırıcılığın askeri olmaktan çıktığı argümanının aksine Mearsheimer, konvansiyonel tehditlerin muharebe alanında gösterdiği caydırıcılığa dikkati çekmiştir. Yazarın

⁶² Huth ve Russett, "What Makes Deterrence Work? Cases from 1900 to 1980".

⁶³ Ani Caydırıcılık tipolojisi Patrick Morgan tarafından ortaya konmuştur. Morgan'a göre caydırıcılık ilişkisi tehditsel durumun aciliyetine göre farklılık göstermektedir. Bu doğrultuda Morgan Ani Caydırıcılık ve Genel Caydırıcılık kavramlarını akademik yazına kazandırmıştır. Ani caydırıcılık karşılıklı iki devlet arasındaki ilişkide bir tarafın saldırıyı ciddi bir şekilde düşündüğü konjontürde diğer devletin cezalandırma tehditini artırma durumunu ele alırken; genel caydırıcılık ise ortada önemli bir saldırı ihtimali bulunmaması halinde tarafların ellerinde bulundurdıkları askeri kabiliyetlerini araçsallaştırarak güvenlik ilişkilerini idare biçimine işaret etmektedir. Morgan'ın bu ayrımının caydırıcılığın yalnızca kriz durumlarında geçerli olduğu eleştirilerine karşı bir cevap sunduğu da ifade edilebilir.

Jervis, "Deterrence Theory Revisited", 293.

Morgan, *Deterrence: A Conceptual Analysis*, 28.

Huth ve Russett'ın çalışmalarının literatürde önemli yankı bulduu söylenebilir. Bu doğrultuda söz konusu araştırmacılar gibi Zagare ve Kilgour da nükleer silahları incelemeyen, deneysel ve genel bir caydırıcılık teorisi ortaya koyma amacıyla yaptıkları çalışmada farklı olarak genel caydırıcılık vakalarını ele almışlardır.

Zagare ve Kilgour, *Perfect Deterrence*.

⁶⁴ Huth ve Russett, "What Makes Deterrence Work? Cases from 1900 to 1980", 523-24.

ifadesiyle: “Konvansiyonel caydırıcılık doğrudan askeri strateji ile ilgilidir, veya daha spesifik bir şekilde, muharebe alanı maksatlarına ulaşmak için askeri kuvvetlerin nasıl kullanıldığı ile bağlantılıdır.”⁶⁵

Mearsheimer caydırıcılığın işleyişini Yıldırım Harbi, Yıpratma Savaşı ve Sınırlı Savaş değişkenleri üzerinden test etmiştir. Çalışmasında vardığı bulgular şu şekildedir: Yıldırım harbi, savunmayı hazırlıksız yakalamasından dolayı caydırıcılığın doğrudan başarısız olmasına yol açmaktadır. Diğer taraftan yıpratma savaşı maliyetleri dayanılmaz boyutlara ulaştıracığından dolayı caydırıcılıkta en çok başarı vadeden değişkendir. Muharebede elde edilen sınırlı bir zafer yıpratma savaşının kapısını araladığında başarılı caydırıcılığa yol açarken aksi durumda caydırıcılık başarısız olacaktır.⁶⁶ Görüldüğü gibi Mearsheimer’ın konvansiyonel caydırıcılık teorisinde maliyetler önemli bir yer tutmaktadır. Aslında yazarın bu çalışmasında caydırıcılık yazınına sağlamış olduğu katkı en az yukarıdaki bulgular kadar maliyetlerin önemi hakkındadır. Buna göre eğer muhtemel bir saldırgan statükoyu değiştirmenin bedelini mutlak maliyetli olarak hesaplırsa caydırıcılık başarılı; olası faydanın maliyetlerden üstün olarak hesaplanması durumunda başarısız olacaktır.⁶⁷

Genel anlamda nükleer ve konvansiyonel kabiliyetler üzerinden açıklanan caydırıcılık yazınına önemli bir katkı, kavrama psikolojik boyutları ekleyen Robert Jervis’ten gelmiştir. Jervis’e göre nükleer silahların asıl etkisi yıkım kabiliyetlerinden ziyade karar vericilerde oluşturduğu algıdır. Yazara göre ikinci saldırı kabiliyeti üzerinden oluşturulan bir ceza yoluyla caydırıcılık yönteminin işlevsel ve etik yönden bir mantığı bulunmamaktadır. Zira cezalandırma amacıyla rakip devlete yöneltilecek bir nükleer saldırı binlerce hayata mal olmasının karşısında politik olarak bir getiri sunmayacaktır. Bu noktada yazar normalize edilmiş ve kanıksanmış olan bu durumun mantıkla açıklanamayacağını, söz konusu durumdaki saldırının insani bir duygu olan intikam isteği ile açıklanabileceğini ifade etmiştir.⁶⁸ Joseph Nye ise psikolojik faktörlerin oynadığı önemli role işaret ederken, ABD-Sovyet Rusya arasındaki caydırıcılık

⁶⁵ John J. Mearsheimer, *Conventional Deterrence* (Londra: Cornell University Press, 1983), 28-29.

⁶⁶ Mearsheimer, 63-64.

⁶⁷ Mearsheimer, 6-10.

⁶⁸ Robert Jervis, *Perception and Misperception in International Politics* (New Jersey: Princeton University Press, 2017).

dinamiklerinin nükleer kabiliyetlerden öte karşılıklı düşmanlıkla açıklanabileceğini öne sürmüştür.⁶⁹ Jervis ve Nye'nin işaret ettiği bu durum esasında caydırıcılık teorisi ile ilgili çok temel bir ikilemi ortaya koymaktadır. Şöyle ki nükleer silahların araçsallaştırılmasında rasyonalite ve hesaplama gibi mantığa dair temeller üzerinde yükselen teorinin geri planda yaslandığı öğeler daha çok algı ve psikoloji ile ilgili bir durumdur. Bunu bir adım ileri götürdüğümüzde Kissinger'ın şu sözü geri plandaki öğelerin ne kadar baskın olduğunu göstermektedir:

*Caydırıcılık öncelikle psikoloji kriterine dayanır. Muhtemel saldırganın neye inandığı, objektif olarak neyin gerçek olduğundan daha önemlidir. Caydırıcılık her şeyden önce insan aklında meydana gelir.*⁷⁰

Jervis psikoloji bağlamında caydırıcılık teorisinin dört önemli sorununa işaret etmiştir:⁷¹

1. Devlet adamları rakiplerinin düşmanca niyetlerini abartma eğilimindedir.
2. Esasında statükoyu koruma niyeti ile yöneltilen karşılıklı tehditler çatışma spirallerine dönüşebilir.
3. Devletler kamuoyu baskısı veya koşullarının kötüye gittiği algısıyla savaşa sürüklenebilir.
4. Baskı altındaki insanların psikolojik süreçleri, caydırıcı tarafın ürettiği tehditlerin inandırıcılığını abartmasını, caydırılmak istenen tarafın ise kendisine yöneltilen tehditleri küçümsemesini açıklayabilir.

Jervis'in bir diğer katkısı ise ikna yoluyla caydırıcılık metodunu ortaya atmak olmuştur. Buna göre ikna yoluyla caydırıcılık, saldırgan tarafın amacına ulaşmasını imkânsız kılacak veya bu yolda kabul edilemez seviyede zarar görmesini sağlayacak şekilde kuvvet kullanım tehdidinin yöneltilmesidir.⁷² Jervis'in bu tanımını o zamana dek teoride ceza yoluyla caydırıcılıktan ibaret olan caydırıcılık yöntemlerinin sayısını ikiye

⁶⁹ Joseph S. Nye, "Nuclear Learning and U.S.-Soviet Security Regimes", *International Organization* 41, sayı:3 (1987): 371.

⁷⁰ Henry A. Kissinger, "Domestic Structure and Foreign Policy", *Daedalus* 95, sayı: 2 (1966): 506.

⁷¹ Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*, 65-67.

⁷² Jervis, 11-12.

çıkarmış ve daha sonra özellikle konvansiyonel caydırıcılık araştırmacıları tarafından sıklıkla kullanılmıştır.

Caydırıcılık yazınına ilişkin üçüncü dalga genel olarak ele alındığında bu dönemde; nükleer silahlara ilaveten konvansiyonel silahların etkilerinin incelenmeye başlandığı, psikoloji faktörünün ağırlıkla irdelendiği ve İkna Yoluyla Caydırıcılık Yönteminin ortaya atıldığı görülmektedir. Bununla birlikte caydırıcılık stratejisinin uygulanmasında güç dağılımı faktörlerinin ağırlığının devam ettiği görülmektedir. Zira önceki dalga çalışmalarında olduğu gibi kapasite inşası ve caydırıcılık metodu seçimi gibi süreçlerde devlet seviyesindeki alt bileşenlere yer verilmediği görülmektedir. Her ne kadar Jervis'in çalışmaları karar alıcıların nükleer silahları algılama biçimlerini ön plana taşımış olsa da söz konusu çalışmaların metodolojik bir yaklaşımdan uzak olduğu görülmektedir. Bahsettiği psikolojik etkilerin boyutlarını ve sonuçlarını somut bir şekilde ortaya koymayan Jervis'in çalışmaları teorik olarak Klasik Realizmin lidere dair bazı varsayımlarını caydırıcılık stratejisi ile tanıştırmak eğilimindedir. Sonuç olarak stratejiye etki eden lider, kurum, stratejik kültür, kamuoyu gibi iç bileşenlerin etkilerine dair bu dönem çalışmalarında kayda değer bir ize rastlanmamaktadır.

1.2.3. Dördüncü Dalga

Soğuk Savaş koşullarında doğup gelişen caydırıcılık kavramının takip eden yeni dönemin şartlarında nasıl şekilleneceği merak konusu olmuştur. Özellikle 11 Eylül saldırıları sonrası caydırıcılığın bir dış politika aracı olarak işlevselliğini koruyup koruyamayacağına şüphe ile yaklaşılmıştır. Bu dönemde teoriye karşı değişen bakış açısını Reuben Steff, Bush doktrini üzerinden açıklamaktadır. Yazara göre tek kutuplu dünya düzeninde bölgesel aktörlerin nükleer güç edinme ihtimalleri ABD merkezli statükoya doğrudan bir tehdit olarak algılanmıştır. Söz konusu aktörler “haydut devletler” olarak tanımlanarak liderlerine dair bir irrasyonelite vurgusu yapılmış ve bu doğrultuda “caydırılmaz” olarak nitelendirilmiştir.⁷³ Anlaşılacağı üzere, caydırıcılığın esas varsayımlarından olan rasyonel aktör algısı sorgulanarak farklı bir strateji olan ön alıcı taarruz (*preemptive strike*) anlayışı ortaya atılmıştır. Bununla birlikte caydırıcılık stratejisini nispeten geri planda kaldığı bu dönemi tek kutuplu güç dengesi koşullarına bağlamak ve “dönemsel bir anomali” olarak değerlendirmek yanlış olmayacaktır. Zira

⁷³ Steff, *Strategic Thinking, Deterrence and the US Ballistic Missile Defense Project: From Truman to Obama*, 24.

güç dengesindeki değişimler karşısında varlığını sürdüren nükleer kabiliyetler daima bir “son çare” enstrümanı olarak güç ilişkilerinde yerlerini korumuşlardır. James DeNardo’nun deyimiyle “kitlesel imha silahları ile düşmanca ilişkiler birlikte var olduğu müddetçe caydırıcılık sorunu ortadan kalkmayacaktır.”⁷⁴

Nükleer kabiliyetlere ek olarak konvansiyonel kabiliyetlerin etki kapasitesinde görülen artış her iki kabiliyeti kesin sınırlarla ayırmadan ele alan çalışmalara ortam sağlamıştır. Bu kapsamda, Frank Zagare ve Mark Kilgour’un nükleer silahlara özel bir ayrıcalık göstermeyen, Soğuk Savaş dinamiklerinden sıyrılarak genel bir caydırıcılık modeli yaratma girişimleri dikkat çekicidir. Yazarlar, stratejinin beklentisinin aksine mevcut durumda meydana gelen nükleer silah azaltmalarına açıklama getirebilme iddiasında bulunmuşlardır. Çalışmalarında oyun teorisine başvuran yazarların getirdiği en önemli yenilik rasyonalite ile inanılabilirlik arasındaki yakın ilişkinin ortaya konmasıdır. Buna göre, karşılıklı caydırıcılığın en başarılı şekilde var olabilmesi için iki tarafın da etkin kabiliyet ve inandırıcılığa sahip olması gerekmektedir.⁷⁵

Anlaşılabacağı gibi Zagare ve Kilgour caydırıcılığı iki taraflı bir kavram olarak değerlendirmekte ve oyun modelini bu düzlemde kurmaktadır. Aslında Klasik Caydırıcılıkta sıklıkla kullanılan Tavuk Oyununa benzeyen modelde temel farklılık, caydırılmak istenen tarafın boyun eğme veya kaçınma tercihinde bulunduğu oyunun sona ermemesi ve yeni durum karşısında tercih sırasının karşı tarafa geçmesidir. Bu doğrultuda yazarlar aktörün statükodan yana karar alması durumunda rakip için en kârlı seçeneğin revizyonist tercih olduğunu savunarak nükleer silahlara atfedilen caydırıcılığın sağlam bir zemin üzerine kurulmadığını öne sürmektedirler.⁷⁶

Yazarların ortaya koyduğu bir diğer önemli nokta ise rasyonalite algısıdır. Rasyonalitenin her zaman aynı anlama gelmediğini ifade eden yazarlar kavramı Prosedürel (*Procedural*) ve Araçsal (*Instrumental*) Rasyonalite olarak ikiye ayırmaktadır. Buna göre, Prosedürel Rasyonalite herhangi bir zaman ve koşul kısıtı olmaksızın erişilebilecek tüm bilgiler dahilinde gerçekleşen karar alma sürecini ifade

⁷⁴ James DeNardo, *The Amateur Strategist: Intuitive Deterrence Theories and the Politics of the Nuclear Arms Race* (New York: Cambridge University Press, 1995), 2.

⁷⁵ Zagare ve Kilgour, *Perfect Deterrence*, 289.

⁷⁶ Zagare ve Kilgour, 30-31.

etmektedir. Söz konusu kavram her ne kadar ideali temsil etse de yazarlar bu durumun gerçek koşulları yansıtmadığını savunarak ikinci kavrama yönelmektedir. Araçsal Rasyonalite, sınırlı bilgi ve zaman koşulları dahilinde aktörün iki seçenek ile karşılaşması ve kendine özgü bir mantık çerçevesinde seçeneklerden birini diğerine tercih etmesi durumudur.⁷⁷ Yazarlara göre caydırıcılık teorisinde çoğu yazarın rasyonaliteden bahsederken kastettiği kavram Araçsal Rasyonalitedir.

2010 yılı sonrası güç rekabeti sahnesine Rusya, Çin, İsrail, Hindistan gibi nükleer aktörlerin dahil olması nükleer caydırıcılığın yeniden gündeme gelmesine yol açmıştır. Therese Delpech “21. Yüzyılda Nükleer Caydırıcılık” adlı çalışmasında konvansiyonel kabiliyet üstünlüğünün güç ilişkilerinde belirleyici olmadığını öne sürerek yeni tehditler karşısında ABD’nin nükleer caydırıcılık üzerine tekrar eğilmesi gerektiğini öne sürmüştür.⁷⁸ Söz konusu dönemde nükleer silahların akademik yazında ağırlıklı olarak ele alınması, bu silahların caydırıcılığına ilişkin farklı boyutların irdelenmesine alan açmıştır. Bu kapsamda Vipin Narang’ın 2013 yılında yayımlanan çalışması dikkat çekicidir. Nükleer silahlara sahip olmanın doğrudan standart bir caydırıcılığı beraberinde getirmeyeceğini savunan Narang, nükleer silahlardan çok nükleer konumlanmanın önemli olduğunu ileri sürmüştür. Bu kapsamda Narang üç farklı konumlanma tipi ortaya koymuştur.⁷⁹

- Katalitik Duruş (*Catalytic Posture*): Üçüncü bir aktörün müdahalesini ve yardımını sağlama amaçlı sınırlı kapasiteye sahip nükleer konumlanma
- Kesin Misilleme Duruşu (*Assured Retaliation Posture*): Nükleer tehditleri caydırma amaçlı ikincil vuruş kabiliyetine sahip nükleer konumlanma
- Asimetrik Tırmandırma Duruşu (*Asymmetric Escalation Posture*): Konvansiyonel tehditleri caydırma amaçlı, konvansiyonel ve stratejik hedeflere yönelik ilk vuruş saldırısını öngören nükleer konumlanma

Narang’ın çalışması uzun zaman verili olarak kabul edilmiş olan nükleer kabiliyetlerin farklı türde caydırıcılıklar sağlayabileceğini göstermesi açısından oldukça önemlidir.

⁷⁷ Zagare ve Kilgour, 38-43.

⁷⁸ Thérèse Delpech, *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy* (Pittsburgh: RAND Corporation, 2012), 22.

⁷⁹ Vipin Narang, *Nuclear Strategy in the Modern Era* (Oxford: Princeton University Press, 2014), 314-320.

Ancak daha da ilgi çekici yanı, bahse konu olan nükleer konumlanmaların tercih edilmesinde etkili olan faktörleri ortaya koyma biçimidir. Narang, öne sürdüğü teoride Neoklasik Realizmin kuramsal çerçevesini kullanarak yapısal değişkenler (patron niteliğindeki üçüncü aktör ile yakın güvenlik çevresi) ile aktör odaklı ara değişkenleri (Sivil-Asker uyumu ile kaynak kısıtlamaları) bir arada kullanmıştır. Böylece farklı nükleer aktörlerin farklı nükleer politikalarını açıklayabilmiştir. Narang'ın teorisinin açıklayabilir niteliği caydırıcılık çalışmalarının geldiği noktayı göstermesi açısından ilham vericidir. Diğer taraftan çalışmanın yalnızca nükleer kabiliyetler üzerine kurulu olması önemli bir sınırlılık olarak göze çarpmaktadır. Benzer durum Reuben Steff'in *Strategic Thinking, Deterrence and the U.S. Ballistic Missile Defense Project* adlı çalışmasında söz konusudur. Steff, Soğuk Savaş sonrasında ABD caydırıcılık anlayışının yapısal güç değişkenlerinden ziyade iç değişkenler kapsamında evrildiğini savunmuştur. Steff'e göre özellikle George W. Bush döneminde lider profili, lobi grupları, ideolojik varsayımlar ve askeri-endüstriyel kompleks gibi iç dinamikler yapısal tehdit algılarını kendi öngörülerini doğrultusunda şekillendirerek caydırıcılık stratejisine yön vermişlerdir.⁸⁰

Soğuk Savaş sonrası dönemde nükleer ve konvansiyonel tehditler ve karar alma mekanizmalarına yönelik önemli çalışmalar yapılmakla birlikte bu dönemin esas belirgin özelliği tehdit yelpazesindeki değişimler olmuştur. Bu doğrultuda haydut devletler, terör örgütleri ve siber saldırılara karşı caydırıcılık teorisinin sunabilecekleri hakkında birçok çalışma ortaya konmuştur.⁸¹ Bu dönemde değişen aktör ve tehditlere karşı farklı şekilde uyum sağlayabilen esnek bir caydırıcılık tanımının hâkim olduğu

⁸⁰ Steff, *Strategic Thinking, Deterrence and the US Ballistic Missile Defense Project: From Truman to Obama*, 159.

⁸¹ Jackson, "Beyond Tailoring: North Korea and the Promise of Managed Deterrence";

Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research", *Military and Strategic Affairs* 3, sayı: 3 (2011): 49-62;

Maurizio Martellini, *Cyber Security: Deterrence and IT Protection for Critical Infrastructures* (Springer Briefs on Computer Science, 2013), DOI 10.1007/978-3-319-02279-6;

Eugenio Lilli, "Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence", *Contemporary Security Policy* 42, sayı: 2: 163-88, <https://doi.org/10.1080/13523260.2021.1882812>;

Almog, "Cumulative Deterrence and the War on Terrorism".

göze çarpmaktadır. Bu doğrultuda Modern Caydırıcılık ve Uyarlanmış Caydırıcılık gibi kavramlara sıklıkla rastlanmaktadır.

Burada dördüncü dalga çalışmaları ile ilgili altı çizilmesi gereken en önemli husus önceki akademik çalışmalara nispeten odak noktasındaki farklılaşmadır. Şöyle ki, Soğuk Savaş dönemi caydırıcılık dalgaları caydırıcılığın kime karşı, hangi araçlarla sağlanacağına kanalize olurken son dönemde temel soru neyin, başka bir deyişle hangi tür saldırıların caydırılacağı olmuştur.⁸² Söz konusu değişikliğin sebebi tehdit ortamının kalıplaşmış sınırlarını terk etmesi ve devletlerin savaş eşğine varmayan çok sayıda hibrit tehdide⁸³ maruz kalmasıdır. Bahse konu olan tehditler eş zamanlı olarak araçsallaştırılabilmektedir. Ayrıca siber tehdit ve dezenformasyon faaliyetlerinden nükleer silahların kullanımına varan çok basamaklı tırmanma mekanizmalarını ihtiva edebilmektedir.⁸⁴

Son dönemde yeni tehditlere karşı klasik caydırıcılık öğretilerinin uygulanabilirliğine dair önemli çalışmalar göze çarpmaktadır. Bu doğrultuda birçok yazar nükleer caydırıcılığın temel metodu olan Ceza Yoluyla Caydırıcılığın yeni tehditlere karşı yetersiz kaldığını öne sürerek İkna Yoluyla Caydırıcılığının rolünü ön plana çıkarmaktadır.⁸⁵ Buna karşın bazı yazarlar siber tehditler özelinde, farklılaşan dönemsel koşullar nedeniyle klasik caydırıcılık gözlüğü ile modern güvenlik tedbirlerini analiz etmenin yanlış olduğunu savunmaktadır. Yazarlar bu doğrultuda Ceza Yoluyla

⁸² Knopf, “The Fourth Wave in Deterrence Research”, 26-27.

⁸³ ‘Hibrit tehditler, konvansiyonel yetenekler, düzensiz taktik ve oluşumlar, terör eylemleri (gelişigüzel şiddet ve zorlama dahil) ve kriminal düzensizlik gibi çeşitli savaş biçimlerini kapsar. Bu çok yönlü faaliyetler, ayrı birimlerce ya da aynı birim tarafından yürütülebilir; ancak aynı muharebe sahasında, taktiksel ve operasyonel düzeyde eşgüdüm içinde yürütülerek sinerjik etkiler yaratmayı amaçlar.’ Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: Potomac Institute for Policy Studies, 2007)

⁸⁴ King Mallory, “New Challenges in Cross-Domain Deterrence” (RAND Corporation, 2018), 7, <https://www.rand.org/pubs/perspectives/PE259.html>.

⁸⁵ Patrick M. Morgan, “The State of Deterrence in International Politics Today”, *Contemporary Security Policy* 33, sayı: 1 (2012): 101;

Knopf, “The Fourth Wave in Deterrence Research”, 24-25;

Stefanie Von Hlatky ve Andreas Wenger, *The Future of Extended Deterrence* (Washington: Georgetown University Press, 2015), 21;

Iasiello, “Is Cyber Deterrence an Illusory Course of Action?”, 67.

Caydırıcılığın sınırları yeniden belirlenmiş bir çerçevede etkinliğini korumaya devam edeceğini iddia etmektedir.⁸⁶ Bununla birlikte kuvvet kullanımından en az seviyede etkilenme ve yeniden toparlanma kabiliyetini ifade eden “dayanıklılık” (*resilience*) teriminin son dönemde yeni bir caydırıcılık metodu olarak akademik yazında sıklıkla çalışıldığı görülmektedir.⁸⁷

Bu çalışmada dördüncü dalga çalışmalarına benzer bir doğrultuda yeni tehdit kavramlarından siber tehditlere karşı caydırıcılığın uygulanma biçimi analiz edilmiştir. Bu tehditlere ilişkin yapılan caydırıcılık çalışmalarında caydırıcılığın üç temel bileşeninden biri olan kabiliyet bileşeninin yeterince üzerinde durulmadığı görülmektedir. Halbuki siber tehditlere karşı oluşturulacak caydırıcılık kapasitesinin nasıl inşa edileceği konusu hangi caydırıcılık metodunun takip edileceğinde belirleyici olmaktadır. Bu doğrultuda takip eden bölümde siber tehditlere karşı caydırıcılık çalışmalarında kabiliyet bileşeni sorunu ele alınmıştır.

1.3. Caydırıcılık Yazınında Kabiliyet Bileşeni Sorunu ve Siber Tehditlere Yansıması

Caydırıcılık, belli bir askeri kabiliyetin kullanımına dair karşı tarafın zihninde inandırıcılık oluşturarak onu olası bir istenmeyen eylemden alıkoyma davranışdır. Bu süreçte en önemli iki değişken kabiliyet ve inandırıcılıktır. Nitekim caydırıcılık yazınının genel olarak bu değişkenlerin üzerine eğildiği görülmektedir. Özellikle inandırıcılık bileşeninin ikinci caydırıcılık dalgası çalışmalarından bu yana araştırmacıların dikkatini daha fazla cezbeden bir konu olduğu ifade edilebilir. Söz konusu durumun iki nedenden kaynaklandığı değerlendirilmektedir.

⁸⁶ Wilner, “US cyber deterrence: Practice guiding theory”, 14;

Amir Lupovici, “The ‘Attribution Problem’ and the Social Construction of ‘Violence’: Taking Cyber Deterrence Literature a Step Forward”, *International Studies Perspectives*, 2014, 9, <https://doi.org/10.1111/insp.12082>.

⁸⁷ Martellini, *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*, 54-55;

Alex Wilner, “Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation”, *Comparative Strategy* 36, sayı: 4 (2017): 310;

Nicole J. Jackson, “Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO”, *Journal of Military and Strategic Studies* 19, sayı: 4 (2019): 117.

Birincisi, inandırıcılığın vaka sınırlarını aşan tarihsel ve psikolojik uzantılarının bulunmasıdır.⁸⁸ Devletlerin bir vakaya karşı benimseyeceği caydırıcılık stratejileri, önceki benzer vaka örneklerine ve geçmiş tutumlarıyla ilişkili psikolojik tutumlarına bağlı olarak değişebilmektedir. Daryl Press'e göre 1938 Münih Konferansı'nda ortaya konulan başarısız inandırıcılık örneği takip eden süreçte ABD dış politikasını etkilemiş ve bu doğrultuda Soğuk Savaş sürecinde Kore, Küba ve Vietnam gibi kriz noktalarında geri adım atmayan bir ABD stratejisinin tetikleyicisi olmuştur.⁸⁹

İkincisi Realizmin temel argümanlarından biri olan rasyonel aktör kavramının nükleer silahlar ile ilişkilendirme sorunudur. "Alışılmadık derecede şiddetli ve yıkıcı"⁹⁰ bir silahın kullanımının temelde irrasyonel olmasına rağmen zorlayıcı diplomasiye eklemlenmesi tartışmaya açık bir araştırma alanı olarak ortaya çıkmıştır. Böylece inandırıcılık kavramı, eldeki sert güç kapasitesinden diplomasi yoluyla nasıl azami fayda sağlanacağı sorusuna yanıt arayan araştırmacılar için genel bir çerçeve sunmuştur. Schelling ve Kahn'ın oyun teorisi katkılarıyla kapısı aralanan bu alan, takip eden süreçte hesaplama, rasyonelite, psikoloji ve karar alma gibi pek çok alt konuyu yelpazesine dahil etmiştir.⁹¹

Diğer taraftan kabiliyet değişkeninin ise daha çok verili kabul edildiği ve inandırıcılığa kıyasla alan yazında daha sınırlı bir yer teşkil ettiği ifade edilebilir. Nükleer kabiliyet üzerine çalışmalar henüz bu silahın yeni ortaya çıktığı, etkilerinin anlamlandırılmaya çalışıldığı birinci caydırıcılık dalgası araştırmalarında önemli bir yer tutmuştur. Lakin Sovyetler Birliği'nin bu imkâna erişmesi sonucu akademik ilgi rakibi manipüle etmeye ve dolayısıyla inandırıcılığa kaymıştır. Bu açıdan bakıldığında ilk vuruş kabiliyeti, ikinci vuruş kabiliyeti, karşılıklı teyit edilmiş imha gibi kabiliyet-odaklı görünen kavramlar esasında inandırıcılık üzerine yapılan çalışmalar çerçevesinde şekillenmiştir.

⁸⁸ Shiping Tang, "Reputation, Cult of Reputation and International Conflict", *Security Studies* 14, sayı: 1 (2005): 38.

⁸⁹ Daryl G. Press, "The Credibility of Power: Assessing Threats during the 'Appeasement' Crises of the 1930s", *International Security* 29, sayı: 3 (2005): 136-38.

⁹⁰ Morgan, "The State of Deterrence in International Politics Today", 86.

⁹¹ Press, "The Credibility of Power: Assessing Threats during the 'Appeasement' Crises of the 1930s"; Snyder, *Deterrence and Defense. Toward a theory of national security.*; Jervis, *Perception and Misperception in International Politics*; Frank C. Zagare ve Stephen L. Quackenbush, "Modern Deterrence Theory: Research Trends, Policy Debates, and Methodological Controversies"; Tang, "Reputation, Cult of Reputation and International Conflict".

Kabiliyet değişkenine olan sınırlı ilginin sebebinin bu silahların şüpheye yer bırakmayan devasa yıkım özelliklerinden kaynaklandığı muhtemeldir. Kullanılmaları durumunda uluslararası toplumu nükleer bir felaket senaryosu ile baş başa bırakacak olan söz konusu silahların etkileri ve doktrinsel konumlandırılmaları akademik yazında daha az ele alınmıştır. Bir bağımsız değişkenden ziyade ara değişken rolünde sunulan kabiliyetlerin geri plandaki bu durumu nükleer silahların şüphe götürmeyen yıkım kapasiteleri nedeniyle akademik alanda bir eksiklik olarak görülmeyebilir. Bununla birlikte son dönem farklılaşan tehdit algılamaları çerçevesinde caydırıcılığı oluşturacak kabiliyetlerin nasıl oluşturulacağı ve nasıl konumlandırılacağı önem arz etmektedir.

İşte bu noktada çalışma akademik yazına katkı sağlamayı hedeflemektedir. Siber uzayda geliştirilecek caydırıcılık stratejisinde nükleer silahlar gibi verili kabiliyetler mevcut değildir. Söz konusu kabiliyetler yazılım ve donanım aygıtlarının geliştirilmesi, bilişim altyapısını kullanan aktörler arasında ortak davranış şekilleri ve tedbir mekanizmalarının geliştirilmesi ve agresif yöntemlerle bilişim farklı internet tabanlı ağlarda sızma, ele geçirme, bilgi elde etme ve zarar verme uygulamaları gibi örnekleri kapsamaktadır. Karşılaşılan tehditlerin henüz yeni olması ve etkilerinin halen keşfedilmekte olması takip edilecek örnek başarılı modellerin yokluğu anlamına gelmektedir. Burada Neorealizmin benzer davranış modellerine gerekçe olarak öne sürdüğü “rekabet” ve “taklit” etkileşimlerinin işlevsiz olduğu görülmektedir. Hangi tür kabiliyetin ne derece etkin olduğu halen denenmekte olduğundan, bu doğrultuda izlenecek politikaların belirlenmesinde lider, kurum, stratejik kültür gibi iç değişkenlerin etkileri kabiliyet inşasında daha belirleyici olmaktadır.

Sonuç olarak bu çalışma caydırıcılık yazınına dair kavramsal ve kuramsal iki boyutta görülen iki eksikliğe cevap verecektir. Bunların ilki caydırıcılığın birinci dalga çalışmalarından bu yana tespit edilen iç değişken kullanımı eksikliğidir. Çalışmada, Neoklasik Realizm kuramsal çerçevesinde, güç dengesi ve tehdit algılaması gibi yapısal faktörlerin yanı sıra kurum ve stratejik kültür iç değişkenleri dış politika analizine dahil edilmiştir. Söz konusu değişkenlerin kullanılması ile elde edilen açıklayabilme özelliği tespit edilen ikinci alan yazın eksikliği için önemlidir. Zira caydırıcılığın pratikte hangi yönetsel ve araçsal kabiliyetler ile sürdürüldüğü akademik çalışmalarda yetersiz bir şekilde ele alınan bir konudur. Söz konusu kabiliyet inşasının belirlenmesinde yapısal

faktörler ve iç değişkenlerin birlikte ele alınması, farklı uygulama biçimlerini ortaya koyma ve açıklama noktasında değerli katkılar sunacaktır.

1.4. Caydırıcılık Metotları

Caydırıcılığın dört dalgası bölümünde alana ilişkin çalışmaların gelişiminde ortaya çıkan farklı caydırıcılık metotlarına değinilmiştir. Bununla birlikte söz konusu metotları ayrı bir bölümde ele alarak açıklamak önemlidir. Zira bu metotlar çalışmanın bağımlı değişkeni niteliğindedir. Çalışmanın yanıt aradığı soru farklılaşan caydırıcılık stratejilerinde iç bileşenlerin etkin olup olmadığıdır. Cevap aranan söz konusu farklılaşmadan kasıt farklı caydırıcılık metotlarının benimsenmesidir. Dolayısıyla iç bileşenlerin etkinliği ve nedensel mekanizmalar irdelenmeden önce bağımlı değişken olarak hangi nominal değerlerin tanımlandığını ortaya koymak önemlidir. Bu yüzden caydırıcılık metotlarını kavramsal olarak izah etmek sebep-sonuç ilişkilerini izah etmek için elzemdir.

Soğuk Savaş başlangıcından günümüze caydırıcılık stratejisi çalışmaları incelendiğinde dört tip caydırıcılık metodundan bahsetmek mümkündür:

- Ceza yoluyla caydırıcılık
- İkna yoluyla caydırıcılık
- Dayanıklılık yoluyla caydırıcılık
- Normlar yoluyla caydırıcılık

Bütün bu caydırıcılık metotlarının amacı rakibi revizyonist bir hamleden alıkoymak için, söz konusu hamlenin uygulanmasından önce başvurduğu fayda-zarar hesaplamasına etki etmektir. Bununla birlikte bahse konu olan hesaplamaya etki şekilleri birbirinden farklılık gösterir.

1.4.1. Ceza Yoluyla Caydırıcılık:

Misilleme tehdidi üzerinden oluşturulan caydırıcılık metodudur. Bu stratejide istenmeyen davranış açıkça belirtilir ve karşı tarafa iletilir. Bu davranışı benimsemesi durumunda karşı karşıya kalacağı durum, başka bir deyişle maruz kalacağı saldırılar ortaya konularak rakipte korku temelli bir etki bırakmak hedeflenir. Rakibin fayda/zarar muhasebesinde istenilen etkiyi oluşturabilmek için tehdit unsuru olan muhtemel son

durumun rakip için katlanılmayacak bir seviyede olması, veya en azından hesaplanan zararların mutlak değerinin muhtemel faydalardan ağır basması gerekir.⁹²

Ceza Yoluyla Caydırıcılığın Karakteristik Özellikleri:

- Korku ve Tehdit temellidir⁹³
- Ofansif askeri kabiliyetlere ağırlık verir⁹⁴
- Misillemeye dayalıdır⁹⁵
- Hedef tespiti ve ilişkilendirme çok önemlidir⁹⁶

1.4.2. İkna Yoluyla Caydırıcılık:

Bu caydırıcılık metodunda rakibe verilen mesaj, istenmeyen davranışı uygulaması durumunda vermiş olduğu kararın kendine büyük maliyetler/zararlar doğuracağıdır.⁹⁷ Amaç, karşı aktörün revizyonist bir politikayı benimseme kararından önce başvurduğu fayda-zarar hesaplamasında zarar hanesinin ağır basmasıdır. Ceza yoluyla caydırıcılıktan farklı olarak, herhangi bir tehdit unsuru veya korku yaratma hedefi taşımaz; esas hedef rakibin saldırgan davranıştan elde edeceği faydayı minimize etmektedir. Rakibin amacına ulaşma ve fayda elde etme kabiliyetini fiziksel olarak imkânsız hale getirmek hedeflenir.⁹⁸

İkna Yoluyla Caydırıcılığın Karakteristik Özellikleri:

- Savunma kabiliyetine ağırlık verir.⁹⁹
- İstismar edilebilecek zafiyetlerin önceden teşhisi büyük önem taşır.¹⁰⁰

⁹² Schelling, *Arms and Influence*, 71-74.

⁹³ Schelling, 23

⁹⁴ Glenn Snyder, *Deterrence and Defense* (New Jersey: Princeton University, 1961)

⁹⁵ Schelling, 197-200

⁹⁶ Joseph S. Nye, "Deterrence and Disuasion in Cyberspace", *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71, doi:10.1162/ISEC_a_00266

⁹⁷ Schelling, 78-79.

⁹⁸ Glenn Snyder, *Deterrence by Denial and Punishment* (New Jersey: Center of International Studies, 1959).

⁹⁹ Patrick Morgan, *Deterrence: A Conceptual Analysis* (Londra: Sage Publications, 1977), 30

¹⁰⁰ Robert A. Pape, "Coercion and Military Strategy: Why Denial Works and Punishment Doesn't", *The Journal of Strategic Studies*, Vol.15, No.4 (December 1992), 431

- Rakibi amaçladığı hedefe ulaştırmama veya çok büyük maliyetlere katlandırma önemlidir.¹⁰¹
- Kamu-Özel sektör iş birliğini esas alır.¹⁰²

1.4.3. Dayanıklılık Yoluyla Caydırıcılık:

Dayanıklılık, maruz kalınan bir saldırı sonrasında iyileşebilme ve içine düştüğü menfi durumu oluşturan koşullara adapte olarak gelecek muhtemel tehditlerin zararlarından kaçınma becerisi olarak tanımlanabilir.¹⁰³ Yakın dönemde tehdit cins ve aktörlerinin sayısındaki artış ve ortaya çıkan hibrit tehditler devletleri bütün tehditlerin gerçekleşmeden aynı anda caydırma imkânının bulunmadığı bir duruma sokmuştur. Bu doğrultuda tehditleri gerçekleşmeden rakibi alıkoymak yerine saldırı sonrası maruz kalınan zararları asgari düzeye çekmek ve gelecek saldırılara karşı daha dirençli hale gelme yaklaşımı son dönemde benimsenen bir stratejidir.

Bu stratejide amaç saldırının öngörülen etkileri doğurmadığını rakibe gösterip bu şekilde istenilmeyen davranıştan alıkoymaktır. Muhtemel faydaların minimizasyonu bakımından dayanıklılık yoluyla caydırıcılık, ikna yoluyla caydırıcılık metodu ile benzerlik içermektedir. Nitekim birçok çalışmada dayanıklılık stratejisi ayrı bir caydırıcılık metodu yerine ikna yoluyla caydırıcılık içerisinde sınıflandırılmaktadır. Bununla birlikte söz konusu iki metot arasında birtakım zamansal ve amaçsal farklılıkların bulunduğu unutulmamalıdır. İkna yoluyla caydırıcılıkta aktör, tedbirlerini muhtemel saldırıdan önce almakta ve savunma odaklı tedbirler alarak saldırının gerçekleşmemesini amaçlamaktadır. Buna karşın, dayanıklılık yoluyla caydırıcılıkta daha reaktif bir yaklaşım sergilenir. Saldırının gerçekleşmesine fırsat verilerek uğranılan zararların etkilerini en aza indirmek ve mevcut olumsuz koşullar ile hatalardan ders çıkarılmak hedeflenir. Sürekli adaptasyon ve yenilenme odaklı bu stratejide bütünsel toplum anlayışı ön plandadır. Birey, toplum, özel sektör gibi devlet altı bileşenler güvenliğin birer paydaşları olarak caydırıcılık stratejisinde önem teşkil etmektedirler.

¹⁰¹ Age, 442-444

¹⁰² Eugenio Lilli, Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence, *Contemporary Security Policy*, 42 (2), 163-188

¹⁰³ Guillaume Lasconjarias, “Deterrence Through Resilience: NATO, the Nations and the Challenges of Being Prepared”, *NATO Defence College Eisenhower Paper*, sayı: 7 (Mayıs 2017): 2.

Dayanıklılık Yoluyla Caydırıcılığın Karakteristik Özellikleri:

- Tehditlerin etkilerinin hafifletilmesine odaklanır.¹⁰⁴
- Kamu-Özel sektör-Toplum iş birliğini esas alır. Bütünsel toplum anlayışı ile toplumun tüm kesimleri muhtemel tehditler hakkında bilinçlendirilir. Toplumsal farkındalık yaratılır. Stratejik iletişim ön plandadır.¹⁰⁵
- Hasar minimizasyonu ve hızlı iyileşme çok önemlidir.¹⁰⁶

Caydırıcılık Metodu	İkna Yoluyla Caydırıcılık	Ceza Yoluyla Caydırıcılık	Dayanıklılık Yoluyla Caydırıcılık
Eylem Biçimi	Savunma	Misilleme	İyileşme
Bedel Ödetme / Faydadan Alıkoyma Eyleminin Gerçekleştirilme Zamanı	Saldırı öncesi safha	Saldırı safhası	Saldırı sonrası safha

Tablo 3: Eylemlerin Gerçekleştiği Safhaya Yönelik Caydırıcılık Metotları¹⁰⁷

1.4.4. Normlar Yoluyla Caydırıcılık:

Normlar, bir grup aktör aktör tarafından uygun görülen davranış biçimlerine ilişkin sahip olunan ortak beklentilerdir.¹⁰⁸ Bu beklentiler kendiliğinden oluşmayıp aktörlerin zaman içerisinde yaşadığı karşılıklı etkileşimlerden kaynaklanmaktadır. Bu etkileşimler sonucunda mutlak kazanç sağlama veya zarara uğramama amacıyla taraflar yazılı olmayan iş birlikçi davranış kalıpları ortaya çıkarmakta ve mütekabiliyet ilkesi çerçevesi bu kurallara uyum sağlamaktadırlar. Söz konusu kurallar sistematik görüşme ve müzakereler doğrultusunda ilan edilebileceği gibi bazı durumlarda ihtiyaç doğrultusunda kendiliğinden de vücut bulabilir. Axelrod'un uluslararası ilişkilerde iş

¹⁰⁴ Alex Wilner, Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation, *Comparative Strategy*, 36(4), 309-318, 2017, 310

¹⁰⁵ Guillaume Lasconjarias, "Deterrence Through Resilience: NATO, the Nations and the Challenges of Being Prepared", *NATO Defence College Eisenhower Paper*, 7, 2017; Jackson Nicole, "Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO", *Journal of Strategic Studies*, 19 (4), 104-125, 2019, 117

¹⁰⁶ Maurizio Martellini, "Cyber Security: Deterrence and IT Protection for Critical Infrastructures", *Springer Briefs on Computer Science*, 2013, DOI 10.1007/978-3-319-02279-6

¹⁰⁷ Ann E Hammer, Trisha H Miller, ve Eva C Uribe, "Cyber Resilience as a Deterrence Strategy" (New Mexico: Sandia National Laboratories, 2020), 14.

¹⁰⁸ Martha Finnemore, *National Interests in International Society*, (Ithaca, NY: Cornell Univ. Press, 1996), 22.

birliđinin gelişimi kapsamında yer verdiği “yaşa ve yaşat” örneđi normların karşılıklı çıkarlara hizmet edecek şekilde nasıl kendiliğinden ortaya çıktığına dair çarpıcı bir örnek sunmaktadır. Birinci Dünya Savaşı ile özdeşleşen siper muharebelerinde İngiliz ve Alman ordularının çatışma dinamiklerini araştıran Axelrod, bu muharebelerde adı konulmamış bir yarı ateşkese işaret etmektedir.¹⁰⁹ Şöyle ki siper muharebelerinin statik doğası geređi birbiri ile uzun süre karşı karşıya kalan iki ordu, bu süre zarfında doğrudan iletişim olmaksızın bir yapılageliş geliştirmiştir. Bu yapılagelişe göre, karşılıklı görmeyerek atışlar sonrası iki tarafın da ağır personel zayıat verdiği görülmüş ve bu durumdan kaçınmak için bir taraftan atışların sıklığı azaltılırken diğer taraftan yapılan atışlar daha çok tali hedeflere yönlendirilmiştir. Axelrod, bu durumun önüne geçmeye çalışan her iki karargâhın da uzun süre bu adı konulmamış normu kıramadığını ifade etmektedir. İşin ilginç yanı içinde misilleme mekanizmasının bulunduğu bir mütekabiliyet esaslı bir davranış ilişkisinden kontrolsüz, rıza merkezli bir davranış biçiminin meydana gelmesidir. Zira yapılan topçu atışları, harekâtı planlayan üst akıl olan karargâhın inşa ettiği bir caydırma mekanizmasına hizmet etmemektedir. Bu durum, yaşanan olayı ceza yoluyla caydırıcılıktan ayırmakta ve kendiliğinden anlaşmanın esas olduğu normlar yoluyla caydırıcılık kategorisine sokmaktadır.

Axelrod’un örneğinde de görüleceđi üzere, normlar yazılı olmamasına karşın uluslararası ilişkilerde önemli bağlayıcılığı olan mekanizmalardır. Ortaklaşa benimsenen davranış kalıplarını terk etmek, dışlanma veya cezalandırılma sonuçlarını doğurabileceğinden devletler ortak rızaya uyumlu bir şekilde hareket etmeye özen göstermektedirler. Bu durum, kabul görmeyen davranışların normlar yolu ile caydırılmasını mümkün kılmaktadır. Çünkü normun haricinde hareket eden devlet, uluslararası düzeyde itibarının zedelenmesi, kınama, yaptırım veya iç kamuoyunda rahatsızlık gibi istemeyen sonuçlarla karşılaşabilir.¹¹⁰ Nye’a göre özellikle siber tehditler karşısında caydırıcılığın sağlanması için normların birer enstrüman olarak kullanılması önem arz etmektedir.¹¹¹ Zira bu ortamdaki gerek saldırıyı belirleme ve

¹⁰⁹ Robert M. Axelrod, *The Evolution of Cooperation*, (New York: Basic Books, 2006), 75-89.

¹¹⁰ N. J. Ryan, “Five Kinds of Cyber Deterrence”, *Philosophy & Technology* 31, sayı: 3 (Eylül 2018): 337

¹¹¹ Nye, Joseph. S., “Deterrence and Dissuasion in Cyberspace”, *International Security*, 41(3) (2017): 44–71.

cezalandırma kabiliyetleri, gerekse saldırıları engelleyici savunma tedbirlerinin güçlüğü devletler arasında oluşturulacak yapılageliş kurallarını birer caydırıcı unsur olarak ön plana çıkarmaktadır.

Normlar Yoluyla Caydırıcılığın Karakteristik Özellikleri:

- Kabul gören davranış kalıpları oluşturma temellidir.¹¹²
- Fayda/maliyet yerine değerleri esas alır. İhlal edilmemesi gerek değerler üzerinde inşa edilir.¹¹³
- Ortak kabul gören davranış kalıpları dışında hareket eden devletler dışlanır.¹¹⁴

Bu bölümde çalışmanın kavramsal çerçevesi olan caydırıcılık stratejisi ele alınmıştır. Öncelikle caydırıcılık kavramı tanımlanmış ve alana dair çalışmaların günümüze kadar oluşturduğu dört caydırıcılık dalgası sunulmuştur. Bu dört dalga caydırıcılığın farklı boyutlarını inceleyen ve farklı bilimsel yaklaşımlar barındıran gelişimsel bir süreci tasvir etmektedir. Bu süreçte kavram ile ilgili ortaya atılan kabiliyet, inandırıcılık ve iletişim bileşenleri irdelenmiş ve dördüncü dalgada çalışmalarında tespit edilen kabiliyet bileşeni eksikliği sorunsallaştırılmıştır. Araştırmanın katkıda bulunmayı amaçladığı noktalardan biri bu doğrultuda siber tehditlere yönelik caydırıcılık çalışmalarında görülen kabiliyet bileşeni eksikliğidir. Zira bu tehditlere karşı oluşturulan caydırıcı kabiliyetler halen inşa sürecindedir ve nükleer silahlar gibi verili olarak ele alınmamalıdır. Bölümün sonunda dört caydırıcılık dalgası boyunca ortaya çıkan dört caydırıcılık metoduna yer verilmiştir. Bunlar; ikna, dayanıklılık, normlar ve ceza yoluyla caydırıcılık metodlarıdır. Söz konusu metodlar çalışmaya ait hipotezde bağımlı değişken olan caydırıcılık stratejisinin almış olduğu nominal değerlerdir. Dolayısıyla bağımlı değişkendeki farklılaşmayı doğru bir şekilde tespit edebilmek için bu metodlarının her birinin karakteristik özelliklerine yer verilmiştir.

¹¹² Lawrence Freedman, “Deterrence: A Reply”, *Journal of Strategic Studies*, 28 (5), 789-801, 2005, 794

¹¹³ Tim Stevens, “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”, *Contemporary Security Policy*, 33:1, 148-170, 177, DOI: 10.1080/13523260.2012.659597

¹¹⁴ Nye, Joseph. S., “Deterrence and Dissuasion in Cyberspace”, 60

KURAMSAL ÇERÇEVE: NEOKLASİK REALİZM

Bir güvenlik stratejisi olan caydırıcılık stratejisi, devletlerin uluslararası ortamda karşılaştığı tehlikelere karşı diğer aktörlere karşı benimsediği bir zorlayıcı diplomasi ürünüdür. Dolayısıyla bir dış politika analizi yaklaşımı ile ele alınmalıdır. Bunun için Uluslararası İlişkiler teorileri kullanışlı bir araçtır. Teori kısaca mantıksal ve içsel bir tutarlılığa sahip açıklayıcı bilgiler kümesi olarak tanımlanabilir.¹¹⁵ Gözleme dayalı oluşturulan ve çeşitli testlerle doğruluğu desteklenen teorilerin belirli bir alana dair nedensel ilişkilerin analizinde kullanılması araştırmanın mantıksal sürecinin takibinde kolaylık sağlar. Bu doğrultuda vaka analizinin takibine rehberlik etmesi ve elde edilen bulguların yorumlanmasına yardımcı olması maksadıyla çalışmada kuramsal çerçeve olarak Neoklasik Realizm Uluslararası İlişkiler teorisine başvurulmuştur.

Bahse konu olan teoriye başvurulmasını sebebi, Uluslararası İlişkilerin genel yapısını inceleyen Realizmin diğer türlerinden farklı olarak Neoklasik Realizmin analiz birimi olarak devleti ele alması ve devletin dış politika davranışlarını anlamlandırmaya çalışmasıdır. Diğer taraftan teorinin analiz çerçevesinde yapısal faktörler ile iç bileşenleri birlikte ele alan yaklaşımı caydırıcılık yazınına dair tespit edilen iç bileşen eksikliği durumuna cevap verecek niteliktedir. Dolayısıyla bu bölümde vaka analizinin icrasına yön veren Neoklasik Realizm teorisi açıklanmıştır. Öncelikle teorinin hangi analiz seviyesindeki ilişkilere dair açıklamalar getirdiği açıklanmış ve bu alanda Neorealizm ile farklılaştığı noktalara işaret edilmiştir. Caydırıcılık stratejisinin kuramsal çerçevesi nükleer silahlar ve bu silahlara dayalı oluşan güç dengesi sisteminden önemli ölçüde etkilenmiştir. Bu doğrultuda klasik caydırıcılık çalışmalarının Neorealizmin varsayımlarına dayanan bir çerçevede şekillendiği ifade edilebilir. Neoklasik Realizmin Neorealizm ile benzerlik ve farklılıklarını ortaya koymak çalışmanın benimsediği özgün bakış açısını ve alan yazına hangi noktada katkıda bulunmayı amaçladığını göstermek açısından önemlidir. Müteakiben dış politika analizinde teorinin bağımsız değişken olarak kullandığı yapısal faktörler incelenmiştir. Bu faktörler Neorealizmin

¹¹⁵ Faruk Sönmezoğlu, *Uluslararası Politika ve Dış Politika Analizi*, 6. Baskı (İstanbul: Der Yayınları, 2014), 94.

varsayımlarının aksine farklı bağlamsal koşullardan etkilenecek devlete etki etmektedir. Bu koşullar yapısal dönüştürücü, açıklık ve stratejik çevre kavramlarıdır. Vakada ele alınan siber tehditlerin yapısal dönüştürücü vasfı bu bölümde incelenerek siber uzaya dair güvenlik koşullarının devleti nasıl etkilediği anlatılmıştır. Son olarak iç değişkenler açıklanmıştır. Teorinin genel olarak bu değişkenleri dış politika analizinde hangi şekillerde kullandığı gösterilmiş ve çalışmaya ait vakada bu değişkenlerin kullanım biçimi aktarılmıştır.

2.1. Analiz Düzeyleri ve Neoklasik Realizm

Neoklasik Realizm, dış politika davranışlarını açıklamada yapısal faktörler ile aktör merkezli değişkenleri birlikte mercek altına alan bir Uluslararası İlişkiler teorisidir. Neoklasik Realizme göre, dış politika karar alma sürecini anlamak için iki temel analitik aşama izlenmelidir. İlk aşamada, devletin uluslararası sistemdeki göreceli konumu ve bu konumun yarattığı fırsatlar ile sınırlılıklar analiz edilir. Bu analiz, devletin karşı karşıya olduğu dışsal baskıları ve stratejik seçeneklerini ortaya koyar. İkinci aşamada ise, yapısal koşulların devletin iç dinamikleri bağlamında nasıl algılandığı ve yorumlandığı incelenir. Burada lider algıları, toplumun stratejik kültürü, siyasal kurumların yapısı ve işleyişi gibi içsel değişkenler devreye girer ¹¹⁶(Ripsman, vd., 2016).

Tehdit algılaması ve güç dağılımı koşulları olarak tanımlanan yapısal faktörler her zaman açık ve net değildir. Bu durumda söz konusu yapısal faktörlerin sunduğu koşulları yorumlamak ve dış politikaya yön vermek için devlet seviyesindeki iç değişkenler devreye girmektedir. ¹¹⁷ Bu doğrultuda dış politika davranışı, yapısal faktörler kapsamında şekillenen ve lider, kurum, stratejik kültür gibi iç değişkenler doğrultusunda açıklanabilen bir süreçtir. Zira devletin içinde bulunduğu bağlam ne kadar önemliyse bu bağlamı algılayan ve yorumlayan iç değişkenler de o kadar önemlidir. Yalnızca bağlamı ele alan veya anarşi düzleminde genellenebilir davranışlar üzerinde yapılan analizler A devletinin neden dış politikada X tercihi yerine Y seçeneğini benimsediğini açıklamada yetersiz kalmaktadır. Bu açıdan bakıldığında Neoklasik Realizmin karşılaşmış olduğu vakaları tüm boyutları ile kavrama ve

¹¹⁶ Norrin Ripsman vd., *Neoclassical Realist Theory of International Politics* (New York: Oxford University Press, 2016).

¹¹⁷ Gideon Rose, "Review: Neoclassical Realism and Theories of Foreign Policy", *World Politics* 51, sayı: 1 (1998): 144-72.

açıklayabilme maksadıyla farklı analiz düzeylerine bir arada başvuran hibrit bir araştırma çerçevesi benimsediğini ifade etmek mümkündür. Bu hibrit çerçeveyi daha iyi anlamak için anarşiye yönelik yaklaşımında benzer durumda olan ancak aktörün ele alınmasında farklılaşan Neorealizme yer vermek gerekir.

Neorealizme göre, sistemde güçlü olan ve başarılı politikalar üreten devletler örnek alınarak taklit edilmektedir. Zira kendine yardım ilkesinin egemen olduğu sistemde en kötü senaryoya göre hareket etmeyen devletler yok olma tehlikesi ile karşı karşıya kalabilmektedir.¹¹⁸ Rekabet ve taklit doğrultusunda sistem ve devletler arasında oluşan sürekli etkileşim hali birbirine benzer aktörler yaratmaktadır. Böylece devletlerin iç bileşenleri söz konusu ilişkileri etkilemede geri planda kalmaktadır. Sistemde hâkim olan benzer şekilde hareket etme güdüsü Waltz'a göre devlet davranışını kesin bir şekilde belirlemese de uygulayabileceği seçenekler bakımından önemli kısıtlamalara tabi tutarak onu yönlendirmektedir.¹¹⁹ Neoklasik Realizmin temel dayanak noktası ise tam olarak bu sınırlama ve belirleme eşikleri arasında devreye girmektedir.¹²⁰

Epistemolojik olarak Neoklasik Realizm, Neorealizmin indirgemeci yapısına karşı kapsayıcılık ve açıklayıcılığı önceleyerek devlet ve sistem analiz seviyelerini birlikte ele almaktadır. Şöyle ki, Neorealizmin basitlik ve tutarlılık adına benimsemiş olduğu indirgemeci yaklaşımı eksik bulan Neoklasik Realizm araştırmacıları, teorinin dış politika tercihlerini açıklamada daha donanımlı olduğunu ileri sürmektedir.¹²¹ Bu noktada göze çarpan bir nokta, her iki teorinin bağımlı değişkeninin ne olduğu, başka

¹¹⁸ Kenneth N Waltz, *Theory of International Politics* (California: Addison-Waley Publishing Company, 1979), 73-75; Eben Coetzee, "No Rest for the Weary: Competition and Emulation in International Politics. A Waltzian Perspective", *Politikon* 46, sayı: 1 (02 Ocak 2019): 1-19, <https://doi.org/10.1080/02589346.2018.1486527>; John M. Hobson, *The State an International Relations* (New York: Cambridge University Press, 2003), 23-26.

¹¹⁹ Waltz, *Theory of International Politics*, 69-73.

¹²⁰ Nicholas Kitchen, "Systemic Pressures and Domestic Ideas: A Neoclassical Realist Model of Grand Strategy Formation", *Review of International Studies* 36, sayı: 1 (Ocak 2010): 136, <https://doi.org/10.1017/S0260210509990532>.

¹²¹ Gustav Meibauer vd., "Forum: Rethinking Neoclassical Realism at Theory's End", *International Studies Review* 23, sy 1 (04 Mart 2021): 4, <https://doi.org/10.1093/isr/viaa018>; Kitchen, "Systemic Pressures and Domestic Ideas"; Realism vd., "Review: Neoclassical Realism and Theories of Foreign Policy"; Michiel Foulon, "Neoclassical Realism: Challengers and Bridging Identities", *International Studies Review*, Eylül 2015, n/a-n/a, <https://doi.org/10.1111/misr.12255>; Tudor Onea, "Putting the 'Classical' in Neoclassical Realism: Neoclassical Realist Theories and US Expansion in the Post-Cold War", *International Relations* 26, sayı: 2 (Haziran 2012): 139-64, <https://doi.org/10.1177/0047117811430674>.

bir deyişle hangi bilinmeyeni açıklama niyetinde olduğudur. Zira sistemin yapısından yola çıkarak tündengelimci bir yaklaşım benimseyen Neorealizm ile bu yaklaşıma ikinci analiz seviyesini dahil ederek tümevarımı ekleyen Neoklasik Realizm ‘yapı ile yapan’¹²² sorunsalına farklı pencerelerden bakmaktadırlar.

Neorealizme göre uluslararası anarşik düzen devletleri belirli davranış kalıplarına kanalize etmekte, bu doğrultuda devletler öngörülen davranış kalıplarını benimseyerek sistemin devamlılığını sağlamaktadır. Nihai olarak sistem ve devletin sürekli etkileşimi ortaya çıkmakta, bu döngü ise birtakım çıkarım ve öngörülerini beraberinde getirmektedir. Neorealizmin açıklama niyetinde olduğu bağımlı değişken işte bu çıkarım ve öngörülerden oluşan bir kurallar bütünüdür. Neorealizm, tek bir devletin münferit dış politika uygulamalarından ziyade, zaman ve koşullardan bağımsız olarak devletlerin belirli güç dağılımı koşullarında genel hareket tarzlarını incelemektedir. Bu doğrultuda teori tahmin etme yeteneğine sahip, test edilebilir ve yanlışlanabilir bir metodoloji ortaya koyması bakımından Realizme ilk kez bilimsel bir nitelik kazandırdığı iddiasındadır.

Neoklasik Realizmin bağımsız değişkeni ele alındığında bu noktada teorinin araştırmacıları arasında farklı bakış açıları göze çarpmaktadır. Şöyle ki ilk yıllarda Neorealizmin açıklamakta yetersiz kaldığı anomalileri ele alan ve tamamlayıcı bir rol üstlenen teori, müteakip dönemde Neorealizmin boyunduruğundan çıkarak bütün dış politika davranışlarını açıklama yoluna gitmiş ve son olarak tıpkı Neorealizm gibi sistemi açıklama iddiasında bulunmuştur.¹²³ Bununla birlikte, teorinin çıkış noktası olarak değerlendirilen ve Neorealizmin eksik kaldığı nokta olarak nitelendirilen “A

¹²² Alexander E. Wendt, “The Agent-Structure Problem in International Relations Theory”, *International Organization* 41, sayı: 3 (1987): 335-70, <https://doi.org/10.1017/S002081830002751X>.

¹²³ Norrin M Ripsman, Jeffrey W Taliaferro, ve Steven E Lobell, *Neoclassical Realist Theory of International Politics* (New York: Oxford University Press, 2016); Nicholas Ross Smith, “Can Neoclassical Realism Become a Genuine Theory of International Relations? *Squandered Opportunity: Neoclassical Realism and Iranian Foreign Policy* . By Thomas Juneau. Stanford, CA: Stanford University Press, 2015. *EU and NATO Relations with Russia: After the Collapse of the Soviet Union* . By Glenn Diesen. Abingdon: Routledge, 2016. *Neoclassical Realist Theory of International Politics* . By Norrin M. Ripsman, Jeffrey W. Taliaferro, and Steven E. Lobell. Oxford: Oxford University Press, 2016.”, *The Journal of Politics* 80, sy 2 (Nisan 2018): 742-49, <https://doi.org/10.1086/696882>; Brian Rathbun, “A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism”, *Security Studies* 17, sy 2 (22 Mayıs 2008): 294-321, <https://doi.org/10.1080/09636410802098917>; Randall L. Schweller, “Unanswered Threats: A Neoclassical Realist Theory of Underbalancing”, *International Security* 29, sayı: 2 (2004): 159-201.

devletinin neden dış politikada X tercihi yerine Y seçeneğini benimsediği” sorusu doğrudan dış politika uygulamalarına yönelik bir sorunsaldır.

Neorealizmin anlamlandırmaya çalıştığı esas çerçeve “yapı”dır. Bu yüzden Waltz her ne kadar “İnsan, Devlet ve Savaş” adlı çalışmasında güvenlik ilişkilerini üç farklı analiz seviyesi üzerinden okuma yoluna gitse de üzerinde önemle durduğu seviye yapıdır. Waltz’a göre yapı, uluslararası sistemi bir bütün olarak kavramaya yarayan soyut bir kavramın ve bu bağlamın sağlıklı bir açıklamasına erişebilmek için sistemi oluşturan birimlerin özellik ve etkileşimlerinden arınmış olmalıdır.¹²⁴ Sistemi meydana getiren birimlerin davranışlarından ziyade esas sorunsal sistemin hangi kurallar çerçevesinde vücut bulduğudur. Söz konusu kuralları, dolayısıyla yapıyı anlayan ve buna göre hareket eden devletler başarılı olacaktır. Bu doğrultuda yapı, soyut fakat bağlayıcı bir dış ortamdır; aynı zamanda değişkenler arasında bir tür değişmeyendir. Zaman ve mekândan bağımsız olarak değişmeyen işleyiş biçimlerini ortaya koyma amacında olan Neorealizm, söz konusu hedef doğrultusunda bağlam ve aktöre dair iç değişkenlerden uzaklaşmak durumunda kalmıştır. Bu tercih Neorealizme birtakım avantajlar ve dezavantajlar sağlamaktadır. Öncelikle teorinin sisteme dair ortaya koymuş olduğu varsayımların taşıdığı kesinlik ve basitlik ona önemli bir popülerite kazandırmıştır. Zaman ve mekândan bağımsız olarak Uluslararası İlişkilerin genel işleyiş mantığına dair basit ve akılda kalıcı tespitlerde bulunan teori, sistemi ve yapı taşları olan aktörleri anlama noktasında kullanışlı bir çerçeve sunmaktadır.

Diğer taraftan zaman ve mekâna bağlı olmaksızın “geçerli olma” amacı güden Neorealizm bu noktada önemli eleştirilere uğramaktadır. Robert Cox’a göre Waltz, “realizmi tarihsel koşulları baz alan kritik bir analiz çerçevesinden alıp mevcut kurum ve güç ilişkilerini kalıcı olarak değerlendiren bir problem çözücü teori hüviyetine büründürmüştür”.¹²⁵ Uluslararası İlişkileri güç, kabiliyet ve benzer devletler gibi evrensel kavramlar üzerinden açıklayan Neorealizmin kültür ve tarihselliği kapsam dışı bırakarak batı merkezli bir bilgi üretimine hizmet ettiği, yöneltilen bir diğer eleştiridir.¹²⁶ Teorinin Soğuk Savaşın sonunu açıklamada yaşadığı güçlük, bağlamı

¹²⁴ Waltz, *Theory of International Politics*, 80.

¹²⁵ Robert Keohane, *Neorealism and Its Critics* (New York: Columbia University Press, 1986), 18.

¹²⁶ Michiel Foulon ve Gustav Meibauer, “Realist Avenues to Global International Relations”, *European Journal of International Relations*, sayı: 4 (Aralık 2020): 3, <https://doi.org/10.1177/1354066120926706>.

dikkate alma açısından, söz konusu eleştirilerin yersiz olmadığına dair bir örnek olarak karşımıza çıkmaktadır. Bütün bu eleştiriler ışığında, Neoklasik Realizmin açıklayabilme amacı ön plana çıkmaktadır. Neorealizm sistemin doğasına ve aktörleri çevreleyen koşullara ilişkin evrensel geçerliliği bulunan varsayımlarda bulunmaktadır. Neoklasik Realizmin esas önceliği ise açıklayabilme kabiliyetidir. Dolayısıyla Neorealizmin evrensel olarak tanımladığı yapısal faktörlere bağlamsal faktörler olan aktöre ilişkin değişkenleri eklemektedir.

Siber tehditler ışığında oluşturulan güvenlik stratejilerini incelemek için Neoklasik Realizm daha açıklayıcı bir perspektif sunmaktadır. Bunun başlıca sebebi siber uzayın oynamakta olduğu yapısal dönüştürücü faktörünün güvenlik stratejilerini evrensel güç dinamikleri çerçevesinde okuma gücü yaratmasından kaynaklanmaktadır. Yapısal dönüştürücü bölümünde ifade edildiği üzere, siber uzay devletlerin karşılaştıkları etki ve bunlara karşı gösterdikleri tepki bakımından önemli yenilikler ve bilinmeyenler barındırmaktadır. Bu yüzden siber uzaya dair birtakım tespitlerde bulunmak için ortamı etkileyen faktörlerin kapsamlı bir şekilde ele alınması gerekmektedir. Başka bir deyişle, siber tehditler geleneksel güç dinamikleri ekseninde yapılan araştırmaları eksik kılmaktadır. Böylece sistem ve devlet eksenindeki değişkenlerin birlikte ele alınmasını gerektirmektedir. Dolayısıyla bu karmaşık ortama dair bazı dış politika stratejisi tespitleri yapabilmek için Neoklasik Realizm uygun kuramsal çerçeveyi sunmaktadır.

2.2. Neoklasik Realizmin Araştırma Metodolojisinde Bağımsız Değişken: Yapı-Aktör Etkileşimi

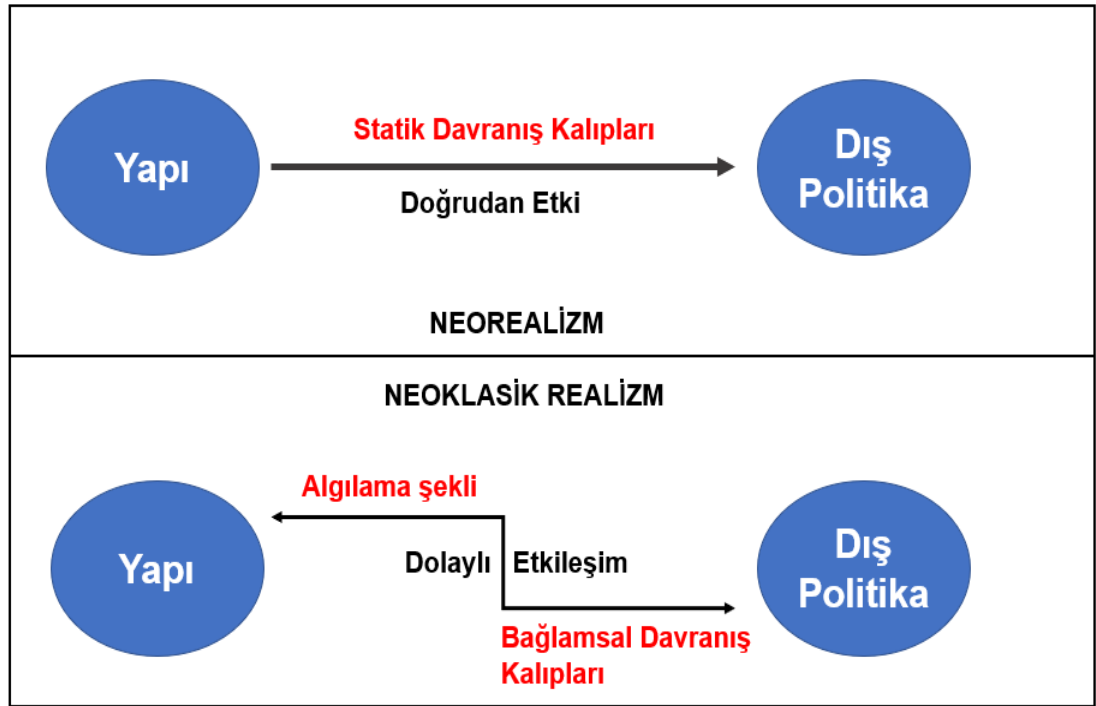
İlk örneklerde¹²⁷ Neorealizmin açıklayamadığı vakaları inceleyen, daha sonra kendi metodolojik sınırlarını çizerek ayrı bir araştırma çerçevesi halini alan Neoklasik Realizm, yine de Neorealizmin kuramsal çerçevesi önemli ölçüde paylaşmaktadır. Bu durumu Lobell, Taliaferro ve Ripsman, teorinin üç ana varsayımı olarak sunduğu aşağıdaki tespitlerde görmek mümkündür:¹²⁸

¹²⁷ Schweller, “Unanswered Threats: A Neoclassical Realist Theory of Underbalancing”; Jack Snyder, *Myths of Empire: Domestic Politics and International Ambition* (New York: Cornell University Press, 1993).

¹²⁸ Ripsman, Taliaferro, ve Lobell, *Neoclassical Realist Theory of International Politics*, 179.

1. Uluslararası düzen anarşiktir ve devletler hayatta kalmak için kendine yardım prensibi ile hareket etmelidir,
2. Hayatta kalma en önemli ulusal menfaattir,
3. Devletleri mutlak fayda yerine göreceli faydaya yönlendirdiğinden dolayı anarşi devletler arası yardımlaşmayı önemli ölçüde zorlaştırır.

Görüldüğü gibi Neoklasik Realizm uluslararası sistemin doğasına ilişkin Neorealizm ile aynı varsayımları paylaşmaktadır. Farklılaşan temel nokta yapı ve dış politika ilişkisinde yatmaktadır. Neorealizme göre bu iki unsur arasında yapının dış politikayı şekillendirdiği doğrudan bir etkileşim bulunmaktadır. Neoklasik Realizme göre ise söz konusu etkileşim dolaylıdır. Zira dış politikanın şekli karar vericilerin içinde bulundukları yapıyı analiz biçimi ve karar alma süreçlerine etki eden değişkenler tarafından belirlenmektedir.¹²⁹



Şekil 2: Yapı-Dış Politika İlişkisi - Neorealizm vs. Neoklasik Realizm

Neorealizme göre devletin dış politikası öncelikle o devletin materyal kabiliyetler üzerinden hesaplanan gücü ve bu güç doğrultusunda uluslararası düzendeki konumu tarafından şekillenmektedir.¹³⁰ Waltz'un yapı lehine tek taraflı olarak tanımladığı bu

¹²⁹ Kitchen, "Systemic Pressures and Domestic Ideas", 140.

¹³⁰ Ripsman, Taliaferro, ve Lobell, *Neoclassical Realist Theory of International Politics*, 56.

şekillendirme davranışını Neoklasik Realizm bir karşılıklı etkileşim olarak yorumlamaktadır. Bu etkileşim biçimi iki boyutta gerçekleşmektedir. Birinci boyut sistem ve devlet arasındadır. Buna göre sistem her devleti aynı oranda ve doğrudan etkilememektedir. Söz konusu etkileşim birtakım koşullar dahilinde farklılık göstermektedir. Bu koşullar şu şekilde ifade edilmektedir.¹³¹

1. Yapısal Dönüştürücüler
2. Açıklık
3. Stratejik Çevre

İkinci boyutta ise dış politika oluşturma sürecinde karar alıcılar, içinde bulundukları sistemi yorumlamakta, bu süreçte oluşan algı ve yaklaşımları iç değişkenlerin etkilerine maruz kalmaktadır. Söz konusu etkilere iç değişkenler bölümünde yer verilmiştir.

Yapısal dönüştürücü, açıklık ve stratejik çevre, yapı-aktör etkileşim biçimlerini belirleyici rol oynamaktadır. Sistem tarafından kabul gören davranış biçimleri ile fırsat ve tehditlere yönelik öngörülen yaklaşımlar aktör tarafından bu üç bileşenin süzgecinden geçtikten sonra algılanmaktadır. Dolayısıyla yapısal faktörler aktörü doğrudan değil, bulunduğu bağlam doğrultusunda etkilemektedir. Bu doğrultuda yapı-aktör etkileşiminin hangi bağlamda gerçekleştiğini ve yapısal faktörlerin aktörü nasıl etkilediğini ortaya koymak için şu sorular sorulmalıdır:

- Anarşinin koşullarını değiştiren yapısal bir dönüştürücü mevcut mu?
- Aktörün fırsat ve tehditler karşısında izlemesi gerek hareket tarzları açık mı?
- Aktörün içinde bulunduğu stratejik çevre güç ilişkileri bakımından aktörü belirli hareket tarzı opsiyonları ile sınırlandırıyor mu?

Söz konusu sorulara verilen cevaplar aktörün dış politika oluşturma sürecinde yapısal faktörlerin ne derecede belirleyici olduğuna ve iç değişkenlerin etkilerine ne kadar alan açıldığına dair bir fikir sunmaktadır. Bu kapsamda yapının “verili” olarak değil, bulunduğu bağlam içerisinde ele alınmasına olanak tanıyan bu üç bileşeni anlamak önem arz etmektedir.

¹³¹ Ripsman, Taliaferro, ve Lobell, 38-56.

2.2.1. Yapısal Dönüştürücüler

Snyder'a göre yapısal dönüştürücüler, yapının temel etkileşim biçimlerini belirli ölçüde değiştiren koşullardır.¹³² Söz konusu koşullar uluslararası sistemi tanımlayan anarşinin öngörülerini farklılaştırabilmektedir. Snyder bu koşullara bütün devletler tarafından eşit şekilde maruz kalındığını ifade ederken, Lobell, Taliaferro ve Ripsman etkilenme biçiminin devlet veya bölge düzeyinde farklılık gösterebildiğini savunmaktadır.¹³³

Yapısal dönüştürücülere örnek olarak normlar, kurumlar, askeri teknoloji ve coğrafya verilmektedir. Snyder tarafından nükleer silahlar örneği yapısal dönüştürücü kavramını anlamak için kullanışlı bir perspektif sunmaktadır. Buna göre, Soğuk Savaş döneminde ABD ve Sovyetler Birliği tarafından elde edilen nükleer ikinci vuruş kabiliyeti, bir taraftan rekabet ortamını tırmandırmakta ve güvenlik ikileminden doğan tehdit ortamını ciddileştirmektedirken diğer taraftan bu silahların devasa yıkım kabiliyetleri her iki aktörün saldırgan girişimlerini sınırlandırmıştır.¹³⁴ Bu doğrultuda anarşinin öngördüğü çatışma ortamı meydana gelmemiştir. Bilakis tarihin en tehlikeli silahlarının hüküm sürdüğü Soğuk Savaş dönemi aynı zamanda “uzun barış” dönemi olarak adlandırılmıştır. Çalışmanın konusu olan siber tehditlerin de tıpkı nükleer silahlar gibi yapısal faktörlerin devlet davranışı üzerindeki etkilerini değiştirici niteliği bulunmaktadır. Nitekim Foulon ve Meibauer siber uzayı, caydırıcılığın ele alınış biçimini doğrudan etkileyen ve değiştiren bir yapısal dönüştürücü olarak tanımlamaktadır.¹³⁵ Siber uzayın yapısal dönüştürücü niteliğini daha iyi kavramak için öncelikle siber kavramını tanımlamak ve siber uzayın kendine has birtakım özelliklerini ortaya koymak önemlidir.

2.2.2. Siber Kavramı ve Bir Yapısal Dönüştürücü Olarak Siber Uzak

Uluslararası aktörler arasındaki ilişkileri güç mücadelesi üzerinden okuyarak “Doğa Hali” tespitini ortaya koyan Hobbes, insanlık tarihi boyunca süregelen çatışma halini kaçınılmaz bir durum olarak açıklamıştır. Rekabet koşulları çerçevesinde şekillenen

¹³² Glenn H. Snyder, “Process Variables in Neorealist Theory”, *Security Studies* 5, sayı: 3 (Mart 1996): 168-71, <https://doi.org/10.1080/09636419608429279>.

¹³³ Snyder, 168-71; Ripsman, Taliaferro, ve Lobell, *Neoclassical Realist Theory of International Politics*, 40-41.

¹³⁴ Snyder, “Process Variables in Neorealist Theory”.

¹³⁵ Foulon, Michiel, and Gustav Meibauer. “How cyberspace affects international relations: The promise of structural modifiers.” *Contemporary Security Policy*. 45(3) (2024): 426-458

ilişkiler bütününde aktörler güç kullanımını politikanın doğal bir uzantısı olarak araçsallaştırmıştır. Bu süreç içerisinde çatışma araçları tabii olarak içinde bulunduğu çağın dinamiklerinden doğrudan etkilenmiş ve tarih boyunca evrim geçirmiştir. Söz konusu evrimin en belirgin kilometre taşı olarak sanayi çağı etkileri gösterilebilir. Buhar makinesinin icadı; silah teknolojisini, orduları ve dolayısıyla savaş stratejilerini derinden etkileyerek muharebelerin hızını ve öldürücülüğünü gözle görülür şekilde artırmıştır. Tren ve demiryollarının icadı ile büyük birlikleri bir noktadan diğer bir noktaya intikal ettirmek kolaylaşmış ve geniş cephelerde muharebe yeteneği ön plana çıkmıştır. Bu doğrultuda, deniz ulaştırmasının üstünlüğü ve geniş yaklaşma istikametlerine ön plana çıkaran deniz hakimiyet teorisine benzer şekilde, birliklerin karada da hareket kabiliyeti kazanması Kara Hakimiyet Teorisinin güçlenmesine ön ayak olmuş; nitekim Almanya'nın her iki dünya savaşında kullandığı iç hat manevralarına dayanak teşkil etmiştir.¹³⁶ Diğer taraftan ateşli silahların eriştiği öldürücülük özellikleri ve süvarilerin yerini alan zırhlı birlikler, çatışma ortamını bir yüzyıllık süre zarfında eşi görülmemiş bir şekilde değiştirmiştir. Kuşkusuz bütün bu örnekler insanlığın gelişim serüvenlerinden bir kilometre taşı olan sanayi çağının birer sonuçlarıdır. Bu doğrultuda yirminci yüzyılın güvenlik ve çatışma ortamını sanayi çağının getirilerinden bağımsız olarak değerlendirmek oldukça eksik bir perspektif sunacaktır.

Sanayi çağının getirileri halen geçerliliğini artarak sürdürmekle birlikte, yirminci yüzyılın sonlarından itibaren insanoğlunun eriştiği bilgi çağı, tıpkı selefi gibi kendine has birtakım karakteristik yenilikleri beraberinde getirmiştir. Bu yeniliklerden biri de siber kavramıdır. Bu kavram bilginin otomatize edildiği ve hızla yayıldığı yeni bir habitata işaret etmektedir. Söz konusu habitata ilişkin tehdit algılamalarını değerlendirmek için öncelikle bu alana dair bazı tanımlamaları ortaya koymak faydalı bir perspektif sunmaktadır.

Siber uzay, siber savaş, siber tehdit gibi kavramların başında kullanılan “siber” tanımlaması içinde bulunduğu tamlamaya “bilgisayar veya internetle bağlantılı”¹³⁷ anlamını veren bir sıfat vazifesi görmektedir. Yunancada yönetici anlamına gelen “*kybernetes*” sözcüğünden gelen bu kavram, “bilginin otomasyonu ve işlenmesini”

¹³⁶ Haldun Yalçınkaya, *Savaş: Uluslararası İlişkilerde Güç Kullanımı* (Ankara: İmge Kitabevi, 2008), 175.

¹³⁷ Cambridge Dictionary. <https://dictionary.cambridge.org/dictionary/english/cyber>

açıklamak maksadıyla ilk olarak 1948 yılında Wiener tarafından kullanılmıştır.¹³⁸ Birleşmiş Milletlerin Siber tanımına baktığımızda “ağ bağlantılı bilgisayarlar, bilişim altyapıları ve veri tabanlarına” işaret edilerek interneti çağrıştıran bir açıklamaya gidildiği görülebilir.¹³⁹ Oysa ki siber sözcüğü internetten daha kapsayıcı bir alana atıfta bulunmaktadır. Söz konusu alanın kapsamı “siber uzay” terimi incelendiğinde daha net anlaşılabilir.

ABD ordusu “JP 3-13 Bilgi Harekâtı Müşterek Yönergesi” siber uzayı şu sözlerle tanımlamaktadır: “Bilgi ortamının içerisinde bulunan internet, telekomünikasyon ağları, bilgisayar sistemleri, işlemci ve kumandaları ihtiva eden, birbirine bağlı bilgi teknolojisi altyapıları ve yerleşik verilerden oluşan küresel alan.”¹⁴⁰ Karmaşık olarak değerlendirilebilecek bu tanım JP 3-12 Siber Uzay Harekâtı yönergesinde siber uzayı meydana getiren bileşenlerin sıralanması ile daha somut hale gelmektedir. Buna göre siber uzay birbirinden farklı fakat karşılıklı bağımlı üç katmandan oluşmaktadır: Fiziksel ağ katmanı, mantıksal ağ katmanı ve siber-karakter katmanı.¹⁴¹ Fiziksel ağ katmanı bilgisayar donanım ve depolama altyapılarını, mantıksal ağ katmanı yazılımsal kod ve internet adreslerini, siber-karakter katmanı ise bireysel veya kurumsal kullanıcı hesapları ile bunların birbirleri arasındaki ilişkiyi kapsamaktadır.¹⁴²

Bütün bu bileşenler göz önüne alındığında siber uzayın tek bir bilgisayara ait donanımsal parçalardan, bu bilgisayar içindeki verileri, bilgisayarın bağlı bulunduğu yerel ağları ile interneti, internete erişimi olan bütün cihazları, telekomünikasyon altyapısı, internet ve kapalı ağ sistemlerini kendi fonksiyon alanlarına entegre eden her türlü kamu/özel kurum, fabrika, altyapı hizmetlerini içine alan muazzam bir sanal coğrafyaya tekabül ettiğini ifade etmek mümkündür. Bu sanal coğrafyanın büyüklüğü ve kendine has özellikleri güvenlik stratejileri bakımından aynı derecede kapsamlı ve yenilikçi uygulamalara ihtiyaç doğurmaktadır. Nitekim, “ABD’nin siber uzayı kara,

¹³⁸ Eric Luijff, “Understanding Cyber Threats and Vulnerabilities”, içinde *Critical Infrastructure Protection*, ed. Javier Lopez, Roberto Setola, ve Stephen D. Wolthusen, c. 7130, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer Berlin Heidelberg, 2012), 53, https://doi.org/10.1007/978-3-642-28920-0_4.

¹³⁹ Steve Winterfeld ve Jason Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, Syngress Basics Series (Amsterdam ; Boston: Syngress/Elsevier, 2013), 17.

¹⁴⁰ “JP 3-13 Information Operations”, 2012, 2-9.

¹⁴¹ “JP 3-12 Cyberspace Operations”, 2018, 22-24.

¹⁴² A.g.e..

deniz, hava ve uzay ortamlarına ilaveten beşinci bir harekât alanı olarak tanımlaması”¹⁴³ siber uzayın güvenlik açısından içinde barındırdığı kabiliyet, tehdit ve tedbir yelpazesinin genişliğine işaret etmektedir. ¹⁴⁴ Bununla birlikte diğer harekât ortamlarından farklı olarak siber uzayın “insan yapımı” olan doğası onu farklı bir yere koymaktadır.

Aslında siber uzay, insan yapımı olan sanal ortamın yanı sıra fiziksel ortam ile kesişen geniş kapsamlı bir coğrafyadır. Bu geniş coğrafyanın fiziksel unsurları, siber uzayın oluşumuna bir taraftan kaynaklık ederken diğer taraftan bilginin sanal ortamda kullanılış şekline doğrudan etkilenmektedir. Başka bir deyişle, siber uzayda yaratılan etkiler yalnızca bu coğrafyada sınırlı kalmamakta, politik, askeri, ekonomik ve sosyal hayatta önemli sonuçlar doğurabilmektedir. Örneğin bir sistem, yöneticisinin sisteme erişimini engelleyerek kendi komutlarının işletilmesini sağlayabilmektedir. Bu örnekte sistem, tek bir bilgisayar veya kullanıcı hesabı olarak alındığında saldırının etkilerinin mantıksal ağ ve siber-karakter katmanları ile sınırlı kaldığını ifade etmek mümkündür. Oysa saldırıya uğrayan sistem, endüstriyel sistemlerin geniş bilgi akışını kontrol eden ve denetleyen SCADA (Supervisory Control and Data Acquisition-Denetleyici Kontrol ve Veri Toplama) olabilir. Böyle bir senaryoda kritik altyapılar olarak nitelendirilen ulaştırma, enerji, haberleşme vb. sektörler ciddi zararlar görebilecektir. Farklı bir örnekte ise saldırgan, sistemin fiili kontrolünden ziyade sistem üzerinden gerçekleşen bilgi alışverişini hedeflemektedir. Bu senaryoda platforma yanlış bilgi girdisi yapılmakta ve dezenformasyon faaliyetleri gerçekleştirilmektedir.¹⁴⁵

Yukarıda sunulan iki saldırı örneği, siber kabiliyetlerin teknik ve aldatma boyutlarına işaret etmektedir. Farklı metotlar ile gerçekleştirilen bu saldırılar siber tehdit yelpazesinin genişliğini göstermektedir. Ortaya çıkan durumun en önemli sebebi siber uzayın bilgi ile ilişkisinde yatmaktadır. Siber uzay elektronik araçlar vasıtasıyla “bilgiyi yaratmak, depolamak, değiştirmek, paylaşmak ve ondan faydalanmak”¹⁴⁶ amacıyla dizayn edilmiş bir coğrafyadır. Bu coğrafyanın bilginin her boyutu ile yakın teması,

¹⁴⁴ Winterfeld ve Andress, *The Basics of Cyber Warfare*, 31.

¹⁴⁵ Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 26-27.

¹⁴⁶ Franklin D. Kramer, Stuart H. Starr, ve Larry K. Wentz, ed., *Cyberpower and National Security* (Potomac Books, 2011), 12, <https://doi.org/10.2307/j.ctt1djmhj1>.

tehdit algılaması kapsamında onu diğer tehdit alanlarından farklı bir konuma koymaktadır.

Anarşinin öngördüğü rekabet ve çatışma ortamı bir ölçek, konvansiyonel çatışma sıklığı ise bu ölçekte bir sabit olarak kabul edildiğinde, çatışma sıklığı bakımından nükleer kabiliyetler ile siber kabiliyetlerin ölçeğin iki karşıt ucunda yer aldığı ifade edilebilir. Zira nükleer silahların çatışma ortamını sınırlandırma davranışı siber kabiliyetler ile karşılaştırıldığında tam tersi bir durum ortaya çıkmaktadır. Siber uzayda gerek bağlayıcı normların henüz var olmayışı, gerekse saldırı için kuvvet üstünlüğüne ihtiyaç bulunmayışı çatışma ortamını akışkan bir hale getirmektedir. “Güçlünün istediğini, zayıfın ise yapmak zorunda olduğunu yaptığı”¹⁴⁷ güç ilişkilerinde siber kabiliyetlerin sağladığı düşük girdi maliyetleri ve gizlilik şemsiyesi, bir bakıma zayıfın da istediğini yapmaya başladığı bir durum yaratmaktadır. Bu durum çatışma ortamı ile ilişkilendirildiğinde etki çapları değişmekle birlikte, nicel olarak kinetik saldırıların alışlagelmişin ötesinde bir sıklıkla meydana geldiğini göstermektedir. O halde şunu ifade etmek mümkündür: Siber kabiliyetler tıpkı nükleer silahlar gibi çatışma sıklığını ve dolayısıyla anarşinin işleyiş biçimini değiştirmiştir. Bu doğrultuda siber kabiliyetler bir yapısal dönüştürücüdür ve güç dengesi koşulları ve tehdit algılamaları gibi yapısal faktörler bu yapısal dönüştürücü süzgecinden geçirilerek incelenmelidir.

Günlük hayatı kolaylaştırmak adına her geçen gün geliştirilen bilişim sektörünün doğurduğu siber ortam, doğası gereği devletleri konvansiyonel ve nükleer silahlardan farklı bir tehdit algılaması ile karşı karşıya bırakmaktadır. Günlük hayatın her kesimine dahil olan siber ortam, tehdit bağlamında araçsallaştırılması sonucu sadece devletleri değil, toplum ve bireyi de hedef alır hale gelmektedir. Ulaştırma sistemlerinden finans sektörüne siber uzayın günlük hayata entegre durumu ve beraberinde gelen teknik hassasiyetler bu ortamı hedef bakımından zengin hale getirmekte ve muhtemel tehditleri asimetrik etkilerle donatmaktadır.¹⁴⁸ Söz konusu asimetri durumu siber kabiliyetlerin “zayıfın silahı” olarak nitelendirilmesine yol açmaktadır.¹⁴⁹ Mevcut hassasiyetleri yer,

¹⁴⁷ Laurie M. Johnson Bagby, “Thucydidean Realism: Between Athens and Melos”, *Security Studies* 5, sayı: 2 (Aralık 1995): 179, <https://doi.org/10.1080/09636419508429266>.

¹⁴⁸ Gary McGraw, “Cyber War is Inevitable (Unless We Built Security In)”, *Journal of Strategic Studies* 36, sayı: 1 (2013): 109-10, <http://dx.doi.org/10.1080/01402390.2012.742013>.

¹⁴⁹ Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare”, *Security studies* 22 (2013): 375.

zaman ve araç bakımından seçebilme imkânı saldırgan tarafa inisiyatif üstünlüğü sağlamakta ve kuvvet üstünlüğünün yerini çeviklik almaktadır.¹⁵⁰ Saldırının kökeninin takip edilmesinde ortaya çıkan güçlükler de hesaba katıldığında siber kabiliyetlerin anarşinin kuvvet dengesi değerlendirmelerini bir kenara bırakarak kuvvet mukayesesine bakmaksızın saldırgan davranışların artış gösterdiği bir durum ortaya çıkmaktadır.

Siber kabiliyetlerin yapısal dönüştürücü rolünü daha iyi anlayabilmek için bu kabiliyetler paralelinde ortaya çıkan tehditlerin niteliğini doğru bir şekilde ortaya koymak önemlidir. Bu kapsamda söz konusu tehditlere ilişkin şu sorular sorulabilir:

2.2.2.1. Hangi aktörler?

Siber tehditler, devletler tarafından yönetilebileceği gibi hacker grupları, bireyler veya terörist gruplar tarafından da gerçekleştirilebilmektedir. Konvansiyonel tehditleri hesaplama bu saldırıları icra edebilecek kuvvet durumları ile kuvvet projeksiyonu tahdidinden dolayı coğrafi yakınlık hesaba katılmaktadır. Diğer taraftan, nükleer saldırıları değerlendirmede öne çıkan husus nükleer güçlerin fırlatma ve taşıma kapasiteleri ile ikinci vuruş yetenekleridir.¹⁵¹ Siber kabiliyetlerde ise bunlara benzer bir kuvvet veya coğrafya kısıtlaması söz konusu değildir. Sınırlı kuvvete sahip devlet dışı aktörler Ddos¹⁵² ve kötü amaçlı yazılım gibi tekniklerle mesafe sınırlaması tanımaksızın farklı devletlerin kamu ve özel siber altyapılarında önemli tahribatlar yaratabilmektedir.¹⁵³ Saldırıları gerçekleştirebilecek muhtemel aktör sayısındaki artış durumu bir yana, bu aktörlerin tespiti ise farklı bir sorun kaynağıdır. Maruz kalınan saldırıları gerçekleştiren aktörü tespit etmek ancak büyük çaplı saldırılar sonrası bu saldırıları gerçekleştirebilecek aktör sayısının sınırlı olduğu durumlarda mümkün

¹⁵⁰ Herbert Lin ve Amy Zegart, *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington: Brookings Institutions Press, 2018), 25-26.

¹⁵¹ William C. Martel ve Paul L. Savage, *Strategic Nuclear War: What the Super Powers Target and Why* (New York: Greenwood Press, 1986), 24-30.

¹⁵² Distributed Denial of Service (Dağıtılmış Hizmet Reddi): Bir çeşit siber saldırı. Bu saldırıda saldırgan herhangi bir servis sağlayıcının ağlarına aşırı miktarda bir kullanıcı girişi yaratarak söz konusu hizmeti meşgul eder. Böylece servisin gerçek kullanıcıları internet adresine geçici ve kalıcı olarak giriş yapamamış olurlar. Jasmeen Kaur Chahal, Abhinav Bhandari, ve Sunny Behal, “Distributed Denial of Service Attacks: A Threat or Challenge”, *New Review of Information Networking* 24, sy 1 (02 Ocak 2019): 32, <https://doi.org/10.1080/13614576.2019.1611468>.

¹⁵³ Haroon Ullah K., *Digital World War* (New Haven: Yale University Press, 2017), 73-94.

olabilmektedir.¹⁵⁴ Saldırgan aktörlerin devletler olsa bile çoğu zaman inkâr yolunu seçmesi siber alanda “yeni normal” olarak tanımlanmakta ve bu şekilde saldırgan aktörler alanın vermiş olduğu gizlilik imkânından faydalanmaktadır.¹⁵⁵ Saldırıları belirli bir aktöre atfedememe sorunsalı, mütekabiliyet ilkesi çerçevesinde karşı yaptırımları sekteye uğratmaktadır.

2.2.2.2. Hangi hedefler?

Muhtemel hedef listesindeki artış, bir yapısal dönüştürücü olarak siber kabiliyetlerin etkisinin ağırlıkla hissedildiği konulardan biridir. Soğuk Savaş boyunca nükleer silahların karşı nükleer kabiliyetlere mi, yoksa yerleşim birimlerine mi tercih edileceği tartışması bizlere iki farklı kategoride hedef kavramı sunmaktadır.¹⁵⁶ Konvansiyonel tehditler ise siyasi iradenin güç yoluyla kabul ettirilmesi önünde engel olan silahlı kuvvetler unsurlarını hedef almaktadır. Siber kabiliyetlere gelindiğinde ise hedef tanımlaması açısından basit bir kategorizasyon yapmak güçtür.

2007-2008 yılları, savaşa varan kriz durumlarında siber tehditlerin hangi unsurları hedef alabileceğine dair dünya kamuoyuna somut örnekler sunmuştur. Bu yıllarda Estonya ve Gürcistan’a ait bankacılık ve kamu hizmetleri altyapıları yoğun bir şekilde botnet¹⁵⁷ ve Ddos saldırılarına uğramıştır. Söz konusu saldırılar kriz durumlarında bir kaos durumu yaratarak devlet otoritesini zayıflatma amacı gütmektedir. Aynı dönemde gerçekleşen Stuxnet¹⁵⁸ saldırısı ise hedef ve etki bakımından siber saldırıların ne kadar “ciddi”

¹⁵⁴ Lindsay, Jon. “Tipping the scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack”. *Journal of Cybersecurity*, 1(1), (2015): 53–67.

¹⁵⁵ Myriam Dunn Cavelty ve Andreas Wenger, “Cyber security meets security politics: Complex technology, fragmented politics, and networked science”, *Contemporary Security Policy* 41, sayı: 1 (2020): 15-17.

¹⁵⁶ Delpech, *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy*, 35-36; Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*, 13-14; Schelling, *Arms and Influence*, 192-94.

¹⁵⁷ Kontrolü ele geçirilen bilgisayarların uzaktan kontrol edilerek toplu spam e-posta gönderimi, Ddos saldırısı, kimlik bilgileri ele geçirme saldırıları gibi eylemlerde kullanılması.

¹⁵⁸ Olimpik Oyunlar kod adıyla 2006 yılında Başkan Bush döneminde başlatılan Stuxnet saldırısı Başkan Obama döneminde sürdürülmüştür. ABD ve İsrail işbirliği çerçevesinde geliştirilen kötü amaçlı bir yazılım olan Stuxnet, İran’ın Natanz nükleer santralini hedef almıştır. Yazılım santralin SCADA Sistemini hedef almış, uranyum zenginleştirici santrifujlarını pasivize ederek İran’ın nükleer faaliyetlerine ciddi darbe vurmuştur. Uluslararası bir aktöre vermiş olduğu ciddi zararların yanı sıra, Stuxnet siber uzaya ilişkin tehdit algılamasına ve buna karşın geliştirilecek tedbirlere ilişkin önemli bir kilometre taşı niteliğindedir. Zira geliştirilen yazılıma ilişkin “siber uzay dışında kinetik etkiler doğuran

seviyeye geldiğini gözler önüne sermiştir. Bu saldırı, siber tehditlerin yalnızca bilişim ağlarını değil, somut fiziksel tahribatlar yaratabilme kabiliyetini göstermesi bakımından önemlidir.¹⁵⁹ Natanz Nükleer tesisinin SCADA¹⁶⁰ sistemine sızdırılan zararlı yazılım, uranyum zenginleştirme işleminde kullanılan santrifüjlerin yer değiştirmesini sağlayarak İran nükleer programını sekteye uğratmayı başarmıştır.¹⁶¹ Diğer taraftan yazılımın yalnızca uranyum zenginleştirme prosedürünü tahrip etmeye angaje olması siber tehditlerin hedef hassasiyetleri boyutunda geldiği noktayı işaret etmektedir.

2021 yılında ABD’de gerçekleştirilen petrol boru hattına yönelik siber saldırı ise kritik altyapıların söz konusu tehditlere karşı kolaylıkla istismar edilebilecek güvenlik zafiyetleri olduğunu göstermiştir. Bölgesel bir petrol dağıtım krizine sebep olan saldırıda şirket yetkilileri kendilerinden istenilen beş milyon dolarlık fidyeyi *Darkside* hacker grubuna ödemek durumunda kalmıştır.¹⁶² SCADA tabanlı siber-fiziksel sistemlerin kritik altyapı işletimine entegre edilmesi, ortaya koymuş olduğu kullanım etkinliğinin yanı sıra birtakım hassasiyetleri beraberinde getirmektedir.¹⁶³ Söz konusu

ilk siber silah” ve “atom bombasının siber eşiği” gibi benzetmeler siber uzayda yaratılan etkiye dair önemli ipuçları sunmaktadır.Lindsay, “Stuxnet and the Limits of Cyber Warfare”, 366.

¹⁵⁹ Eugenio Lilli, “President Obama and US Cyber Security Policy”, *Journal of Cyber Policy* 5, sayı: 2 (03 Mayıs 2020): 277, <https://doi.org/10.1080/23738871.2020.1778759>.

¹⁶⁰ Supervisory Control and Data Acquisition: Denetleyici Kontrol ve Veri Toplama

Kritik altyapıların işletim sistemi dört ana bileşenden oluşmaktadır:

Endüstriyel Sistemi (ICS)

Merkezi Denetleme Kontrol ve Veri Toplama Sistemi (SCADA)

Dağıtılmış Kontrol Sistemi (DCS)

İşletme Teknolojisi

SCADA, ICS altında faaliyet gösteren, sensörler ile çalışma istasyonları arasında sürekli ve çift yönlü bir iletişim sağlayan yazılım tabanlı bir gözetim/kontrol sistemidir.

Martti, Lehto ve Pekka Neittaanmaki.ed., *Cybersecurity: Critical Infrastructure Protection*. 2022. Sf.26

¹⁶¹ A.g.e..

¹⁶² New York Times, “Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity”, 14 Mayıs 2021, <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>.

¹⁶³ Martti Lehto ve Pekka Neittaanmaki, ed., *Cybersecurity: Critical Infrastructure Protection* (Barcelona: Springer, 2022), 31-32.

entegrasyon siber tehditler için bir saldırı zemini yaratmaktadır. Saldırgan aktörler sistemlerde kullanılan yazılımların açıklarını sürekli test etmekte ve buldukları açıkları istismar ederek sistemin kontrolünü ele geçirmeye veya işleyiş düzenini bozmaya çalışmaktadır.

Yukarıdaki örnekler siber tehditlerin hedef yelpazesinin genişliğine dair bir fikir sunabilir. Bu ortamdaki hedefler kritik altyapı tesisleri, nükleer reaktörler, bankacılık uygulamaları, devlet arşivleri, resmî sosyal medya hesapları, elektronik devlet hizmet sağlayıcıları gibi farklı karakteristik özellikler taşıyan birimlerdir. Söz konusu birimlerin ortak özelliği ise işletim sistemlerinde açık veya kapalı ağların kullanılmasıdır. Günümüzde gelinen noktada otomasyon ve 5G¹⁶⁴ teknolojileri göz önünde bulundurulduğunda; siber tehditlerin birey, toplum ve devlet seviyesinde her türlü erişim, hizmet ve kapasiteyi hedef alabildiği bir durum ortaya çıkmaktadır.

2.2.2.3. Hangi silah/vasıtalar?

Nükleer silahlar ile birlikte ortaya çıkan caydırıcılık stratejisi, ABD ve Sovyetler Birliğinin karşılıklı teyit edilmiş imha durumunu meydana getirmesi neticesinde oluşan statüko durumu ile özdeşleşmiştir. Söz konusu duruma erişilmesinde esas belirleyici faktör, tarafların ikinci vuruş kapasitelerine erişmeleri olmuştur. İkinci vuruş kapasitesi; nükleer bir savaş durumunda, saldırıya uğrayan bir aktörün sahip olduğu nükleer kabiliyetlerin bir kısmını koruyarak misilleme yapabilme yeteneğidir.¹⁶⁵ Bahse konu olan silahların yıkım kabiliyetleri göz önüne alındığında, böyle bir senaryo iki aktörün karşılıklı imhasına yol açabileceğinden caydırıcılık otomatik olarak devreye girmektedir. İşte tam bu noktada tehdit vasıtalarının önemi ortaya çıkmaktadır. Zira, aktarılan senaryodaki aktörler ikinci vuruş kabiliyetlerine nükleer başlıklarını taşıyan vasıtaları çeşitlendirerek erişmişlerdir. Şöyle ki önceleri yalnızca stratejik bombardıman uçakları ile yöneltilen tehditler, sonraki dönemde kapsamına kıtalararası füzeleri ve denizaltı platformlarını ekleyerek tespit edilmesi ve önlenmesi güç bir hal almıştır.

Caydırıcılığın vasıtalar üzerinden tanımlanmasına yalnızca nükleer düzlemde rastlanılmamaktadır. Konvansiyonel ortamda caydırıcılıkla ilgili olarak

¹⁶⁴ 5. Nesil Mobil Telekomünikasyon Hizmeti: Yüksek frekanslarda çalışan, internet bağlantılı cihazlar arasında ço

¹⁶⁵ Wohlstetter, “The Delicate Balance of Terror”, 8-9.

Mearsheimer, orduların kullandığı silah ve vasıtaların önemine işaret etmektedir. Prusya ve Fransa arasındaki Jena (1806) ve Sedan (1870) muharebelerini karşılaştıran Mearsheimer, iki muharebe arasında Prusya'nın kuyruktan doldurmalı tüfek ve demiryolu teknolojisine erişmesini hızlı bir zaferin habercisi olduğunu nitelemektedir. Bu doğrultuda hızlı bir zaferin öngörülebildiği durumlarda saldırgan politikalar ağır basarak caydırıcılık başarısız olurken; savunma yönünün ağır bastığı ve uzayan bir yıpratma savaşının öngörüldüğü hesaplamalarda caydırıcılık başarılı bir şekilde tesis edilecektir.¹⁶⁶

Konvansiyonel ve nükleer ortamda caydırıcılık stratejisi analizlerine dahil edilen silah/vasıta değişkenlerini siber ortama adapte edebilmek güçtür. Zira siber saldırılar ofansif amaçlar doğrultusunda üretilmiş silahlar aracılığıyla değil, günlük hayatın her alanında kullanılan bilişim altyapısı üzerinden gerçekleşmektedir. Söz konusu altyapının saldırı düzleminde araçsallaştırılmasının etkileri ise halen tecrübe edilmektedir. Kötü amaçlı yazılımlardan, erişim engelleyici Ddos saldırılarına kadar geniş bir yelpazeyi kapsayan saldırıları gerçekleştiren siber sistemlerin nitel ve nicel kabiliyetleri, konvansiyonel ve nükleer silahların ölçülebilir özellikleri ile benzerlik taşımamaktadır.

2.2.2.4. Ne zaman?

„Caydırıcılık stratejisinin doğmuş olduğu nükleer tehdit ortamı, iki süper gücün karşılıklı teyit edilmiş imha durumunu yaratması ile birlikte şekillenmiştir. Bununla birlikte bahse konu olan konjonktürü tetikleyen davranış ABD'nin Hiroşima ve Nagasaki'ye atmış olduğu nükleer bombalardır. İkinci Dünya Savaşının sonunu getiren bu olay, nükleer silahların devasa yıkım kabiliyetlerini bütün dünyanın gözleri önüne sermiştir. Tanık olunan yıkımın tekrar gerçekleşmemesi doğrultusunda Soğuk Savaş boyunca krizler sıcak çatışmaya evrilmeden sonlanmıştır. Buradan hareketle nükleer silahların yıkım kabiliyetleri ile bu silahlara fiilen başvuru miktarının tamamen ters orantılı bir ilişki içinde olduğu ifade edilebilir. Söz konusu ilişki konvansiyonel tehditler için daha ılımlı seviyededir.

¹⁶⁶ Mearsheimer, *Conventional Deterrence*, 15-16.

Tarihsel düzlemde savaş üzerine yapmış oldukları çalışmada Sarkees ve Wayman, 1816-2007 yılları arasında 95 adet savaş meydana geldiğini ifade etmektedir.¹⁶⁷ Bu sayı, incelenen dönemde kabaca ortalama her iki senede bir savaş yaşandığına işaret etmektedir. Konvansiyonel silahların kullanımına yönelik daha kapsamlı bir resim oluşturabilmek için savaşa varmayan devletler arası çatışmaları da ele alan veri tabanını incelemekte fayda vardır. Bu araştırmaya göre 2011-2014 yılları arasında çatışma sıklığı sene bazında ortalama 30.25'tir.¹⁶⁸ Bu rakam, nükleer silahlardan farklı olarak konvansiyonel silahların devletlerarası anlaşmazlıklarda aktif olarak kullanıldığını göstermektedir.

Nükleer tehditlerden konvansiyonel tehditlere doğru belirgin bir artış gösteren saldırıya dönüşme eğilimi, siber tehditlere gelindiğinde çarpıcı sonuçlar göstermektedir. Konvansiyonel saldırılar ile karşılaştırılabilmesi açısından 2014 yılında gerçekleşen siber saldırılar Maryland Üniversitesi Siber Saldırı Veri Tabanı verilerine göre incelendiğinde bir yıl içinde 632 adet saldırı gerçekleştiği görülmektedir.¹⁶⁹ Bilişim altyapısının yayılımı ve 5G teknolojileri göz önünde bulundurulduğunda bu sayıların artan bir şekilde devam edeceğini düşünmek mümkündür. Zira aynı veri tabanının 2018-2023 yılları arasında tespit edebildiği siber saldırı miktarının 10.425 olduğu görülmektedir.¹⁷⁰ Siber saldırıların en önemli özelliğinin gizlilik olduğu ve eylemini gerçekleştirdikten sonra dahi pek çok zaman fark edilememe durumu da göz önünde bulundurulduğunda, saldırılara dair gerçek sayıların çok daha yüksek olduğunu ifade etmek yanlış olmaz.

¹⁶⁷ Sarkees Meredith R. ve Wayman Frank W., *Resort to War: A Data Guide to Inter-State, Extra-State, Intra-state, and Non-State Wars, 1816-2007* (Washington: CQ Press, 2010).

¹⁶⁸ Glenn Palmer vd., "The MID5 Dataset, 2011–2014: Procedures, Coding Rules, and Description", *Conflict Management and Peace Science* 39, sayı: 4 (Temmuz 2022): 477, <https://doi.org/10.1177/0738894221995743>.

¹⁶⁹ "University of Maryland Cyber Attacks Database" (Maryland Üniversitesi), erişim 24 Şubat 2023, <https://cissm.liquifiedapps.com/#charts>.

¹⁷⁰ "University of Maryland Cyber Attacks Database".

TEHDİT ORTAMLARI VE KARAKTERİSTİK ÖZELLİKLERİ			
	Nükleer	Konvansiyonel	Siber
Saldırgan Aktör	Nükleer silah sahibi devletler	Kuvvetçe üstün veya denk devletler	Siber ortama erişimi olan herhangi bir devlet veya devlet-dışı aktör
Hedefler	Yerleşim birimleri Nükleer silahlar	Silahlı Kuvvet Unsurları	Kritik altyapılar, Tedarik zincirleri, Nükleer reaktörler, Bankacılık uygulamaları, Elektronik devlet sistemleri, Resmi Web sayfaları, Devlet arşivleri, Telif hakkı sahipleri vb.
Silah/vasıtalar	Nükleer Başlıklar Ağır Bombardıman Uçakları Kıtalararası Balistik Füzeler Balistik Füze Denizaltıları	Kara, Hava ve Deniz Kuvveti Unsurları	Bilgi ve İletişim Teknolojileri
Kinetik saldırıya dönüşme sıklığı	Tarihte bir defa	30 adet saldırı*/Sene	2000 üzeri saldırı**/Sene
Kısıtlamalar	Normlar, Misilleme tehdidi, Kuvvet Projeksiyonu Kabiliyeti	Normlar, Kuvvet üstünlüğü, Kuvvet Projeksiyonu Kabiliyeti	Herhangi bir kısıtlama bulunmamakta
* Correlates of War Projesi (COW) Veritabanı MID5 verilerine göre 2011-2014 yılları arasında tespit edilen çatışma sıklığıdır.			
**Maryland Üniversitesi Siber Saldırı Veritabanı verilerine göre 2017-2023 yılları arasında tespit edilen siber saldırıların yıl adedine bölünmüş halidir. Araştırmacılar tarafından tespit edilemeyen siber saldırıların da varlığı göz önüne alındığında ortaya konulan sayı artış gösterecektir.			

Tablo 4: Tehdit Ortamları ve Karakteristik Özellikleri

2.2.2.5. Hangi sınırlamalar?

Siber tehditlerin fiili saldırıya dönüşmesi bağlamında ortaya konulan yüksek sayılar, bu tehditlerin nükleer ve konvansiyonel tehdit konjonktürünün maruz kaldığı birtakım sınırlamalara tabi olmamasından kaynaklanmaktadır. Bu sınırlamaların başında normlar gelmektedir. Normlar, ortak kabul görmüş davranış biçimleridir. Sagan, nükleer silahlara sahip olma durumunu normlar bağlamında değerlendirirken şu soruyu sormaktadır: “1960’lı yıllarda nükleer silah testleri prestijli ve yasal iken neden günümüzde yasa dışı ve sorumsuzluk olarak nitelendirilmektedir?”¹⁷¹ Cevap için Nükleer Silahsızlanma Anlaşması’na işaret eden Sagan, bu anlaşma ile prestij kriteri olarak kabul edilen normun nükleer silahlara sahip olmaktan çıkarak anlaşmaya taraf

¹⁷¹ Scott D. Sagan, “Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb”, *International Security* 21, sayı: 3 (1996): 76, <https://doi.org/10.2307/2539273>.

olmak üzerinden yeniden teşkil edildiğini ifade etmektedir.¹⁷² Tüm dünyaca prestij sahipliği olarak algılanan durum birkaç yıl içerisinde “yasa dışı” olarak kabul edilmiştir.¹⁷³

Üst otoritenin ve dolayısıyla yaptırım gücünün bulunmadığı uluslararası sistemde normların işlevselliği konusunda March ve Olsen’in çalışması dikkat çekicidir. “Uygunluk mantığı” kavramını ortaya atan yazarlara göre, devletlerin davranışlarını fayda/maliyet hesaplaması kadar neyin doğru ve toplum tarafından kabul edilebilir olduğu hususları da etkilemektedir.¹⁷⁴ Nükleer silahların yıkıcılığı ve yayılması durumunda karşı karşıya kalınacak tehditler göz önünde bulundurulduğunda NPT¹⁷⁵ anlaşması ile ortaya konulan norm nükleer silah bulunduran devletleri “sorumlu” davranmaya davet etmektedir. Dolayısıyla tehdit etkisi bu derecede büyük silahlar kinetik saldırılara araç olmamaktadır.

Konvansiyonel tehditler için normların rolünden söz etmek mümkündür. Birleşmiş Milletler Antlaşması ile devletlerin Uluslararası İlişkilerde kuvvet kullanması yasaklanmıştır. Meşru Müdafaa istisnası ile bütün devletlerce tanınan bu durum her ne kadar şiddet uygulamasının önüne tamamen geçememiş olsa da “politikanın diğer yollar ile devamı” şeklinde tanımlanan savaş algısını değiştirmiştir. Siber tehdit ortamında ise uluslararası sistemde bu örneklerle benzer bir norm oluşmamıştır. Geleneksel hukuk kuralları çerçevesinde uygulanmaya çalışılan normlar siber ortamın özgün doğası nedeniyle işlevsiz kalmaktadır.¹⁷⁶ Söz konusu özgün doğaya ilişkin birtakım düzenleyici kuralların oluşturulması noktasında hemfikir olan devletlerin BM çatısı altında sürdürdükleri diyaloglarda somut bir kurallar çerçevesi henüz ortaya çıkmamıştır.¹⁷⁷ Bu

¹⁷² Sagan, 76.

¹⁷³ Maria Rost Rublee ve Avner Cohen, “Nuclear Norms in Global Governance: A Progressive Research Agenda”, *Contemporary Security Policy* 39, sayı: 3 (03 Temmuz 2018): 323, <https://doi.org/10.1080/13523260.2018.1451428>.

¹⁷⁴ Michael Moran, Martin Rein, ve Robert E. Goodin, ed., *The Oxford Handbook of Public Policy*, The Oxford Handbooks of Political Science (Oxford ; New York: Oxford University Press, 2006), 690.

¹⁷⁵ The Nuclear Non-Proliferation Treaty: Nükleer Silahların Yayılmasının Önlenmesi Anlaşması

¹⁷⁶ Matthew Crandall ve Collin Allan, “Small States and Big Ideas: Estonia’s Battle for Cybersecurity Norms”, *Contemporary Security Policy* 36, sayı: 2 (04 Mayıs 2015): 351-52, <https://doi.org/10.1080/13523260.2015.1061765>.

¹⁷⁷ Tim Stevens, “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”, *Contemporary Security Policy* 33, sayı: 1 (Nisan 2012): 164-65, <https://doi.org/10.1080/13523260.2012.659597>.

sorunun sebebi olarak meşru müdafaa hakkı, uluslararası çatışma hukuku ve karşı tedbirlerin kullanımı gibi mevcut normların siber ortama angaje edilmesinde ortaya çıkan görüş ayrılıklarıdır.¹⁷⁸ Dolayısıyla nükleer ve konvansiyonel tehditler üzerinde sınırlandırıcı bir etkiye sahip olan normlar, siber tehditler özelinde benzer bir işlevi yerine getirememektedir.

Nükleer silahsızlanma normunun yanında etkili diğer bir sınırlandırıcı husus misilleme tehdididir. Nükleer tehditlerin kinetik saldırıya dönüşmesi noktasında karar alıcıları asıl endişelendiren konu savaşın ilk safhası yerine son safhasıdır.¹⁷⁹ Zira karşılıklı iki nükleer aktörün çatışmasında ilk saldırının gerçekleşmesi, karşı taraftan gelecek bir nükleer misillemeyi kuvvetle muhtemel kılacaktır. Nükleer silahların yıkıcı etkileri göz önünde bulundurulduğunda söz konusu misilleme saldırısının yaratacağı hasar karar alıcılar için nadiren tolere edilebilir düzeydedir. İşte bu çekince bir “dehşet dengesi” yaratarak nükleer tehditlerin kinetik saldırılara dönüşmesine engel olmaktadır. Siber saldırıların yaratmayı hedeflediği hasarların ise nükleer çatışmaya nispetle daha tolere edilebilir olduğunu ifade etmek mümkündür. Dolayısıyla siber uzayda taraflar arası bir şiddet sınırlandırmasından söz etmek mümkün değildir.

Normlar ve misilleme tehdidine ilaveten üçüncü bir sınırlayıcı faktör coğrafi mesafedir. Devletler menfaatleri doğrultusunda başka bir devlet üzerinde askeri güç kullanımı seçeneğine gelişigüzel bir biçimde başvurmamaktadır. Saldırının gerçekleştirileceği bölge askeri gücün etki sahası içinde bulunmalıdır. Kuvvet projeksiyonu olarak ifade edilen bu durum askeri kabiliyetlerin istenilen etkiyi yaratabilme kabiliyetine işaret etmektedir. Söz konusu etkiyi “kuvvet kaybı gradyanı” ile formüle eden Boulding, devletin bulunduğu coğrafi merkezden uzaklaştıkça kuvvet projeksiyonu kabiliyetinin azaldığını savunmaktadır.¹⁸⁰ Bu durum kuşkusuz ulaştırma ve ikmal kısıtlarından kaynaklanmaktadır. Tarihte uzak coğrafyalarda kuvvet projeksiyonu yapabilme yeteneğinin dönemin süper güçlerine özgü bir kabiliyet olduğundan söz edilebilir. Nitekim 19. yüzyılda Birleşik Krallık, günümüzde ise ABD bu kabiliyeti uygulamaya yansıtabilmiştir. Üstün askeri deniz gücü ile mümkün kılınan bu kabiliyetin inşası ve idamesi ancak bu kabiliyeti destekleyecek büyük ekonomik güç doğrultusunda mümkün

¹⁷⁸ Alex Grigsby, “The End of Cyber Norms”, *Survival* 59, sayı: 6 (02 Kasım 2017): 113, <https://doi.org/10.1080/00396338.2017.1399730>.

¹⁷⁹ Waltz, “Nuclear Myths and Political Realities”, 733-34.

¹⁸⁰ Kenneth E. Boulding, *Conflict and Defense: A General Theory* (Lanham, MD: University Press of America, 1988), 245-47.

olabilmektedir. Dolayısıyla orta ve küçük ölçekteki devletler tehdit algılamalarını ve güvenlik etki sahalarını yakın coğrafya ile sınırlandırmak durumunda kalmaktadır.

Siber saldırıların etki sahasına bakıldığında söz konusu coğrafi uzaklık faktörünün belirleyici bir sınırlandırma işlevinin bulunmadığı görülmektedir. Bunun sebebi siber uzayda fiziksel mesafenin anlamlı bir değişken rolü oynamamasıdır. İnsan yapımı sanal bir coğrafya olan siber uzayda herhangi bir fiziksel bölgede bulunan internet servis sağlayıcısı aracılığıyla sisteme erişim sağlayan aktörler birbirlerine zarar verebilmektedir. Whyte ve Mazanec, meydana gelen koşulların etki sahasına ilişkin yansımalarını incelerken “siber kabiliyetlerin herhangi bir devlete doğrudan süper güç düzeyinde bir kuvvet projeksiyonu kabiliyeti bahsettiği” yorumunu yapmaktadır.¹⁸¹

Mevcut siber saldırılara dair saldırgan ve hedef devletler incelendiğinde, küresel kuvvet projeksiyonu yapabilme kabiliyetinin siber uzayda süper güçlerin tekelinden çıktığı; küçük ve orta ölçekteki devletlerin konvansiyonel etki sahaları dışında herhangi bir devlete siber saldırıda bulunabildiği görülmektedir. Ortaya çıkan durumda konvansiyonel anlamda küresel ve bölgesel çatışma alanları ve aktörlerine dair sınırlamanın siber uzayda geçersiz olduğu, bu doğrultuda her aktörün birbirini tehdit edebildiği bir çatışma alanının doğduğu görülmektedir.

Siber uzayın yapısal dönüştürücü etkisine dair söz konusu değerlendirmeler ışığında bu ortamda üretilen tehditlerin nükleer ve konvansiyonel tehditlerden önemli derecede ayrıştığı görülmektedir. Bu haliyle siber uzay, güç dağılımı ve tehdit algılaması gibi yapı-aktör ilişkisinde belirleyici olan etkenlerde önemli değişiklikler yaratmaktadır. Bu doğrultuda geleneksel anlamda dış politika uygulamalarında mutlak ağırlığı olan söz konusu faktörlerin siber uzayda daha muğlak hale geldiği ifade edilebilir. Dolayısıyla siber uzayda karşılaşılan tehditlere karşı uygulanan caydırıcılık stratejisinin analizinde yalnızca yapısal aktör odaklı bir analiz eksik bir çerçeve sunacaktır. Bu tespit yapısal faktörler ile iç değişkenlerin birlikte ele alınması zaruriyetini bir kez daha kanıtlamaktadır.

2.2.3. Açıklık ve Stratejik Çevre

Neorealizme göre benzer aktörlerden oluşan anarşi düzlemi, sistemi oluşturan aktörlere aynı şekilde etki etmektedir. Aktörlerin birbirine yönelik niyetleri ve güç hesaplamalarına ilişkin kesinlik hiçbir zaman net bir şekilde ortada olmadığından dolayı

¹⁸¹ Christopher Whyte ve Brian Mazanec, “Understanding Cyber Warfare”, 90.

belirsizlik sürekli mevcuttur. Neoklasik Realizme göre ise Waltz'un sistemik faktörler ile ilgili tespiti doğru olmakla birlikte yetersizdir. Buna göre belirsizlik kavramı muğlak ve indirgemeci olup açıklayıcılıktan uzaktır. Bahse konu olan sorun, belirsizlik kavramının yapıya dair verili ve değişmez bir sabit olarak ele alınması ve dış politika üretiminde aktöre etkilerinin net bir şekilde ortaya konulmamasından kaynaklanmaktadır. Neoklasik Realistler, belirsizlik kavramını verili olarak kabul etmeyi reddetmektedir. Başka bir deyişle belirsizlik kavramını sisteme ait temel bir özellik olarak ele almaktan ziyade onu yapı-aktör ilişkisinin bir çıktısı olarak değerlendirme yoluna gitmektedir.¹⁸²

Lobell, Taliaferro ve Ripsman'a göre, Waltz'un öne sürdüğü, sistem tarafından belirli yönlendirme ve sınırlamalara tabi tutulan aktör ilişkisi, mekanik bir şekilde ortaya çıkmamaktadır. Nitekim sistem tarafından aktöre sunulan bilgi ve mesajlar açıklık durumuna göre değişkenlik göstermektedir. Bu doğrultuda yazarlar söz konusu bilgi ve mesajların açıklığını üç bileşene bağlamaktadır.¹⁸³

1. Tehdit ve fırsatların ayırt edilebilirliği
2. Tehdit ve fırsatlara ilişkin zaman aralığı
3. Uygun politika seçeneklerinin belirginliği.

Ortaya konulan değişkenler Neorealizmin iki temel iddiası olan rekabet ve taklit etme ile dengeleme stratejilerine dayanan yapı-aktör ilişkisini analiz etmek için kullanışlı bir perspektif sunmaktadır. Şöyle ki Neoklasik Realizme göre aktörler yapı tarafından sunulan sınırlamalara ilişkin öngörülen davranışları ancak tehditlerin belirgin, zamanca yakın ve tehdiye yönelik uygun politika seçeneklerinin mevcut olduğu durumlarda sergilemektedirler. Neoklasik Realizm bu doğrultuda sistemin belirsizlik düzeyini yüksek ve düşük açıklık seviyesi olarak bir değişken olarak ele almaktadır. Yüksek açıklık seviyesinde aktörlerin dış politikası yapısal faktörler ışığında şekillenirken, belirsizlik ortamının yüksek olduğu düşük açıklık ortamında lider, stratejik kültür, kurumlar gibi aktör merkezli değişkenler dış politika seçeneklerinde belirleyici olabilmektedir.¹⁸⁴

¹⁸² Ripsman, Taliaferro, ve Lobell, *Neoclassical Realist Theory of International Politics*, 51.

¹⁸³ Ripsman, Taliaferro, ve Lobell, 46.

¹⁸⁴ Ripsman, Taliaferro, ve Lobell, 49-50.

Neoklasik Realizmin ortaya koyduğu diğer bir yapısal faktör stratejik çevredir. Buna göre tehditlerin önem ve ivedilik derecesi doğrultusunda stratejik çevre kısıtlayıcı veya serbest bırakıcı olarak sınıflandırılmakta ve mevcut politika seçenekleri yelpazesi bu iki sınıf arasında değişkenlik göstermektedir.¹⁸⁵ Kısıtlayıcı çevrede güç rekabeti koşulları, aktörü yapı tarafından ortaya konulan statik rekabet ve taklit etme davranışlarına zorlarken, serbest bırakıcı çevre takip edilecek güvenlik politikalarında karar vericilere hareket alanı sağlamaktadır. Siber uzayda halen güç dengelerinin oluşmamış olması, taklit edilebilir örneklerin bulunmaması ve anarşi ortamında sınırlandırıcı mekanizmaların gelişmemiş olması dolayısıyla yapısal dönüştürücü fonksiyonunun açıklık ve stratejik çevre kavramlarına da etki ettiği ifade edilebilir. Bu kapsamda siber uzay tehdit ve kabiliyetlerin açık olmadığı, stratejik çevrenin ise farklı uygulama örneklerine alan açan serbest bırakıcı mahiyette olduğu bir ortamdır. Söz konusu durum yapısal faktörlerin belirleyiciliğinin iç değişkenler lehine azaldığı bir analiz ortamı sunmaktadır.

2.3. İç Değişkenler

“Dengeleyici bir ağırlık unsuru bulunmadığında devletin iç dürtüleri galip gelir.”¹⁸⁶ NATO’nun Soğuk Savaş sonrası varlığını koruması sonrası Realizme yöneltilecek eleştirilere ilişkin Waltz’un başvurduğu bu tespit iç değişkenlerin rolüne temel teşkil etmektedir. Böylece Waltz’un devletleri sadece benzer siyah kutu olarak değil, farklı renk ve malzemelerden yapılmış kutular olarak görmeye yaklaştığı ifade edilebilir. Adı geçen farklı malzemeleri ortaya koymak ve dış politikaya etkilerini incelemek Neoklasik Realizmin en önemli katkılarından biri olarak değerlendirilmektedir.

Waltz’un sistemik faktörlerin devlet dış politika davranışlarında “belirleyici” değil “sınırlayıcı” olduğu tezini sorunsallaştıran Neoklasik Realizm, sistem-dış politika çıktısı arasındaki süreci “transmisyon kayışı” (*transmission belt*) analojisi üzerinden kurmaktadır.¹⁸⁷ Motorda üretilen gücü mekanik ekipmana aktaran ve bu sayede hareketi

¹⁸⁵ Ripsman, Taliaferro, ve Lobell, 52-56.

¹⁸⁶ Kenneth N Waltz, “Structural Realism after the Cold War”, *International Security* 25, sayı: 1 (2000): 24.

¹⁸⁷ Gustav Meibauer, “Neorealism, Neoclassical Realism and the Problem(s) of History”, *International Relations*, 5; Gustav Meibauer, “Interests, Ideas, and the Study of State Behaviour in Neoclassical Realism”, *Review of International Studies* 46, sayı: 1 (Ocak 2020): 22,

mümkün kılan transmisyon kayışı analogisi, esas itici faktörleri yaratan sistemin nasıl bir süreçten geçerek dış politika davranışına dönüştüğüne ilişkin mekanizmaya karşılık gelmektedir. Bu mekanizmanın işleyişinde aktör, yapısal faktörleri yorumlamakta ve dış politika kararını bazı iç değişkenler süzgecinden geçerek vermektedir. Oluşan resimde tarif edilen mekanizma, yapısal faktörler ve iç değişkenler arasında dıştan-içe ve içten-dışa yönelen etkilerin buluşarak harmanlandığı bir orta seviyeyi işaret etmektedir. Söz konusu resme ilişkin akla gelen ilk örneklerden biri Putnam'ın iki düzeyli oyun teorisisidir. Putnam'a göre dış politika kararları alan devlet liderleri iki farklı oyun tahtasında hamleler yapmaktadır. Oyun tahtalarının birini diğer devlet başkanları ile paylaşan lider, bir taraftan devlet menfaatleri doğrultusunda dış politikada optimal anlaşmaları imzalamaya çalışırken diğer tahtada bu anlaşmaları iç menfaat gruplarına onaylatma gereksinimi duymaktadır.¹⁸⁸ Farklı türde hassasiyetlerin ön plana çıktığı iki düzlemin kesişiminde yer alan lider, dıştan-içe yönelen sistemik faktörler ile içten-dışa yönelen iç değişkenlerin önceliklerine en iyi şekilde hizmet edecek kararı vermeye çalışmaktadır.

Transmisyon kayışı analogisi her ne kadar farklı analiz seviyelerindeki hassasiyetlerin bir arada göz önüne alınması bakımından Putnam'ın modeli ile benzerlik gösterse de ikisinin arasında önemli farklılıklar mevcuttur. Öncelikle, Putnam'ın iki düzeyli oyununda karar alıcı olarak lider alınırken mevcut farklılaşan hassasiyetler doğrultusunda dış politika kararlarının nasıl alındığına dair yol gösterici teorik bir çerçeve sunulmamaktadır.¹⁸⁹ Nitekim Putnam, her iki tür hassasiyetin birbirine karşı sınırlayıcı veya teşvik edici rol oynadığı ve liderlerin bu etkilerin ışığında bağlamsal kararlar aldığı bir süreci tarif etmektedir. Diğer bir farklılık da düzeyler arası hiyerarşi sorunsalıdır. Putnam'ın ortaya koyduğu oyun modelinde karar alıcı için hangi düzeyin daha önemli olduğu belirtilmemektedir.¹⁹⁰ Bu ise öncelikle hangi düzeye ilişkin hassasiyetlerin yorumlanması gerektiği, düzeylerin birbiri üzerinde oynadığı değiştirici veya engelleyici rollere ilişkin soruların yanıtsız kalmasına yol açmaktadır.

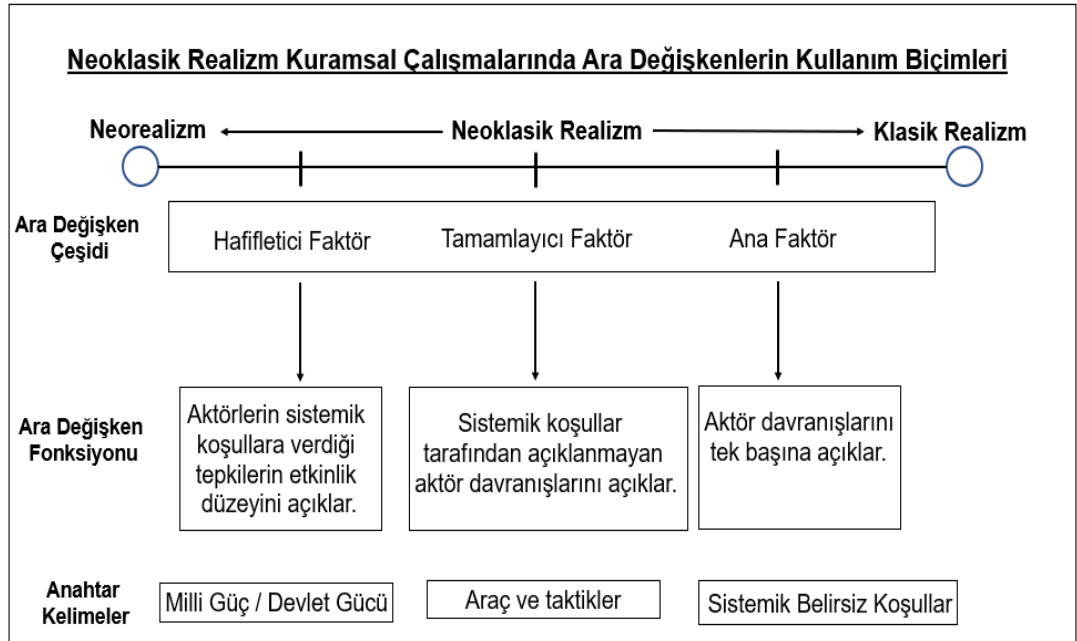
<https://doi.org/10.1017/S0260210519000214>; Ripsman, Taliaferro, ve Lobell, *Neoclassical Realist Theory of International Politics*, 117.

¹⁸⁸ Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games", *International Organization* 42, sayı: 3 (1988): 427-60, <https://doi.org/10.1017/S0020818300027697>.

¹⁸⁹ Michiel Foulon, "Neoclassical Realism: Challengers and Bridging Identities", *International Studies Review*, Eylül 2015, 641, <https://doi.org/10.1111/misr.12255>.

¹⁹⁰ A.g.e.

Düzeyler arasındaki hiyerarşinin, Neoklasik Realizmde iç değişkenlerin rolüne ilişkin tespitlerde bulunurken üzerinde önemle durulması gereken konulardan biri olduğu ifade edilebilir. Zira iç değişkenlerin transmisyon sürecine nasıl ve hangi aşamada dahil olacağı sorunu üzerinde oldukça tartışılan bir konudur. Legro ve Moravcsik, dış politika davranışını açıklamada iç değişkenleri dahil etmenin teorik olarak rasyonel olmadığını, iç değişkenler üzerinden yapılan bir okumanın teoriyi Realizm çerçevesinden çıkararak Liberalizme yaklaştırdığını öne sürmektedir.¹⁹¹ Rathbun ise söz konusu eleştiriye ilişkin olarak iç değişkenlere, Neorealizmin öngördüğü sınırlandırılmış davranış kalıplarını göstermedeki başarısızlıkları açıklama rolünün verilmesi gerektiğini savunmaktadır.¹⁹² Bahse konu olan eleştiriler karşısında iç değişkenlerin teorideki konumlanmasına dair Elias Götz'ün çalışması dikkat çekicidir. Neoklasik Realizm çerçevesini benimseyen çalışmaları analiz eden araştırmacı, iç değişkenlerin farklı kullanımlarına dikkati çekerek bunları sınıflandırma yoluna gitmiştir.



Tablo 5: Neoklasik Realizm Kuramsal Çalışmalarında Ara Değişkenlerin Kullanım Biçimleri¹⁹³

¹⁹¹ Jeffrey W. Legro ve Andrew Moravcsik, "Is Anybody Still a Realist?", *International Security* 24, sayı: 2 (Ekim 1999): 5-55, <https://doi.org/10.1162/016228899560130>.

¹⁹² Rathbun, "A Rose by Any Other Name", 312.

¹⁹³ Elias Götz, "Neoclassical Realist Theories, Intervening Variables, and Paradigmatic Boundaries", *Foreign Policy Analysis* 17, sayı: 2 (16 Şubat 2021): 9, <https://doi.org/10.1093/fpa/oraa026>.

Neoklasik Realizme bir araştırma çerçevesi olarak başvuran araştırmacılar, iç değişkenlere farklı rol ve fonksiyonlar yüklemektedirler. Götz'e göre söz konusu farklı kullanım biçimleri, çalışmaları Klasik Realizm ile Neorealizm arasında farklı noktalarda konumlandırmaktadır.¹⁹⁴ Buna göre Neoklasik Realizmin Neorealizmin doğal bir uzantısı olarak kullanılması gerektiğini savunan Rathbun'un görüşünü en iyi yansıtan kullanım biçimi "hafifletici faktörlerdir".

Ara değişkenlere birer hafifletici faktör fonksiyonu yükleyen çalışmalarda söz konusu değişkenler bağımsız değişkenin bağımlı değişken üzerindeki etki derecesini açıklamaktadır.¹⁹⁵ Diğer bir deyişle bu değişkenler, devletlerin sistemik koşullar tarafından çerçevesi belirlenen davranış kalıplarına hangi derecede uygun hareket ettiğini ortaya koyma amacı gütmektedir. Bu doğrultuda, ilgili çalışmalarda öne çıkan kavramlardan biri milli güç-devlet gücü ayrımıdır. Zakaria, devlet gücünü ülkedeki her türlü ekonomik, askeri, demografik materyal kabiliyetlerin toplamından ziyade bunları belli bir siyasi amaca kanalize edebilme becerisi olarak tanımlamaktadır. Devlet gücü kavramı, Zakaria tarafından 19. Yüzyıl ABD'sinin yapısal faktörlerin teşviklerine rağmen kendi kıtasında yayılmadaki gecikmesini açıklamak için kullanılmıştır.¹⁹⁶ Bu çalışmada devlet-toplum ilişkisi, incelenen gecikmeyi doğuran bir ara değişken olarak gösterilmiştir. Örnekte de görüldüğü üzere, iç değişkenleri bir hafifletici faktör olarak kullanan çalışmalarda yapısal faktör-iç değişken arasında kesin bir hiyerarşi söz konusudur. İç değişkenlerin farklılaşan dış politika uygulamaları yerine, yapısal faktörlerin öngördüğü davranış kalıplarına uyma başarısızlıklarını açıklamak için kullanıldığı görülmektedir.

Götz'ün çalışmasında, "tamamlayıcı faktörler" olarak tanımlanan iç değişkenler Neoklasik Realizmin ayrı bir kuram olarak ele alınmasını daha mümkün kılmaktadır. Buna göre yapısal faktörler ve iç değişkenler hiyerarşik bir ilişki içinde birlikte hareket ederek bağımlı değişkenin kapsamı ve yapısını belirlemektedir. Daha açık bir ifadeyle, yapısal faktörler devletlerin izleyeceği ana stratejileri belirlerken bu stratejilerin uygulanmasında hangi taktik ve araçlara başvurulacağı iç değişkenler aracılığıyla

¹⁹⁴ A.g.e..

¹⁹⁵ A.g.e., 3-5

¹⁹⁶ Fareed Zakaria, *From Wealth to Power* (New Jersey: Princeton University Press, 1998); Götz, "Neoclassical Realist Theories, Intervening Variables, and Paradigmatic Boundaries", 3.

belirlenmektedir.¹⁹⁷ Dolayısıyla iç değişkenlere verilen misyon, taktiksel ve araçsal farklılıkları açıklamaktır.

Bahsedilen mantığa örnek olarak Vipin Narang'ın *Nuclear Strategy in the Modern Era* adlı çalışması verilebilir. Narang'a göre, bölgesel aktörler nükleer silah edinme kararını stratejik çevresindeki tehdit algılamaları doğrultusunda vermekte, ancak bu kabiliyetlerin taktiksel düzenlemesini sivil-asker ilişkileri ve kaynak ayırma sınırlılıkları çerçevesinde yapmaktadır.¹⁹⁸ Bu doğrultuda Narang, nükleer güç olma yoluna giren devletlerin benimsedikleri nükleer konumlanma şekillerini katalitik, temin edilmiş misilleme ve asimetrik tırmandırma olarak sınıflandırmaktadır.¹⁹⁹ Böylece yazar, stratejide benzer, taktikte ise farklı yaklaşımları iç değişkenler üzerinden açıklamaktadır.²⁰⁰

İç değişkenlerin üçüncü bir uygulama biçimi “ana faktör” olarak ifade edilmektedir. Bu anlayışa göre yapısal faktörler ve iç değişkenlerin dış politika uygulamalarını açıklamada sahip olduğu ağırlık, aktörün stratejik çevresi tarafından belirlenmektedir.²⁰¹ Yapısal koşulların aktöre belirsiz tehdit ve fırsatlar sunduğu ortamlar serbest bırakıcı çevre olarak tanımlanmakta ve ara değişkenlerin dış politikadaki ağırlığını artırmaktadır. Bu doğrultuda, stratejik çevrenin serbest bırakıcı özellikler barındırdığı durumlarda yapısal faktörler iç değişkenlere alan açan koşulları belirlemede kullanılmakta ve bu değişkenleri bir ana faktör olarak konumlandırmaktadır.

Siber tehditlere yönelik caydırıcılık stratejilerinin analiz edildiği bu çalışmada iç değişken okuması için uygun fonksiyon tanımlaması “tamamlayıcı faktördür”. Zira siber uzayın yapısal dönüştürücü vasfı istisnasız olarak sistemin tüm aktörlerini serbest bırakıcı stratejik çevrenin içinde bırakmaktadır. Ortaya çıkan belirsizlik ortamı, optimal davranış biçimlerinin tespitini zorlaştırmakta; sistem tarafından “başarılı” bulunan ve “kabul gören” davranış biçimlerinin henüz ortaya çıkmaması, Neorealizmin öngördüğü benzeşen uygulamaları sekteye uğratmaktadır. Bu durum, mevcut tehditler karşısında

¹⁹⁷ Götz, “Neoclassical Realist Theories, Intervening Variables, and Paradigmatic Boundaries”, 5.

¹⁹⁸ Narang, *Nuclear Strategy in the Modern Era*.

¹⁹⁹ A.g.e..

²⁰⁰ A.g.e..

²⁰¹ Ripsman, Taliaferro, ve Lobell, *Neoclassical Realist Theory of International Politics*.

optimal davranış arayışına giren devletler nezdinde iç değişkenlerin belirleyiciliğini artırmaktadır. Bununla birlikte uygulanacak caydırıcılık stratejisinin analizinde yalnızca iç değişkenler üzerinden okuma yapmak doğru değildir. Zira her ne kadar güç dağılımı ve tehdit algılaması gibi yapısal faktörlerin ağırlığı siber uzayda azalmış olsa da bu etkenler halen devletlerin genel güvenlik politikalarına yön vermektedir. Dolayısıyla bu çalışmada yapısal faktörler caydırıcılık stratejisine başvurulmasında genel yaklaşımı belirleyen, iç değişkenler ise kullanılacak caydırıcılık metodunu ortaya koyan etkenler olarak analizde yer bulmuştur.

Çalışmada iç değişken olarak iki kavram incelenmiştir: stratejik kültür ve kurum. Özellikle stratejik kültür, bir devletin uluslararası sisteme ve güvenlik meselelerine yönelik tarihsel olarak inşa edilmiş algı ve reflekslerini ifade eder. Stratejik kültür, devletin dış tehditlere vereceği tepkileri kalıcı biçimde biçimlendirerek rasyonel hesaplarının ötesinde davranış kalıpları üretmesine neden olabilir.²⁰² Stratejik kültürün dış politika analizinde bir değişken olarak kullanımına ilişkin Colin Dueck ve Jack Snyder'in çalışmaları dikkat çekicidir. Dueck, ABD'nin İkinci Dünya Savaşı sonrası farklılaşan müdahaleci ve izolasyoncu politikalarını; Snyder ise Sovyetler Birliği'nin Soğuk Savaş sırasında öngörülerin aksine nükleer silahları bir esnek karşılık mekanizması olarak kullanmama tercihini stratejik kültür farklılıkları üzerinden açıklamaktadır.²⁰³

Rose'a göre "ara değişken" işlevi gören kurumlar liderin tehdit algılamasını ve dış politika kararlarını etkileme kapasitesine sahip bürokratik unsurlardır.²⁰⁴ Bürokratik yapıların etkinliği, karar alıcıların yetki alanları ve iç siyasal rekabetin düzeyi gibi unsurlar, uluslararası sistemden gelen baskıların devlete nasıl yansıdığını belirleyen

²⁰² Alastair Johnston, "Thinking about Strategic Culture", *International Security*, Sayı:19 (4): (1995)

²⁰³ Colin Dueck, *Reluctant Crusaders: Power, Culture and Change in American Grand Strategy* (Princeton: Princeton University Press, 2006).

Jack L. Snyder, "The Soviet Strategic Culture: Implications for Limited Nuclear Operations", *Rand Corporation Reports*, (1977)

²⁰⁴ Gideon Rose, "Review: Neoclassical Realism and Theories of Foreign Policy" *World Politics*, Sayı:51 (1) (1998)

kritik faktörlerdir.²⁰⁵ Meclis, Dışişleri ve Savunma Bakanlığı gibi kurumlar arasındaki görüş ayrılıklarının etkilerine yer veren Randall Schweller, devletlerin sadece sistemin "zorlamalarına" tepki vermediğini, aynı zamanda içsel çıkarımlar ve siyasal dinamikler doğrultusunda farklı stratejiler geliştirebileceğini öne sürmüştür.²⁰⁶ Jeffrey Taliaferro, kurumların yönetici ve toplum arasında bir pazarlık sonucu meydana geldiğine ve bu süreç doğrultusunda dış politikada kurum etkisinin her devlette farklılık gösterebildiğine işaret etmektedir.²⁰⁷ Yönetimde yetkisel sınırların somut anlamda çizildiği ABD örneğinde Dueck, Kongre'nin başkanların karar alma çerçevesini genel anlamda sınırlandırdığını ifade etmekle birlikte başkanın bu alan içinde önemli bir hareket alanına sahip olduğunu belirtmektedir.²⁰⁸

Stratejik kültür ve kurum değişkenlerini dış politika analizine ekleyen bu yaklaşımlar, klasik realizmin aktör-merkezli analizlerini ve yapısal realizmin sistem-merkezli analizlerini sentezleyerek, daha esnek ve bağlama duyarlı bir dış politika teorisi sunmaktadır.

Çalışmanın bu bölümünde kuramsal çerçeve olan Neoklasik Realizm ele alınmıştır. Caydırıcılık stratejisi gibi Neorealizm kuramsal yaklaşımının egemen olduğu bir süreçte doğup gelişen bir çalışma alanının Neoklasik Realizm gözlüğü ile ele alınması çalışmanın işaret etmiş alan yazın eksikliğinin (iç değişkenlerin göz ardı edilmesi) giderilmesi için büyük önem arz etmektedir. Bu doğrultuda kuramın öncelikle Neorealizm ile benzeşen taraflarına yer verilmiştir. Müteakiben Neoklasik Realizmin Uluslararası İlişkiler Disiplinine getirmiş olduğu yenilik olan iç değişken kullanımı anlatılmıştır. Çalışmada Neoklasik Realizmin, Neorealizm ile benzeşen ve farklılaşan yönlerinin sırasıyla aktarılması yoluyla açıklanması şu açıdan önemlidir: Caydırıcılık stratejisi halen yapısal faktörlerden önemli ölçüde etkilenmektedir. Ancak iç

²⁰⁵ Brian Rathbun, "A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism", *Security Studies*, Sayı:17 (2) (2008)

²⁰⁶ Randall L. Schweller, "Unanswered Threats: A Neoclassical Realist Theory of Underbalancing", *International Security*, 29 (2) (2004)

²⁰⁷ Jeffrey W. Taliaferro, "State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State", *Security Studies*, Sayı:15 (3) (2006)

²⁰⁸ Norrin M. Ripsman vd., *Neoclassical Realism, Theory and the State* (Cambridge: Cambridge University Press, 2009:147).

değişkenleri ele almadan yapılan bir analiz dış politika kararları hakkında eksik bir çerçeve sunmaktadır. Dolayısıyla bu kararları doğru analiz edebilmek için mutlaka yapısal faktörler ve iç değişkenler birlikte ele alınmalıdır.

Bölümde kuramın dış politika analizi biçimi ortaya konulduktan sonra yapısal faktörlere yaklaşımı incelenmiştir. Zira kurama göre yapıdan her devlet eşit şekilde etkilennemektedir. Söz konusu etkileşim açıklık, stratejik çevre ve yapısal dönüştürücü kavramlarının süzgecinden geçerek meydana gelmektedir. Bu noktada çalışmanın vaka konusu olan siber tehditlerin bir yapısal dönüştürücü olduğundan bahsedilmiştir. Bu tehditlerin beraberinde getirmiş olduğu saldırgan aktör, hedef, silah ve sınırlama belirsizlikleri anarşinin alışagelmış işleyişinin dışında güvenlik ilişkileri meydana getirmektedir. Bahse konu olan belirsizlik örnek davranış kalıplarının oluşturulmasını zorlaştırmakta ve takip edilecek caydırıcılık stratejisi için iç değişkenlerin etkisine alan açmaktadır. Bu doğrultuda iç değişkenlerin kullanım biçimine yer verilmiştir. Alan yazında iç değişkenlerin dış politika analizinde kullanım biçimine dair farklılıklar bulunmaktadır. Bu değişkenlerin hafifletici faktör, tamamlayıcı faktör veya ana faktör olarak kullanımları mevcuttur. Bu çalışmada analizde yer verilen stratejik kültür ve kurum değişkenleri birer tamamlayıcı faktör olarak ele alınmıştır. Zira caydırıcılık stratejisinin öncelikle yapısal faktörlerden etkilendiği ve daha sonra bu değişkenler tarafından belirlendiği öngörülmektedir. Çalışmanın kavramsal ve kuramsal çerçevesinin oturtulması ile birlikte sıra vaka analizi yoluyla kuramın test edilmesine gelmiştir. Dolayısıyla vaka analizi bölümüne geçmeden önce bir sonraki bölümde analizin yapılış mantığını aktaran yöntem bölümüne yer verilmiştir.

VAKA ANALİZİ: ABD SİBER CAYDIRICILIK POLİTİKALARINDA YAPISAL VE İÇ DEĞİŞKEN ETKİLERİNİN İNCELENMESİ

2009-2021 yılları arasındaki ABD siber güvenlik politikalarının vaka olarak ele alındığı bu bölümde Obama ve Trump dönemleri karşılaştırılmıştır. Çalışmanın ana sorusu olan caydırıcılık stratejisindeki iç bileşen etkisini ortaya koymak için bölüm her bir araştırma sorusunun ayrı olarak ele alındığı üç alt başlık şeklinde oluşturulmuştur. Bu doğrultuda ilk başlıkta söz konusu döneme etki eden yapısal faktörlerin ağırlığı sorgulanmış müteakiben ikinci başlıkta ise iki başkan döneminde caydırıcılık stratejilerinin kullanılan metot bakımından farklılaşıp farklılaşmadığı incelenmiştir. Son başlıkta ise elde edilen farklılaşma bulgusunun iç değişkenlerden kaynaklanma durumu sorgulanmıştır. Bu kapsamda kurama uygun olarak sırasıyla stratejik kültür ve kongre değişkenleri caydırıcılık stratejisi üzerindeki etkileri bakımından analize tabi tutulmuştur.

3.1. Yapısal Faktörlerin Etkileri: ABD'nin Küresel Güç Dağılımındaki Yeri ve Tehdit Algılaması

Bu bölümde, çalışmanın ilk araştırma sorusu olan yapısal faktörlerin caydırıcılık stratejisine etkisi araştırılmıştır. Yapısal faktör olarak ele alınan bileşenler küresel düzlemdeki güç dağılımları ve tehdit algılamalarıdır. Kurama göre devletlerin dış politika tercihleri öncelikle devletin içinde bulunduğu sistemin koşulları doğrultusunda şekillenmektedir. Dolayısıyla söz konusu iki bileşenin ABD'ye etkilerini ortaya koymak bu devletin caydırıcılık stratejisine dair genel yaklaşımını anlamak için önemli bir perspektif sunmaktadır.

ABD'nin Soğuk Savaş sonrasında elde ettiği tek kutuplu güç dengesi üstünlüğünü 2000'li yıllardan itibaren kaybettiği görülmektedir. Singer, Bremer ve Stuckey'nin Ulusal Kabiliyet Bileşik Endeksi söz konusu göreceli düşüşü somut bir şekilde ortaya koymaktadır. Devletlerin güç dağılımındaki yerlerini askeri harcama, nüfus, asker sayısı gibi veriler üzerinden inceleyen bu çalışmada devletlere toplam güçleri nispetinde bir

puan verilmektedir. Ulusal Kabiliyet Bileşik Endeks Puanı olarak adlandırılan bu puana göre 2000 yılında Çin'in ABD'ye kıyasla 1.13 kat üstünlüğü bulunurken 2010 yılında bu oranın 1.42'ye, 2016 yılında ise 1.73'e yükseldiği görülmektedir.²⁰⁹ Veri tablosu ABD-Rusya açısından incelendiğinde ise önemli bir değişim bulunmadığı görülmektedir. Böylece güç dağılımı bakımından ABD'nin Soğuk Savaş sonrası kuvvet üstünlüğünü kaybettiğini ve Çin'in küresel güç dengesinde önemli bir rakip olarak belirlediğini ifade etmek mümkündür.

Devlet	Sene	Askeri Harcama (Dolar)	Askeri Personel Sayısı (x1000)	Demir-Çelik Üretimi (x1000 Ton)	Birincil Enerji Tüketimi (x1000 ton kömür)	Toplam Nüfus (x1000)	Şehir Nüfusu (x1000)	Ulusal Kabiliyet Bileşik Endeks Puanı *
ABD	2000	303136000	1366	101803	3283713	278357	75342	.14268766
	2002	348555000	1414	91587	3227356	290270	157321	.15347439
	2004	455980000	1450	99681	3267987	295487	162073	.1514481
	2006	521840000	1546	98557	3245355	300943	166465	.15419258
	2008	616073000	1498	91350	3258397	306657	172381	.14751531
	2010	693600000	1580	80495	3211750	312247	177349	.14757971
	2012	655388000	1569	88695	3169126	317505	183712	.13892639
	2014	581000000	1492	88174	3315793	317719	190421	.12940805
	2016	604452000	1381	78475	3293117	322180	197817	.13305758
RUSYA	2000	52000000	1004	59136	1056740	146934	66484	.051474065
	2002	50800000	988	59777	1083957	145521	50475	.049559519
	2004	61500000	999	65583	1131021	144331	50920	.047631226
	2006	24577000	1027	70830	1196170	143715	51410	.041070685
	2008	40484000	1027	68510	1240975	143677	52216	.040875051
	2010	41944000	1027	66942	1259488	143618	53043	.039090596
	2012	58765000	956	70209	1327053	143170	53585	.039631136
	2014	70048000	845	71461	1335859	143761	55623	.039191708
	2016	46626000	798	70453	1322198	143965	56926	.036472768
ÇİN	2000	42000000	2810	127236	1872095	1277558	588453	.16233304
	2002	68963000	2270	182249	2127269	1295322	294634	.15354699
	2004	84303000	2253	272798	2861534	1310414	319782	.1680482
	2006	35223000	2255	421024	3570019	1326146	347428	.17945626
	2008	60187000	2105	512339	4048898	1342733	376397	.19062871
	2010	76361000	2285	638743	4889792	1359821	407821	.20924728
	2012	102643000	2285	731040	5724311	1377065	440254	.2203252
	2014	129408000	2333	822698	5858015	1390110	493364	.22868057
	2016	145039000	2333	807609	5679028	1403500	526464	.23061772

* **Ulusal Kabiliyet Bileşik Endeks Puanı (UKBEP):** Ölçüme tabi tutulan 6 parametrenin (askeri harcama, askeri personel sayısı, demir-çelik üretimi, birincil enerji tüketimi, toplam nüfus ve şehir nüfusu) her birinde devletin ürettiği kabiliyetin yıllık olarak küresel çapta üretilen toplam kabiliyete denk gelen oranlarının eşit ağırlıkla ele alınarak toplanması sonucu elde edilen orandır.

UKBEP: Devletin ürettiği yıllık bileşik kapasite/O yıl küresel çapta üretilen toplam kapasite

Tablo 2: ABD'nin ve Rusya Ulusal Kabiliyet Bileşik Endeks Puanları 210

Tehdit algılaması açısından bakıldığında da Çin ve Rusya'nın ABD güvenlik politikalarına yön verici etkilerinin arttığı ifade edilebilir. Bu durumu ABD Ulusal Güvenlik Strateji Belgelerinde takip etmek mümkündür. 2002 Strateji belgesinde Çin ekonomik ve diplomatik ilişkilerde potansiyel bir ortak olarak tanımlanırken, 2006 belgesinde Çin'in askeri yapılanması ve otoriter uygulamalarından duyulan endişelere yer verilmiştir. 2010 ve 2015 belgelerinde Çin, Güney Çin Denizi bölgesindeki mevcut

²⁰⁹ David J. Singer, Stuart Bremer, ve John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1964 (6. versiyon)", içinde *Peace, War, and Numbers* (Beverly Hills: SAGE Publications, 2021), 19-48, <https://correlatesofwar.org/data-sets/national-material-capabilities/>.

²¹⁰ Singer, Bremer, ve Stuckey.

istikrarı bozabilecek bir bölgesel aktör olarak değerlendirilirken, 2017 belgesinde ise ilk kez ABD çıkarlarını tehdit eden “revizyonist” bir aktör olarak tanımlanmıştır. ABD Güvenlik Belgelerindeki değişen tavır Rusya için de benzer bir seyir sergilemektedir. 2002 belgesinde Rusya, terörizm gibi küresel tehditlere karşı potansiyel bir ortak olarak ele alınırken, 2006 belgesinde demokratik değerler aleyhindeki uygulamaları eleştirilmektedir. Kırım’ın işgali ile 2015 belgesinde küresel istikrarı bozucu bir tehdit olarak ifade edilirken, 2017 belgesinde tıpkı Çin gibi revizyonist bir aktör olarak tanımlanmıştır.

Güç dağılımındaki değişim ve konvansiyonel tehdit algılamasındaki farklılaşma siber güç düzleminde paralellikler barındırmaktadır. Siber saldırıları kaynak ve hedef devlet ile saldırı tipolojisine göre sınıflandırarak bir veri havuzu ortaya koyan Maness ve Valeriano’ya göre ABD’nin 2009-2020 yılları arasında uğramış olduğu 125 siber saldırının 49’u Çin, 37’si Rusya tarafından gerçekleştirilmiştir.²¹¹ Aynı tarih aralığında yapılan Avrupa Siber Olay Deposu verilerine göre, ABD’ye yapılan 288 saldırıdan 62’si Çin, 37’si Rusya tarafından gerçekleştirilmiştir.²¹² Her iki çalışma da ABD’nin en fazla siber saldırıya maruz kaldığı devlet olarak Çin ve Rusya’ya işaret etmektedir. Eldeki veri ışığında bir değerlendirme yapıldığında, ABD’nin küresel güç dağılımında nispeten gerilediği, Çin’in dengeleyici bir rakip olarak ön plana çıktığı, Rusya ve Çin’in bölgesel statüko bozucu eylemlerinin arttığı görülmektedir. Dahası, ortaya konulan rekabet ortamı siber uzayda karşılık bulmakta ve ABD bu iki devlet tarafından sıklıkla saldırılara maruz kalmaktadır. Dolayısıyla siber güç kapsamında tespit edilecek ABD ulusal menfaatlerinin ve caydırıcılık stratejisinin söz konusu rekabet ortamına uygun biçimde şekillenmesi anarşi ortamında beklenen bir davranıştır.

3.2.Farklılaşan Caydırıcılık Stratejileri: Obama ve Trump Dönemleri Siber Güvenlik Politikalarının Karşılaştırılması

Bir önceki başlıkta yapısal değişken olan güç dağılımı ve tehdit algılaması faktörlerinin ABD’yi siber tehditler kapsamında caydırıcı tedbirler almaya sevk ettiği ortaya

²¹¹ Ryan C. Maness vd., “The Dyadic Cyber Incident and Campaign Dataset”, Temmuz 2022, <https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV> .

²¹² European Repository of Cyber Incidents (Eurepoc), “Global Dataset of Cyber Incidents”, 2024, <https://doi.org/10.5281/zenodo.11108195> .

konulmuştur. Bu bölümde ise ABD'nin söz konusu doğrultuda caydırıcılık stratejisini benimseme biçimi incelenmiştir. Vaka analizinde amaç bağımlı değişken olan caydırıcılık stratejisi benzerlik ve farklılıklarını ortaya koymak, sonrasında ise söz konusu veriler ile yapısal ve iç değişkenler arasında nedensel bağları ortaya koymaktır. Bu doğrultuda Barack Obama ve Donald Trump başkanlıklarını kapsayan 2009-2021 yılları arasındaki dönem esas alınarak siber politikalar öncelikle kronolojik sıraya göre ortaya konulmuştur. Araştırma hipotezinin bağımlı değişkeni olan caydırıcılık stratejileri verili değildir. Dolayısıyla bu stratejileri ortaya çıkarmak ve söz konusu stratejilere dair dönemselsel farklılıklar üzerinden nedensel bağlantılar çıkarmak bir süreç takibini gerektirmektedir. Bu nedenle, bahsedilen döneme dair ele alınan veriler, strateji belgeleri, başkanlık icra emirleri, siyaset direktifleri, kurumlar ve caydırıcı tedbirleri kapsayacak şekilde oluşturulmuştur. Zira strateji belgeleri uygulanan stratejilerin algılama ve karar alma boyutlarına işaret ederken, kurumlar ve tedbirler söz konusu politikaların uygulamaya dökülme biçimine dair somut fikirler sunmaktadır. Bu şekilde araştırmanın bağımlı değişkeni olan caydırıcılık stratejisi ve bu değişkenin aldığı farklı nominal değerler olan caydırıcılık metotları elde edilmiştir.

3.2.1. Barack Obama Dönemi (2009-2016)

Bu başlık altında Obama'nın iki dönemi kapsayan başkanlık sürecinde siber güvenlik ile ilgili Ulusal Güvenlik Strateji Belgeleri, Başkanlık Siyaset Direktifleri, İcra Emirleri ve Savunma Bakanlığı Raporlarından oluşan toplam 18 adet resmi güvenlik belgesi incelenmiştir. Bunlara ilaveten söz konusu dönem içerisinde meydana gelen ve güvenlik politikalarını etkileyen Siber Komutanlığın kurulması, İran, Kuzey Kore, Çin ve Rusya tarafından gerçekleştirilen siber saldırılar gibi olaylara da yer verilmiştir. İncelemeye tabi tutulan her bir belge tehdit algılaması, ağırlık noktaları, amaç ve araç bakımından değerlendirilmiştir. Nihayet bu farklı açıların değerlendirilmesi sonucunda belgenin hangi caydırıcılık metoduna hizmet eden güvenlik tedbirlerini ihtiva ettiği ortaya çıkarılmıştır. Her bir belge için izlenen bu süreç ve ortaya çıkarılan caydırıcılık metodu doğrultusunda başkanlık döneminin genelinde hakim olan caydırıcılık metodu elde edilmiştir.

- **Siber Uzak Politika Deęerlendirmesi: Güvenilir ve Dayanıklı Bilgi ve İletişim Altyapısının Oluşturulması (2009)²¹³**

Obama'nın başkanlık döneminin ilk siber dokümanı olan Siber Uzak Deęerlendirmesi, 76 sayfalık bir rapor olup mevcut tehditler, içinde bulunulan durum ve muhtemel hareket tarzlarını ortaya koyan bir durum tespiti niteliğindedir. Belgenin başında yer alan yönetici özeti, siber uzayda meydana gelen mevcut statükonun kabul edilemez olduğunu vurgulamaktadır. ABD'nin söz konusu statükoyu aşmada bir kavşak noktasında bulunduğu ve ne şekilde açacağına dair gerekli koordinasyonun vakit kaybetmeksizin başlatılması gerektiği vurgulanmaktadır. Gerek yurt dışı gerekse yurt içi ortaklıklara yapılan vurgu dikkat çekicidir. ABD'nin siber uzayda güvenliği tek başına sağlayamayacağı, teknik ve hukuki normların oluşturulmasında uluslararası paydaşlar ile ortak çalışmanın önemi ifade edilmektedir. Yurt içine yönelik olarak ise belgede özel sektörün rolüne dair ağırlıkla değinildiği görülmektedir.

Tehdit Algılaması: Siber uzayın tanımına yer vererek başlayan belge, nispeten yeni ve bilinmeyen bu tehdit ortamının önemini vurgulamaktadır. Günlük hayatın her alanına giderek daha fazla entegre olan siber uzayın yaratmış getirmiş olduğu kolaylıkların aynı zamanda beraberinde istismar edilebilecek hassasiyetler getirdiği ifade edilmektedir. Siber uzayda yürütölen kötü amaçlı faaliyetlerin ABD'nin rekabetçi yapısını, sivil hak ve özgürlüklerin korunmasını, millî güvenliği ve toplumsal güven ve huzur ortamını bozabilecek tehlikesinin altı çizilmektedir. Muhtemel tehditlerin gerçekleşmesi durumunda üç tehlike ön plana çıkarılmaktadır:

1. Kritik altyapıların zarar görmesi
2. Küresel ekonomik faaliyetlerin sekteye uğratılması. Kişi ve kurumlara ait hesapların ele geçirilmesi.
3. Fikri mülkiyet ve verilerin çalınarak ABD ekonomik çıkarlarının sistematik olarak kayba uğratılması

Devletler ile birlikte devlet dışı aktörlerin de bir tehdit kaynağı olarak sunulduğu belgede teknolojik devrimin beraberinde getirdiği karşılıklı etkileşimin dikkatle ele alınması gerektiği vurgulanmaktadır. Küresel etkileşimin siber araçlarla istismarının millî güvenlik, toplum ve ekonomiyi hedef alabileceği ifade edilmekle birlikte muhtemel tehlikelerin daha çok ekonomik perspektiften ele alındığı ifade edilebilir. Zira

²¹³ ABD Başkanlık İcra Ofisi, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009.

tehditlere dair muhtemel senaryoların ifadesinde askerî ve sosyal boyutlara sınırlı yer verilirken; ABD ekonomisi, küresel ekonomi ve kritik altyapılara ağırlıkla değinildiği görülmektedir.

Ağırlık noktaları: Tehdit tanımının ve tehdit aktörlerinin değişim geçirdiği siber uzayda konvansiyonel anlamdaki ABD üstünlüğünün iz düşümüne bu yeni ortamda rastlanmadığı vurgulanmaktadır. Bu yeni alanda ABD liderliğine olan ihtiyacın altı çizilmektedir. Bununla birlikte, ABD'nin söz konusu adımı yalnız atamayacağı, benzer fikirdeki devletler ile birlikte hareket etmesi gerektiği belirtilmektedir. Siber tehdit ortamına ilişkin bulgu ve tavsiyeler beş ana başlık altında sunulmaktadır.

- ABD liderliği
- Dijital toplum için gerekli kapasite inşası
- Siber uzayda sorumluluk paylaşımı
- Bilgi paylaşımı ve olaylara karşı reaksiyon
- Geleceğin siber mimarisini inşa etmek

Bu başlıklar kapsamında uluslararası iş birliği, toplumsal bilinç ve kurumsal iş birliği konularının ön plana çıktığı görülmektedir. Belgedeki kısa ve orta vadeli aksiyon planlarına göz atıldığında, planlarda yer alan maddelerin neredeyse tamamının özel sektörü de içine alan kurumlararası iş birliğine dayandığı görülmektedir. Bu doğrultuda tehditlere karşı dayanıklılığı artırıcı ve reaksiyon gösterici tedbirlerin inşasında etkin bir bilgi ve sorumluluk paylaşımının altının çizilmektedir.

Amaçlar: Belgede mevcut durumda toplumun bütün paydaşlarını içine alan bir stratejik vizyon eksikliğinden söz edilerek bu ihtiyaca yönelik ulaşılmak istenen bir son durum ortaya konmaktadır. Bu doğrultuda başta federal hükümet olmak üzere, özel sektör ve diğer paydaşların ortaklaşa hareket ederek teknolojik bağlamda değişmeyen güvenlik hedefleri belirlemesi amaçlanmaktadır. Bu süreçte paydaşlar arasında kesintisiz bilgi akışının sağlanması vurgulanmaktadır. Muhtemel tehdit alanlarına karşı paydaşların hem kendi güvenliklerini sağlaması, hem de kolektif olarak bütün kamu yararının korunduğu bir güvenlik ekosistemi yaratılması hedeflenmektedir.

Araçlar: Belgede en fazla dikkat çeken konulardan biri Beyaz Saray'da oluşturulması öngörülen siber güvenlik koordinatörlüğü görevidir. Belge siber uzayda ABD'nin uluslararası liderliği elde etmesi hedefi ile başlamaktadır. Lakin diğer devlet ve devlet dışı aktörler ile etkileşim sınırlı şekilde ele alınmaktadır. Bunun yerine, ABD'nin diğer aktörlere örnek teşkil etmesi için kendi içindeki paydaşların uyumunun önemi

vurgulanmaktadır. Bahse konu olan uyumun sağlanmasında siber kurumlararası güvenlik koordinatörüne önemli sorumluluk yüklenmektedir. Koordinatörün hassasiyetleri göz önüne alacak şekilde eş güdüm sağlaması, güvenlik bütçesine siber tehditlere cevap verecek şekilde yön vermesi, kararlaştırılan stratejilerin uygulama takibi ve başkanı siber faaliyetlerin kilit noktaları ile bilgilendirmesi öngörülmektedir. Koordinatörün ayrıca, siber politikalara ilişkin alınan kararların pürüzsüz bir şekilde uygulamaya konulması için Kongre ile doğrudan diyalog halinde çalışması öne çıkan konulardan biridir. İlgili mekanizmaların sorunsuz işletilmesi için gerekli kanunların çıkarılmasında aktif rol alması gerektiği ifade edilmektedir. Paydaşlar arası yetki karmaşasını önlemek adına sınırlı belirli yetki ve sorumluluk alanları tahsis etmek koordinatörün bir diğer görevidir.

Devlet organları ve özel sektöre dair ihtiyaçların önemle vurgulandığı belgede toplumsal boyut ise farkındalık üzerinden ele alınmaktadır. Bilgiye erişimde muhtemel risklere dair durumsal farkındalığın öneminin belirtildiği belgede özel sektör paydaşları ile eğitim alanında iş birliğinin yine siber güvenlik koordinatörü tarafından yürütülmesi öngörülmektedir. Sonuç olarak, amaçlanan güvenlik ortamına ulaşılması için kritik altyapıların, ekonomik sistemin, sivil hak ve özgürlüklerin dayanıklılığı vurgulanmakta ve kurumsal iş birliği bu süreçte ön plana çıkmaktadır. Söz konusu iş birliğini tesis edecek esas enstrüman olarak Siber Güvenlik Koordinatörlüğü makamının tesisi öngörülmektedir.

Caydırıcılık Metodu: Belge genel itibarıyla siber güvenliğe ilişkin bir durum tespiti ve iyileştirme önerileri niteliğindedir. Süregelen tehditlere karşı dağınık vaziyette olan kapasitenin birbiriyle uyumlaştırılması ve geliştirilmesi amaçlanmaktadır. Kurumlararası eş güdüm ve siber güvenlik iş gücünün oluşturulması adımları caydırıcılık çerçevesinden bakıldığında doğrudan kabiliyet inşasına yönelik adımlardır. Diğer taraftan uluslararası aktörler ile iş birliğine değinilmekle birlikte bu bağlamda ABD liderliği teması işlenmektedir. Bu doğrultuda ortak bir yapılageliş ve norm oluşturma kavramları yeterli yer bulamamaktadır. Belgede sıklıkla yer alan iş birliği ve eş güdüm kavramları uluslararası seviyeden çok devlet içi kurumlara ilişkin ifade edilmektedir.

Belgede en öne çıkan kavramın gerek devlet kurumlarını, gerekse özel sektörü içine alan eş güdüm faaliyeti olduğu görülmektedir. Söz konusu eş güdümün sağlanması için siber güvenlik koordinatörü makamına önemli yetki ve sorumluluklar yüklenmiştir. Koordinatörün sahip olduğu yetkiler vasıtasıyla muhtemel tehditlere karşı kolektif bir

tutum ve farkındalık oluşturarak savunma mekanizması oluşturması beklenmektedir. Tehditlere karşı proaktif bir tutumdan ziyade savunma ve dayanıklılık boyutlarını artırıcı reaktif bir tutum sergilenmektedir. Bütün bunlar göz önüne alındığında Obama dönemi ilk resmî siber belgesinin savunma ve dayanıklılık öğelerini önceleyen İkna Yoluyla Caydırıcılık metodunu yansıttığını ifade etmek mümkündür.

- **Ulusal Güvenlik Stratejisi (2010)**²¹⁴

1986 yılında yürürlüğe giren Gold-Nichols kanunu ile başlayan ulusal strateji yayımlama sorumluluğu ABD askeri kuvvet planlama ve uygulama basamakları arasında eş güdümün sağlanmasında önemli bir yer teşkil etmektedir. Belge, başkanlık seviyesinde tehdit değerlendirmesini ve güvenlik stratejilerini ihtiva eden ve taktik birimlere ışık tutan bir kılavuz kaynak niteliğindedir. Önleyici kuvvet kullanımı ve “biz ve onlar” kavramlarının ön planda olduğu saldırgan Bush politikalarının ardından Obama’nın ilk güvenlik stratejisi olan bu belge, müteakip dönemdeki güvenlik yaklaşımlarına dair önemli ipuçları sunmaktadır. Söz konusu ipuçları arasında en önemlilerinden biri “gereklilik” vurgusudur. Bush döneminin proaktif ve saldırgan güvenlik anlayışına dayanan önleyici kuvvet kullanımına karşın bu belgede “gereklilik” hususu vurgulanarak savaştan önce mevcut tüm seçeneklere başvurulacağı ifade edilmektedir.²¹⁵ Bu açıdan bakıldığında 2010 Ulusal Güvenlik Belgesi güvenlik anlayışı değişimini gösteren önemli bir belge niteliğindedir. Bahse konu olan belgede siber güvenlik; kuvvet kullanımı, Afganistan’da devam eden harekât, nükleer silahlar gibi başlıkların yanında yedi güvenlik başlığından biri olarak ele alınmaktadır.

Tehdit algılaması: Güvenlik strateji belgesinde internetin, ABD askeri ve ekonomik üstünlüğünü pekiştiren bir araç olmasının yanı sıra aynı zamanda bir hassasiyet odağı olduğu ifade edilmektedir. Söz konusu hassasiyetleri hedef alan tehditler hackerlardan devletlere uzanan geniş bir aktör yelpazesini barındırmaktadır. Kritik altyapılara olan bağlılığın siber yollarla istismar edilmesi sonucu kitlesel menfi sonuçların yaşanabileceğinin altı çizilmektedir. Ekonomi ve kritik altyapı güvenliği, belgenin söz konusu bölümünde öne çıkan tehdit alanlarıdır.

Ağırlık noktaları: Belgede en dikkat çekici kavramlardan biri iş birliğidir. Ortaya konulan tehdit algılaması karşısında başvurulacak tedbirlerde paydaşlar arası

²¹⁴ ABD Başkanlık İcra Ofisi, “National Security strategy” (Beyaz Saray, 2010).

²¹⁵ C. Henderson, “The 2010 United States National Security Strategy and the Obama Doctrine of ‘Necessary Force’”, *Journal of Conflict and Security Law* 15, sayı: 3 (01 Aralık 2010): 418, <https://doi.org/10.1093/jcsl/krq025>.

koordinasyona dikkat çekilmektedir. Söz konusu paydaşlar hem yurt içi siber savunma ağının oluşturulmasında birlikte hareket edecek kamu-özel sektör ikilisi, hem de yurt dışında birlikte hareket edilecek ve yapılageliş biçimleri oluşturulacak devletlerdir.

Amaçlar: Belgede birçok farklı altyapı ile bağlantılı olan dijital altyapı stratejik bir varlık olarak nitelendirilmektedir. Bu altyapının korunması için güvenli, güvenilir ve dayanıklı ağların inşa edilmesi amaçlanmaktadır.

Araçlar: Belgede siber saldırılardan korunma, caydırma ve meydana gelen saldırıları müteakiben süratle toparlanma amacıyla iki yolun izlenmesi öngörülmektedir: İnsan ve teknolojiye yatırım ile ortaklıkların güçlendirilmesi. Bu kapsamda öncelikle siber tehditlere karşı savunma boyutunu geliştirmek için ARGE yatırımlarına dikkat çekilmektedir. Nitekim savunmanın teknoloji ve insan gücü boyutlarına işaret edilerek bir taraftan yenilikçi tedbirlerin önemi vurgulanırken diğer taraftan durumsal farkındalık ve dijital okuryazarlığın altı çizilmektedir. Buna ilaveten, söz konusu savunma tedbirlerinin tek bir paydaş tarafından icra edilemeyeceği savunulmaktadır. Devlet-özel sektör iş birliği ile diğer benzer yapıda düşünen devletler ile yardımlaşma adımları takip edilmesi gereken süreçler olarak ifade edilmektedir.

Caydırıcılık Metodu: Belgede siber tehditlere yönelik olarak iki türlü caydırıcılık metodu ön plana çıkmaktadır: İkna-dayanıklılık ve normlar yoluyla caydırıcılık. Kritik altyapıların güvenliğinin sağlanması, dijital altyapıların güvenilir, güvenli ve dayanıklı kılınması için ortaya konulan teknoloji ve insan odaklı tedbirler ikna ve dayanıklılık yoluyla caydırıcılık metotlarını tasvir eder niteliktedir. Diğer taraftan söz konusu tedbirlerin tek bir aktör tarafından uygulanmasının yeterli olmayacağı düşüncesi, uluslararası aktörlerle birlikte çalışarak yapılageliş biçimleri oluşturma süreçlerini ve dolayısıyla normlar yoluyla caydırıcılık metodunu akıllara getirmektedir.

- **Siber Komutanlığın Kurulması (2009)**

Siber uzay mimarisinin sürekli gelişmesi ve kendine has birtakım tehditleri beraberinde getirmesi, bu alandaki askerî tedbirlerin senkronizasyonu için resmî kurumların varlığını gerektirmektedir. Her ne kadar söz konusu kurumlar farklı isimler altında²¹⁶ 90'lı yıllardan itibaren Savunma Bakanlığı bünyesi altında işlev göstermiş olsa da siber harekâtın ofansif ve defansif boyutlarını tek bir çatı altında toplayan Siber Komutanlığın kurulması önemli bir adım niteliğindedir. Küresel boyutta siber tehditlerin

²¹⁶ Örneğin, Küresel Ağ Harekatı Müşterek Görev Kuvveti (Joint Task Force-Global Network Operations ve Ağ Merkezli Savaş Müşterek Fonksiyonel Birim Komutanlığı (Joint Functional Component Command-Network Warfare gibi.

yoğunlaşması ve ABD ulusal güvenlik anlayışında ağırlığının artması sonucu 2009 yılında kurulan yapının gelişimine önem verilmiştir. Bu doğrultuda mevcut ihtiyacın aciliyeti göz önüne alınarak Stratejik Komutanlığın bir alt unsuru olarak kurulan Siber Komutanlık, Ulusal Güvenlik Ajansı ile aynı yerleşkede konuşlandırılmıştır.²¹⁷ Korgeneral Keith Alexander'ın her iki kurumun başkanlığını yürüttüğü çift yapı, Siber Komutanlığın, Ulusal Güvenlik Ajansı'nın personel, teçhizat ve tecrübesinden azami şekilde faydalanarak ivedi şekilde operasyonel yetenek kazanması hedefini gütmüştür. Kurulan yeni komutanlığın görev kapsamı şu şekilde ifade edilmiştir:²¹⁸

1. Siber Uzay harekâtı komutasını merkezileştirmek
2. Savunma Bakanlığının Siber Uzay kabiliyetlerini güçlendirmek
3. Savunma Bakanlığının siber faaliyetlerini birleştirmek ve geliştirmek

Diğer taraftan Savunma Bakanlığı tarafından belirlenen Siber Komutanlık misyonunda şu ifadeler yer almıştır:²¹⁹

Savunma Bakanlığı bilişim ağlarının güvenliğini sağlamak; her türlü harekât ortamındaki faaliyetleri destekleyecek şekilde tam kapsamlı siber uzay askeri harekâtı icra etmeye hazır olmak; ABD ve müttefiki devletler için siber uzayda hareket serbestisi sağlamak ve rakipleri bu imkândan mahrum bırakmak.

Gerek Siber Komutanlığın Ulusal Güvenlik Ajansının sağladığı istihbarat yeteneğinden doğrudan faydalanması, gerekse misyon ifadelerinde yer alan ifadeler siber komutanlığın ofansif faaliyetlerine dair önemli bir beklenti oluşturmuştur. Nitekim Alexander'ın "benim işim bütün ulusu değil, Savunma Bakanlığı ağlarını korumak!"²²⁰ ifadesi söz konusu beklentileri ılımlaştırıcı bir çaba niteliği olarak yorumlanabilir. Bununla birlikte ABD'nin siber uzaya ilişkin askeri kabiliyet inşasında öncü devletlerden biri olması, örnek teşkil edecek uluslararası bir benzer teşkilatın yokluğunda kurumun gelişimi zaman içerisinde farklılaşan süreçleri yaklaşımları barındırmaktadır. Söz konusu gelişim sürecindeki farklılaşmaları 2011 yılında Savunma Bakanlığı tarafından yayımlanan aşağıda iki belge gözler önüne sermiştir.

²¹⁷ U.S. Cyber Command. "Our History" Erişim adresi: <https://www.cybercom.mil/About/History/>

²¹⁸ Lilli, "President Obama and US Cyber Security Policy", 276.

²¹⁹ Stefan Soesanto, "The Evolution of US defense strategy in cyberspace" (Zürich: Center for Security Studies, 2019), 15.

²²⁰ Soesanto, 15.

- **Savunma Bakanlığı Siber Uzayda Harekât Stratejisi Belgesi (2011)**²²¹

Tehdit Algılaması: Belgede siber uzayın günlük yaşama entegrasyonu sonucu artan riskler ile önceki belgelerden farklı olarak daha kapsamlı ve detaylı bir tehdit tanımlaması yapıldığı görülmektedir. Nitekim Savunma Bakanlığı'nın siber tehditlerin dört boyutuna angaje olduğu vurgulanmaktadır:

1. Dış tehdit aktörleri
2. İç tehditler
3. Tedarik zinciri hassasiyetleri
4. Savunma Bakanlığının operasyonel kabiliyetlerine yönelen tehditler

Dış tehditler kapsamında devlet merkezli aktörlerden ziyade yalnız hareket eden siber suçluların yaratmakta olduğu asimetrik etkilere dikkat çekilmektedir. Yoğunlukla ekonomik tahribata yol açan söz konusu tehditlerin bir hizmet şeklinde üçüncü taraflara tahsis edilebilmesi kaygı yaratan bir unsur olarak gösterilmektedir. Savunma Bakanlığı'nın sürdürmekte olduğu faaliyetlere dair insan gücü ve teçhizat kapsamındaki risk belirlemeleri dikkat çekicidir. Bu kapsamda, dış tehditler kadar casusluk faaliyetlerinin potansiyel yıkıcı etkileri vurgulanırken diğer taraftan yazılım ve donanım anlamında yabancı menşeli ekipmanın kullanılması önemli bir sorun sahası olarak nitelendirilmektedir. Kritik altyapıların karşı karşıya olduğu risk faktörlerinin diğer belgeler gibi yinelandığı belgede fikri mülk haklarının korunmasının aynı şekilde önemli bir güvenlik sorunu olduğu dile getirilmektedir. Bunlara ek olarak, Savunma Bakanlığı bilişim ağlarında henüz tespit edilemeyen kötü amaçlı siber faaliyetlerin olabileceği kabul edilmekte, böylece tehdit ve tedbir arasındaki dengesizlik durumu akıllara getirilmektedir.

Ağırlık noktaları: Belgede ABD'nin sahip olduğu yetişmiş insan gücü, bilgi birikimi, kamu ve özel sektörün siber uzayda yürüttüğü ARGE faaliyetleri ve Savunma Bakanlığının bu kabiliyetleri kullanma durumu ele alınmaktadır.

Amaçlar: Belgede güvenliğin siber uzay tarafından yeniden tanımlandığı ve Savunma Bakanlığı'nın kendine atfedilen görevleri yerine getirebilmesi için siber uzayı tıpkı kara, deniz ve hava gibi ayrı bir harekât ortamı olarak yorumlayacağı ifade edilmektedir. Bu doğrultuda bu yeni harekât alanında; gizlilik hakları, kişisel özgürlükler gibi hassasiyetleri göz önünde bulundurarak, mevcut karmaşık tehditlere tedbir getirmekle beraber ortaya çıkacak fırsatlardan da yararlanmak amaçlanmaktadır.

²²¹ "Department of Defense Strategy for Operating in Cyberspace" (ABD Savunma Bakanlığı, 2011).

Araçlar: Ortaya konulan amaçlar için izlenmesi gereken beş yol çizilmektedir:

1. Etkin şekilde organize olmak, hazırlanmak ve gerekli ekipmana sahip olmak için siber uzayı bir harekât alanı olarak tanımlamak ve bu şekilde siber uzayın bütün potansiyelinden faydalanmak
2. Savunma Bakanlığı bilişim ağlarını korumak için yeni işletim konseptlerine başvurmak
3. Bütünsel devlet anlayışını yansıtan bir siber uzay güvenlik stratejisi için diğer kamu kurumları ve özel sektör ile iş birliğine gitmek
4. Kolektif siber güvenlik için ABD müttefikleri ve diğer uluslararası aktörler ile sağlam ilişkiler kurmak
5. Eşsiz bir siber iş gücü oluşturmak ve teknolojik yenilikleri hızlandırmak

Belgede siber uzay görevlerini yürütmek amacıyla Stratejik Komutanlık bünyesinde oluşturulan Siber Komutanlığın Savunma Bakanlığı'nın şu ihtiyaçlarına cevap vereceği ifade edilmektedir:

- Eğitim ve durumsal farkındalık yoluyla siber risklerle mücadele etmek, güvenli ve dayanıklı bilişim ağları inşa etmek
- Ortak bir harekât resmi oluşturarak, iş birliklerine giderek ve kolektif savunma anlayışı ortaya koyarak siber güvenlikte bütünlüğü tesis etmek
- Diğer kuvvet ve kurumlara ait siber kabiliyetleri entegre ederek ihtiyaç anında ihtiyaç yerine yönlendirilmesini sağlamak

Belgede Siber Komutanlık ve Ulusal Güvenlik Ajansı'nın çiftli yapısının önemine dikkat çekilerek bu yapının görev etkinliğine fayda sağlayacağı vurgulanmaktadır. Özellikle iş gücü eğitiminin önemi ifade edilmekte ve senaryoya dayalı tatbikatlarda saldırgan tarafı canlandırılan kırmızı ekiplerin rolünün altı çizilmektedir. Gerek iç gerekse dış tehditlere karşı siber hijyen uygulamasının durumsal farkındalık ve etkin mücadele için elzem olduğu vurgulanmaktadır. Belgede bütünsel devlet anlayışı önemle vurgulanmaktadır. İç Güvenlik Bakanlığı, Savunma Sanayii ve özel sektör ile iş birliğinin yaratacağı sinerji önemle vurgulanmaktadır. Özellikle iş gücünün temini ve eğitimi konusunda yalnızca kamu mantığı ile hareket etmenin bir hata olduğu dile getirilmektedir. Özel sektörün rekabetçi yapılarına ayak uydurularak, ihtiyaç duyulan nitelikteki çalışanları teşvik edici yöntemlerin izlenmesine dair detaylı ifadeler dikkat çekicidir.

Caydırıcılık Metodu: Belgede diğer kaynaklarda olduğu gibi, uluslararası aktörler ile iş birliği, sorumlu davranışa davet etme inisiyatifleri ve kabul gören yaklaşımları belirleme çalışmalarının önemine kayda değer bir yer ayrılmıştır. Bu durum, normlar yoluyla caydırıcılığın önemini koruduğunu göstermektedir.

Diğer taraftan iş gücü temini ve eğitimi konusu belgede en ağırlıkla ele alınan konudur. Siber harekâtı yürütecek personelin nitelikli olması, durumsal farkındalık sahibi olması, siber hijyen yaklaşımını benimsemesi caydırıcılık kapsamında muhtemel saldırıları başarısız kılacak savunma tedbirlerinin geliştirilmesi olarak yorumlanabilir. Buna ek olarak özellikle özel sektörün kabiliyetlerini de içine alacak şekilde yürütülmesi hedeflenen kurumlararası iş birliği ve bütünsel devlet anlayışı, kritik altyapıların korunmasında önemli bir kolektif yaklaşımın yansımasıdır. Savunma ve dayanıklılık odaklı bu girişimler savunma ve ikna yoluyla caydırıcılık metodunun örnekleridir.

Belgede dikkat çekilmesi gereken bir nokta siber komutanlığa ilişkin ofansif kabiliyetlere yer verilmemesidir. Her ne kadar belgenin amaç kısmında siber uzay harekât alanı bir tehdit ortamı olduğu kadar muhtemel fırsatlar kaynağı olarak betimlense de söz konusu fırsatları değerlendirecek ofansif kabiliyetlerden söz edilmemektedir. Bunun yerine daha çok siber komutanlık genel olarak kurumlararası entegrasyon ve iş gücü yetiştirme anlamında ele alınmaktadır. Dolayısıyla ofansif kabiliyetler aracılığıyla misillemeyi esas alan bir ceza yoluyla caydırıcılık metodundan söz etmek mümkün değildir.

- **Savunma Bakanlığı Siber Uzay Politika Raporu (2011)²²²**

Savunma Bakanlığı'nın aynı yıl içerisinde ikinci bir siber faaliyet resmî belgesi çıkarmasının sebebi Ike Skelton Ulusal Güvenlik Kanunu'nun öngördüğü şekilde bütçe görüşmeleri öncesi Kongrenin söz konusu faaliyetlere ilişkin sorularını yanıtlamaktır. Diğer resmî strateji belgelerinden farklı olarak rapor, Kongrenin belirlediği ana başlıklar altındaki konular hakkında bilgi aktarımında bulunmaktadır.

Tehdit algılaması: Belgede mevcut tehdit ortamı betimlenmek yerine Siber Uzayda Harekât Stratejisi Belgesine atıfta bulunulmakta ve siber uzaydaki gelişmelerden aynı şekilde tehdit ve fırsatlar olarak bahsedilmektedir.

Ağırlık noktaları: Belgede Kongre tarafından sunulan 13 adet sorunun cevabı bulunmaktadır. Söz konusu soruların dört adedi doğrudan caydırıcılık metodu ile ilgili

²²² "Savunma Bakanlığı Siber Uzay Politika Raporu" (ABD Savunma Bakanlığı, Kasım 2011).

olup diğerk sorularda kinetik operasyonların, saldırganı belirleme sorunsalının ve uluslararası normların işleyiş biçimlerinin ağırlık teşkil ettiğı görölmektedir.

Amaçlar: Raporda yöneltilen sorular caydırıcılığın nasıl sağlanacağı, misilleme durumu, kinetik operasyonlar, diğerk kurumlar ve uluslararası aktörler üzerinedir. Sorulara verilen cevaplar bir bütün şeklinde ele alındığında savunma tedbirlerinden, cezalandırma prosedürlerine ve normların rolüne kadar her türlü seçeneğın değerlendirildiğı ve farklı metotların uygulandığı kapsamlı bir caydırıcılık stratejisinin tarif edildiğı görölmektedir.

Araçlar: Ortaya atılan tedbirlerde iş birliğı ve siber komutanlık kavramları ağırlık kazanmaktadır. İş birliğı konusunda Savunma Bakanlığının diğerk kurumlar ile koordineli olarak saldırgan aktörün tespiti, üçüncü bir devletin dahil olma durumu ve muhtemel reaksiyon tarzları konularında birlikte hareket pratikleri vurgulanmaktadır. Diğerk taraftan uluslararası düzeyde hangi kabiliyetlerin siber silah olarak tanımlanması gerektiğı ve kuvvet kullanımında gözetilecek eşiklere dair oluşturulmak istenen normlar için eş güdümün altı çizilmektedir.

Saldırgan aktörlerin tespiti konusu, yeni kurulan Siber Komutanlık ile ilişkilendirilerek ele alınmaktadır. Şöyle ki Siber Komutanlığın Ulusal Güvenlik Ajansının kabiliyetlerinden faydalanacak şekilde konuşlandırılmasının hedef geliştirme, siber harekât planlama ve icra konularında önemli katkılar sağlayacağı ifade edilmektedir. Ayrıca kurum bünyesinde teşkil edilen siber adli birimlerin uğranılan saldırıyı atfetme sorunsalını önemli oranda ortadan kaldıracığı öne sürölmektedir. Tespit edilen siber saldırı ardındaki aktöre karşı siber harekâtın yanı sıra kinetik operasyonların da seçenekler arasında olduğu belirtilmektedir.

Caydırıcılık Metodu: Raporda, daha önce ele alınan belgelerde olduğu kritik altyapı güvenliğinin artırılması maksadıyla kurumlararası; tehdit tanımlamaları ve kuvvet kullanım biçimleri bağlamında yapılageliş şekilleri oluşturmak maksadıyla uluslararası iş birliğı vurgulanmaktadır. Dolayısıyla ikna, dayanıklılık ve normlar yoluyla caydırıcılık metotlarına işaret eden ifadeler bu belgede mevcuttur. Raporu farklı kılan nokta ise ofansif kabiliyetlere ilişkin ifadelerdir. Önceki belgelerden farklı olarak raporda misilleme kavramı açıklıkla ele alınmaktadır. Bu kapsamda, aşağıdaki ifadeler dikkat çekicidir:

Gelecekteki hasımlarımız “ağırlık merkezlerimizi”²²³ felce uğratmayı başaramadığı takdirde, muhtemelen ABD Başkanının elindeki ulusal güvenlik seçeneklerinden oluşan menüyü daha iyi anlayacaklardır. ...Başkan tarafından uygun görüldüğü şekilde, reaksiyon tarzları siber veya kinetik kabiliyetler şeklinde olabilir.

Bir önceki bölümde saldırgan aktörün tespiti hususundaki titiz çalışmalar ve yukarıda farklı nitelikte reaktif tedbirleri içeren ifadeler ABD menfaatlerinin zarara uğratılması halinde saldırgan aktöre cezalandırıcı bir misilleme anlayışına işaret etmektedir. Dolayısıyla diğer metotlara ek olarak ele alınan bu raporda belirgin bir ceza yoluyla caydırıcılık metodundan bahsetmek mümkündür.

- **ABD Başkanı’nın Siber Uzak Uluslararası Stratejisi (2011)²²⁴**

Siber güvenliğe ilişkin Beyaz Saray’ın bakış açısını yansıtan 30 sayfalık bu belge, Obama’ya göre ABD’nin diğer uluslararası aktörler ile siber faaliyetlerin tamamında müşterek bir yaklaşımı esas alan ilk çalışma niteliğindedir.²²⁵ Belgenin Stuxnet saldırısının açığa çıkmasından kısa bir süre yayımlanması, saldırı kapsamında aşılın siber kuvvet kullanım eşiği ve uluslararası koordinasyona yapılan vurgu dikkate alındığında Stuxnet etkilerini onarıcı bir amaç güttüğü çıkarımı yapılabilir.

Tehdit algılaması: ABD ekonomisinin, kritik altyapılarının ve ulusal güvenliğinin referans noktası olarak alındığı diğer güvenlik belgelerinden farklı olarak bu strateji belgesinde siber tehditlerin uluslararası toplumu bir bütün olarak tehdit ettiği ifade edilmektedir. Dolayısıyla söz konusu tehditlere karşı uluslararası kolektif çabanın gerekliliği vurgulanmaktadır.

Ağırlık noktaları: Belgede ağırlıklı ele alınan konu siber uzayda istikrar ve güvenliğinin sağlanması için normlara duyulan ihtiyaçtır. Bu kapsamda temel hak ve özgürlüklerin korunması, meşru müdafaa hakkı gibi mevcut normların adaptasyonu ele alınırken diğer taraftan güvenilir erişim, çoklu yönetim gibi yeni normların siber uzaya ilişkin faaliyetlerde takip edilmesi gerektiği ifade edilmektedir.

²²³ Bir önceki cümleden ağırlık merkezlerinin kritik altyapılar olduğu anlaşılıyor.

²²⁴ Barack Obama, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World: (688502011-001)” (American Psychological Association, 2011), <https://doi.org/10.1037/e688502011-001>.

²²⁵ Lilli, “President Obama and US Cyber Security Policy”, 277.

Amaçlar: Belgede ABD'nin küresel çapta gayret göstererek, açık, uyumlu, güvenilir bir bilgi altyapısının tesis edilmesi ve bu şekilde uluslararası ticaret ve güvenliğe katkı sağlanması amaçlanmaktadır.

Araçlar: Ortaya konulan amaç için sorumlu davranışları esas alan normların devletlerin uygulamalarına yön vereceği bir çevre yaratılacağı belirtilmektedir. İstenen bu son durum için üç alandaki faaliyetlere ağırlık verileceği ifade edilmektedir:

1. Diplomasi
2. Savunma
3. Ağ merkezli teknolojilerin güvenlik ve erişilebilirliğin geliştirilmesi

Bu kapsamda siber uzaya ilişkin faaliyetlerin koordinesi için hükümetler, akademi, sivil toplum ve özel sektörün paydaş olduğu çoklu bir yönetim yapısı oluşturulması öngörülmektedir. Maruz kalınan siber saldırılara ilişkin durumsal farkındalığın artırılması, hassas noktaların tespiti ve reaktif planların özel sektör ile eş güdüm içerisinde yürütülmesi gerektiği ifade edilmektedir. Bunlara ek olarak, sahip olduğu kaynak ve tecrübeye dayanarak, ABD'nin diğer ülkelerin siber kapasite inşasını destekleyeceği ve bu yolla her devletin kendi ağlarını koruyabildiği bir senaryoda siber uzayda bir istikrar ortamının mümkün olacağı belirtilmektedir.

Caydırıcılık Metodu: Belgenin tehdit algılaması, ağırlık noktaları, amaç ve araçları incelendiğinde neredeyse tamamında iş birliğine yapılan vurgu dikkati çekmektedir. Siber tehditlerin tek bir devlet yerine uluslararası toplumun tamamını hedef aldığı saptamasından hareketle ortak kapasite inşasının, görüş alışverişinin, mevcut ve gelişen normların önemi vurgulanmaktadır. Bu doğrultuda açık bir şekilde normlar yoluyla caydırıcılığa işaret edildiği dile getirilebilir. Diğer taraftan bilgi altyapısının korunmasında özel sektör ile iş birliği, hassas noktaların tespiti ve kriz yönetim tedbirleri gibi savunma düzeyini geliştirici girişimler ikna ve dayanıklılık yoluyla caydırıcılık metoduna ait uygulama biçimleridir.

- **Siber Uzayda Güvenilir Kimlikler için Ulusal Strateji (2011)²²⁶**

Tehdit algılaması: Strateji belgesinde internet ortamındaki kimlik hırsızlığının internetin güvenli kullanımında yarattığı tahribata dikkat çekilmektedir. Belgede kişisel veri hırsızlığı, kullanıcı adı/parola hırsızlığı, kullanıcıların bilgilerini açığa çıkarmalarını amaçlayan oltalama saldırıları, zayıf kimlik doğrulama sistemleri gibi tehdit ve

²²⁶ “National Strategy for Trusted Identities in Cyberspace” (Beyaz Saray, Nisan 2011).

hassasiyetlerin kişileri internet ortamında güvenle işlem yapmaktan alıkoyduğu ifade edilmektedir.

Ağırlık noktaları: Belgede kullanıcı seviyesinde güvenli internet ekosistemini sağlamak için çözüm önerileri geliştirilmektedir. Bu kapsamda, bireysel kullanıcıların güvenilir internet kullanımını en fazla sekteye uğratan konu olarak kimlik ve veri hırsızlığı konusu masaya yatırılmaktadır. Kimlik doğrulama sistemleri, mahremiyet korunması için geliştirici tedbirler, özel sektör-kamu-akademi iş birliği ve kullanıcı merkezli çözümler belgenin önemle üzerinde durduğu konu başlıklarıdır.

Amaçlar: Strateji belgesi, kişi ve kurumların internet ortamında çevrimiçi işlem ve etkileşimlerini güvenle yapabildiği, kullanıcı mahremiyetinin ön planda tutulduğu, emniyetli ve dayanıklı bir kimlik ekosistemine dayalı bir sanal uzaya erişmeyi hedeflemektedir.

Araçlar: Öngörülen amaçlara ulaşmak için öne sürülen temel araç Kimlik Ekosistemi Çerçevesidir. Güvenilir kimlik doğrulama mekanizmalarının tesisi maksadıyla söz konusu çerçeve kapsayıcı birlikte çalışabilirlik standartlarını, risk modellerini ve mahremiyet haklarını barındırmaktadır. Buna göre ekosistemde yer alan kamu, özel sektör ve akademi paydaşlarının sorumlulukları belirlenmektedir. Söz konusu sorumlulukların yerine getirilmesinin takibi için denetleyici bir akreditasyon grubu oluşturulmaktadır. Çerçeve, tüm paydaşlarını içine alacak şekilde başta düşük seviyede koşul ve gerekliliklerin ortaya konulduğu bir ortak inisiyatifi benimsemektedir. Dolayısıyla tek bir bağlayıcı metinden ziyade paydaşların sürekli birbiriyle angajman içinde olarak daha etkin prosedürleri ortaya koyduğu güvenli geliştirici bir inşaa sürecini esas almaktadır. Teknik anlamda, kriptolama, gizlilik sağlayıcı serverlar gibi kullanıcı bilgilerinin toplanmasını ve açığa çıkarılmasını minimize eden Mahremiyet Geliştirici Teknolojilerin kullanımına önemle işaret edilmektedir.

Caydırıcılık Metodu: Siber Uzayda Güvenilir Kimlikler için Ulusal Strateji belgesi, siber uzayı kişi ve kurumların etkileşimleri için daha güvenli bir yer haline getirmeyi amaçlamaktadır. Kullanıcı bilgilerinin daha etkin korunmasını öngören, teknik ve idari tedbirlerin geniş bir paydaş yelpazesi tarafından ele alındığı bir güvenlik geliştirme süreci belgenin ortaya koyduğu ana yeniliktir. Siber uzayda kimlik ve veri hırsızlığı yoluyla gerçekleşen siber saldırıların başarı şansını azaltmayı, bu saldırılara karşı sistemin tüm paydaşları ile birlikte dayanıklılığını artırmayı ve söz konusu süreçte kamu-özel sektör iş birliği konusunda net mesajlar vermeyi amaçlayan belgenin izlediği strateji ikna ve dayanıklılık yoluyla caydırıcılık stratejisi olarak yorumlanabilir.

- **Başkanlık Siyaset Direktifi-20 (2012)**

Tehdit algılaması: Defansif ve Ofansif Siber Etki Operasyonlarının tanımlarını²²⁷ ortaya koyarak başlayan belgede söz konusu operasyonların sonuçları tarafından çizilen bir tehdit algılaması yer almaktadır. Bahse konu olan operasyonlara ilişkin belgede yer alan şu ifadeler dikkat çekicidir:

Siber uzay küresel çapta birbirine bağlıdır. Bu yüzden Defansif ve Ofansif Siber Etki Operasyonları ilave koordinasyon ve politika değerlendirmelerini gerektiren eşi görülmemiş millî güvenlik endişelerini ortaya çıkarabilir. Bu operasyonlar, gizlilik içinde ve ustalıkla yapılsa bile, amaçlanan hedefin ötesindeki coğrafyalarda siber etkiler yaratabilir ve bu etkiler Amerikan millî menfaatlerini zedeleyici yan sonuçlar doğurabilir.

Kullanılan ifadelerden anlaşılacağı üzere, direktifte tehdit olarak doğrudan ABD tarafından gerçekleştirilen siber etki operasyonları sonucu oluşan ortam (Stuxnet örneği) belirtilmektedir. Söz konusu etkilerin kontrolsüz yayılma durumu, bütün devletleri etkileme olasılığı ve saldırıya uğrayan aktörler tarafından muhtemel tırmandırma senaryosu belgenin tehdit algılamasının sınırlarını çizmektedir.

Ağırlık noktaları: Direktifin ağırlık noktaları olarak Defansif ve Ofansif Siber Etki Operasyonları yer almaktadır. Bu operasyonlara hangi hallerde başvurulacağı, hangi prosedürlerin takip edileceği, karar alma sürecinde yer alacak kurumsal paydaşlar ve başvurulacak tamamlayıcı etkiler direktifte üzerinde durulan konu başlıklarıdır.

Amaçlar: Direktifte siber etki operasyonlarının ortaya çıkaracağı kontrolsüz ortamın önüne geçilmesi amaçlanmaktadır. Bu doğrultuda nihai karar vericinin ABD Başkanı olduğu ve ilgili kurumları karar alma sürecine dahil eden bütünsel devlet anlayışının tesis edilmesi amaçlanmaktadır.

Araçlar: Direktif ortaya konulan amaca ulaşılması için öngörülen prensip ve uygulamalar şu şekildedir:

²²⁷ Defansif Siber Etki Operasyonları: ABD hükümeti tarafından veya onun adına gerçekleştirilen, siber ağ savunma faaliyetlerinin dışında kalan, ABD bilişim altyapısına yönelik devam eden siber saldırılar veya yakın zamanda öngörülen tehditler karşısında ulusal menfaatleri koruma amacıyla yapılan hareket ve faaliyetler.

Ofansif Siber Etki Operasyonları: ABD hükümeti tarafından veya onun adına gerçekleştirilen, siber ağ savunma faaliyetlerinin dışında kalan ve ABD bilişim ağları dışında siber etkiler oluşturmamayı amaçlayan hareket ve faaliyetler.

1. Siber etki operasyonlarının icrasına yönelik planlamalarda uluslararası hukuk ve egemenlik hakları gibi normların daima göz önünde bulundurulması,
2. Tehditlere karşı geliştirilecek tedbirlere ilişkin prosedürleri oluştururken resmî kurumlar ve ilgili özel sektör temsilcilerinin görüş ve onayının alınması,
3. Operasyonların icrasında nihai onay makamının ABD Başkanı olması,
4. Operasyonların değerlendirilmesinde dış politika, fayda/maliyet, etkinlik, risk faktörleri, siyasi sonuçlar gibi kriterlerin ele alınması ve diplomatik, istihbari, ekonomik diğer tedbir seçeneklerinin gözden geçirilmesi.

Caydırıcılık Metodu: Direktifte, siber etki operasyonlarına ancak bilgi ağı güvenlik tedbirleri yetersiz kaldığında başvurulacağını altı çizilmektedir. Savunma ağlarının geliştirilmesi için kurumsal paydaşların ve bunları koordine edecek siber güvenlik koordinatörünün rolüne dikkat çekilmektedir. Belgede ofansif bir operasyon için askeri istihbaratın yeterlilik kriteri aranmakta ve siber operasyonlara dair askeri yeteneklerin sivil iradeye tabi durumu tesis edilmektedir.²²⁸ Ofansif operasyon yetkisini alt kademelerden alıp doğrudan kurumlararası süreç ve akabinde başkana bağlayan bu belge özünde bir kendi kendini sınırlandırma adımıdır. Obama yönetimi bu belge ile siber uzayda çatışma ortamını tırmandırıcı inisiyatifleri engelleyerek Stuxnet saldırısı sonrası bu konuda bir örnek davranış sergileme yoluna gitmiş ve bu şekilde uluslararası platformda bir norm inşasına ön ayak olma hedefi gütmüştür. Bu doğrultuda normlar yoluyla caydırıcılık tercih edilen metot görünümündedir. Belgenin kapsam itibarıyla ofansif kabiliyetleri ve dolayısıyla ceza yoluyla caydırıcılığın uygulama biçimlerinin detaylandırması beklenirken, ofansif etkilerin önündeki bürokratik prosedür ve algısal mekanizmaları kuvvetlendirmesi dikkat çekicidir. Dolayısıyla bu belge, ABD'nin siber uzaya ilişkin güvenlik önlemleri bakımından ceza yoluyla caydırıcılık metodunu ciddi derecede geri plana atan bir adım niteliğindedir.

- **Savunma Bakanlığı Savunma Bilimi Kurulu Raporu – Dayanıklı Askeri Sistemler ve Gelişmiş Siber Tehdit Raporu²²⁹ (2013)**

Savunma Bilimi Kurulu, sivil uzmanlardan oluşan ve Savunma Bakanlığı yetkililerine bilimsel ve teknik konularda görüş bildiren bir yapıdır. Söz konusu rapor, Savunma

²²⁸ Jason Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace”, *Journal of Cybersecurity* 5, sayı: 1 (01 Ocak 2019): 3, <https://doi.org/10.1093/cybsec/tyz008>.

²²⁹ “Dayanıklı Askeri Sistemler ve Gelişmiş Siber Tehdit” (Savunma Bakanlığı Savunma Bilimi Kurulu, 2013), <https://dsb.cto.mil/reports.htm>.

Bakanlığı ağlarının siber saldırılara karşı dayanıklılığını artırıcı öneriler ortaya koymak, Bakanlığın süreç geliştirme ve yatırım önceliklerine yön vermek amacıyla kurulan 24 kişilik bir uzman grubunun tespit ve değerlendirmeler bütünü niteliğindedir.

Tehdit algılaması: Siber tehditleri oldukça teknik ve detaylı bir bakış açısıyla ele alan 146 sayfalık belgede söz konusu tehditler tekdüze bir formatta kabul edilmekten öte, kapasite ve etkilerine göre sınıflandırılmaktadır. Bu doğrultuda, kişisel kazanç hedefi güden basit hackerlardan devlet destekli gelişmiş saldırılar icra eden kişi ve grupları kapsayan bir tehdit ve aktör yelpazesi sunulmaktadır. Bu doğrultuda karşı karşıya olunan tehdit durumunun risk bileşenleri ve aktör değişkenliği açısından karmaşıklığı vurgulanmaktadır.

Söz konusu hassasiyetlerin nedenleri olarak şu noktalara dikkat çekilmektedir:

1. Saldırkanı tespit etmedeki güçlük
2. Kusursuz yazılımları üretmenin neredeyse imkânsız oluşu
3. Piyasa için üretilen ve güvenlik kaygısı geri planda olan yazılım ve donanım aygıtları
4. Güvenilir olmayan deniz aşırı aktörlerce üretilen yazılım ve donanım aygıtları

Müteakip bölümde siber tehditlerin yansımalarını askerî açıdan ele alan raporda söz konusu tehditlerin muhtemel sonuçları olarak şu hususlar ifade edilmektedir:

1. Amerikan birliklerinin muhabere sistemlerinin çökertilmesi
2. Veri manipülasyonu yoluyla birliklerin yanlış yönlendirilmesi ve bilgiye olan güvenin azaltılması
3. Silah sistemlerinin amaçlanan şekilde işlev göstermemesi ve hatta Amerikan birliklerine zarar verecek şekilde çalışması
4. Uçak, uydu, insansız hava aracı gibi sistemlerin imhası

Görüldüğü üzere başlangıçta siber tehditlerin niteliğine yönelik kapsayıcı bir çerçeve sunan raporun tehdit algılaması, takip eden bölümde askeri faaliyetleri mercek altına alarak siber tehditlerin muhtemel sonuçlarına dair açık ve net senaryolar ortaya koymaktadır. Diğer taraftan Savunma Bakanlığı sistemlerinin siber ağlara olan bağımlılığının gelecekte azalmayacağı, aksine artacağı ifade edilerek tehditlerin de orantılı olarak artış göstereceği sonu gelmeyen bir mücadele ortamı ön kabulü yapılmaktadır.

Ağırlık noktaları: Raporda bilişim ağlarının güvenliğini sağlayıcı savunma tedbirlerinin geliştirilmesi, ofansif kabiliyetlerin siber harekâtındaki yeri ve hasmın siber kabiliyetlerine yönelik istihbarat faaliyetlerinin önemi üzerinde ağırlıkla durulan konulardır.

Amaçlar: Tehdit algılaması bölümünde ifade edildiği üzere, raporun genel teşhisi siber uzayın saldırgana avantaj sağladığı ve söz konusu dengesizlik doğrultusunda bütün askerî sistemleri tam zamanlı olarak her türlü tehdide karşı savunmanın olanaksız olduğudur. Bunun yerine raporu kaleme alan uzmanlar savunma ile caydırıcılığın bütünleşik şekilde uygulandığı bir siber risk yönetiminin tesis edilmesini amaçlamaktadır.

Araçlar: Ortaya konulan amaçlara ulaşmak için yedi maddelik bir öneri listesi sunulmaktadır:

1. Nükleer saldırıyı bir caydırıcı unsur olarak muhafaza etmek
2. Gelişmiş bir hasım karşısında girişilecek bir harekât için kullanılacak siber, konvansiyonel ve nükleer kabiliyetleri belirlemek
3. Hasmın siber kabiliyetlerini, plan ve niyetlerini anlamak için istihbarat temini ve analizi konularına eğilmek
4. Dünya çapında ofansif siber kabiliyetler oluşturmak ve muhafaza etmek
5. Düşük ve orta seviye tehditlere karşı savunma tedbirlerini geliştirmek
6. Savunma Bakanlığı'nın siber güvenlik kültürünü değiştirmek
7. Siber dayanıklı bir kuvvet inşa etmek

Görüldüğü üzere rapor, Savunma Bakanlığı'nın halihazırdaki siber güvenlik politikalarını eleştirmekte ve kapsamlı değişiklikler önermektedir. Bu önerilerden en dikkat çeken siber angajmanın münferit bir çatışma ortamı olarak değerlendirilmeyip başta nükleer kabiliyetler olmak üzere eldeki tüm askeri seçenekleri ihtiva eden topyekûn bir angajman tarzının ortaya konulmasıdır.

Caydırıcılık Metodu: Raporda sadece savunmanın asimetric üstünlüğe sahip siber saldırılara karşı yetersiz olacağı ifade edilmektedir. Reaktif anlamda, hasmın zarara uğratılmasını esas alan ve geniş bir yelpazedeki ofansif kabiliyetleri ihtiva eden bir yaklaşım benimsenmektedir. Söz konusu yaklaşım bir ceza yoluyla caydırıcılık örneğidir. Belgede ayrıca özellikle nispeten zayıf saldırgan aktörlerin yöneltmekte olduğu tehditlere karşı savunma tedbirlerinin geliştirilmesi ve dayanıklılığın artırılması

konusu, ofansif kabiliyetlerin yanında bir tamamlayıcı tedbir olarak öne sürülmektedir. Bu da ceza, ikna ve dayanıklılık yoluyla caydırıcılık metotlarının birlikte ele alındığı bir caydırıcılık stratejisini ifade etmektedir.

- **Başkanlık Siyaset Direktifi-21²³⁰ ve İcra Emri 13636²³¹ (2013)**

ABD Başkanlık makamı tarafından kaleme alınan bu iki belgenin birlikte incelenmesinin sebebi aynı konuyu ele almaları ve aynı tarihte yayımlanmalarıdır. 12 Şubat 2013 tarihli bu iki belge Kritik Altyapı güvenliğini ele almaktadır. Başkanlık icra emri kritik altyapıların tespiti, sorumlu makamların tesis ve koordinesi gibi genel konuları içerirken; tamamlayıcı nitelikte olan icra emri kritik altyapı güvenliğinde daha somut adımları ihtiva eden detaylı bir belgedir.

Tehdit algılaması: Belgelerin tehdit algılaması tamamen kritik altyapıların yüz yüze olduğu sabotaj tehditlerine yöneliktir. Stuxnet saldırısı sonrası kuvvet kullanım eşiğinin aşılması ve kritik altyapıların doğrudan hedef haline gelmesi, bu noktada ABD yönetimini doğrular niteliktedir. Bu doğrultuda kritik altyapıların çeşitli ve karmaşık olduğu, toplumun refah ve işleyişi için hayati öneme sahip olduğu ve bunların korunması için gösterilecek çabaların proaktif ve koordineli bir şekilde yürütülmesi gerektiğinin altı çizilmektedir.

Ağırlık noktaları: Belgelerde kritik altyapıların güvenliği için sorunun tespiti ve çözümü için koordineli bir sürecin inşası ön plana çıkmaktadır. Şöyle ki başkanlık siyaset direktifinde 16 adet kritik altyapı sıralanmakta, her bir altyapı birimine kendine özgü karakteristikleri doğrultusunda bir sorumlu sektöre özel kurum atanmaktadır. Sektöre özel kurumların ve diğer çözüm paydaşlarının genel koordinesi için İç Güvenlik Bakanlığı belirlenmektedir. Tanımlanan kritik altyapı sektörleri ve atanan sektöre özel kurumlar Tablo-7’de sunulmuştur.

²³⁰ “Başkanlık Siyaset Direktifi-21”, 12 Şubat 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

²³¹ “İcra Emri-13636” (ABD Başkanlık Makamı, 12 Şubat 2013), <https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636>.

	Kritik Altyapı Sektörü	Sektöre Özel Kurum
1	Kimyasal	İç Güvenlik Bakanlığı
2	Ticari Faaliyetler	İç Güvenlik Bakanlığı
3	İletişim	İç Güvenlik Bakanlığı
4	Kritik İmalat	İç Güvenlik Bakanlığı
5	Barajlar	İç Güvenlik Bakanlığı
6	Savunma Sanayii Yapılanması	Savunma Bakanlığı
7	Acil Durum Hizmetleri	İç Güvenlik Bakanlığı
8	Enerji	Enerji Bakanlığı
9	Finansal Hizmetler	Hazine Bakanlığı
10	Gıda ve Tarım	Tarım ve Sağlık Bakanlıkları
11	Yönetim Hizmetleri	İç Güvenlik Bakanlığı ve İdari Hizmetler Yönetimi
12	Sağlık Hizmetleri	Sağlık Bakanlığı
13	Bilgi Teknolojisi	İç Güvenlik Bakanlığı
14	Nükleer Reaktör, madde ve atıklar	İç Güvenlik Bakanlığı
15	Ulaştırma Hizmetleri	İç Güvenlik ve Ulaştırma Bakanlıkları
16	Su ve Atık Su Sistemleri	Çevre Koruma Kurumu

Tablo 3: 13636 Sayılı Başkanlık İcra Emrinde Tanımlanan Kritik Altyapı Tesisleri

İcra emrinde ise kritik altyapı güvenliğini belli başlı standartlara oturtmak, izlenecek adımları belirlemek maksadıyla standartlar enstitüsüne bir Siber Güvenlik Çerçevesi belgesi hazırlaması görevi verilmiştir.

Amaçlar: Belgelerde ortaya konulan amaç kritik altyapıların güvenliğini sağlamak, bunlara yönelik tehditleri ortadan kaldırmak, kritik altyapıları dayanıklı kılmak ve reaksiyon sürelerini hızlandırmaktır.

Araçlar: Ortaya konulan amaç için iki çeşit araç belirlenmiştir. Bunlardan birincisi güvenlik geliştirici süreçlerin sorumlusu kurumun belirlenmesidir. Her sektörün kendi faaliyet alanlarına ilişkin özgün dinamikleri de göz önünde bulundurularak devlet ve özel sektörden oluşan paydaşları bir araya getirme, gerekli koordinasyonu sağlama ve uygulama prensipleri oluşturma görevi İç Güvenlik Bakanlığı'na verilmiştir. Kısaca ifade etmek gerekirse, İç Güvenlik Bakanlığı kritik altyapı güvenliği konusunda sorumlu ve tam yetkili makam haline gelmiştir. İkinci olarak ortaya konulan araç güvenlik tedbirleri için takip edilecek ortak bir kontrol belgesinin oluşturulmasıdır. Millî Standartlar ve Teknoloji Enstitüsüne bir yıl içerisinde Siber Güvenlik Çerçevesi belgesinin yayımlanması görevi verilmiştir. Söz konusu belgenin kullanım maksadı, kritik altyapı güvenliğinde takip edilecek standartları belirlemek, çözüm esasları ortaya

koymak ve bu alandaki güvenlik için tüm paydaşlar arasında bütünsel devlet anlayışını yansıtan ortak bir hareket tarzı oluşturmaktır.

Caydırıcılık Metodu: Kritik altyapı güvenliği konusu daha önce birçok resmî belgede ele alınmakla birlikte Başkanlık Siyaset Direktifi-21 ve İcra Emri-13636 belgelerinde güvenlik artırıcı tedbirlerin artırılması bağlamında oldukça somut adımlar atıldığı görülmektedir. Gerek sorumlu birimlerin tayin edilmesi gerekse güvenlik standartlarının oluşturulması ve takibinde izlenecek yol haritalarının teknik detayları ihtiva edecek şekilde tasarlanması savunma artırıcı tedbirlere net bir örnek bir örnek teşkil etmektedir. Bu doğrultuda ilgili belgelerde ikna yoluyla caydırıcılık metodunun takip edildiği çıkarımı yapılabilir.

- **İran, Kuzey Kore, Çin ve Rusya tarafından Gerçekleştirilen Siber Saldırıları (2012-2016)**

2012 yılından itibaren ABD devlet bağlantılı birçok kapsamlı siber saldırının hedefi olmuştur. İran'ın Devrim Muhafızları ile bağlantılı grupların gerçekleştirdiği iddia edilen saldırılarda bankacılık sistemleri ve New York yakınlarındaki bir baraj hedef alınmıştır. Çeşitli bankaların müşteri internet erişimlerine yönelik Ddos saldırıları on milyonlarca dolarlık ekonomik kayba mal olurken, diğer taraftan bir baraja ait su akış hızı kontrolleri geçici süre ile geçirilmiştir.²³² Özellikle baraja yapılan saldırı, siber uzayda yapılan etkilerin fiziksel ortamda yarattığı sonuçlar bakımından Stuxnet saldırısını akıllara getirmektedir. Nitekim İran'ın Cumhuriyet Muhafızlarına bağlı bir grup tarafından gerçekleştirilen saldırılar, ABD'li kaynaklar tarafından, Stuxnet sonrası İran'ın siber güç inşasının yansıması ve uğradığı zararın misillemesi olarak yorumlanmıştır. Stuxnet saldırısını Pandora'nın kutusunun açılışı olarak niteleyen yetkililerden bir siber güvenlik şirketi CEO'sunun siber uzayı ve ABD politikalarını

²³² Thomas Brewster ve Forbes Staff, "U.S. Accuses 7 Iranians Of Cyberattacks On Banks And Dam", Forbes, 24 Mart 2016, <https://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/?sh=6e7a30c37255>; Mark Thompson, "Iranian Cyber Attack on New York Dam Reveals Future of War", Time, 24 Mart 2016, <https://time.com/4270728/iran-cyber-attack-dam-fbi/>; Caitlin McFall ve Jake Gibson, "FBI Charges Three Iranians in Cyber Attacks Targeting Local US Governments, Power Companies", FoxNews, 14 Eylül 2022, <https://www.foxnews.com/politics/fbi-charges-three-iranians-cyber-attacks-targeting-local-us-governments-power-companies>.

eleştirici şu ifadeleri dikkat çekicidir: “Eğer bir cam odada bulunuyorsanız birbirinize taş atmamalısınız.”²³³

İran tarafından gerçekleştirilmiş olan siber saldırıları Kuzey Kore ve Çin saldırıları takip etmiştir. Sony Yapım’a karşı gerçekleştirilen siber saldırılar sonucunda Holywood film sektöründe devam eden çekimler, anlaşmalar ve çalışan bilgileri gibi kapsamlı bir veri havuzunu ele geçirilmiş ve kötü amaçlı siber faaliyetlerde kullanılmak üzere söz konusu veriler satışa çıkarılmıştır.²³⁴ Kuzey Kore devleti bağlantılı Lazarus adlı grubun gerçekleştirdiği saldırı sonucu ABD ilk kez bir devleti kendine yönelik siber saldırı yapmakla resmî olarak suçlamış, bu doğrultuda Obama yönetimi ticari yaptırımlara alan açan bir icra emri yayınlamış, bağlantılı kişilerin banka hesaplarına el konulmuş, üç kişi hakkında soruşturma açılmıştır.²³⁵ Diğer taraftan 2014 yılında ortaya çıkan olayda Çin devleti ile bağlantılı kişilerin nükleer santral, güneş enerjisi, metal endüstrisi gibi kritik altyapıların ağlarına sızarak casusluk faaliyetlerinde bulunduğu ve ele geçirmiş olduğu hassas ticari sırlar ve işletim bilgileri ile Çinli firmalara haksız rekabet üstünlüğü sağladığı tespit edilmiştir.²³⁶ Dahası, söz konusu siber saldırıların C-17 Kargo Uçağı, F-22 ve F-35 Savaş Uçağı sistemlerine ait bilgileri sızdırma amaçlı olarak gerçekleştiği ortaya atılan iddialar arasındadır.²³⁷ Siber casusluk faaliyetini icra ettiği tespit edilen altı Çin Halk Kurtuluş Ordusu mensubu altı Çin vatandaşı için 5-15 yıl arasında hapis istemiyle dava açılmıştır.²³⁸

²³³ Ellen Nakashima, “Iran blamed for cyberattacks on U.S. banks and companies”, Washington Post, 21 Eylül 2012, https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html.

²³⁴ Andrea Peterson, “The Sony Pictures hack, explained”, The Washington Post, 18 Aralık 2014, <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>.

²³⁵ Steve Holland ve Matt Spetalnick, “Obama Vows U.S. Response to North Korea over Sony Cyber Attack”, Reuters, 19 Aralık 2014, <https://www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141219>; Dan Roberts, “Obama Imposes New Sanctions against North Korea in Response to Sony Hack”, The Guardian, 02 Ocak 2015, <https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview>.

²³⁶ “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage”, ABD Adalet Bakanlığı, 19 Mayıs 2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

²³⁷ Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, Second edition (New York: Public Affairs, 2017), 111-13.

²³⁸ “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage”.

Siber uzayda ABD'ye yönelik tehditlerin en fazla ses getireni 2016 yılında gerçekleştirilen Rusya bağlantılı saldırı olmuştur. Donald Trump ve Hillary Clinton arasında geçen 2016 Başkanlık seçimleri öncesi Rus İnternet Araştırma Ajansı bağlantılı gruplar Trump lehine seçimlerin sonuçlanması için Clinton aleyhine birtakım iletişim içeriklerini kamuoyuna servis etmiş, sahte hesaplar açarak dezenformasyon faaliyetlerinde bulunmuş ve seçmen kayıt veri tabanlarına erişim sağlayarak seçmen bilgilerini ele geçirmiştir.²³⁹ Her ne kadar ABD'li yetkililer tarafından müdahalenin seçim sonuçlarını değiştirici bir etkisi bulunmadığı ifade edilse de demokratik sürecin işleyişine yapılan bu saldırı, egemenlik hakları kapsamında ABD ve uluslararası ortamda büyük yankı uyandırmıştır. Saldırıya yanıt olarak bir icra emri yayımlayan Obama yönetimi, Rus istihbarat servislerine yönelik kapasitesini genişleterek 35 Rus diplomatını sınır dışı etmiştir.²⁴⁰

- **İcra Emri-13687-Kuzey Kore'ye Ek Yaptırımların Uygulanması-2015²⁴¹**

2015 yılı Ocak ayında yayımlanan bu icra emri, doğrudan Kuzey Kore yönetimine yönelik ekonomik yaptırımları ele almaktadır. Belge, 2014 yılında gerçekleşen Sony yapım şirketine yönelik saldırı dolayısıyla Holywood film endüstrisinin maruz kaldığı zararlara bir tepki niteliği taşımaktadır.

Tehdit Algılaması: Diğer belgelerden farklı olarak icra emrinin doğrudan tek bir devlete, Kuzey Kore'ye yönelik olarak kaleme alındığı görülmektedir. Bu doğrultuda ilk kez somut bir şekilde bir devlet aktörü, gerçekleştirmiş olduğu siber saldırı sebebiyle icra emrinin esas konusu olmuştur. Söz konusu durum, siber güç dengesinde ABD karşısında diğer uluslararası aktörlerin gelmiş olduğu kabiliyet derecesini teyit eder niteliktedir.

²³⁹ Abigail Abrams, "Here's What We Know So Far About Russia's 2016 Meddling", Time, 18 Nisan 2019, <https://time.com/5565991/russia-influence-2016-election/>; Kim Zetter, "How Close Did Russia Really Come to Hacking the 2016 Election", 26 Aralık 2019, <https://time.com/5565991/russia-influence-2016-election/>.

²⁴⁰ Lauren Gambino ve Sabrina Siddiqui, "Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking", The Guardian, 30 Aralık 2016, <https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack>.

²⁴¹ "İcra Emri-13687" (ABD Başkanlık Makamı, Ocak 2015), [https://www.govinfo.gov/content/pkg/DCPD-201500002/pdf/DCPD-201500002.pdf#:~:text=\(a\)%20Any%20transaction%20that%20evades,in%20this%20order%20is%20prohibited](https://www.govinfo.gov/content/pkg/DCPD-201500002/pdf/DCPD-201500002.pdf#:~:text=(a)%20Any%20transaction%20that%20evades,in%20this%20order%20is%20prohibited).

Ağırlık noktaları: Belgenin ağırlık noktaları, uygulanacak ekonomik yaptırımların niteliğinin ve söz konusu yaptırımların hedeflediği kesimin ortaya konulmasıdır.

Amaçlar: Belgede Kuzey Kore tarafından gerçekleştirilen eylemin Amerikan ulusal güvenliğine, dış politikasına ve ekonomisine zarar verdiği ve uluslararası hukuk teamüllerine aykırı davrandığı ifade edilmiştir. Buradan hareketle, gerçekleştirmiş olduğu aykırı eylemlerden ötürü sorumlu tutulması, gelecekteki muhtemel benzer eylemlerinden alıkonulması ve diğer kötü niyetli aktörlere örnek teşkil etmemesi maksadıyla cezai yaptırımlara maruz bırakılması amaçlanmaktadır.

Araçlar: Belgede ifade edilen cezai yaptırım ekonomik varlıkların dondurulmasıdır. Bu doğrultuda Hazine Bakanlığı'na verilen yetki ile birlikte;

- a. Kuzey Kore hükümeti veya Kore İşçi Partisi'ne bağlı kurumların,
- b. Kuzey Kore hükümeti yetkililerinin,
- c. Kuzey Kore hükümeti tarafından ekonomik, teknolojik veya hizmet desteği alan şahıs ve kurumların,
- d. Kuzey Kore hükümeti tarafından kontrol edilen veya onun adına doğrudan/dolaylı icrai eylemlerde bulunan şahıs ve kurumların ABD sınırları içerisinde bulunan bütün malvarlıklarına bloke konulması kararlaştırılmıştır.

Caydırıcılık Metodu: Belgede herhangi bir suç tanımı veya gerekçe anlatımına gidilmeksizin Kuzey Kore Hükümeti bağlantılı olma kriteri yaptırımın uygulanması için yeterli olarak ifade edilmiştir. Bu durum, caydırıcılığın temel bileşenlerinden, saldırgan aktöre verilecek mesajın sert bir şekilde uygulandığını göstermektedir. Sony saldırısı özelinde, Amerikan menfaatlerinin siber yollar ile saldırıya uğraması, Kuzey Kore'ye yönelik caydırıcılık stratejisinin başarısız olduğunun bir işaretidir. Gelecekte meydana gelebilecek benzer saldırılardan korunmak maksadıyla cezai yaptırım kararını alan ABD yönetimi bu icra emri ile birlikte söz konusu yaptırımların ekonomik minvalde gerçekleşeceğini göstermiştir. Ceza yoluyla caydırıcılık metodunun bir örneği olan bu durum, önceki Obama dönemi tedbirlerine benzer şekilde alan içi siber misilleme saldırılarından ziyade alan dışı uygulamalara başvurulduğu stratejinin bir diğer örneğidir.

- **Ulusal Güvenlik Stratejisi (2015)²⁴²**

Obama'nın ikinci başkanlık döneminin güvenlik algısını yansıtan 2015 Ulusal Güvenlik Stratejisi, 2010 yılında yayımlanan versiyonunun yarısı kadar uzunlukta olup güvenlik konularını daha genel ifadelerle ele almaktadır. Belgede küresel anlamda gittikçe birbirine bağlı hale gelen günlük hayatın yaratmış olduğu hassasiyet ve fırsatlara değinilmektedir. ABD liderliğine olan ihtiyaç vurgulanırken aynı zamanda kaynakların sınırsız olmadığı hatırlatılmakta, "stratejik sabır ve süreklilik" ilkelerinin önemine dikkat çekilmektedir.

Tehdit algılaması: 2010 yılı Güvenlik Strateji belgesinde siber güvenlik konusu, güvenlik başlığı altında belirlenmiş olan yedi gündem maddesinden biriyken, bu belgede siber güvenliğe "Ortak Alanlara Erişim Temini" başlığı altında yer verildiği görülmektedir. Hava ve deniz alanları gibi ortak coğrafi alanların güvenli ortak kullanımına benzer bir yaklaşım ile internetin kesintisiz ve "güvenli" kullanımı savunulmaktadır. Söz konusu vurgunun bir sebebi olarak 2012-2016 yılları arasında gerçekleşen ve özellikle bankacılık sektörünü hedef alan Ddos saldırının varlığı akla getirilebilir. Buna ek olarak, önceki belgelerde olduğu gibi, kritik altyapıların siber saldırılar karşısındaki hassasiyetleri tehdit algılamasının bir diğer konusunu teşkil etmektedir.

Ağırlık noktaları: Belgede internetin ABD topraklarında doğduğu ifade edilerek, bugün gelinen noktada ağ bağlantılı küresel ekonominin korunmasında ve ortak yapılageliş biçimlerinin meydana getirilmesinde ABD'nin öncü rolüne dikkat çekilmektedir.

Amaçlar: Belgede açık, güvenli ve erişilebilir bir internet ortamının muhafazasının sağlanması, kritik altyapıların korunması ve dolayısıyla bu iki boyutun doğrudan etkilediği Amerikan menfaatlerinin korunması amaçlanmaktadır.

Araçlar: Belirlenen amaca erişmek için ortaya konulan araçlar; kritik altyapı güvenliğinde kamu-özel sektör yardımlaşması, siber güvenlik çerçevesinin işletilmesi, siber suçlulara karşı etkin yargı süreçlerinin izlenmesi ve uluslararası iş birliğinin tesis edilmesidir.

²⁴² "Ulusal Güvenlik Stratejisi-2015" (ABD Başkanlık Makamı, Şubat 2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.

Caydırıcılık Metodu: Belgenin siber güvenlik bölümü kısa bir yer teşkil etmesine rağmen üç farklı caydırıcılık metodunu kapsayan bir caydırıcılık stratejisi ortaya koyduğu görülmektedir. Kritik altyapıların güvenliği için hazırlanan Siber Güvenlik Çerçevesi Belgesi savunma ve dayanıklılık artırıcı tedbirler kapsamına girmektedir. Dolayısıyla ikna ve dayanıklılık yoluyla caydırıcılığın kullanımına işaret etmektedir. Küresel çapta ABD liderliği vurgusu yapılmakla birlikte diğer aktörler ile iş birliği ve ortak davranış biçimlerinin oluşturulmasına dikkat çekilmektedir. Böylece normlar yolu ile caydırıcılık yaklaşımı diğer Obama dönemi belgelerinde olduğu gibi varlığını sürdürmektedir. Ceza yolu ile caydırıcılık metoduna ilişkin ifadeler ise dikkat çekicidir. Başkanlık Siyaset Direktifi-21 ve İcra Emri-13636'daki anlayışa uygun şekilde, tespit edilen siber saldırılara karşı siber uzayda başvurulabilecek misillemelerden söz edilmemektedir. Bunun yerine saldırganları bir devlet yerine kişi olarak ele alıp şahıslara yönelik adli süreçlerin yürütülmesinin gerekliliği ortaya konulmaktadır. Bu doğrultuda ceza yoluyla caydırıcılığın ceza bileşenin temkinli şekilde ele alındığı ve tırmandırıcı davranışlardan kaçınıldığı görülmektedir.

- **İcra Emri-13691- Özel Sektör Siber Güvenlik Bilgi Paylaşımını Geliştirme (2015)²⁴³**

Tehdit Algılaması: Belgede siber saldırıların kamu sağlığını, kamu güvenliğini, ulusal ve ekonomik güvenliği tehdit ettiği ifade edilerek söz konusu saldırıların toplumun tüm paydaşlarını olumsuz yönde etkilediğine işaret edilmektedir.

Ağırlık Noktaları: Karşı karşıya olunan tehdit ortamında ortak güvenlik tedbirlerinin önemine işaret edilmektedir. Ağırlıklı olarak özel sektör-kamu arasındaki bilgi paylaşımının geliştirilmesi konusu ele alınmaktadır.

Amaçlar: Belgenin ana amacı siber güvenlik düzleminde kamu-özel sektör yardımlaşmasını geliştirmektir. Siber güvenlik hazırlık ve reaksiyon seviyesinin artırılması maksadıyla ortaklıkların, bilgi paylaşım forumlarının ve işbirlikçi girişimlerin önünü açan bir ortamın hazırlanması hedeflenmektedir.

Araçlar: Belgede söz konusu amaçları gerçekleştirmede İç Güvenlik Bakanlığı merkezi bir rol üstlenmektedir. Bu kapsamda bakanlık sektör, bölge ve ilgi alanı bazında Bilgi

²⁴³ “İcra Emri-13691 Özel Sektör Siber Güvenlik Bilgi Paylaşımını Geliştirme” (ABD Başkanlık Makamı, Şubat 2015), <https://www.govinfo.gov/app/details/DCPD-201500098>.

Paylaşımı ve Analiz Kurumlarının oluşumunu ve gelişimini destekleyecektir. Bu kurumlar vasıtasıyla özel sektör paydaşları ile daha kapsayıcı bir şekilde etkileşim hedeflenmektedir. Söz konusu etkileşim sürecinde kamu-özel sektör arasında örnek uygulamalar ve olay raporlarının paylaşımını öngören platformların oluşturulması, tespit, hasar minimizasyonu ve reaksiyon için ortak kabiliyetlerin geliştirilmesi öngörülmektedir. Bahse konu olan süreçlerde özel sektör katılımının gönüllülük esasına bağlı olması ile mahremiyet haklarının korunması üzerinde önemle durulan iki konudur.

Caydırıcılık Metodu: Belge; tespit, teşhis, hasar minimizasyonu ve karşı reaksiyon adımlarını, ortak kabiliyetlerin geliştirilmesini, bilgi paylaşımının artırılmasını ve bu doğrultuda toplumun tüm paydaşları ile topyekûn bir savunma anlayışını benimsemektedir. Bu açıdan ikna ve dayanıklılık yoluyla caydırıcılık metodunun belirgin bir şekilde öne çıktığı görülebilir. Zira belgenin öngördüğü kamu-özel sektör iş birliği çerçevesi siber güvenlikte savunma tedbirlerinin artırılmasını, muhtemel saldırılara yönelik proaktif önlemlerin geliştirilmesini içermektedir. Beyaz Saray bu belge yoluyla muhtemel saldırgan aktörlere saldırılarının başarısız olacağı mesajını vermektedir.

- **İcra Emri-13694- Önemli Kötü Amaçlı Siber Faaliyetlerde Bulunan Şahıslarının Malvarlıklarının Bloke Edilmesi (2015)²⁴⁴**

Kötü amaçlı siber faaliyetlerin yoğunlaşması ve kritik altyapılara yönelik saldırı tehdidinin artış göstermesi üzerine aynı yıl Kuzey Kore hükümeti bağlantılı şahıs ve kurumları kapsayacak şekilde tasarlanan yaptırım uygulaması, bu icra emri ile birlikte herhangi bir milleti işaret etmeyecek şekilde kapsam artışına gitmiştir.

Tehdit algılaması: Belgede ABD vatandaşlığı dışında kalan deniz aşırı şahıs veya kurumlara işaret edilmektedir. Bu aktörlerin siber yollar ile ABD ulusal güvenliğini, dış politikasını, ekonomisini ve finansal istikrarını hedef alan tehditler konu alınmaktadır.

Ağırlık Noktaları: Belgede ABD Hazine Bakanlığı'nın ekonomik yaptırım uygulayacağı kişileri belirlemesi için takip edeceği kriterler ortaya konulmaktadır.

²⁴⁴ “İcra Emri-13694” (ABD Başkanlık Makamı, Nisan 2015), <https://onlinelibrary.wiley.com/doi/10.1111/j.1741-5705.2009.03698.x>.

Amaçlar: Belgede ABD menfaatlerine karşı siber yollar ile saldırı gerçekleştiren fakat ABD topraklarında ikamet etmemesi ve ABD vatandaşlığı bulunmaması sebebiyle caydırıcı cezai yaptırımlar ile karşılaşmayan şahıs ve kurumlara tedbir getirmek istenmektedir. Bu doğrultuda daha önce mevcut olan ve caydırıcılığı engelleyen yasal boşlukların önüne geçilmesi amaçlanmaktadır.

Araçlar: Belgede ABD ulusal güvenliğine ve ekonomik istikrarına zarar veren siber eylemlere girişen şahıs ve kurumların cezalandırılması öngörülmektedir. Söz konusu cezalandırmanın Hazine Bakanlığı tarafından, mal varlığı blokesi şeklindeki ekonomik yaptırımı ihtiva ettiği ifade edilmiştir. Söz konusu yaptırımların uygulanacağı kişilerin belirlenmesi için,

- a. ABD kritik altyapılarına zarar vermek,
- b. Bilgi hırsızlığı yoluyla ekonomik rekabette haksız avantaj sağlamak ve bu şekilde ABD ekonomik menfaatlerine zarar vermek,
- c. İnternet ulaşımını engelleyici veya kesintiye uğraticı faaliyetlerde bulunmak gibi belirli kriterler ortaya konulmuştur.

Caydırıcılık Metodu: Belge her ne kadar Kuzey Kore hükümeti bağlantılı kişilere uygulanan cezai yaptırımların ABD vatandaşlığı dışındaki bütün siber saldırgan aktörlere genişletilmesini esas alsın da yaklaşım bakımından daha proaktif bir tutumu benimsemektedir. Zira Kuzey Kore örneğinde başarısız bir caydırıcılık örneği mevcutken bu icra emrinde gelecekte karşılaşılabilecek deniz aşırı siber saldırılara karşı misilleme tehdidi vurgulanmaktadır. Ceza yoluyla caydırıcılık metodunun bir örneğini gösteren belgede tedbir bakımından uygulanan davranış biçimi alan dışı niteliktedir. Diğer örneklerde de olduğu gibi siber saldırılara karşı ceza tehdidi siber kabiliyetlerden ziyade farklı kabiliyetler üzerinden şekillendirilmiştir.

• **İcra Emri-13718-Ulusal Siber Güvenliği Geliştirme Komisyonu²⁴⁵ (2016)**

İcra Emri-13718, kritik altyapı savunmasının geliştirilmesine dair ABD Başkanına somut önerilerde bulunması öngörülen ve alanında uzman kişilerden oluşturulacak siber güvenlik komisyonunun kurulmasını öngören bir belgedir.

²⁴⁵ “İcra Emri-13718” (ABD Başkanlık Makamı, Şubat 2016).

Tehdit algılaması: Belgede doğrudan tehditlere ilişkin ifadeler yer almamakla birlikte komisyona verilen öneri görevlerinin kapsamı, internet erişiminin sürekliliği, bilgi ağlarının ve kritik altyapılarının güvenliğine işaret etmektedir.

Ağırlık noktaları: Belgede komisyonun yapısı, görevleri ve siber güvenliğe ilişkin hangi konularda önerilerde bulunması beklendiği ifade edilmektedir.

Amaçlar: Belgede toplumun bütün kesimlerini dahil edecek şekilde güvenliğin sağlanması ve vatandaşların farkındalık düzeylerinin artırılması hedeflenmektedir. Böylece belgenin amaçlarının iki ana temada toplandığını ifade etmek mümkündür:

1. Siber güvenlik tedbirlerini artırıcı uzman görüşlerini uygulama için hazır hale getirmek
2. Toplumun bütün paydaşlarında siber güvenliğe ilişkin durumsal farkındalığı geliştirmek

Araçlar: Belgede söz konusu amaçları sağlamak için oluşturulan komisyonun sene sonunda ABD Başkanı'na bir rapor sunması öngörülmektedir. Söz konusu raporda siber uzayda güvenliğin daha etkin sağlanmasına yönelik şu konu başlıklarına bulunmaktadır:

- Yönetim hizmetleri
- Kritik altyapı güvenliği
- Siber kabiliyet araştırma ve geliştirme faaliyetleri
- Siber iş gücünün oluşturulması
- Kimlik tanımlama
- Durumsal farkındalık ve eğitim.

İlgili konu başlıkları kapsamında uzman kişilerin görüşleri ile oluşturulması öngörülen yol haritası, bahse konu olan topyekûn siber güvenlik hedefine ulaşmak için somut bir araç olarak sunulmaktadır.

Caydırıcılık Metodu: Belgede uzman kişilerin göreve çağırılması ve muhtemel hassasiyet alanlarına yönelik öneride bulunma görevi verilmesi siber uzaya dair faaliyetlerde savunma ve dayanıklılık tedbirlerini artırıcı bir adımdır. Bu yolla bütünsel devlet anlayışını yansıtan bir kamu-özel sektör-akademi iş birliği öngörülmektedir. Dayanıklılık ve savunma alanında ortaya konulan bu tedbir artırıcı eylem ikna ve dayanıklılık yoluyla caydırıcılık metodunun uygulanmasına hizmet etmektedir.

- **Savunma Bakanlığı Siber Stratejisi (2015)** ²⁴⁶

2015 yılında yayımlanan Savunma Bakanlığı Siber Strateji Belgesi, Bakanlığın siber tehditlere ilişkin yaklaşımlarını açık bir dille betimleyen detaylı bir belge niteliğindedir. 2011 yılında yayımlanan bir önceki belgeye kıyasla Siber tehditlerle mücadeleye daha detaylı yer verilmiştir. Bu mücadelede Bakanlığa düşen roller, inşa edilen ofansif ve defansif kabiliyetler ev izlenen kapasite artırımı süreçlerine ilişkin gerek kamuoyuna gerekse rakip aktörlere mesaj niteliği taşıyan bir bildiri niteliği taşımaktadır.

Tehdit algılaması: 2011 yılı belgesine kıyasla tehdit aktörlerini daha açıkça niteleyen belgede tehditlerin devletlerden, devlet dışı örgütlerden, siber suçlulardan veya bunların birlikte hareket ettiği hibrit yapılardan gelebildiği kompleks yapı tasvir edilmektedir. Siber saldırıların politik bir araç haline gelmesinin uluslararası ilişkilerde tehlikeli bir trend haline geldiği vurgulanmaktadır. Belgede hassas veri sistemlerinin söz konusu aktörlere iştah kabartıcı hedefler sunduğu ve bu hassasiyetlerin istismarının stratejik avantajlar yaratabildiği ifade edilmektedir. Özel sektöre ayrı bir yer verilen tehdit değerlendirmesinde, siber altyapıların %90'ının özel şirketlerin kontrolünde olduğu hatırlatılmaktadır. Dolayısıyla etkin bir siber savunmanın ancak özel sektör bilinci ve çabası doğrultusunda mümkün olabileceği dile getirilmektedir. Bu ifade, siber savunmanın federal bir sorumluluk olduğu ve özel sektör ile koordinasyonu tamamen devlet aygıtına yükleyen diğer belgelerden farklı bir noktadadır. Nitekim bütünsel bir durumsal farkındalık eksikliğinin yarattığı tehlikelere dikkat çekilmektedir.

Ağırlık noktaları: Belgede ağırlıkla üzerinde durulan konular, Savunma Bakanlığı'nın siber güvenliğe ilişkin vazifeleri, bu vazifelerin yerine getirilmesinde belirlediği stratejik amaçlar, amaçların icrasında başvurulacak kapasite geliştirme süreçleri ve bütün bu basamaklara ışık tutacak caydırıcılık yaklaşımlarıdır.

Amaçlar: Savunma Bakanlığı'nın siber uzaya ilişkin sorumluluklarının belirtilmesi sonrasında söz konusu alanlara ilişkin varılması hedeflenen beş stratejik amaç sıralanmaktadır:

1. Siber uzay harekâtının yürütülmesi için gerekli kuvvet ile kapasiteyi inşa ve muhafaza etmek

²⁴⁶ "Savunma Bakanlığı Siber Stratejisi-2015" (ABD Savunma Bakanlığı, Nisan 2015), <https://nsarchive.gwu.edu/document/21384-document-25>.

2. Savunma Bakanlığı bilişim ağlarını savunmak, bakanlık verilerini korumak ve gerçekleştirilen harekâtlara yöneltilen riskleri azaltmak
3. Amerika topraklarını ve Amerikan menfaatlerini yıkıcı etkiler doğuran siber saldırılara karşı korumak için hazırlıklı olmak
4. Bütün aşamalarda çatışma ortamını şekillendirmek ve çatışma tırmanışını kontrol altında tutmak için geçerli seçenekler üretmek ve bunları hazır bulundurmak,
5. Ortak tehditleri caydırmak ve uluslararası güvenliğe katkı sağlamak için uluslararası ittifak ve ortaklıklar kurmak

Araçlar: Söz konusu amaçlara ulaşmak için ortaya konulan süreç basamakları oldukça detaylı bir şekilde ele alınmıştır. Bu doğrultuda kuvvet kapasitesinin inşası için “Siber Görev Kuvveti” birimi ön plana çıkmaktadır. 2013 yılında Savunma Bakanlığı tarafından başlatılan ve 6200 personelden oluşan 133 Siber timinin teşkil edilmesini öngören Siber Görev Kuvveti Konseptine ilişkin söz konusu iş gücünün geliştirilmesi konusuna dikkat çekilmektedir. Sürekli bir eğitim atmosferinin oluşturulması, personel için teşvik edici kariyer olanaklarının ortaya konulması, aktif bir değerlendirme ve geri besleme sisteminin teşkilini kapsayan yol haritasında sivil iş gücünün temini ve özel sektör ile iş birliği konularına özellikle değinilmektedir.

Savunma Bakanlığı ağlarının korunması hususunda Tekil Güvenlik Mimarisi kavramı dikkat çekicidir. Şöyle ki kuvvet komutanlıklarının kendine has dinamikleri ön planda tuttuğu farklılaşan siber savunma yapılanmalarının terkedilmesi gerektiği ifade edilmektedir. Bunun yerine daha gelişmiş tehdit ve hassasiyet belirleme tekniklerini ihtiva eden ve bütünsel bir durumsal farkındalık imkânı sunan kapsamlı bir güvenlik yapısının kurulması öngörülmektedir.

Daha geniş bir tehdit tanımlamasını ihtiva eden ABD menfaatlerinin korunmasına ilişkin olarak siber saldırıların gerekirse gerçekleşmeden önce imhası ve etkin bir savunmanın tesisi vurgulanmaktadır. Bunu sağlamak noktasında etkin bir araç olarak istihbarat birimleri ile sürekli koordinasyonun altı çizilmektedir. Belgede tüm tehditlere karşı yalnızca siber kabiliyetler ile mücadelenin yetersiz olduğu ifade edilmektedir. Bunun yerine siber seçeneklerin de masada olduğu politik, ekonomik, askeri ve hukuki tedbirler listesinin hazır bulundurulmasının gerekliliği vurgulanmaktadır. Son olarak ABD menfaatlerini küresel anlamda tehdit eden siber faaliyetlere ilişkin müttefik

devletler ile istihbarat paylaşımı, kötü amaçlı yazılımlara karşı birlikte mücadele ve ortak kabiliyetlerin oluşturulması gibi girişimlerin yapılması gerektiği dile getirilmektedir.

Caydırıcılık Metodu: ...siber tehditlere karşı caydırıcılık yalnızca siber politikaların revizesi ile sağlanamaz. Bunun yanında emare ve uyarıların iletimi, politikaların ilanı, defansif konumlanma, etkin yanıt prosedürleri ve genel Amerikan ağlarının dayanıklılığını ihtiva eden davranışlar bütünü benimsenmelidir.

Belgenin 10. Sayfasında yer alan bu ifade, Savunma Bakanlığının caydırıcılık anlayışını özetler niteliktedir. Savunma Bakanlığı'nın koordinatör rolü, özel sektör ile iş birliği, etkin iş gücünün oluşturulması gibi tedbirler savunma ve dayanıklılık yoluyla caydırıcılık metoduna hizmet etmektedir. Diğer taraftan saldırıların olgunluğa erişmeden önlenmesi, devletin tüm cezai araçlarının kapsam içine alındığı bir yaptırım listesinin oluşturulması ve saldırganın belirlenmesi için istihbarat örgütleri ile iş birliği aşamaları ceza yoluyla caydırıcılığa örnek teşkil etmektedir. Aslında bu belge, doğrudan caydırıcılık metotlarını açık bir dille ifade etmesi bakımından bir ilki teşkil etmektedir. İkna, dayanıklılık ve ceza kavramlarının ayrı paragraflar halinde açıkça ele alınmaktadır. Yazıda ceza yoluyla caydırıcılık kapsamında Obama yönetimi tarafından benimsenen “ABD tarafından belirlenen yer, zaman ve şekilde karşılık verilmesi” hususu vurgulanmaktadır. Bunun yanında, ikna ve dayanıklılık metotlarının başarıya ulaşmasının yegâne yolu olarak özel sektör ile iş birliği gösterilmektedir.

- **Başkanlık Siyaset Direktifi-41: ABD Siber Olay Koordinasyonu (2016)²⁴⁷**

2016 yılında yayımlanan belgede yaşanan bir siber saldırıya verilecek tepkiye ilişkin kurumların rolleri ve sorumlulukları ortaya konulmaktadır.

Tehdit algılaması: Belgede siber saldırıların nitelik bakımından gelmiş olduğu gelişmiş noktaya dikkat çekilmektedir. Söz konusu tehditlerle ancak ilgili kişi, kurum ve kuruluşların koordineli bir şekilde görevlerini yerine getirmesiyle başa çıkılabileceği belirtilmektedir.

Ağırlık noktaları: Belgede siber olaylara verilecek tepkide izlenmesi gereken beş prensibe yer verilmektedir:

²⁴⁷ “Başkanlık Siyaset Direktifi-41” (ABD Başkanlık Makamı, Temmuz 2016), <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.

1. Sorumluluk paylaşımı: Ulusal siber ağların korunmasında kişi, özel sektör ve devlet kurumlarının ortak sorumluluğu.

2. Risk-Odaklı Tepki: Uğranılan saldırılara verilecek tepkilerin belirlenmesinde söz konusu tehditlerin taşıdığı risk faktörlerinin ve ayrılması gereken kaynakların göz önünde bulundurulması.

3. Etkilenen kurumlara karşı hassasiyet: Başta özel sektör olmak üzere siber saldırılardan etkilenen birimlerin gizlilik haklarına riayet ederek tepki planlarının oluşturulması.

4. Devlet çabasında birlik: Devlet kurumlarının birbiri ile etkin koordinasyonu ve yerel otoriteler ile yardımlaşma.

5. Yeniden düzenleme ve toparlanmanın sağlanması: Saldırıya uğrayan kurumlara ilişkin soruşturma faaliyetlerinin yoğunluğunun kurumun operatif etkinliğini sekteye uğratmayacak şekilde ilerletilmesi.

Amaçlar: Siber olaylara karşı tehdit-odaklı reaksiyon, birim-odaklı reaksiyon ve istihbarat paylaşımı olmak üzere üç farklı boyutta kurumlararası eş güdümün sağlanması hedeflenmektedir.

Araçlar: Belgede kritik altyapıların savunması için daha önce ortaya konulmuş olan sorumluluk paylaşımları üzerinden hareket edilerek koordinasyon mekanizmaları kurulması öngörülmektedir. Bu doğrultuda federal ve sivil paydaşlar arasında koordinasyonu sağlayacak olan Birleşik Siber Koordinasyon Grubunun teşkili kararlaştırılmıştır. Esas yetkili kurum ve sektöre özel kurumların birlikte çalışmasını sağlayacak olan grup, siber saldırılara verilecek reaksiyonlara ilişkin geliştirme ve uygulama süreçlerini takip edecektir. Bu kapsamda reaksiyonun boyutu ile bağlantılı şekilde esas yetkili kurum olarak belirlenen bakanlıklar aşağıdaki gibidir.

Reaksiyon Tarzı	Esas Yetkili Kurum	Esas Yetkili Kurumun Sorumlu Birimi
Tehdit-odaklı	Adalet Bakanlığı	FBI ve Ulusal Siber Soruşturma Müşterek Görev Kuvveti
Birim odaklı	İç Güvenlik Bakanlığı	Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi
İstihbarat Paylaşımı	Ulusal İstihbarat Başkanlığı	Siber Tehdit İstihbaratı Entegrasyon Merkezi

Tablo 4: 41. Başkanlık Siyaset Direktifi Kapsamında Federal Kurumlara Verilen Sorumluluklar

Bu şekilde daha önce Başkanlık Siyaset Direktifi-21’de Kritik Altyapı Sektörlerine bir sorumlu bakanlık atama ve tedbir süreçlerini etkinleştirme girişiminin derinleştirildiği

görülmektedir. Şöyle ki öncelikle tehditlere karşı geliştirilecek reaksiyonlar kapsamında bir tanımlama ve sınıflandırmaya gidilmiştir. Tehdit, birim ve istihbarat konularından oluşan alt başlıklar yaratılarak verilecek reaksiyonun cinsine ve boyutuna yönelik bir tanımlamalar yapılmıştır. Buna ek olarak oluşturulan Birleşik Siber Koordinasyon Grubu, sektöre özel kurumların mevcut sorumlulukları devam etmek kaydıyla, Adalet ve İç Güvenlik Bakanlıkları ile Ulusal İstihbarat Başkanlığının esas yetkili kurum olduğu etkin bir reaksiyon sürecini yürütecek şekilde teşkil edilmiştir. Bu doğrultuda, bir önceki örneğinden farklı olarak Başkanlık Siyaset Direktifi-41'in, kritik altyapı güvenliğine ilişkin yalnızca tanımlama ve sorumluluk atama yaklaşımından bir adım öteye geçtiği görülmektedir. Verilecek reaksiyonun karakteristiğine uygun olacak koordinatör ve uygulayıcı makamları da saptadığı, mevcut sorunların çözümünde daha müdahil bir tavır sergilediği görülmektedir.

Caydırıcılık Metodu: Birleşik Siber Koordinasyon Grubunun teşkili, bu birime verilen sektöre özel kurum ve özel sektör paydaşlarını bir araya getirme görevi bütünsel bir devlet anlayışını ihtiva etmektedir. Kritik altyapı güvenliğinin etkinliğini artırmaya yönelik söz konusu girişimler ikna ve dayanıklılık yoluyla caydırıcılık kapsamına girmektedir.

Diğer taraftan reaksiyon tarzlarının doğrudan sektöre özel kurumların inisiyatifine bırakılmayarak öncelikle bir sınıflandırmaya gidilmesi önemlidir. Zira siber saldırılara karşı verilecek reaksiyonların her bir çeşidi farklı bir caydırıcılık metoduna tekabül etmektedir. Şöyle ki kritik altyapı savunma güvenliğini artırıcı tedbir, kontrol ve değerlendirme süreçlerini kapsayan birim-odaklı reaksiyon ikna yoluyla caydırıcılığa tekabül etmektedir. Buna karşın söz konusu sınıflandırmanın birinci maddesinde yer alan tehdit odaklı reaksiyon, saldırgan aktörlerin tanımlanmasına ve bedel ödetilmesine dayanmaktadır. Bahse konu olan reaksiyona esas yetkili kurum olarak Adalet Bakanlığı'nın atanması ise Obama yönetiminin ceza yolu ile caydırıcılıkta başvurduğu alanlar arası tedbir stratejisine denk düşmektedir.

- **İcra Emri-13757: Kötü Amaçlı Siber Faaliyetlere İlişkin Ulusal Acil Duruma Yönelik Ek Tedbirler (2016)**

Aralık 2016'da yayımlanan belge, ABD menfaatlerine zarar verme amacıyla kötü amaçlı siber faaliyetlere girişen ve ABD ile vatandaşlık bağı bulunmayan kişilere yönelik ekonomik yaptırımlarını içermektedir. Bu doğrultuda daha önce yürürlüğe

girmiş olan İcra Emri-13694'ün devamı niteliğindedir. Belgede mal varlıkları dondurulacak ilave şahıs ve kurumlara yer verilmektedir. Bu doğrultuda söz konusu belge, İcra Emri-13694 ile tehdit algılaması, ağırlık noktaları, amaçlar, araçlar ve caydırıcılık metodu yönlerinden herhangi bir farklılık göstermemektedir.

Obama'nın başkanlık dönemi etkileri ve yoğunluğu artan siber tehditlere karşı somut bir farkındalığın ortaya konulduğu bir güvenlik anlayışı ile başlamıştır. Nitekim başkanlığının henüz ikinci ayında yayımlanan Siber Politika Değerlendirme Belgesi zayıflık, hassasiyet ve kapasitenin belirlenmesi açısından bir durum tespiti niteliği taşımaktadır. Belgede ayrıca mevcut durumun ötesinde alınması gereken tedbirlere ilişkin bir vizyon ortaya konulmaktadır. ABD'nin sahip olduğu göreceli kuvvet üstünlüğünün siber uzayda paralel bir iz düşün bulmadığını ifade eden belgede tehditlerin meydana geldiği siber uzayın daha iyi anlaşılması ve ABD önderliğine tedbir mekanizmaları getirilmesi gerekliliği vurgulanmaktadır. İş birliği ve etkileşim kavramlarına sıklıkla başvuru belgede söz konusu kavramların kullanım biçimi ise uluslararası ve ulusal düzeyde farklılık göstermektedir. Şöyle ki siber tehditlere karşı diğer uluslararası aktörlerle yapılacak yardımlaşma daha çok ABD'nin doğru ve etkin uygulamaları ortaya koyması ve diğer aktörlerin onu takip etmesi şeklinde sunulmaktadır. Bu doğrultuda ortak karar ve rıza kanalı ile meydana gelen normlar yoluyla caydırıcılık stratejisinin bu aşamada ABD güvenlik yönetimi gündeminde olmadığı ifade edilebilir. Yardımlaşma kavramının tam anlamıyla karşılık bulduğu düzey ulusal düzeydir. Belgede siber tehditlerin toplumun tüm paydaşlarını etkilediği, sadece devlet marifetiyle alınacak tedbirlerin bu tehdit düzleminde yetersiz kalacağına değinilerek kamu-özel sektör-akademi iş birliğinin önemi ağırlıkla vurgulanmaktadır. Söz konusu iş birliği kapsamında gerçekleşecek siber güvenlik iş gücü yetiştirilmesi ve kritik altyapı savunmasının güçlendirilmesi konuları doğrudan savunma tedbirlerini artırıcı girişimler olup ikna ve dayanıklılık yoluyla caydırıcılık alanına girmektedir.

ABD yönetiminin siber uzayda diğer aktörlere liderlik etme yaklaşımının aynı yıl ortaya çıkan Stuxnet saldırısı ile evrimleştiği ifade edilebilir. Stuxnet saldırısı, Başkan Bush döneminde büyük bir gizlilikle başlayan ve Obama döneminde devam eden, İran'ın nükleer silah üretme sürecini siber saldırı yoluyla engelleme/geciktirme girişimidir. Saldırı siber uzaydaki güvenlik anlayışını kökten etkileyen bir kilometre taşı niteliğindedir. Zira bu saldırı ile ilk kez devlet eliyle başka bir devletin fiziksel

kapasitesinde siber yolla kinetik etkiler oluşturulmuş, kuvvet kullanım eşliğinde yeni bir seviyeye gelinmiştir. Böylece kritik altyapı tesislerinin söz konusu saldırılara karşı ne kadar hassas olduğu ortaya çıkmıştır. Gerçekleştirilen saldırı o zamana dek yaygın kanaat olan siber silahların yalnızca zayıfın kullanacağı bir asimetrik harp unsuru olduğunu fikrini çürütmüştür. Nitekim bir süper güç tarafından kullanılarak büyük güçler arasındaki siber rekabetin dozunu artırmıştır. Obama'nın bahse konu olan saldırı sonrası ABD'ye yöneltilebilecek tehditlerin muhtemel etkilerini görerek özellikle uluslararası alanda daha temkinli ve yatıştırıcı siber güvenlik politikaları izlediği ifade edilebilir. Bu yaklaşımın iki ana ürünü Siber Uzay Uluslararası Stratejisi ve 20. Başkanlık Siyaset Direktifi olmuştur.

Goldman'a göre 2011 tarihli Siber Uzay Uluslararası Stratejisi ABD Dışişleri Bakanlığı'nın günümüze dek yayımlanmış olduğu en yol gösterici siber belge durumundadır.²⁴⁸ Siber uzaya dair belirsizlik ve rekabet ortamına ilişkin istikrar arayışını ele alan belgede öne çıkan temel unsur Uluslararası normların inşa edilmesidir. Bu doğrultuda söz konusu strateji belgesi ABD'ye;

- Siber uzaydaki sorumlu davranış prensiplerin oluşturulması için görüş birliği oluşturulması ve bu doğrultuda vakit kaybetmeden diyalog kanallarını oluşturması,
- Siber uzay normlarına ilişkin uluslararası ortak anlayış inşası,
- Bahse konu olan gerekliliğin uluslararası örgütlerin gündemlerine taşınması,
- Kötü niyetli aktörlerin bu normları ihlal etmekten caydırılması,
- Siber güvenlik kapasite inşasına ön ayak olmak gibi birtakım misyonlar yüklemektedir.²⁴⁹

20. Başkanlık Siyaset Direktifi ile birlikte daha önce siber komutanlık bünyesinde olan ofansif siber harekât yürütme yetkisi devralınmış, nihai karar vericinin Başkan olduğu ve içinde ilgili bakanlıkların ve Ulusal Güvenlik Ajansının bulunduğu çok paydaşlı bir onay mekanizması kurulmuştur. Kurulan mekanizmanın ofansif siber harekâtın icrasını zorlaştırdığı kuşkusuzdur. Direktifin de bu şekilde süreci yavaşlatarak ani ve kontrolsüz ofansif siber eylemlerden kaçınmayı hedeflediği çıkarımı yapılabilir. Yine de direktifin

²⁴⁸ Robert Chesney, James Shires, ve Max Smeets, ed., *Cyberspace and Instability* (Edinburgh: Edinburgh University Press, 2023), 157.

²⁴⁹ A.g.e.

Stuxnet sonrası çıkan infial durumunu yatıştırdığını söylemek mümkündür. Muhtemel tehditlere karşı alternatif tedbirlerin gözden geçirilmesi için esneklik kazandırdığı iddia edilen direktif esasında askeri planlamanın yetki alanını önemli ölçüde kısıtlama yoluna gitmiştir.²⁵⁰ Sonuç olarak gerek Obama'nın kamuoyu önünde yaptığı çeşitli açıklamalarda, gerekse almış olduğu bürokratik tedbirler aracılığıyla ofansif siber operasyonları sınırlandırmasıyla siber gücün kullanımı konusunda diğer aktörlere gerginlik azaltıcı bir davranış kalıbı göstermiştir. Söz konusu davranışın tırmanmayı önleyici bir norm oluşturma çabası olduğu değerlendirilebilir.

Obama başkanlık döneminin en fazla öne çıkan siber güvenlik konu başlıklarından biri siber komutanlığın kurulmasıdır. Siber operasyonların icrasını tek bir çatı altında toplamayı amaçlayan oluşumun inşa süreci dikkat çekicidir. Zira Savunma Bakanlığı'na bağlı olan kuruluş, kapasite inşasının kolaylaştırılması ve ortak yeteneklerden faydalanılması amacıyla Ulusal Güvenlik Ajansı ile aynı yerleşkeye konuşlandırılmıştır. Başkanına her iki kurumun idare yetkisinin verildiği çift şapkalı bir statü verilmiştir. Caydırıcılık açısından değerlendirildiğinde, ofansif siber kabiliyetleri oluşturması ve kullanması öngörülen Siber Komutanlığın söz konusu hibrit konumu, dönemin siber güvenlik yaklaşımına uygun olacak şekilde askeri yetenekler üzerinde sivil kontrolünü kolaylaştıran bir mekanizma doğurmuştur. Kurumun ortaya koyacağı ofansif siber kabiliyetlere ilişkin direktör General Keith Alexander'ın "Benim görevim bütün ulusu değil, Savunma Bakanlığı ağlarını korumak" açıklaması Siber Komutanlığın ofansif kabiliyet bakımından ilk yıllarında mütevazı anlayışını yansıtır niteliktedir. Takip eden süreçte ise Savunma Bakanlığı tarafından yayımlanan Siber Uzay Politika Raporu, Savunma Bilimi Kurulu Raporu ve Siber Strateji Belgesi ofansif siber kabiliyetlerin diğer konvansiyonel ve nükleer kabiliyetler ile birlikte konumlandırıldığı kapsayıcı ve tehditkâr bir ceza yoluyla caydırıcılık profili resmetmektedir. Buna karşın Başkanlık tarafından yayımlanan belgelerde bu yaklaşımın yansıma bulmadığı belirtilebilir. Zira Obama'nın siber saldırılara karşı verilecek reaksiyona ilişkin kullandığı "bizim seçtiğimiz yer, zaman ve şekilde" ifadesi şekil açısından tırmandırmayı azaltıcı alan dışı tedbirlerin kullanımı şeklinde hayat bulmuştur.

²⁵⁰ Max Smeets, No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (Londra: Hurst&Co. Publishers, 2022), 54.

Söz konusu dönemde Rusya, Çin, İran, Kuzey Kore gibi aktörler tarafından icra edilen saldırılara maruz kalan ABD, siber saldırılara karşı benzer türde misillemeler yapmak yerine farklı yaptırımlara yönelmiştir. Bu kapsamda mal varlığı dondurma ve hapis cezası gibi uygulamalara yönelen Obama yönetimi, söz konusu devletleri doğrudan hedef almak yerine kişi ve kurumlara yaptırım uygulamıştır. Bu kapsamda ceza yoluyla caydırıcılığın daha az yüzleşmeci, yatıştırıcı ve alan dışı yaptırımlarının kullanıldığı yumuşak bir versiyonunun tercih edildiği düşünülebilir. Obama yönetiminin siber güvenliğe ilişkin icra emirleri incelendiğinde İç Güvenlik, Hazine ve Adalet Bakanlıklarına yaptırımlar için önemli görev ve sorumluluklar verildiği görülmektedir. Buna karşın Savunma Bakanlığının kapsam dışında tutulması söz konusu caydırıcılık anlayışında ofansif siber kabiliyetlere yönelik soğuk tavır gösteren bir diğer husustur.

Obama başkanlık döneminin siber caydırıcılık stratejisinde defansif ve ofansif kabiliyetlere ilişkin bakış açısını gösteren en somut açıklamalardan biri dönemin Savunma Bakan yardımcısı William Lynn'den gelmiştir. Lynn'e göre Savunma Bakanlığı Siber Stratejisi beş ana maddeye dayanmaktadır: Siber Uzayı ayrı bir harekât alanı olarak ele almak, aktif savunma tedbirleri uygulamak, kritik altyapıların korunmasında İç Güvenlik Bakanlığını desteklemek, müttefiklerle kolektif savunmayı güçlendirmek ve saldırgan aktörlerin internet ortamında sahip oldukları avantajları sınırlandırmak.²⁵¹ Lynn'in açıklamaları Savunma Bakanlığı'nın caydırıcılığın tesisine ilişkin savunma odaklı tedbirlerin ağırlığını göstermektedir. Nitekim Lynn, "geniş yelpazede farklı şekilde kabiliyetlerimiz mevcut, ancak stratejimizin esas dayanağı savunmadır" ifadesiyle saldırgan aktörleri savunma tedbirlerinin geliştirilmesi yoluyla tesis edilen caydırıcılık anlayışını açık bir şekilde dile getirmektedir.

Obama döneminde tercih edilen en önemli siber caydırıcılık stratejisi ikna ve dayanıklılık yoluyla caydırıcılıktır. Özellikle Stuxnet sonrası kritik altyapıların hassasiyetlerinin gündeme gelmesi ile birlikte bu tesislere yönelik saldırıların caydırılması girişimlerinde savunma tedbiri artırımı ağırlıklı yaklaşım olmuştur. Obama dönemi icra emirleri siber güvenlik açısından ele alındığında bunların büyük kısmının kritik altyapı savunmasını güçlendirici kamu-özel sektör işbirliğini geliştirici idari tedbirleri barındırdığı görülmektedir. İç Güvenlik Bakanlığının ana koordinatör olarak kullanıldığı bu adımlarda bir taraftan siber güvenlik koordinatörü makamı tesis edilerek

²⁵¹ Defense.gov, "Cyber Strategy's Thrust is Defensive"

kamu-özel sektör eş güdümünün artırılması hedeflenmiş, diğer taraftan Siber Güvenlik Çerçevesi gibi belgeler ile her iki paydaş için ortak güvenlik adımları belirlenmiştir. Böylece paydaşlar arası etkileşimi azami seviyeye çıkartarak topyekûn bir savunma anlayışını öngören bütünsel devlet yaklaşımı sürdürülmüştür.

3.2.2. Donald Trump Dönemi (2017-2021)

Bu başlık altında Trump başkanlık sürecinde siber güvenlik ile ilgili Ulusal Güvenlik Strateji Belgeleri, Ulusal Güvenlik Başkanlık Memorandumları, İcra Emirleri ve Savunma Bakanlığı Raporlarından oluşan toplam 11 adet resmi güvenlik belgesi incelenmiştir. Bunlara ilaveten söz konusu dönem içerisinde meydana gelen ve yönetimin caydırıcılık yaklaşımına dair net ipuçları sunan Siber Komutanlığın muharip statüsüne çıkarılması ve Beyaz Saray Siber Güvenlik Koordinatörlüğü görevinin sonlandırılması gelişmelerine yer verilmiştir. Bir önceki başlıkta olduğu gibi her bir belge tehdit algılaması, ağırlık noktaları, amaç ve araç bakımından değerlendirilmiş ve bu doğrultuda başkanlık dönemine ait bir caydırıcılık çerçevesi ortaya çıkarılmıştır.

- **İcra Emri-13800: Federal Ağların ve Kritik Altyapıların Siber Güvenliğini Güçlendirmek (2017)**²⁵²

Mayıs 2017’de yayımlanan ve Trump döneminin ilk siber konulu resmî belgesi olan İcra Emri-13800, kritik altyapıların siber güvenliğinde merkezi yönetimin rolünün altını çizmektedir. İlaveten kamu kurumlarına bazı bağlayıcı sorumluluklar getirmektedir.

Tehdit algılaması: Tehdit tanımının geniş yapıldığı belgede siber tehditlerin sosyal medyayı, akıllı cihazları, istihbarat sistemlerini, giyilebilir teknolojiyi, mobil ve dijital hizmetleri hedef aldığı belirtilmektedir. Savunma Bakanlığının çağa ayak uyduramayan ve siber tehditlere karşı savunulamaz bilişim sistemlerini kullandığı tespiti dikkat çekicidir. Belgede bilinen fakat giderilmeyen hassasiyetler en önemli tehditler arasında gösterilmektedir. Bu hassasiyetlerin bazılarının yazılım ve donanım aygıtlarında üretici güvenlik güncellemelerinin kullanılmaması, üretici destek garantisi süresi dışında kullanımının devam etmesi ve güvenlik odaklı konfigürasyon rehberlerinin uygulanmaması olduğu belirtilmektedir.

Ağırlık noktası: Üzerinde ağırlıkla durulan konu, federal birimlerin kritik altyapı savunmasında esas koordinatör makam olarak görev yapması gerektiğidir. Bu süreçte

²⁵² Beyaz Saray, “İcra Emri 13800: Federal Ağların ve Kritik Altyapıların Siber Güvenliğini Güçlendirmek”, Mayıs 2017, <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.

takip edilmesi gereken süreçler ve Ulusal Teknoloji ve Standartlar Kurumu tarafından geliştirilen Millî Siber Güvenlik Çerçevesi Belgesinin uygulanma durumu üzerinde durulmaktadır.

Amaçlar: Belgenin amacı federal ağların ve kritik altyapıların güvenlik seviyelerini kuvvetlendirmek için yetkili kurum angajmanlarını artırmaktır. Bu doğrultuda ilgili kurum yöneticilerinin siber güvenlik risk yönetimi bağlamında başkana karşı doğrudan sorumlu olduğu vurgulanmaktadır. Böylece yetki tahsisi ve sorumluluk konularında bir durumsal farkındalığın yaratılması hedeflenmektedir.

Araçlar: Belgenin en fazla dikkat çeken çıktılarında bir tanesi, İcra Emri-13636 aracılığıyla oluşturulan Millî Siber Güvenlik Çerçevesinin kamu kurumları tarafından uygulanmasının zorunlu hale getirilmesidir. İlgili çerçevenin uygulanmasında yetkili kurum yöneticilerinin bilfiil sorumlu olduğu ve başkana çerçevenin uygulanmasına dair risk yönetim süreçlerini rapor etmelerini öngören ifadeler dikkat çekicidir. Bu doğrultuda başkana verilecek raporda,

- Stratejik, operasyonel ve bütçe merkezli yaklaşımların,
- Kabul edilen risklerin,
- Çerçevenin uygulanmasında takip edilecek aksiyon planının bulunması gerektiği belirtilmektedir.

Söz konusu adımlar incelendiğinde belgenin istenen duruma ulaşabilmek için şu araçlara başvurduğu değerlendirilebilir:

1. Kurum liderlerine verilen doğrudan sorumluluk
2. Başkan ve kurum liderleri arasında siber güvenliğe ilişkin etkin bir diyalog,
3. Başkan ve kurum liderleri nezdinde artan bir durumsal farkındalık,
4. Takip edilmesi zorunlu bir Siber Güvenlik Çerçeve Metni

Caydırıcılık Metodu: Belgede daha önce yayımlanan icra emirlerine önemli atıflar yapılmaktadır. Bu emirlerde yer alan adımları pekiştirme amaçlı bir yaklaşım söz konusudur. Söz konusu yaklaşımda daha önce ortaya konulan ancak takip ve kontrolüne dair keyfi bir durumun mevcut olduğu güvenlik artırıcı tedbirlerin titizlikle takibi ön plana çıkmaktadır. Siber Güvenlik Çerçeve Belgesinin etkin bir şekilde uygulanmasının sağlanması esas vurgudur. Bunun için kurum liderlerinin doğrudan sorumlu ilan edilmesi ve başkan-liderler arasında diyalog zemininin artırılması tehdit algılamasında işaret edilen hassasiyetlere ilişkin savunma tedbiri artırıcı bütünsel devlet anlayışını yansıtmaktadır. Söz konusu yaklaşım, bir ikna yoluyla caydırıcılık örneğidir.

- **Ulusal Güvenlik Stratejisi (2017)**²⁵³

Trump başkanlığının birinci senesinde, 2017 Aralık ayında yayımlanan belgede güvenlik mimarisi altı sütun kapsamında ele alınmaktadır. Siber uzaya ilişkin değerlendirmeler; Amerikan halkının, topraklarının ve yaşam tarzının korunmasını esas alan birinci sütun ve barış yoluyla Amerikan gücünün korunmasını esas alan üçüncü sütunda yer almaktadır.

Tehdit algılaması: Belgede siber uzayın ABD menfaatlerini hedef alan bir tehdit kaynağı olduğu kadar, ABD küresel menfaatlerine hizmet edecek bir kabiliyet olarak değerlendirildiği görülmektedir. Belgede geçen, *“Siber çağın tehdit ve fırsatlarına karşı verilecek reaksiyonların ABD’nin gelecek refah ve güvenliğini doğrudan etkileyeceği”* ifadesi bu yaklaşımı kanıtlar niteliktedir. Önceki belgelere benzer olarak, internete olan bağımlılığın ortaya koyduğu hassasiyetler birer risk faktörü olarak tanımlanmaktadır. Devlet ve devlet dışı aktörler tarafından yöneltilen tehditlerin federal ağlar ve kritik altyapılara ilişkin oluşturduğu tehditlerin altı çizilmektedir. Belgede ayrıca siber saldırıların toplumun devlete dair güvenini sarsıcı bir etki silahı olduğu vurgulanmaktadır.

Ağırlık noktaları: Belgede siber tehditlerle mücadelede risk faktörüne önemle değinilmektedir. Ulusal güvenlik, enerji, bankacılık, sağlık, iletişim ve ulaştırma başlıklarından oluşan altı farklı alandaki tehditlerin gerçekleşme ve zarar olasılıkları risk değerlendirilmesine tabi kılınmıştır. Böylece savunma ve kabiliyet oluşturma süreçlerinde buna göre bir önceliklendirme yapılacağı ifade edilmektedir. Ayrıca ABD’nin siber uzaya ilişkin her adımında risk farkındalığına sahip olacağı ancak risk almaktan çekinmeyeceği ifadesi mevcut tehditlere karşı risk yönetim süreçlerine dair bakış açısını yansıtmaktadır.

Amaçlar: Belgede siber tehditlere karşı devlet ve özel sektörün iş birliğini esas alan, önleme, savunma ve dayanıklılık kavramlarının reaktif değil proaktif bir şekilde uygulandığı bir tedbir sisteminin inşası hedeflenmektedir. Dolayısıyla caydırıcılık bakımından daha aktif bir siber güvenlik mimarisinin hedeflendiği ifade edilebilir.

Araçlar: Belgede ortaya konulan güvenlik mimarisinin inşası için atılacak adımlar şu şekildedir:

- Risk yönetim süreçlerini uygulamak

²⁵³ ABD Başkanlık İcra Ofisi, “National Security Strategy 2017” (Beyaz Saray, Aralık 2017), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

- Bilgi teknolojileri aygıtlarını modernize etmek
- Kritik altyapı savunması ile sorumlu birimleri gerekli yetki, bilgi ve kapasite ile donatmak
- Saldırgan aktörün belirlenmesinde istihbarat paylaşımını artırmak
- Özel sektör ile iş birliğini esas alan katmanlı bir savunma ağı tesis etmek
- Etkin bir siber iş gücü inşa etmek
- İstihbarat, bilgi paylaşımı, planlama, uygulama ve kabiliyet inşası konularında mevcut engellerin önüne geçmek için Kongre ile birlikte çalışmak.

Caydırıcılık Metodu: Belgede ilgili kurumların gerekli yetki ve kapasite ile donatılması, saldırgan aktörü belirleme hedefine yönelik adımlar, kötü amaçlı aktörlerin hızlı ve sert reaksiyonlarla karşılaşacağı ifadesi ve tehditlerin önceden önlenmesini esas alan proaktif yaklaşım ceza yolu ile caydırıcılığı işaret eden temalardır. Bunların yanında özel sektör ve Kongre ile iş birliğinin yürütülmesi, bilişim ağlarının yazılım ve donanım anlamında modernizasyonu ve sektör bazlı risk değerlendirmelerini esas alan kritik altyapı savunması artırıcı tedbirler ikna ve dayanıklılık yoluyla caydırıcılık metodu kapsamındadır.

- **Siber Komutanlığın Birleşik Muharip Komutanlık Statüsüne Yükseltilmesi (2017)**

2009 yılında ayrı bir komutanlık olarak ihdas edilen Siber Komutanlık, hâlihazırda Ulusal Güvenlik Ajansının bulunduğu Fort Meade yerleşkesine konuşlandırılmıştır. Bu kurumun mevcut yeteneklerinden faydalanılması için aynı direktör tarafından komuta edilen çift kurumlu bir yapı tesis edilmiştir. Diğer taraftan Siber Komutanlık emir komuta ilişkisi bakımından Stratejik Komutanlığa bağlanmıştır. Stratejik Komutanlık, Savunma Bakanlığı'nın kontrolünde farklı coğrafi veya fonksiyonel alanlarda faaliyet gösteren Birleşik Muharip Komutanlıklardan biridir. Birleşik Muharip Komutanlıkların vazifesi, kendi sorumluluk alanlarına ilişkin operasyonel faaliyetlerin planlama ve uygulamasını icra etmektir. Esas itibarıyla nükleer silahların kontrolü ve caydırıcılıktan sorumlu bulunan Stratejik Komutanlığın komutasına Siber Komutanlığın bir alt operasyonel unsur olarak yerleştirilmesi ABD yönetiminin siber tehdit ve caydırıcılık ilişkisine bakış açısını göstermesi bakımından dikkate değerdir. Diğer taraftan Savunma Bakanlığı ile Siber Komutanlık arasında ek bir denetleyici kademenin tahsisi, Ulusal Güvenlik Ajansı ile birlikte konuşlandırılması neticesinde siber harekât ve istihbarat

faaliyetlerinin kesin çizgilerle ayrıştırılmaması Obama dönemi çoklu denetim ve sivil bürokrasi denetiminin izlerini taşımaktadır.

Başkan Donald Trump Ağustos 2017’de yayımlamış olduğu başkanlık memorandumunu ile Siber Komutanlığı Birleşik Muharip Komutanlık statüsüne çıkarmıştır.²⁵⁴ Söz konusu adım siber kabiliyetlere ABD yönetiminin bakış açısını göstermesi bakımından önemlidir. Savunma Bakanlığı bünyesinde günümüzde coğrafi bölge veya fonksiyon alanına göre yetkilendirilmiş 11 adet Birleşik Muharip Komutanlık bulunmaktadır.²⁵⁵ Kendi sorumluluk alanlarında müstakil operasyonel faaliyetlerini icra eden bu komutanlıklar doğrudan Savunma Bakanlığı’na bağlıdır. Başkan Trump, Siber Komutanlığın Muharip Komutanlık seviyesine yükseltilmesi adımının üç faydasına işaret etmiştir:²⁵⁶

1. Siber tehditlere karşı ABD yönetimi kararlılığını göstererek müttefiklere güven vermek ve rakipleri caydırmak
2. Siber operasyon planlama-icra kademelerine kararda çeviklik kazandırarak zamanında müdahaleleri kolaylaştırmak
3. Siber operasyonlara daha fazla maddi kaynak aktarımını mümkün kılmak

Görüldüğü üzere Başkan Trump, yapmış olduğu açıklamada caydırıcılığın tüm bileşenlerine atıfta bulunmaktadır. Şöyle ki Siber Komutanlığın güvenlik yönetimi teşkilatlanmasında en üst kademelerde yer alması muhtemel saldırgan aktörlere inandırıcılığa dair somut bir mesaj niteliği taşımaktadır. Diğer taraftan artan maddi kaynak havuzu siber kabiliyetlerin geliştirilmesinde önemli yere sahiptir. Bununla birlikte, Trump’ın açıklamasındaki en dikkat çeken unsur “kararda çeviklik” vurgusudur. Doğrudan Savunma Bakanlığı’na bağlı pozisyona getirilen Siber Komutanlık çoklu denetim mekanizmalarından sıyrılarak daha fazla ofansif siber harekât yapabilme serbestisine erişmiştir. Kuşkusuz bu adım Savunma Bakanlığı’nın

²⁵⁴ “Presidential Memorandum for the Secretary of Defense” (Beyaz Saray, 18 Ağustos 2017), <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-secretary-defense/>.

²⁵⁵ Afrika Komutanlığı, Merkezi Komutanlık, Avrupa Komutanlığı, Hint-Pasifik Komutanlığı, Kuzey Komutanlığı, Güney Komutanlığı, Siber Komutanlık, Stratejik Komutanlık, Uzay Komutanlığı, Özel Kuvvetler Komutanlığı, Ulaştırma Komutanlığı

²⁵⁶ Thomas Gibbons-Neff ve Ellen Nakashima, “President Trump Announces Move to Elevate Cyber Command”, Haber, The Washington Post, 18 Ağustos 2017, <https://www.washingtonpost.com/news/checkpoint/wp/2017/08/18/president-trump-announces-move-to-elevate-cyber-command/>.

savunma ağırlıklı caydırıcılık konumlanmasından öteye giderek ofansif siber kabiliyetlerin ön planda olduğu ceza yoluyla caydırıcılık stratejisinin önünü açmıştır.

- **Ulusal Güvenlik Başkanlık Memorandumu-13 (NSPM-13 - 2018)**

Hatırlanacağı üzere 20. Başkanlık Siyaset Direktifi (PPD-20), Obama döneminde yayımlanan bir başkanlık makamı belgesidir. Direktif, Stuxnet saldırısı sonrası ofansif siber kabiliyetlerin kullanımında Beyaz Saray başta olmak üzere çeşitli üst düzey bakanlık ve kurumların onayının alınmasını gerekli kılmıştır. Ofansif kabiliyetlere ve dolayısıyla ceza yoluyla caydırıcılığa yaklaşımı açısından söz konusu direktif Obama yönetimi anlayışına ışık tutan kilit bir belge niteliğindedir. Ağustos 2018 tarihinde yayımlanan NSPM-13 ile Başkan Trump işte bu direktifin düzenlemelerinde ciddi değişikliklere gitmiştir. Resmî makamlarca doğrulanmayan, fakat yazılı basında geniş yer bulan değişikliğe göre Siber Komutanlık tarafından geliştirilen ofansif kabiliyetlerin kullanımının önü açılmıştır.²⁵⁷

Tehdit Algılaması: NSPM-13 esas olarak siber caydırıcılıkta Siber Komutanlığın konumlandırılmasını sorgulamakta ve mevcut tehditlere karşı daha etkin kılmayı amaçlamaktadır. Buna dair tehdit algılamasını anlamak için aynı yıl yayımlanan Siber Komutanlık Vizyon Belgesi somut bir çerçeve sunmaktadır. Belgede siber uzay üstünlüğün sürekli el değiştirdiği dinamik bir ortam olarak tarif edilmektedir. Ayrıca hızlı ve yerinde aksiyonların bu sürekli angajman ortamında belirleyici olduğu ve mevcut bürokratik düzenlemelerin ABD'nin bu alanda etkinliğini azalttığı ifadesi dikkat çekicidir.²⁵⁸ Uluslararası aktörlerin her geçen gün ofansif siber kabiliyetlerini geliştirdiği ortamda ABD'nin benzer kabiliyetleri kullanmadaki sınırlılıkları, asimetrik etkiler yaratan önemli bir hassasiyet olarak değerlendirilmektedir.

Ağırlık Noktaları: Değişiklik, Siber Komutanlığın Ofansif Kabiliyetlere başvurmasının kolaylaştırılmasına yönelik tedbirleri ele almaktadır.

Amaçlar: Değişiklikte güdülen amacın, devlet ve devlet-dışı aktörlerin başvurmuş olduğu ofansif siber kabiliyetlere karşı reaksiyonun niteliğini artırmayı hedeflemektedir. Bu doğrultuda yalnızca alanlar arası caydırıcılık tedbirlerini ihtiva eden hukuki, ekonomik ve ticari yaptırımlardan ziyade Siber Komutanlığın elinde bulundurduğu

²⁵⁷ Soesanto, "The Evolution of US defense strategy in cyberspace", 22.

²⁵⁸ "ABD Siber Komutanlığı Vizyon Belgesi" (ABD Siber Komutanlığı, Nisan 2018), <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.

ofansif siber kabiliyetleri kullanmak amaçlanmaktadır. Söz konusu kullanıma engel teşkil eden bağlayıcı bürokratik sınırlandırmaların ortadan kaldırılması hedeflenmektedir.

Araçlar: PPD-20 ofansif siber kabiliyetlerin kullanımını, aralarında Ulusal Güvenlik Ajansı, Ticaret Bakanlığı, Dışişleri Bakanlığı gibi birimlerin olduğu, nihai kararın Beyaz Saray’da olduğu çok paydaşlı bir bürokratik sürecin onayına tabi kılmıştır.²⁵⁹ NSPM-13 ise bahse konu olan bürokratik değerlendirme sürecini, Beyaz Saray onayı da dahil olmak üzere askıya almıştır. Emir komuta zincirinde Siber Komutanlık direktörüne siber harekât düzenleme yetki ve inisiyatifi tanımıştır.²⁶⁰ Bu doğrultuda hedeflenen ofansif güvenlik anlayışına ulaşmada esas araç olarak kararda ve icrada çevikliği artırıcı yetki tahsisi düzenlemeleri kullanılmıştır.

Caydırıcılık Metodu: Başkan Trump’ın PPD-20 düzenlemesi açık bir şekilde ceza yolu ile caydırıcılık metoduna hizmet eden bir adım niteliğindedir. Ofansif siber harekâtların daha çevik ve etkin hale gelmesi, bürokratik süreçlerin doğurduğu engelleme ve gecikmelerden arındırılması saldırgan aktörlere yönelik net bir misilleme tehdidi sunmaktadır. Diğer taraftan daha önce başkana kadar uzanan karar verme inisiyatifinin emir-komuta zincirinin alt kademelerine kaydırılması, Schelling’in nükleer caydırıcılığa ilişkin irrasyonelitenin rasyonalitesi kavramını akıllara getirmektedir.²⁶¹ Şöyle ki yaptırım yetkisinin değerlendirme mekanizmalarının azaldığı, zaman zaman tek bir komutanın elinde bulunduğu durumlar, söz konusu yaptırımın uygulanacağı konusunda karşı tarafa daha açık ve net mesajlar verebilmektedir. Böylece ceza yoluyla caydırıcılıkta ilk kez belirgin bir şekilde ceza bileşeni tırmandırma kaygısı gözetmeksizin işletilmiştir. Bu açıdan bakıldığında söz konusu memorandum Obama ve Trump dönemi caydırıcılık anlayışı farklılığını yansıtmaması bakımından kilit bir rol oynamaktadır.

²⁵⁹ Tim Starks, “Ramifications of Trump revoking Obama’s cyber offense order”, Politico.com, 17 Ağustos 2018, <https://www.politico.com/newsletters/morning-cybersecurity/2018/08/17/ramifications-of-trump-revoking-obamas-cyber-offense-order-320741>.

²⁶⁰ Erica Borghard ve Shawn Lonergan, “What Do the Trump Administration’s Changes to PPD-20 Mean for U.S. Offensive Cyber Operations”, Council on Foreign Relations, 10 Eylül 2018, <https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations>; Eric Geller, “Trump scraps Obama rules on cyberattacks, giving military freer hand”, Politico.com, 16 Ağustos 2018, <https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095>.

²⁶¹ Schelling, *Arms and Influence*, 38; Kahn, *Thinking about the Unthinkable*, 48.

- **Savunma Bakanlığı Siber Stratejisi (2018)²⁶²**

Tehdit Algılaması: Belgede Ulusal Güvenlik Stratejisine benzer şekilde siber uzay tehdit ve fırsatlar üzerinden değerlendirilmektedir. Rusya ve Çin'in yürüttüğü ofansif siber faaliyetlere ve kapasite artırımına değinen belge, önceki örneklerinden farklı olarak tehdit aktörüne verilen ağırlık konusunda farklılık göstermektedir. Şöyle ki devlet, devlet dışı kurum ve siber suçluları kapsayacak şekilde saldırgan aktör çeşitliliğinin yarattığı karmaşık tehdit ortamını aktaran diğer belgelerden farklı olarak Savunma Bakanlığı Siber Stratejisi, tehdit aktörü olarak devletleri ele almaktadır.

Ağırlık Noktaları: Belgede yer alan ağırlık noktaları şunlardır:

- Kaynağı yerinde yok etmeyi esas alan ilerde savunma anlayışı
- Günden güne değişen cari siber rekabeti şekillendirmek
- Konvansiyonel harekâtı destekleyecek şekilde siber kabiliyeti geliştirmek.

Bu doğrultuda strateji belgesinde proaktif anlayışı benimseyecek şekilde rakipler ile sürekli angajman ve bahse konu olan angajmanı günlük olarak yürütebilecek kapasitenin inşası konularına ağırlık verilmektedir.

Amaçlar: Belgede beş adet amaç ön plana çıkmaktadır:

- Karmaşık siber uzay düzleminde müşterek görev kuvvetini verilen görevi başaracak düzeye getirmek,
- Siber operasyonlar düzenleyerek müşterek kuvvet kabiliyetlerini artırmak,
- Kötü amaçlı yazılımlara karşı Savunma Bakanlığı bilgi sistemlerini emniyete almak,
- Önemli etkiler yaratabilecek siber tehditlere karşı Savunma Bakanlığı bilgi ağlarını geliştirmek
- Kurumlararası, özel sektör ve uluslararası aktör desteğini alarak siber harekât kapsamını geliştirmek

Araçlar: Bahse konu olan amaçları yerine getirebilmek için birbirini destekleyen adımlı bir stratejik yaklaşım benimsenmiştir:

²⁶² ABD Savunma Bakanlığı, “DoD Cyber Strategy-2018”, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

1. Daha öldürücü bir kuvvet inşası: Siber kabiliyetlerin esnek kullanıma yönelik olarak inşa edilmesini kapsamaktadır. Buna göre yenilikçi Ar-Ge çalışmalarının öncülük ettiği siber kabiliyet inşası, hem bilişim ağlarının korunması hem de konvansiyonel harekâta destek olarak müşterek kuvvetin etkinliğini artırıcı rol oynayacaktır.
2. Siber Uzayda Rekabet ve Caydırma: Kritik altyapıların savunma ve dayanıklılığını artırma maksadıyla özel sektör ile iş birliği geliştirilecektir. Bunun yanı sıra savunmanın ilerde teşkil edilerek rakiplerin muhtemel saldırılarını önceden engelleyici sürekli angajman anlayışını yerleştirilecektir. İlaveten caydırıcılığın siber kabiliyetler ile başarısız olması durumunda askerî seçeneklerin de birer araç olarak masaya konulacağı ifadesi dikkat çekicidir.
3. İttifakları Kuvvetlendirme ve Yeni Ortaklıklar Kurma: Özel sektör ile sürdürülen iş birliğinin yanı sıra müttefik devletlerin siber kapasitelerinin ABD siber kabiliyetleri ile birbirini tamamlayacak şekilde geliştirilecektir. Bunun haricinde, en son 2015 yılında somut bir sonuç belgesi ortaya koyabilen fakat sonra görüş ayrılıkları nedeniyle işlevini yitiren Birleşmiş Milletler Uluslararası Güvenlik Kapsamında Bilişim ve Telekomünikasyon Alanlarındaki Devlet Uzmanları Grubuna (UNGGE) işaret edilmektedir. UNGGE tarafından ortaya konulan bağlayıcı olmayan normların takip edilmesi konusunda uluslararası partnerler ile iş birliğinin altı çizilmektedir.
4. Bakanlıkta Düzeltmeler Yapmak: Farkındalık ve sorumluluk hususlarını kapsamaktadır. Bu kapsamda bakanlığın her düzeyindeki personelin siber harekâta ilişkin durumsal farkındalıkları artırılacaktır. Daha da önemlisi, gerçekleştirmiş olduğu siber faaliyetler ve siber uzaya ilişkin almış olduğu kararlara ilişkin olarak Bakanlık yetkilileri ve özel sektör ortaklarının doğrudan sorumlu tutulması öngörülmektedir. Bunun yanı sıra bilişim teknolojilerin ayak uyduran ve sürekli geliştirilebilen teknolojik altyapıların kullanılması hususu vurgulanmaktadır.
5. Yetenek Geliştirme: Etkin bir siber iş gücünün oluşturulması kapsamında kadrolar askerî ve sivil personel olmak üzere dengeli bir şekilde oluşturulacaktır. Yetenekli personelin istihdamı için her türlü kurum içi ve kurum dışı kaynaklar kullanılacak ve personele teknoloji, mühendislik, matematik ve yabancı dil alanlarında eğitim verilecektir.

Caydırıcılık Metodu: Belgede bütün caydırıcılık metotlarına ilişkin ifadelere rastlamak mümkündür. Teknik altyapının geliştirilmesine yönelik adımlar ikna ve dayanıklılık yoluyla caydırıcılığa; ilerde savunma, sürekli angajman, tehditleri yerinde yok etme anlayışları ceza yoluyla caydırıcılığa; uluslararası ortaklar ile birlikte normların tesis edilmesi davranışları normlar yoluyla caydırıcılığa işaret etmektedir. Bununla birlikte “ilerde savunma” kavramına ayrı bir parantez açmak gerekmektedir. Şöyle ki söz konusu kavram Trump başkanlığının siber uzaya ilişkin güvenlik bakış açısını yansıtmaktadır. Bu kavram ile tehdit odaklarına karşı sürekli proaktif bir angajman halinde olan ofansif siber kabiliyet kullanımını ifade edilmektedir. Bu anlayışta, siber uzayın tabiatına uygun olarak Siber Komutanlık operatörleri muhtemel rakiplerin faaliyetlerini takip ederek ve angajman halinde olarak inisiyatif sürekli elde bulundurmaktadır. Gerekli koşulların oluşması durumunda tıpkı diğer saldırgan aktörler gibi gizlilik şemsiyesi altında tahribatlar yaratabilmektedir.²⁶³

Caydırıcılığa ilişkin belgede geçen birkaç kavram daha kesin bir değerlendirmeyi mümkün kılmaktadır. Bunlardan ilki, daha öldürücü bir kuvvetin oluşturulması ifadesidir. Konvansiyonel güçleri siber kabiliyetler ile donatarak daha etkin kılmak ve siber caydırıcılığın siber imkânlar ile sürdürülemediği noktada askerî seçeneklere başvurmak ceza yoluyla caydırıcılığın keskin bir ifadesi niteliğindedir. Diğer önemli kavram ise sorumluluktur. Siber uzayda sonuç doğurabilecek davranışlara ilişkin Bakanlık personelinin yanı sıra özel sektör ortaklarının da sorumlu tutulması bir taraftan bütünsel devlet anlayışını yansıtırken diğer taraftan siber savunma tesisinin ne derece ciddi bir şekilde ele alındığını göstermektedir. Üçüncü kavram ise teknolojik altyapıdır. Daha önceki belgeler genellikle siber faaliyetlere ilişkin metot ve prosedürleri ele alırken bu belgede söz konusu faaliyetlerin icrasında en modern ve teknolojik gelişimlere ayak uydurabilen yazılım ve donanım aygıtlarının kullanımı vurgulanmaktadır. Dolayısıyla siber savunmanın teknik boyutuna ve iş gücü etkinliği boyutlarına somut tedbirler getirmesi bakımından ikinci ve üçüncü altı çizilen kavramlar ikna ve dayanıklılık yoluyla caydırıcılığı vurgular niteliktedir.

²⁶³ Alan Mears ve Joe Mariani, “The Temporal Dimension of Defending Forward”, *The Cyber Defense Review* 5, sayı: 1 (Kasım 2019): 57.

- **Ulusal Siber Strateji Raporu (2018)**²⁶⁴

Trump başkanlığının 18. Ayında yayımlanan rapor, siber uzayda yeni bir stratejik rekabet döneminin ve yeni tehditlerin varlığına dikkat çekmektedir. Yeni gerçekliklere cevap veren, hassasiyetleri azaltan, rakipleri caydıran ve Amerikan halkının refahı için fırsatları değerlendiren yeni bir güvenlik stratejisinin gerekliliğine işaret etmektedir. Ulusal Güvenlik Stratejisi konu başlıklarını takip edecek şekilde oluşturulan belgede siber uzaya ilişkin algı ve uygulamalar; Amerikan yaşam tarzının korunması, refahın sürdürülmesi, kuvvet yoluyla barışın muhafazası ve Amerikan etkisinin geliştirilmesi maddelerinden oluşan dört konu altında aktarılmaktadır.

Tehdit algılaması: Belgede Rusya, İran, Çin, Kuzey Kore gibi aktörler doğrudan hedef gösterilmektedir. Siber uzayın egemenlik prensibi arkasına sığınarak suistimal edildiği ve mevcut ortamda ABD menfaatlerinin büyük zarar gördüğü ifade edilmektedir. Özellikle barış zamanında kritik altyapılara yöneltilen saldırılar karşısında ABD'nin önemli zafiyetlerinin bulunduğu vurgulanmaktadır. Saldırgan aktörlerin sürekli kapasite artırımına gittiğine işaret edilmektedir. Mevcut tehditler karşısında ABD yönetiminin agresif müdahalelerinin başladığı dile getirilmektedir. Geliştirilecek tedbirler kapsamında, yalnızca teknik odaklı çözümlerden ziyade bedel ödetme anlayışını da içeren reaksiyon biçimlerinin gerekliliği vurgulanmaktadır.

Ağırlık noktaları: Belgede federal ağların ve kritik altyapıların savunmasına odaklanılmaktadır. Yenilikçi tedbirlerin geliştirilmesinde ve güvenlik standartlarının oluşturulmasında özel sektörün rolüne ağırlık veren devlet-özel sektör iş birliği anlayışı üzerinde önemle durulmaktadır. Diğer taraftan cezai yaptırımların önemi ve niteliğine dikkat çekilmektedir. Bu alanda ABD'nin gerek kendi başına gerekse müttefikler ile olan girişimleri vurgulanmaktadır.

Amaçlar: Belgede siber uzaya ait mevcut hassasiyetler ile etkin bir şekilde baş edilmesi hedeflenmektedir. Bu doğrultuda;

- Ağ, sistem, faaliyet ve verilerin korunması,
- Siber olaylara karşı reaksiyon ve dayanıklılık mekanizmalarının geliştirilmesi,

²⁶⁴ ABD Başkanlık İcra Ofisi, "National Cyber Strategy-2018" (Beyaz Saray, Eylül 2018), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

- ABD menfaatlerine yönelik kötü amaçlı siber faaliyetlerin önlenmesi veya azaltılması,
- Sorumlu davranış kapsamına girmeyen siber eylemlerin ceza yoluyla caydırılması,
- ABD'nin siber kabiliyetleri millî güvenlik hedeflerine ulaşabilmek için kullanabilmesi amaçlanmaktadır.

Araçlar: Kritik altyapıların ve federal ağların korunması konusunda İcra Emri-13800'de yer alan yetki paylaşımı ve görevlendirmelere ilave olarak merkezileştirme süreçlerinin eklenmesi öngörülmektedir. Şöyle ki ilgili alanlarda ana koordinatör makam olarak belirlenen İç Güvenlik Bakanlığı'na diğer yetkili kurumların bilgi sistemlerine erişim ve faaliyet yürütme izni verilmektedir. Böylece reaksiyon sürelerinin hızlandırılması öngörülmektedir. Buna ek olarak; İç Güvenlik Bakanlığı aracılığıyla kabiliyet, araç ve faaliyetlerin merkezileştirme anlayışının devam edeceği belirtilmektedir. Federal ağların korunması konusunda, risk değerlendirme süreçlerinin etkin yürütülmesine işaret edilmektedir. Sadece devlet kurumlarının değil, sözleşme bazlı çalışan özel sektör şirketlerinin de güvenlik prosedürlerini takip durumunun İç Güvenlik Bakanlığı tarafından kontrol edilmesi öngörülmektedir. Kritik altyapıların saldırıya uğraması durumunda saldırgan aktöre bedel ödetileceği ifade edilmektedir. Söz konusu reaksiyonun yalnızca hukuki ve ekonomik yaptırımları kapsamayacağı ifadesi dikkat çekicidir.

Belgede kamu-özel sektör iş birliğine ayrı bir parantez açılmaktadır. Şöyle ki idarenin siber güvenlik konusunda sürekli gelişim, adaptasyon, yenilikçi teknolojiler konusunda teknoloji piyasasının desteğine ihtiyaç duyduğu ifade edilmektedir. Teknolojik altyapının tedarikinde güvenlik öncelikli bir anlayışın tesis edileceği belirtilmektedir. Buna yönelik piyasa ve bürokrasi kaynaklı engellerin kaldırılacağı, özel sektör girişimlerinin merkezde olduğu bir uygulama biçimi sunulmaktadır. Benzer ifadeler, internete genel erişimin muhafaza edilmesi kapsamında da geçmektedir. Siber uzay yönetiminin yenilikleri ve verimliliği engelleyen devlet merkezli anlayıştan ziyade çok paydaşlı yönetime evrilmesi gerekliliği vurgusu dikkate değerdir. Etkin bir siber iş gücünü oluşturulması konusunda iş alım ve eğitim süreçlerini kolaylaştırıcı uygulamaların takip edilmesi için Kongre ile iş birliği yapılacağı ifade edilmektedir. İş

gücü tedariginde yerli personel kadar nitelikli göçmenlerin de değerlendirileceği belirtilmektedir.

Uluslararası yapılageliş biçimlerine yönelik olarak güvenlik artırıcı ve istikrar sağlayıcı normların inşasının önemi vurgulanmaktadır. ABD'nin bu normların inşası ve muhafazasında aktif rol oynayacağı, diğer uluslararası aktörleri teşvik edeceği belirtilmektedir. ABD ve müttefiklerini hedef alan saldırıların yanıtsız kalmamasının önemine dikkat çekilmektedir. Bu konuda yapılacak cezai yaptırımların diplomatik, istihbarı, askeri (siber ve kinetik), ekonomik ve hukuki kabiliyetleri kapsamına alacağı ifade edilmektedir. Gelecekteki saldırıların caydırılması adına cezai yaptırımların hızlı ve mesaj niteliği taşıyacak şekilde kamuoyuna açık şekilde yapılacağı dile getirilmektedir. Müttefikler ile siber alanda ortaklık konusunda, tehdidin niteliğine göre biçimlendirilen stratejilerin uygulanması için Siber Caydırıcılık Girişimi adlı koalisyonun kurulması ifadesi bu alanda atılan önemli somut adımlardan birini teşkil etmektedir.

Caydırıcılık Metodu: Belgede tüm caydırıcılık metotlarına işaret eden ifadeler bulunmaktadır. Bununla birlikte Savunma Bakanlığı Strateji Belgesinde olduğu gibi ceza yoluyla caydırıcılık metodunun öngördüğü misilleme kapsamlı ifadeler dikkat çekicidir. Yapılacak misillemenin hızlı ve şeffaf olması gerektiğini içeren ifadeler Schelling'in caydırıcılığın üç ana bileşeninden biri olarak tarif ettiği “iletişim” ile örtüşür niteliktedir. Cezai yaptırım olarak devletin tüm kabiliyetlerinden faydalanılacağı hususu dile getirilmektedir. Askerî tedbirler konusunda özellikle siber kabiliyetlerin ayrı bir parantez içinde yer alması daha önceki belgelerden farklı bir cezai anlayışı yansıtmaktadır.

İkna ve dayanıklılık yoluyla caydırıcılık konusunda özel sektörü yalnızca bağlamsal bir ortak olarak konumlandırmak yerine, gelecek güvenlik mimarisini şekillendirecek ve güvenlik standartlarını belirleyecek bir paydaş olarak nitelendirilmektedir. Bu anlamda uygulanacak tedbirler kapsamında devlet-özel sektör iş birliğine bakış açısının önemli bir farklılık taşımaktadır. Diğer taraftan kritik altyapıların korunmasında cari hassasiyetlerin giderilmesine yönelik olarak İç Güvenlik Bakanlığı özelinde yetki ve kabiliyet merkezileştirilmesine gidilmektedir. Bu durum, savunma artırıcı tedbirlerin verimliliğini artırmaya yönelik bir diğer somut adımı teşkil etmektedir.

Normlar yolu ile caydırıcılık konusunda ABD başta olmak üzere istikrar sağlayıcı kabul edilmiş davranış biçimlerinin giderek daha fazla devlet tarafından benimsenmesi gerektiği ifade edilmektedir. Bununla birlikte uluslararası kamuoyu yanında ABD müttefiklerine ilişkin ifadeler önemlidir. Kabiliyetlerin ortaklaşa kullanılması, cezai yaptırımların ve kapasite artırımlarının ortaklaşa icra edilmesi hedefleri doğrultusunda kurulması hedeflenen Siber Caydırıcılık Girişimi, ABD'nin siber uzayın yönetimine ilişkin müttefiklerine karşı yapıcı bakış açısını yansıtmaktadır.

- **Beyaz Saray Siber Güvenlik Koordinatörü Kadrosunun İptal Edilmesi (2018)**

Başkan Trump, Mayıs 2018 tarihinde yayımlanmış olduğu emirle Obama döneminde teşkil edilmiş olan ve ulusal güvenlik konseyinde yer alan Beyaz Saray Siber Güvenlik Koordinatörü kadrosunu yürürlükten kaldırmıştır.²⁶⁵ Söz konusu adım, Trump'ın bürokratik süreçleri azaltma ve yetki merkezileştirme yaklaşımlarını yansıtır niteliktedir. ABD'nin kayda değer siber saldırılara maruz kaldığı ve uluslararası aktörlerin ofansif siber kabiliyetlerini artırdığı bir dönemde birimler arası koordinasyonu sağlayan ve etkin bir siber stratejiyi ortaya koymakla görevli olan bir kadronun iptal edilmesi yoğun eleştirilere yol açmıştır.²⁶⁶

- **İç Güvenlik ve Ticaret Bakanlıkları Raporu: Botnet ve Diğer Otomatik Dağıtık Tehditlere Karşı İnternet ve İletişim Ekosisteminin Dayanıklılığını Artırmak (2018)²⁶⁷**

Mayıs 2018 tarihinde yayımlanan rapor, 2017 tarihli, “Federal Ağların ve Kritik Altyapıların Siber Güvenliğini Güçlendirmek” konulu İcra Emri-13800'ün devamı niteliğindedir. İlgili emrin öngördüğü şekilde, Başkan tarafından İç Güvenlik ve Ticaret Bakanlıklarına verilen -siber uzay yönetimi paydaşlarının hareket tarzlarını belirleyici şeffaf bir süreç başlatma- görevine ilişkin olarak hazırlanmıştır.

²⁶⁵ Nicole Perlroth ve David E. Sanger, “White House Eliminates Cybersecurity Coordinator Role”, New York Times, 15 Mayıs 2018, <https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html>.

²⁶⁶ Alex Johnson, “Trump eliminates job of national cybersecurity coordinator”, News.com, 15 Mayıs 2018, <https://www.nbcnews.com/politics/white-house/trump-eliminates-job-national-cybersecurity-coordinator-n874511>.

²⁶⁷ ABD Ticaret Bakanlığı, “A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats” (ABD Ticaret Bakanlığı, Mayıs 2018), <https://www.commerce.gov/data-and-reports/reports/2018/05/report-president-enhancing-resilience-against-botnets>.

Tehdit Algılaması: Belge, otomatik ve dağıtık saldırıların hedef aldığı tek bir şirket veya sektörün daha ötesinde tüm bilişim sistemlerine zarar verici kitlesel etki boyutlarına ulaştığı tespiti ile başlamaktadır. Dağıtık Hizmet Engelleme (Ddos), kitle haline Spam email gönderimi, Klavye Dinleme Sistemi (Keylogger) ve botnet üzerinden fidye amaçlı saldırılar gibi tehditlerin bilişim ağları kapasitelerinde aşırı yükleme meydana getirdiği, verilerin rehin alındığı, kitlelerin manipüle edildiği bir ortam yarattığı ifade edilmektedir. Söz konusu saldırılardan sonra normale dönme süreçlerinin zaman aldığı ve kritik faaliyetlerin aksadığı belirtilmektedir.

Ağırlık Noktaları: Belgede Federal, Ticari ve Günlük Bilişim Ağlarının mevcut durumda yüz yüze olduğu tehdit ortamı ortaya konulmaktadır. Söz konusu problemlere ilişkin özel sektörün merkezde olduğu çok paydaşlı tedbir adımları sıralanmaktadır.

Amaçlar: Belgede ortaya konulan amaçlar şu şekildedir:

- Uyumlu, sürdürülebilir ve güvenli bir teknoloji pazarı için yol haritası belirlemek
- Evrimleşen tehditlere dinamik bir şekilde adapte olmayı sağlayıcı altyapı yeniliklerini teşvik etmek
- Otomatik ve dağıtık saldırıları önlemek, tespit etmek ve etkilerini azaltmak için bilişim ağlarında yenilikleri teşvik etmek
- Yurt içinde ve yurt dışında güvenlik, altyapı ve uygulamalı teknoloji toplulukları arasında kurulacak koalisyonları teşvik etmek ve desteklemek
- Bilişim ekosistemine dair farkındalık ve eğitim düzeyini artırmak

Araçlar: İç Güvenlik Bakanlığı ve Ticaret Bakanlığı, söz konusu raporun oluşturulmasında özel sektör, akademi ve sivil toplumdan uzman ve paydaşların bulunduğu geniş bir kaynak havuzundan elde etmiş olduğu görüş ve önerileri ele almıştır. Toplanan veriler doğrultusunda ortaya koymuş olduğu amaçlara ulaşmada izlenecek yol haritası için şu adımları uygulamayı teklif etmiştir:

- Federal ağların güvenlik gereksinimlerini karşılamak için güvenlik sağlayıcı parametrelerin ve teknolojik özelliklerin piyasa tarafından belirlenerek talep ve arz standardizasyonunun sağlanması. Örnek uygulamaların belirlenerek emsal gösterilmesi. Dağıtık Hizmet Engelleme saldırılarını önleyici yazılımların geliştirilmesi konusunda yenilikçi girişimlerin desteklenmesi ve teşvik edici kaynakların yaratılması.

- Siber Güvenlik Çerçevesi Belgesinin oluşturulmasında, Dağıtık Hizmet Engelleyici Saldırıların önlenmesi ve etkisinin azaltılması maksadıyla, internet servis sağlayıcı ve ortaklarının belirleyici rol alması. Geliştirilen güvenlik tedbirleri ve yazılımlarının kullanılmasında devlet kurumlarının öncülük etmesi ve bu konuda özel sektörü teşvik etmesi
- Ağ bağlantılı bilgisayarların birbirleri ile iletişimini sağlayan IPV4 internet protokolünün kısıtlılığından dolayı geliştirilen IPV6 protokolü kullanımının siber güvenlik yönetimi açısından incelenmesi. Ev ve ticari ağlardaki veri trafiğinin güvenliği için ürün geliştirme çabalarının artırılması. Özellikle ev ağları ve akıllı cihazların kullandığı ağların kullanıcı tarafından daha kolay anlaşılır ve kullanılır hale getirilmesi
- Siber güvenlik ve uygulamalı teknoloji çalışanları arasında etkileşimin artırılması
- Toplumda siber güvenlik farkındalığını artırıcı çalışma ve kampanyalar yürütülmesi. Tüm mühendislik disiplinlerine ait akademik eğitim süreçlerinde siber güvenlik eğitiminin zorunlu hale getirilmesi

Caydırıcılık Metodu: Raporda siber güvenliğe ilişkin teknik standartların oluşturulması, yenilikçi girişimlerin teşvik edilmesi ve uygulama örneklerinin belirlenmesi konularında özel sektöre alan açan bir yaklaşım mevcuttur. Bunun sebebi olarak özel sektörün barındırdığı yaratıcı düşünce ve özgün fikir ortamının sürekli evrimleşen dinamik tehdit çerçevesine uyum sağlayabilme becerisi olarak gösterilebilir. Özel sektör tarafından üstlenilen kritik altyapı yönetimi, öngörülen gereksinimler ve atılması gereken adımlara dair devlet ve özel sektörün aynı dili konuşması tedbirleri bu sektörün potansiyeline işlerlik kazandırmaktadır. Dolayısıyla savunma ve dayanıklılık kabiliyetlerindeki artışa sebebiyet vermektedir. Yaşanan siber saldırıların piyasada ekonomik amaçlı geliştirilen kötü amaçlı yazılımlar aracılığıyla geliştirildiği ve asimetrik yapısı düşünüldüğünde, güvenlik tedbirlerinin en etkin şekilde teknoloji piyasası aktörlerince geliştirileceği düşünülebilir. Dolayısıyla söz konusu raporda devlet tarafından desteklenmesi öngörülen özel sektör güdümlü teknik ve idari adımların savunma kabiliyetlerini geliştirmesi ve paydaşlar arasındaki farkındalığı artırması bakımından ikna ve dayanıklılık yoluyla caydırıcılık metotları kapsamına girdiği ifade edilebilir.

• **İcra Emri-13870: Amerikan Siber Güvenlik İş Gücü (2019)**²⁶⁸

Mayıs 2019 tarihinde yayımlanan icra emri, daha önce yürürlüğe konulan İcra Emri-13800 ile koordineli olarak, kritik altyapıların ve federal ağların korunmasında görev alacak siber iş gücünün istihdamı, eğitimi ve değerlendirme kriterlerini kapsamaktadır.

Tehdit algılaması: Belgede siber güvenlik iş gücünün Amerikan halkının, yurdunun ve yaşam biçiminin korunmasında stratejik bir varlık olduğu ifade edilmektedir. Diğer taraftan söz konusu iş gücü kapasitesinde yetenek ve kabiliyet açısından eksiklik yaşandığı ifade edilmektedir. Bu eksikliğin giderilmesine yönelik olarak siber güvenliğe dair bilgi ve yeteneğin oluşturulmasında yenilikçi yaklaşımların gerekliliği vurgulanmaktadır.

Ağırlık noktaları: Belgede etkin siber iş gücünün oluşturulmasında kurumlara verilen yetkiler, kurum ve personele dair değerlendirme süreçleri ile iş gücü potansiyeline yönelik ödül ve teşvik mekanizmaları ele alınmaktadır.

Amaçlar: Belgede siber güvenlik iş gücünün oluşturulmasına yönelik amaçlar şu şekilde belirtilmektedir:

- Siber güvenlik iş gücü ihtiyaçlarına yönelik devlet ve özel sektör yeteneklerinin birlikte kullanımını kapsayan ulus çapında bir farkındalık oluşturulması
- Dinamik ve kapsamlı bir iş gücünün oluşturulması sürecinde etkin bir öğrenme ortamının tahsisi
- Eğitimlerin güvenlik uygulamaları gereksinimleri ile örtüşecek şekilde teşkil edilmesi, koordinasyonun geliştirilmesi ve personelin hayat boyu kariyerlere hazırlanması
- İş gücü yatırımlarının verimliliğini ölçen değerlendirme kriterlerinin oluşturulması

Araçlar: Belgede siber güvenlik faaliyetlerinde alınan karar ve uygulamalara karşı doğrudan başkana karşı sorumlu tutulan kurumsal liderlerin aynı zamanda iş gücü verimliliği konusunda da sorumlu olacağı belirtilmektedir. İş gücü bilgi birikiminin paylaşılması ve personelin rotasyonel olarak farklı siber birimlerde görev alması planlanmıştır. BU doğrultuda Yönetim ve Bütçe Başkanlığı ile Personel Yönetim Başkanlığı ile koordine bulunmak kaydıyla İç Güvenlik Bakanlığı esas yetkili birim olarak görevlendirilmiştir. İç Güvenlik Bakanlığı bu görevlendirme kapsamında,

²⁶⁸ “İcra Emri 13870 - Amerikan Siber Güvenlik İş Gücü” (ABD Başkanlık Makamı, Mayıs 2019), <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/>.

- İç Güvenlik Bakanlığı başta olmak üzere yetkili kurumlarda görev alacak siber iş gücü personelinin tespiti,
- Siber Güvenlik İş Gücü Eğitimi Ulusal Girişim Çerçevesinin²⁶⁹ iş gücü tedariki kapsamında uygulanma durumu
- Katılımcılara uygulanacak eğitim müfredatı
- Entegrasyonu geliştirici birim içi rehberlik konularında Başkana rapor vereceği belirtilmektedir.

Belgede ayrıca birimler arası rekabet ortamının teşvik edilerek performans niteliklerinin geliştirilmesi hedeflenmektedir. Bu doğrultuda en iyi birey ve ekiplerin para ve şerit rozet gibi ödüller ile teşviki ortaya konulan bir araçtır.

Caydırıcılık Metodu: İç Güvenlik Bakanlığına verilen koordinasyon ve takip yetkisi, Ulusal Siber Stratejide görülen merkezileştirme yaklaşımının bir benzeri niteliğindedir. İş gücüne dair saptanan kabiliyet eksikliğine yönelik olarak birtakım somut tedbirler ortaya konulmaktadır. Bunlar; bilgi aktarımını artırıcı rotasyonel görev planlamalarının oluşturulması, eğitim için ortak bir müfredatın uygulanması, personeli ve görev aldığı denetleyici yapıların oluşturulması ve ödül mekanizmalarının teşkilidir. Bahse konu olan tedbirler kritik altyapıların korunmasında savunma tedbirlerini artırıcı bir nitelik taşımaktadır. Dolayısıyla öngörülen girişimler ikna ve dayanıklılık yoluyla caydırıcılık metodunun kapsamına girmektedir.

• **İcra Emri-13873: Bilgi ve İletişim Teknolojileri ile Tedarik Zincirini Emniyete Almak (2019)**²⁷⁰

Belge bilgi ve iletişim teknolojilerine ilişkin tedarik zinciri süreçlerindeki hassasiyetlerin önüne geçilmesini konu almaktadır.

Tehdit algılaması: Belgede uluslararası rakiplerin kritik altyapıların korunması, dijital ekonominin işleyişi, acil durum hizmetleri gibi konularda hassas bilgileri saklayan ve aktaran bilgi ve iletişim teknolojilerindeki hassasiyetleri istismar ettiği ve kötü amaçlı siber faaliyetlerde kullandığı ifade edilmektedir. Söz konusu aktörlere ilişkin bir

²⁶⁹ NICE Framework

²⁷⁰ “İcra Emri 13873-Bilgi ve İletişim Teknolojileri ile Tedarik Zincirini Emniyete Almak” (ABD Başkanlık Makamı, Mayıs 2019), <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>.

tanımlama yapılmamaktadır. Bununla birlikte son dönemde bilişim teknolojilerinde atılım yapan ve bilgi teknolojileri altyapılarında önde gelen firmalar ile doğrudan ilişkisi olan Çin yönetiminin kastedildiği değerlendirilmektedir.

Ağırlık noktaları: Belgede kötü amaçlı siber faaliyetlerde kullanılabilecek bilgi teknolojileri verilerinin kullanımı ve kısıtlandırılmaları konuları ele alınmaktadır.

Amaçlar: Belgede bilgi teknolojilerine erişimi olan kurum ve şahısların eriştikleri hassas bilgileri yabancı devletler ile paylaşmasının önüne geçilmesi amaçlanmaktadır.

Araçlar: Söz konusu amaca yönelik olarak İç Güvenlik Bakanlığı tarafından ABD ulusal güvenliğine karşı tehdit ve risk oluşturan tüzel kişilik, donanım, yazılım ve hizmetlerin belirlenmesi öngörülmektedir. Ayrıca halihazırda kritik altyapı faaliyetlerinin dayandığı yazılım donanım ve hizmetlerinin değerlendirmesini konu alan bir rapor hazırlanması hususu yer almaktadır. Hassas içerikli bilgilere erişimi olan kişi ve kurumların bunları yabancı devletler ile paylaşmaları veya yabancı devletlerin erişim sağlayabileceği şekilde kullanması yasaklanmıştır.

Caydırıcılık Metodu: Belgede kritik altyapılara ve federal ağlara yönelik risk faktörü oluşturabilecek bilgilerin korunması amaçlanmaktadır. Savunma tedbirlerinin artırıcı bu girişim ikna yoluyla caydırıcılık kapsamına girmektedir. Diğer taraftan söz konusu belge her ne kadar yabancı aktör tanımlamasına gitmese de tedarik zinciri ve bilgi teknolojilerindeki mevcudiyeti bakımından Çin'i hedef almaktadır. Ticaret özgürlüğü, serbest rekabet gibi ABD tarafından öncülük edilen hakların aksine Huawei gibi Çin bağlantılı şirketleri hedef alan bu belge Çin'e ABD menfaatlerinin korunması kararlılığını gösteren doğrudan bir mesaj niteliğindedir. Dolayısıyla caydırıcılık stratejisinin iki önemli bileşeni olan inandırıcılık ve iletişim kavramlarının somut biçimde uygulandığı görülmektedir.

• **İcra Emri-13942 ve 13943 Bilgi ve İletişim Teknolojileri ile Tedarik Zincirini Emniyete Almada Ek Tedbirler- Tiktok ve WeChat Tarafından Yöneltilen Tehditlere Tedbir Almak (2020)**²⁷¹

İcra Emri-13873'ün yürürlüğe konulmasından bir yıl sonra, 06 Ağustos 2020 tarihinde aynı gün içinde yayımlanan iki resmî belge, 13873'te öngörülen söz konusu tedbirlere ek olarak TikTok ve WeChat mobil uygulamalarına yönelik olarak hazırlanmıştır.

²⁷¹ "İcra Emri 13942-Bilgi ve İletişim Teknolojileri ile Tedarik Zincirini Emniyete Almada Ek Tedbirler-Tiktok ve WeChat Tarafından Yöneltilen Tehditlere Tedbir Almak" (ABD Başkanlık Makamı, Ağustos 2020), <https://www.govinfo.gov/app/details/DCPD-202000579>.

Tehdit Algılaması: Belgede ABD’de 175 milyon defadan fazla indirilen TikTok ile WeChat mobil uygulamalarının kişilerin arama geçmişlerini ve konumlarını sakladığı belirtilmektedir. Bu bilgilerin Çin Komünist Partisi tarafından kişisel bilgilerin kullanılması ve federal yetkililerin konumlarının takip edilmesi gibi faaliyetlerde kullanılabileceği değerlendirilmektedir. Ayrıca söz konusu uygulamaların toplumu yanlış yönlendirici Çin kaynaklı dezenformasyon faaliyetlerinde kullanılabileceği ifade edilmektedir.

Ağırlık noktaları: Belge, TikTok ve WeChat uygulamalarının oluşturmakta olduğu tehditleri ve sahipleri ByteDance ile Tencent Holdings Limited şirketlerinin ABD’deki varlığını kısıtlamaya yönelik tedbirleri ele almaktadır.

Amaçlar: TikTok ve WeChat uygulamalarının aracılığıyla elde edilen kişisel bilgilerin Çin Hükümeti ile paylaşılmasını önlemek amaçlanmaktadır.

Araçlar: ABD vatandaşları, kurum ve şirketlerinin ByteDance ve Tencent Holdings Limited Şirketleri ile herhangi bir ticari ilişki içine girmesi yasaklanmıştır. Söz konusu durum şirketin, dolayısıyla uygulamanın reklam almasını ve AppStore’da yer almasını engelleyici adımları içermektedir.²⁷²

Caydırıcılık Metodu: Kişisel bilgilerin korunması ve bu bilgilere erişim ve paylaşımaya yönelik getirilen kısıtlamalar söz konusu verilerin istismarı üzerinden gerçekleştirilecek muhtemel siber saldırılara karşı önlem alma niteliğindedir. Dolayısıyla söz konusu adımın ikna yoluyla caydırıcılık kapsamına girdiği ifade edilebilir. Diğer taraftan dikkat çeken nokta belgede Çin bağlantılı bir ticari şirketin doğrudan hedef alınmasıdır. Belirli bir uluslararası aktöre karşı sınırları ve kapsamı belli net yaptırımların ortaya konulması, caydırıcılığın inandırıcılık ve iletişim bileşenlerine hizmet eder niteliktedir ve Trump döneminin siber politikalarında çoğunlukla rastlanmaktadır.

- **İcra Emri-13984: Kötü Amaçlı Siber Faaliyetlere İlişkin Ulusal Acil Duruma Yönelik Ek Tedbirler Almak (2021)**²⁷³

Trump döneminin son icra emri niteliğinde olan belge, bulut sistemlerinin kötü amaçlı siber faaliyetler maksadıyla istismarının önlenmesini konu almaktadır.

²⁷² Bobby Allyn, “Trump Signs Executive Order That Will Effectively Ban Use Of TikTok In the U.S. _ NPR.pdf”, NPR.Org., 06 Ağustos 2020, <https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s>.

²⁷³ “İcra Emri-13984: Kötü Amaçlı Siber Faaliyetlere İlişkin Ulusal Acil Duruma Yönelik Ek Tedbirler Almak” (ABD Başkanlık Makamı, Ocak 2021).

Tehdit Algılaması: Belgede bulut bilişim hizmet modeli olarak faaliyet gösteren Servis olarak Altyapı (IAAS) sistemlerinin barındırmış olduğu hassasiyetlere dikkat çekilmektedir. Bu hizmette müşterilere işletim sistemlerini, uygulamalarını ve yazılımlarını kullanabileceği bir sanal alan tahsis edilmektedir. Sunucuların bakımı ve işletim sistemlerine dair sorumluluk müşteriye ait değildir. Söz konusu alanların kullanımı müşteriye bilgi altyapısının kontrolü kapsamında birtakım yetkiler sunmaktadır. Herhangi bir sorumluluğu beraberinde getirmeksizin bilgi teknolojilerine erişimin sağlanması kötü amaçlı siber faaliyetlerin uygulanması için uygun zemin yaratmaktadır. Belgede, söz konusu zeminden kaynaklı olarak gizlilik arkasına sığınarak yabancı aktörlerin fikri mülk hakları hırsızlığı, hassas verilerin kullanımı yoluyla kritik altyapı ve milli güvenliğe zarar verdiği ortaya konulmaktadır.

Ağırlık Noktaları: Belge, IAAS sistemlerinde kullanıcı hesabı olan yabancı kişilerin tespit edilmesini ele almaktadır.

Amaçlar: Belge, mevcut düzendeki kanun ve yönetmeliklerin IAAS sistemlerinden faydalanan yabancı aktörlerin faaliyetlerini denetlemede yetersiz kaldığını belirtmektedir. Bu doğrultuda ilgili yasal boşlukların önüne geçerek söz konusu hizmetlerden faydalanan şahısları tespit etmek, hassas bilgilerin kullanımının önüne geçmek ve bu bilgilerin istismarı durumunda bahse konu olan şahıs ve aktörlere cezai yaptırım uygulamak amaçlanmaktadır.

Araçlar: Belgede, IAAS servisi sağlayan şirketlerin müşterilerine ait kullanıcı hesaplarının incelenerek yabancı kullanıcı profillerinin Ticaret Bakanlığı ile paylaşılması zorunluluğu getirilmektedir.

Caydırıcılık Metodu: TikTok ve WeChat uygulamalarına getirilen kısıtlamalara benzer olarak İcra Emri-13694, hassas bilgilerin yabancı aktörler tarafından kötü amaçlı siber faaliyetlerde kullanılmasının önüne geçilmesini amaçlamaktadır. Bu doğrultuda ortaya konulan tehdit algılaması kapsamında mevcut yasal boşluk ve hassasiyetler tespit edilerek siber saldırıların başarı şansı zorlaştırılmakta ve başarılı olduğu takdirde saldırgan aktörü tespit etme sorunsalının önüne geçilerek cezai yaptırımların önü açılmaktadır. Bu koşullarda, söz konusu düzenlemenin hem ikna hem de ceza yoluyla caydırıcılık metotlarına hizmet ettiği çıkarımı yapılabilir.

Trump dönemi siber güvenlik politikalarının konu bakımından geniş bir alana yayıldığı görülmektedir. Bulut sistemleri, Tik Tok, We Chat gibi uygulamalara ilişkin düzenlemeler, nitelikli siber iş gücü inşası esasları, Savunma Bakanlığı bilişim altyapı yetersizliğine ilişkin çözümler ve Siber Komutanlık ofansif harekât kabiliyetleri bu çok çeşitli tedbirler bütünü'nün farklı örnekleridir. Bununla birlikte söz konusu dönemde atılan adımlarda iki kavramın ön plana çıktığı değerlendirilmektedir: Çatışmacı yaklaşım ve Merkeziyetçilik.

Obama dönemi değerlendirmesi bölümünde ele alındığı üzere, Stuxnet saldırısı sonrası ABD yönetimi tarafından benimsenen sınırlandırmacı yaklaşım bu dönemde yerini daha agresif usuller barındıran çatışmacı yaklaşıma bırakmıştır. Yayımlanan Başkanlık İcra Emirlerinde üstü kapalı mesajlar ve genel kapsayıcı tedbirlerden ziyade doğrudan Çin'in hedef alındığı, TikTok, WeChat gibi uygulamalar doğrudan hedef gösterilerek bunların ABD'deki faaliyetlerine sınırlandırma getirme çabaları görülmektedir. Trump dönemi güvenlik politikalarının ilk rehberi niteliğinde olan 2017 Ulusal Güvenlik Stratejisi belgesinde siber güvenliğe ilişkin “ABD risklerin farkında olacak ancak risklerden kaçınmayacaktır” ifadesi yeni dönemde Siber Komutanlık ve diğer unsurlar tarafından izlenecek aktif güvenlik anlayışını yansıtmaktadır. Yine aynı belgede belirtilen saldırganlara hızlı ve maliyetli zararlar verme vurgusu, yalnızca savunma ağırlıklı anlayışın terk edilerek saldırgan aktörlere bedel ödetme eğiliminin ortaya çıktığını göstermektedir. Nitekim bu belgeden bir sene sonra Savunma Bakanlığı tarafından kaleme alınan Ulusal Siber Strateji Belgesi söz konusu değişimi kavramsal çerçeveye oturtmaktadır. Bu belge ile birlikte ortaya atılan “ilerde savunma” kavramı, tehditlerin beklendiği ve savunma tedbirlerinin artırıldığı reaktif yaklaşımdan farklı olarak; tehditleri arayan, bulan, sürekli angajman halinde bulunan, gerektiğinde ön alıcı tahribatlar yaratarak inisiyatifli sürekli elinde bulunduran proaktif bir savunma anlayışını temsil etmektedir.²⁷⁴

2017 Ulusal Güvenlik Strateji Belgesinde ceza yoluyla caydırıcılık stratejisine dair önemli göndermeler bulunmaktadır. Bunların en önemlisi daha öldürücü bir kuvvetin oluşturulması söylemidir. Bu doğrultuda bir taraftan yazılım ve donanım olarak Savunma Bakanlığı'nın çağın gerektirdiği kabiliyetlere erişmesi esas alınırken diğer taraftan operasyonel faaliyetleri gerçekleştirecek siber iş gücünün inşası üzerinde durulmaktadır. Aslında caydırıcılığın kabiliyet bileşenine ilişkin detay odaklı geliştirme

²⁷⁴ Mears ve Mariani, “The Temporal Dimension of Defending Forward”, 57.

abaları yalnızca gvenlik strateji belgesine mahsus deėildir. 2017 yılında yayımlanan Federal Aėların ve Kritik Altyapıların Siber Gvenliėini Glendirmek konulu Baėkanlık İcra Emri, 2018 yılında İ Gvenlik ve Ticaret Bakanlıėı tarafından ortaklaėa yayımlanan Botnet ve Diėer Otomatik Daėıtık Tehditlere Karėı İnternet ve İletiėim Ekosisteminin Dayanıklılıėını Artırmak konulu rapor, 2018 Ulusal Siber Strateji Belgesi ve 2019 yılında yayımlanan Amerikan Siber Gvenlik İė Gc konulu Baėkanlık İcra Emri siber gvenliėin gerektirdiėi yazılım ve donanımsal yksek teknoloji ile yetiėmiė iė gc kapasitesine eriėilmesi iin somut adımları ngrmektedir.

2017 Ulusal Gvenlik Strateji Belgesinde caydırıcılık ile ilgili gze arpan hususlar yalnızca teknoloji ve insan kapasitesi geliėimi ile sınırlı deėildir. Maruz kalınan saldırılara karėı ofansif siber araların yetersiz kaldıėı durumlarda askeri seeneklere baėvurulabileceėi ifade edilerek siber caydırıcılık konusunun diėer sert g unsurları ile olan dayanıėması gndeme getirilmiėtir. Diėer yandan bakıldığında, siber uzayda maruz kalınan tehditlere karėı askeri yeteneklere baėvurulabileceėi mesajı Trump ynetiminin muhtemel bir kriz durumunu tırmandırma ihtimalini gsteren atıėmacı yaklaėımının bir gstergesidir. Buna ek olarak 2018 yılında yayımlanan Baėkanlık Siber Gvenlik Stratejisinde yer alan cezai yaptırımların hızlı ve kamuoyuna aık şekilde yapılacaėı ifadesi saldırgan aktrlere gelecekte uėrayacaėı zararlar zerine net mesajlar vermeyi amalamaktadır. Buradan yola ıkılarak caydırıcılıkta kullanılan cezalandırıcı aralara ve bunun zerinden oluėturulan iletiėim bileėenine ne derecede ciddi nem verildiėi grlmektedir. Schelling'in rakip aktre verilecek mesajın caydırıcılıktaki nemini hatırlatan bu ifadeler ofansif siber kabiliyetlerin kullanımında kendini sınırlamayan atıėmacı yaklaėımın siber caydırıcılıkta ne derecede aėırlıklı olduėunu gstermektedir. Trump dnemi siber caydırıcılık uygulamalarında ne ıkan diėer husus merkeziyeti yaklaėımdır. Bu kapsamda iki nemli geliėme bahse deėerdir: Beyaz Saray Siber Gvenlik Koordinatr Kadrosunun iptal edilmesi ve 13. Ulusal Gvenlik Baėkanlık Memorandumu (NSPM-13). Beyaz Saray Siber Gvenlik Koordinatrlė grevi Obama dneminde oluėturulan, Baėkan adına siber gvenlik faaliyetlerinden sorumlu olacak bir birim belirleme arayıėının sonucudur. Sz konusu makam zel sektr, kamu ve diėer paydaėların siber gvenlik tedbirlerinin belirlenmesi ve uygulanmasında ortak zeminde buluėmasını saėlayan koordinatrlk grevini stlenmektedir. Obama dneminde yoėun olarak grlen kamu – zel sektr etkileėimi ile ofansif siber kabiliyetlerin kullanımından nce devreye giren ok aktrl karar alma yapısı gz

önüne alındığında bahse konu olan makamın siber güvenlikte üstlendiği koordinatörlük görevi daha iyi anlaşılabilir. Görevi yürüten Rob Joyce'un Ulusal Güvenlik Ajansı'na geçmek üzere görevinden ayrılması üzerine makama atama yapılmayarak kadronun iptali Trump'ın güvenlik danışmanı John Bolton tarafından "basitleştirici bir düzenleme" hamlesi olarak yorumlanmıştır.²⁷⁵ Söz konusu yaklaşım, koordinatöre ait görevlerin yeniden güvenlik danışmanında toplanması, bürokraside ek bir kademenin azaltılması ve Obama dönemi çoklu denetim mekanizmasından uzaklaşılması olarak yorumlanabilir. Bahse konu olan gelişme Trump'ın NSPM-13 belgesi ile birlikte yorumlandığında daha aydınlatıcı olabilir.

Başkan Trump Siber Koordinatörlük görevinin iptali ile aynı yıl içerisinde imza attığı Başkanlık Memorandumu ile Obama döneminin ses getiren düzenlemelerinden biri olan 20. Başkanlık Siyaset Direktifinin (PPD-20) yeniliklerini köklü bir şekilde değiştirmiştir. Şöyle ki, ofansif siber kabiliyetlerin kullanımı öncesi aralarında Ulusal Güvenlik Ajansı, İç Güvenlik Bakanlığı olmak üzere birçok bakanlık ve kurumun bulunduğu çoklu denetim sürecini öngören mekanizma ortadan kaldırılmıştır. Operasyon planlama ve düzenleme yetkisi doğrudan Siber Komutanlık Direktörüne bırakılmıştır. Caydırıcılık kapsamında değerlendirildiğinde bu adım Schelling'in irrasyonelitenin rasyonalitesi ilkesini akıllara getirmektedir. Cezai yaptırımların uygulanması öncesinde devletin en üst kademesinde gerçekleştirilecek çok paydaşlı istişare süreci, yaptırımın meydana getireceği muhtemel menfi neticeler de göz önüne alınarak daha ılımlı tedbirlerin benimsenmesine yol açabilecektir. Diğer taraftan karar alma sürecinde yaşanan koordinasyon faaliyetleri belirli bir vakit kaybına yol açarak uğranılan zarar ve ödetecek bedel arasındaki doğrusallığı zayıflatabilecek, caydırıcılık stratejisinin mesaj bileşenini etkisizleştirebilecektir. Halbuki ceza planlama ve uygulama kararının bürokrasinin alt kademelerinde tek bir askeri birimde bulunması saldırgan aktörü ani ve ağır yaptırımlarla karşı karşıya kalabilme tehlikesi ile yüzleştirmektedir. Bu etkinin bilincinde olan güvenlik karar alıcılarının ofansif kabiliyet kullanım yetkisini alt kademelere devretmesi saldırgan aktörlere net bir mesaj niteliği taşımaktadır. Aynı zamanda ceza yoluyla caydırıcılık stratejisinin uygulanması noktasında kararlılığı gösteren bir inandırıcılık bileşeni örneğidir.

Schelling'e göre rakip aktöre statükoyu bozması durumunda ödeyeceği bedeller sözlü ve yazılı olarak iletilebileceği gibi bazen doğrudan güç kullanımı yoluyla da

²⁷⁵ Johnson, "Trump eliminates job of national cybersecurity coordinator".

gerçekleşebilir. Siber Komutanlığa devredilen operasyon icra etme yetkisi sonrası birim komutanı General Paul Nakasone'un "artık ofansif anlamda kenarda köşede olmayacağız" açıklaması mesajın saldırgan aktörlere sözlü olarak iletimidir. Trump döneminin ilk iki senesinde Obama döneminin toplam sekiz senesinden daha fazla ofansif operasyon gerçekleştirilmesi ise uygulama yoluyla caydırıcılık mesajının iletilmesine örnektir.²⁷⁶ Bununla birlikte icra edilen siber operasyon sayısındaki artışın nedeni olarak yalnızca Siber Komutanlık yetkilendirmesini göstermek eksik bir perspektif sunacaktır. Bu noktada söz konusu dönemde Siber Komutanlığın Birleşik Muharip Komutanlık statüsüne yükseltilmesi kararından bahsetmek gerekir. Daha önce Stratejik Komutanlığın bir alt birimi olan Siber Komutanlık, doğrudan Savunma Bakanlığına bağlanmıştır. Bu şekilde sorumlu bulunduğu alanda operasyonel planlama ve icra kapasitesine sahip 11 Birleşik Muharip Komutanlıktan biri haline gelmiştir. Kuşkusuz bu adım, nitelikli siber iş gücünün oluşturulması, teknolojik altyapının düzenlenmesi ve istihbarat faaliyetlerinde önemli bir kaynak artışına imkân tanımıştır. Nitekim komutanlığın bünyesinde yetiştirilen 133 Siber Misyon Timinin muharebeye hazır hale erişmesi söz konusu kaynak artırımının sonuçları arasındadır.²⁷⁷

Trump döneminde öne çıkan merkeziyetçi yaklaşım yalnızca kendini ceza yoluyla caydırıcılık stratejisinde göstermemektedir. Savunma tedbirlerinin ağırlıkta olduğu ikna yoluyla caydırıcılığın tesisi kapsamında atılan adımlarda da bu anlayışın izleri görülmektedir. Bunlardan en önemlisi İç Güvenlik Bakanlığına verilen koordinasyon görevidir. 13800 sayılı Başkanlık İcra Emri ile siber güvenlikle ilgili takip edilmesi gereken usul ve esasları belirleyen Siber Güvenlik Çerçeve Belgesinin uygulanması kamu kurumlarına zorunlu hale gelmiştir. Öncesinde teşvik etme ve gönüllülük esasının arandığı söz konusu düzenlemelerde kamu kurumlarından başlayarak özel sektöre doğru yayılan bir kontrol mekanizması oluşturulmaya çalışılmıştır. İç Güvenlik Bakanlığı söz konusu sürecin denetleyicisi olmuştur. Kritik altyapı tesislerinin siber saldırılardan korunması konusunda 2018 yılında yayımlanan Ulusal Siber Strateji Belgesi maruz kalınan saldırılara karşı reaksiyon sürelerinin kısaltılması ve dayanıklılık tedbirlerinin artırılması amacıyla İç Güvenlik Bakanlığı'na diğer kurumların bilgi sistemlerine

²⁷⁶ Ken Dilanian, "Under Trump, U.S. Military Ramps up Cyber Offensive against Other Countries", NBC News, 23 Haziran 2019, <https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281>.

²⁷⁷ David E Sanger, "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict - The New York Times", *The New York Times*, 17 Haziran 2018, <https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html>.

eriřim ve bu aęlar üzerinde faaliyet yrtme yetkisi tanımıřtır. Siber iř gcnn temini, eęitimi ve deęerlendirmesi faaliyetlerinde farklılık arz eden sreęleri ortadan kaldırmak maksadıyla 13870 sayılı İcra Emri ile bakanlık esas koordinatr makam tayin edilmiřtir. Buna ek olarak, daha nce siber gvenlik tedbirlerinin uygulanması konusunda ABD Bařkanına doęrudan sorumlu hale getirilen kamu kurum yetkilileri, aynı icra emri ile siber iř gcnn verimlilięinin saęlanması aęısından bařkana hesap verir hale getirilmiřtir.

Normlar yoluyla caydırıcılık stratejisine bu dnemde Obama dneminde kıyasla daha az bařvurulduęu grlmektedir. Her ne kadar Ulusal Gvenlik Stratejisi ve Ulusal Siber Strateji Belgelerinde siber uzayda kabul edilebilir davranıř řekilleri ve ceza mekanizmalarının belirlenmesi gereklilięi ifadeleri yer alsa da, Obama dneminde grlen rnek olma ve bir yapılageliř oluřturma ęabalarının bu dnemde bir benzeri grlmemektedir. Bundan ziyade Siber Caydırıcılık Giriřimi kapsamında uluslararası aktrlerle ve zellikle mttefik lkelerle ortak kapasite inřası gibi adımlara aęırlık verildięi grlmektedir.

3.2.3. Obama ve Trump Dnemi Siber Gvenlik Politikalarının Caydırıcılık Metotları Bakımından Deęerlendirilmesi

Bu blmde ęalıřmanın baęımlı deęiřkeni olan caydırıcılık metotları ortaya konulmuřtur. Veri setinin analiz edilmesi ile ortaya ęıkan bulgular caydırıcılık metodunun ç nominal deęiřkeni olan normlar yoluyla caydırıcılık, ceza yoluyla caydırıcılık ve ikna/dayanıklılık yoluyla caydırıcılık kavramsal ęeręevesleri ıřıęında incelenerek iki lider dneminde baęımlı deęiřkenler arasındaki farklılařmalar ortaya konulmuřtur.

Normlar Yoluyla Caydırıcılık: Her iki bařkan dneminde yayımlanan gvenlik belgeleri incelendięinde, uluslararası platformda siber saldırılara iliřkin kuvvet kullanım eřiklerinin belirlenmesi, ortak cezai yaptırımların tespiti ve resmi diyalog kanalları oluřturulması ęaęrılarının dile getirildięi grlmektedir. Buna karřın Obama dneminde, gvenlik belgelerinde sunulan yazılı ifadelerinden bir adım nne geęilerek uygulama anlamında bir kuvvet kullanım normu oluřturma gayretinin bulunduęu gzlemlenmektedir. Bunun en somut rneęi 20. Bařkanlık Siyaset Direktifi uygulamalarıdır. Siber Komutanlıęın elde bulundurduęu ofansif siber kabiliyetlerin aktif kullanım ncesi ęok paydařlı denetim mekanizmasından geęmesi ve nihai olarak Bařkanın onayına tabi olması yoluyla sınırlandırılması, siber uzayda kuvvet kullanımına

ilişkin diğer aktörlere bir mesaj niteliğindedir. Diğer taraftan Trump dönemi belgeleri de siber uzay normlarının oluşturulmasına ilişkin ifadeler barındırmakla birlikte, söz konusu ifadelerdeki iş birliği kavramının daha ağırlıklı olarak müttefiklere yönelik ortak kapasite oluşturma anlamında kullanıldığı görülmektedir. Dolayısıyla Normlar Yoluyla Caydırıcılık stratejisinin Obama döneminde daha fazla benimsendiği ve bunun tesisine yönelik somut ve belirgin adımlar atıldığını belirtmek mümkündür.

Ceza yoluyla caydırıcılık: İki başkan dönemi caydırıcılık anlayışı farklılığının en belirgin olduğu caydırıcılık metodudur. Her iki dönem arasında öngörülen ceza bileşenin niteliği ve kullanım sıklığı arasında önemli farklar mevcuttur. Daha önce belirtildiği üzere PPD-20 ofansif siber kabiliyetlerin kullanımına önemli sınırlandırmalar getirmiştir. Nitekim bu kabiliyetlerin kullanım sıklığına bakıldığında Obama'nın iki başkanlık dönemini kapsayan süreçte gerçekleşen ABD siber operasyon sayısına Trump döneminin henüz ilk iki senesinde ulaşıldığı görülmektedir. Bu durum her iki dönem arasında bir ceza bileşeni olarak siber kabiliyetlerin kullanımına ışık tutmaktadır. Obama döneminde tesis edilmeye çalışılan ceza yoluyla caydırıcılık metodu, ceza bileşeni bakımından alanlar arası bir yaklaşım barındırmaktadır. Alan içi cezai tedbirler getirecek Siber Komutanlık ve Savunma Bakanlığı yerine, alan dışı yaptırımlar üretecek Ticaret, Dışişleri, Adalet ve Hazine Bakanlığına başvurulduğu görülmektedir. Kuzey Kore, Çin gibi aktörlerin siber saldırılarına maruz kaldığı bu dönemde doğrudan bu devletler yerine, tespit edilen kurum ve kişiler cezalandırılmıştır. Ayrıca bahse konu olan yaptırımlarda ofansif siber kabiliyetler yerine ticari, diplomatik ve hukuki tedbirler benimsenmiştir. Bu doğrultuda Obama döneminde siber uzayda bir kuvvet kullanım normu oluşturma çabasının bu caydırıcılık metoduna da etki ettiği görülmektedir. Müttekabilyet mantığıyla ofansif siber kabiliyetlerin kullanıldığı tırmandırıcı bir yaklaşımdan ziyade daha yatıştırıcı ve yumuşak bir ceza yoluyla caydırıcılık metodunun takip edildiğini ifade etmek mümkündür.

Diğer yandan Trump'ın başkanlık dönemin bakıldığında 13. Başkanlık Güvenlik Memorandumu ve Siber Komutanlığın muharip komutanlık statüsüne çıkarılması, ceza yoluyla caydırıcılık metodunun ciddi bir şekilde kullanımının önünü açmıştır. Zira Obama döneminde tesis edilen çok paydaşlı denetim mekanizması ve başkan onayı zorunluluğu ortadan kaldırılarak ofansif siber operasyon icra etme yetkisi doğrudan Siber Komutanlığa devredilmiştir. Diğer taraftan daha önce hiyerarşik kademelerin alt taraflarında bulunan Siber Komutanlığın doğrudan Savunma Bakanlığı'na bağlı olacak

şekilde muharip komutanlık düzeyine çıkarılması, planlanacak operasyonel faaliyetlerin geliştirilmesi, icrası ve takibi açısından önemli bir kaynak artışı beraberinde getirmiştir. Bu doğrultuda Trump yönetimi siber uzaya dair caydırıcılık anlayışını mütakabiliyet odaklı inşa etmiştir. Böylece bir taraftan caydırıcılığın kabiliyet bileşenini kaynak artırımı ile geliştirirken diğer taraftan saldırgan aktörlerle mücadele konusunda kararlılığını ileten mesaj bileşenini de net bir şekilde ortaya koymuştur. Bu açıdan bakıldığında, ceza yoluyla caydırıcılık metodu kapsamında Obama dönemi sınırlandırıcı ve yatıştırıcı tedbirlerin aksine Trump döneminde ceza kavramının kabiliyet, inandırıcılık ve mesaj bileşenleri ışığında etkin bir kullanımı söz konusudur.

İkna ve Dayanıklılık Yoluyla Caydırıcılık: Her iki başkan döneminde de önemli bir yer teşkil etmektedir. İki dönemde de siber ağların savunulması ve muhtemel bir saldırıya uğranılması durumunda hasar minimizasyonunun sağlanması doğrultusunda tedbirler alınmıştır. Özellikle kritik altyapılara yönelik saldırıların caydırılmasında özel sektörün önemine vurgu yapılmıştır. Ulaşım, haberleşme, iletişim gibi günlük hayatı doğrudan etkileyen hizmetler özel sektör tarafından yürütüldüğünden dolayı devlet-özel sektör iş birliği esaslı iki dönemde de önem verilen konular arasındadır. Bununla birlikte Obama döneminde özel sektörün gönüllü katılımını sağlayıcı teşvik edici idari tedbirlerin ağırlıkta olduğu görülmektedir. Bununla birlikte siber güvenliğe ilişkin birçok sorumlu birim oluşturulmuş ve fonksiyon alanları doğrultusunda görev paylaşımı yapılmıştır. Diğer taraftan Trump döneminde özel sektörün güvenlik pratiklerine dahil edilmesi sürecinde daha zorlayıcı tedbirlerin alındığı görülmektedir. Bu tedbirlerden bazıları; kurum liderlerinin doğrudan siber güvenlik ve siber iş gücünün verimliliği hakkında hesap vermesi, İç Güvenlik Bakanlığı'nın özel sektör-kamu etkileşimini geliştirici mekanizma olarak tayini ve bu kuruma güvenlik tedbirleri doğrultusunda diğer kurumların bilişim ağlarına girme yetkisinin verilmesidir. Bunlara ilaveten siber ağların yazılımsal ve donanımsal modernizasyonunu ihtiva eden teknolojik tedbirler ve siber iş gücünün temini, geliştirilmesi ve denetimini içeren idari tedbirler caydırıcılığın kabiliyet bileşenine dair önemli adımlar arasındadır.

İkna ve Dayanıklılık yoluyla caydırıcılığın uygulanış biçimlerindeki farklılığa ilişkin olarak Beyaz Saray Siber Güvenlik Koordinatörlüğü görevi önemli ipuçları sunmaktadır. Zira Obama döneminde tesis edilen makam ve yapılan görevlendirme Trump döneminde sona erdirilmiştir. Başlıca görevi kamu kurumları arasında ve kamu-

özel sektör paydaşları arasında koordinasyonu sağlamak ve Başkan adına siber güvenlik politikalara yön vermek olan makam, Trump döneminde yavaşlatıcı bir bürokratik kademe olduğu gerekçesiyle sonlandırılmıştır. Söz konusu gelişme iki başkan döneminde bürokratik kademelerin etkinliğine ve paydaşlar arasındaki görüş alışverişine ilişkin bir bakış açısı sunmaktadır.

Bu kapsamda ikna ve dayanıklılık yoluyla caydırıcılık metodunun her iki başkan döneminde de benimsendiğini, ortak tedbir ve kabiliyet oluşturma sürecinde Obama döneminde kamu-özel sektör arasında güven artırıcı ve teşvik edici yaklaşımların, Trump döneminde ise kabiliyet oluşturma anlamında daha spesifik sorun tespit edici ve sorumluluk tayin edici yaklaşımların benimsendiğini ifade etmek mümkündür.

3.3. İç Değişkenlerin Etkileri: İki Başkan Döneminde Farklılık Gösteren Siber Güvenlik Politikalarının Nedenleri

Bir önceki bölümde siber tehditlere karşı caydırıcılık stratejisine dair metotsal farklılaşma incelenmiştir. Yapılan analizde iki başkanlık dönemine ilişkin en belirgin farkın ceza yoluyla caydırıcılık metodu kapsamında meydana geldiği tespit edilmiştir. Bu bölümde çalışmanın üçüncü araştırma sorusu olan: “Caydırıcılık stratejisindeki farklılaşmada stratejik kültür ve kurum etkileri nelerdir?” sorusuna yanıt aranmaktadır. Hatırlanacağı üzere çalışmanın başında güç dağılımı ve tehdit algılaması yapısal faktörlerinin siber tehditler kapsamında ABD dış politikasını etkileme durumu incelenmiştir. Söz konusu faktörlerin gelişen siber tehditlere karşı ABD yönetimine uyarıcı bir nitelik taşıdığı, ABD yönetimini caydırıcılık stratejisi kapsamında geliştirici kararlar almaya davet ettiği tespitinde bulunulmuştur. Diğer yandan siber uzayın yapısal dönüştürücü özelliğinden dolayı bahsedilen kararların mahiyetini, başka bir deyişle caydırıcılık metodunu belirlemede yapısal faktörlerin yetersiz kaldığı ifade edilmiştir. İki başkan döneminde ceza yoluyla caydırıcılık bakımından farklı uygulamaların tespit edilmesi, başkanlık dönemi ve caydırıcılık stratejisi arasında incelemeye değer bir ilişkiyi ortaya koymaktadır. Bununla birlikte tespit edilen caydırıcılık stratejisi farklılaşmasının liderin benimsediği stratejik kültürden kaynaklandığını öne sürmek için bu iki değişken arasındaki nedensel ilişkiyi kanıtlamak gerekir. Söz konusu nedensel mekanizmanın varlığını incelemek için süreç takibi metoduna başvurulmuştur.

Süreç takibinde gözlemlenen bulguların gerek şart ve yeter şartı karşılama durumları nedensel bağın varlığı konusunda belirleyici rol oynamaktadır.²⁷⁸ Gerek şart, nedensel bağın incelenmesi için temel koşulken yeter şart ise karşılanması durumunda hipotezin geçerliliğine büyük katkı sağlayan koşullardır.²⁷⁹ Her iki şartın varlığı stratejik kültür-caydırıcılık stratejisi ilişkisinin somut bir şekilde ortaya konulması için güçlü bir delil ortaya koyacaktır.

Söz konusu nedensel ilişki için gerek şart, farklılaşan caydırıcılık metodunun doğrudan lider inisiyatifi ile meydana gelmesidir. Çünkü alternatif durumda, söz konusu farklılaşmanın bir kongre tasarısı sonucu meydana gelmesi, kongre etkisinin lider ile birlikte analize dahil edilmesini gerektirecektir. Bu durum ise liderin benimsediği stratejik kültür etkisinin sağlıklı bir şekilde test edilmesini engelleyecektir.

Bir önceki bölümde, iki başkan dönemine dair ceza yoluyla caydırıcılık farklılığının PPD-20 ve NSPM-13 belgelerinden kaynaklandığı vurgulanmıştı. Sırasıyla Obama ve Trump tarafından yürürlüğe koyulan bu iki belge caydırıcılık stratejisindeki farklılaşma ile lider inisiyatifini bağlamaktadır. Zira gerek Başkanlık Siyaset Direktifi (PPD) gerekse Ulusal Güvenlik Başkanlık Memorandumu (NSPM), ABD başkanının güvenlikle ilgili konularda kongre onayı aramaksızın yayımladığı, yasamaya dair önemli yetkiler barındıran bağlayıcı belgelerdir. Dolayısıyla incelenen vakanın hipotez testi için gerek şartı karşıladığı görülmektedir.

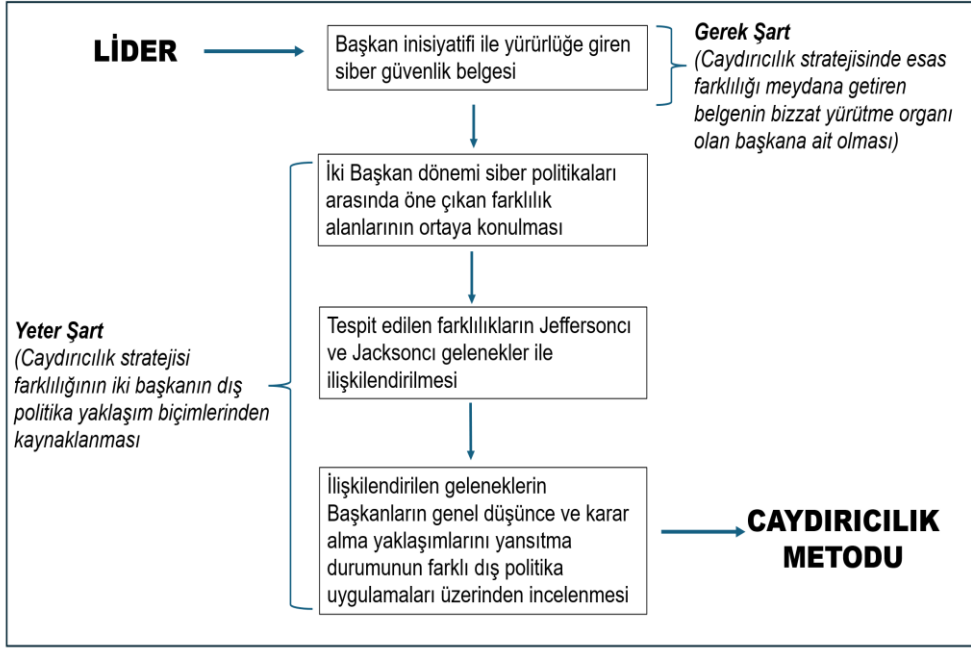
Yeter şart, karşılandığı durumda muhtemel alternatif hipotezleri çürüten ve teste tabi tutulan hipotezin geçerliliğini önemli ölçüde artıran bir araçtır.²⁸⁰ Sürecin bu adımında yeter şart olarak liderin benimsediği stratejik kültür belirlenmiştir. Stratejik kültürün tespit edilen farklı caydırıcılık stratejileri ile örtüşme durumunu incelemek, bu iki değişken arasındaki sebep-sonuç ilişkisi için somut deliller sunacaktır.

²⁷⁸ David Collier, "Understanding Process Tracing" *Political Science&Politics* 44(4) 1999: 823-830

James Mahoney, "The Logic of Process Tracing Tests in the Social Sciences" *Sociological Methods & Research* 41(4) 2012:573

²⁷⁹ Collier, 827

²⁸⁰ Collier, 827



Şekil 3: Stratejik Kültür - Caydırıcılık Metodu İlişkinin Nedensellik Analizinde Süreç Takibi Aşamaları

Takip edilen stratejik kültür biçimlerini belirli bir şablonla aktarmak için Walter Russell Mead'in ABD dış politika gelenekleri çalışmasından faydalanılmıştır. Söz konusu geleneklerden Jeffersonculuk ve Jacksonculuk ayrıntılı bir biçimde ele alınarak farklılıkları ortaya konulmuştur. Ardından iki başkan dönemi arasındaki caydırıcılık stratejisi farklılaşmasını doğuran PPD-20 ve NSPM-13 belgeleri, Jeffersoncu ve Jacksoncu gelenek penceresinden analiz edilmiştir. Müteakiben analiz bulgularının başkanların genel dış politika kararları ile örtüşme durumları Suriye'de hava taarruzu kararı ve dron kullanımı gibi ofansif kabiliyet kullanma örnekleri ile test edilmiştir. PPD-20/NSPM-13, stratejik kültürü yansıtan gelenek ve başkanın diğer ofansif harekât kararları arasında tespit edilecek paralellik, stratejik kültür ve caydırıcılık stratejisi arasındaki nedensel bağı gösterecektir.

Kurum değişkeninin incelendiği sonraki kısımda ise ABD Kongresinin siber güvenlikle ilgili yasama ve denetim faaliyetleri incelenmiştir. Bu kapsamda yasa tasarılarının onaylanma durumları ve komisyon faaliyetleri ele alınarak başkanların izledikleri caydırıcılık stratejilerine etkileri ortaya konulmuştur.

3.3.1. Lider Değişkeni – Alternatif Açıklamalar

Stratejik kültür bileşenini ele almadan önce akademik yazında liderin dış politikadaki belirleyiciliğine eğilen bazı çalışmalara yer verilmiştir. Dış politikası farklılaşmasını lider karakteri özelinde analiz eden bu çalışmalar aynı başkan döneminde farklılık arz

eden birtakım politika tercihlerini açıklamada yetersiz kalmaktadır. Söz konusu yetersizliklerin ortaya konulması, lider karakterinden ziyade liderin etkilendiği stratejik kültürün bir değişken alınması gerekliliğini daha açık bir şekilde ortaya koyacaktır.

Lider, Waltz'un analiz seviyelerinden birey ve devletin buluşma noktasını teşkil eden hassas konumdaki bir aktördür. Liderler aracılığıyla alınan kararlar, her ne kadar uzun bürokratik süreçlerin ve karargâh çalışmalarının ürünü niteliğinde olsa da diğer taraftan dünyaya bakış açıları ve düşünme biçimlerinden oluşan bir perspektif süzgecinden geçerek nihai duruma erişmektedir. Putnam'ın²⁸¹ çalışmasından hatırlanacağı üzere, liderler temsil ettikleri devlet adına uluslararası rekabet ortamında siyaset yürüten aktörler olmakla birlikte, aynı zamanda bu ortamda takip ettikleri karar ve uygulamalar bakımından ulusal düzeydeki siyasi desteğe muhtaç durumdadırlar. Aslında söz konusu siyasi destek bu göreve talip olan siyasilerin dış politika sorun ve fırsatlarına ilişkin kamuoyuna yansıtılmış oldukları yaklaşımlar ile görev süresinin başından itibaren şekillenmektedir. Başkanların gerek sözlü/yazılı ifadeleri gerekse uygulamaları ile göstermiş oldukları dış politika perspektifleri bir taraftan kendisine ilişkin destek ve muhalefeti şekillendirirken diğer taraftan dış politika analizine de ışık tutmaktadır. Söz konusu perspektifin nasıl anlamlandırılacağı konusu ise bilimsel araştırmalarda farklı şekillerde ele alınan bir sorunsal niteliğindedir.

Başkanın dış politika üretim sürecine doğrudan etki ettiğini savunan birçok yazar bahse konu olan etkiyi başkanın bilişsel özelliklerine bağlamakta ve bu bağlamda düşünme ve karar alma tipolojileri geliştirerek bağımsız değişkenlerini bu tipolojiler üzerinden inşa etmektedir.²⁸² Söz konusu çalışmalardan biri Alexander George'un "Operasyonel Kod" modelidir. George'a göre liderler dış politikaya ilişkin konuları bir algılama

²⁸¹ Putnam, "Diplomacy and Domestic Politics".

²⁸² Dennis M. Foster ve Jonathan W. Keller, "Leaders' Cognitive Complexity, Distrust, and the Diversionary Use of Force", *Foreign Policy Analysis* 10, sayı: 3 (Temmuz 2014): 205-23, <https://doi.org/10.1111/fpa.12019>; Y. E. Yang, "Leaders' Conceptual Complexity and Foreign Policy Change: Comparing the Bill Clinton and George W. Bush Foreign Policies toward China", *The Chinese Journal of International Politics* 3, sayı: 4 (01 Aralık 2010): 415-46, <https://doi.org/10.1093/cjip/poq015>; Margaret G. Hermann, "Explaining Foreign Policy Behavior Using the Personal Characteristics of Political Leaders", *International Studies Quarterly* 24, sayı: 1 (Mart 1980): 7, <https://doi.org/10.2307/2600126>; Oz Hassan ve Christopher Featherstone, "Trump's Low Conceptual Complexity Leadership and the Vanishing 'Unpredictability Doctrine'", *Cambridge Review of International Affairs* 34, sayı: 3 (04 Mayıs 2021): 407-29, <https://doi.org/10.1080/09557571.2020.1853054>; Asaf Siniver ve Christopher Featherstone, "Low-Conceptual Complexity and Trump's Foreign Policy", *Global Affairs* 6, sayı: 1 (01 Ocak 2020): 71-85, <https://doi.org/10.1080/23340460.2020.1734953>.

süzgecinden geçirerek kendilerine özgü bir uygulama kodu geliştirmektedir.²⁸³ Şöyle ki liderlerin davranışları; ne kadar gücün gerekli olduğuna ilişkin bakış açılarına, diğer aktörler nezdinde oluşturdıkları iyimser/kötümser rol kalıplarına ve güncel sorunların ne kadar kontrol edilebilir olduğuna bağlı olarak farklılık göstermekte; bu doğrultuda iş birliği veya tırmandırma davranışları sergileyebilmektedir.

Bilişsel mekanizmalara ilişkin önde gelen çalışmalardan bir diğeri de Margaret Hermann'ın "Kavramsal Karmaşıklık" modelidir.²⁸⁴ Buna göre kavramsal karmaşıklık liderin dünyayı, olay, fikir ve kişileri algılayış biçimlerini, yeni fikirleri değerlendirme ve özümseme derecelerini ifade eden bir tanımdır.²⁸⁵ Düşük kavramsal karmaşıklık düzeyindeki liderler dünyayı iki ihtimalli şekilde iyi veya kötü şeklinde algılamakta, yoğun bilgi aktarımından ziyade daha sınırlı çaptaki bilgiyle hareket etmeyi tercih etmekte, öğrendiklerinden ziyade sezgilerine göre hareket etmekte ve anlık karar almada daha çevik davranabilmektedir.²⁸⁶ Diğer taraftan yüksek kavramsal karmaşıklık düzeyindeki liderler iki ihtimal yerine çoklu ihtimalleri hesaba katmakta, her türlü bilgiyi işlemeye istekli davranmakta, karar vermeden önce tüm olasılıkları ve muhtemel çözümleri gözden geçirmeyi tercih etmekte ve grup çalışmasında ortaya çıkan fikirlere değer vermektedir.²⁸⁷ Sinivier ve Featherstone, Trump'ın NATO'ya yaklaşımı, Meksika sınırına duvar inşası, Müslüman ülkelerden girişleri engellemesi gibi dış politika uygulamalarını ele aldığı çalışmalarında analiz edilen verinin kavramsal karmaşıklık modeli ile açıklanabileceğini, Trump'ın düşük kavramsal karmaşıklık düzeyindeki lider profiline güzel bir örnek teşkil ettiğine işaret etmektedir.²⁸⁸

²⁸³ Alexander L. George, "The Operational Code: A Neglected Approach to the Study of Political Leaders and Decisionmaking", *International Studies Quarterly* 13, sayı: 2 (1969): 190-222.

²⁸⁴ Hermann, "Explaining Foreign Policy Behavior Using the Personal Characteristics of Political Leaders"; Margaret G. Hermann ve Thomas Preston, "Presidents, Advisers, and Foreign Policy: The Effect of Leadership Style on Executive Arrangements", *Political Psychology* 15, sayı: 1 (Mart 1994): 75, <https://doi.org/10.2307/3791440>; Stephen G. Walker, Akan Malici, ve Mark Schafer, ed., *Rethinking Foreign Policy Analysis: States, Leaders, and the Microfoundations of Behavioral International Relations* (New York: Routledge, 2011).

²⁸⁵ Yang, "Leaders' Conceptual Complexity and Foreign Policy Change", 424.

²⁸⁶ Yang, "Leaders' Conceptual Complexity and Foreign Policy Change"; Foster ve Keller, "Leaders' Cognitive Complexity, Distrust, and the Diversionary Use of Force".

²⁸⁷ A.g.e.

²⁸⁸ Sinivier ve Featherstone, "Low-Conceptual Complexity and Trump's Foreign Policy"; Hassan ve Featherstone, "Trump's Low Conceptual Complexity Leadership and the Vanishing 'Unpredictability Doctrine'".

Hermann'ın kavramsal karmaşıklık modeli başkanlık bilişsel süreçlerinin dış politika analizinde yer bulmasına faydalı bir bakış açısı sunmakla birlikte nispeten kısa süreli ve münferit karar ve uygulamaları açıklamak için kullanılmaktadır. Bununla birlikte başkanlık döneminin tamamına yayılan dış politika yaklaşımları ve doktrinler için kısır bir perspektif sunmaktadır. Söz konusu modele dair analizlerin Trump dönemine yoğunlaşmasının sebebi olarak Trump'ın sıra dışı söylem ve uygulamaları doğrultusunda bir temel strateji takip etmediği ve dış politika kararlarını gelişigüzel bir biçimde aldığı görüşünden kaynaklandığı düşünülebilir. Buna karşı Trump'ın dört senelik başkanlık dönemini tamamen anlık karar ve bilişsel süreçlere bağlayan bir analiz oldukça indirgemeci bir çerçeve sunmaktadır. Dimitrova'ya göre bir grand stratejide bulunması gereken dört temel bileşen: millî menfaatler, millî menfaatlere yönelik tehditler, tehditlere karşı başvurulacak stratejik tepkiler ve dış politika ana hatları Trump'ın söylem ve strateji belgelerinde açıkça yer almaktadır.²⁸⁹ Bu doğrultuda Dimitrova, Trump yönetiminin bir grand strateji barındırmadığı iddialarını aksi yönde yanıtlamaktadır. Dolayısıyla belirli bir grand strateji barındırmadığı gerekçesiyle başkanlık dönemini münferit kararlar ve bilişsel süreçler üzerinden analiz etmek yerine başkanların belli başlı dış politika konularına ilişkin temel yaklaşımlarını ele alan bir analiz çerçevesi daha açıklayıcı olacaktır.

İki Dünya Savaşı arası dönem veya Soğuk Savaş sonrası dönem gibi süreçlerin de konjonktür etkisiyle başkanların izlemiş olduğu stratejiler, realist/idealist başlıkları altında açıklanabilmektedir.²⁹⁰ Wilson dönemi dış politikası, iş birliği ve değerleri esas alan idealist bir dış politika çerçevesi benimsemesi bakımından realist bakış açısına ciddi bir alternatif teşkil etmiş ve takip eden dönemin dış politika analizine ilişkin realist ve idealist yaklaşımları iki ana düzlem olarak ön plana çıkarmıştır. Bununla birlikte söz konusu dış politika yaklaşımlarını idealist ve realist ikilemesi üzerinden analiz etmek bir diğer indirgemeci yaklaşım olarak değerlendirilebilir. Zira devletlerin uluslararası alanda karşılaştıkları meselelerin tür ve nitelikleri aktör, coğrafya gibi değişkenlere bağlı olarak oldukça geniş bir yelpazede değişiklik gösterebilmektedir. Bu yelpazenin farklı noktalarında yer alan konulara ilişkin yaklaşımları topyekûn rekabetçi veya iş

²⁸⁹ Anna Dimitrova, "Trump's 'America First' Foreign Policy: The Resurgence of the Jacksonian Tradition?," *L'Europe En Formation* n° 382, sayı: 1 (06 Şubat 2018): 35-36, <https://doi.org/10.3917/eufor.382.0033>.

²⁹⁰ Robert G. Kaufman, "E. H. Carr, Winston Churchill, Reinhold Niebuhr, and US: The Case for Principled, Prudential, Democratic Realism", *Security Studies* 5, sayı: 2 (Aralık 1995): 314-53, <https://doi.org/10.1080/09636419508429270>.

birlikçi yaklaşım üzerinden analiz etmek sorunsalın özüne ilişkin eksik bir değerlendirmeyi doğurmaktadır. Diğer taraftan McDougall'a göre realist/idealist ikilemi dış politika analizi için doğru bir çerçeve sunmamaktadır. Zira söz konusu iki düşünce biçimi millî menfaatlerin nasıl yerine getirileceğine ilişkin farklı dış politika uygulamalarını öneren bir tez-antitezden ziyade daha temelde millî menfaatin ne olduğunu farklı şekillerde yorumlayan kalıplardır.²⁹¹ Morgenthau'ya göre ise millî menfaatler özünde ahlaki değerler barındıramayacağından ötürü söz konusu ikileme dış politika analizine yapıcı bir değer katmayan soyut tanımlamalardan öteye gidememektedir.²⁹²

Başkanların dış politika tercihlerine ilişkin farklı bir analiz çerçevesi Thomas Henriksen tarafından sunulmaktadır. Henriksen'e göre ABD dış politikası başkanların uluslararası angajman ve iç politika odaklı yaklaşımlarını yansıtacak şekilde döngülerden oluşmaktadır.²⁹³ Henriksen, her bir başkanın bir öncekinden tamamen farklı politikalar benimseyerek dış politikada müdahaleci veya geri çekilmeci uygulamalar benimsediğini ifade etmektedir.²⁹⁴ Bahsedilen analiz çerçevesinin de aynı şekilde fazla genellemeci olduğunu ifade etmek mümkündür. Zira aynı başkan döneminde iki farklı dış politika uygulaması müdahale veya geri durma açısından farklılık gösterebilmektedir. Clinton döneminde Bosna ve Ruanda vakaları, Obama döneminde ise Suriye ve Libya vakaları kendi içerisinde yalnızca müdahalecilik yaklaşımları üzerinden açıklanmayacak şekilde farklı bağlamsal detayları barındıran dış politika uygulamalarıdır.

3.3.2. Güvenlik Politikalarına Etki Eden bir Bileşen olarak Dış Politika Gelenekleri
ABD dış politika analizine ilişkin dikkat çeken bir çerçeve Walter Russell Mead tarafından ortaya konulmuştur. Mead'e göre ABD dış politikası, 18'inci yüzyıldan günümüze dek, kurucu babalarının ortaya koymuş olduğu perspektif etrafında toplanan, birbirinden farklı fakat aynı zamanda birbirini tamamlayıcı dört ana geleneğin ışığında

²⁹¹ Walter A McDougall, *Promised Land, Crusader State* (Boston: Houghton Mifflin Company, 1997), 8-10.

²⁹² Hans J. Morgenthau, "The Mainsprings of American Foreign Policy: The National Interest vs. Moral Abstractions", *American Political Science Review* 44, sayı: 4 (Aralık 1950): 854, <https://doi.org/10.2307/1951286>.

²⁹³ Thomas H. Henriksen, *Cycles in US Foreign Policy since the Cold War* (Cham: Springer International Publishing, 2017), 4-5, <https://doi.org/10.1007/978-3-319-48640-6>.

²⁹⁴ Henriksen, 7.

şekillenmektedir: Wilsonculuk, Hamiltoncılık, Jeffersoncılık ve Jacksoncılık.²⁹⁵ ABD'nin kuruluş ve bir büyük güç olma sürecinde önemli payı olan bu kurucu babaların temsil ettiği görüşler, ABD başkanlarının dış politika uygulamalarında sergilediği yaklaşımlar için farklı alternatif düşünceler barındırmaktadır. Bu kapsamda Wilsoncu yaklaşım ABD'nin açık kader²⁹⁶ fikrinden yola çıkarak özgürlük ve değerlerini yayma amaçlı müdahaleciliği, Hamiltoncu yaklaşım ABD merkezli global bir ticaret ağını, Jeffersoncu yaklaşım özgürlükçü ve demokratik bir ulusal yönetimi, Jacksoncu yaklaşım ise ekonomik korumacılık ile gelişmiş askeri yetenekleri temsil etmektedir.²⁹⁷ Clarke ve Ricketts, söz konusu dört dış politika geleneğinin ulusal ve uluslararası eğilimlerine dikkat çekerek Wilsoncu ve Hamiltoncu yaklaşımın dünyanın geri kalanını kendine benzetmeye çalışan müdahaleci²⁹⁸ yapısına; Jeffersoncu ve Jacksoncu yaklaşımın ise cumhuriyetin erdemlerini mükemmelleştirmeyi esas alan içe dönük²⁹⁹ yapısına dikkat çekmektedir.³⁰⁰

Bahse konu olan dört dış politika geleneği millî menfaatlerin korunması, müdahalecilik, iş birliği ve güç artırımı gibi değişkenler bakımından farklı görüş ve yaklaşımlar bütünü temsil etmektedir. Bentley ve Holland'a göre Mead'in ortaya koymuş olduğu gelenekler, liderlerin esas politika tercihlerini ve muhtemel etkileşimlerini anlamlandırmak için kullanışlı bir anahtar niteliği taşımaktadır.³⁰¹ Yazarlar söz konusu geleneklerin kültürel ve sosyal boyutlara odaklı geniş analiz çerçevesine işaret ederek dış politikadaki bağlamsal farklılıkları da açıklayabilme kabiliyetlerini vurgulamaktadır.³⁰² Quinn'e göre dış politika yalnızca içinde bulunan uluslararası

²⁹⁵ Walter Russell Mead, *Special Providence: American Foreign Policy and How It Changed the World*, 1st ed (New York: Knopf, 2001).

²⁹⁶ Manifest destiny

²⁹⁷ A.g.e.

²⁹⁸ Yazarlar burada ABD'nin aktif politikalarına dinsel bir amaç da ekleyerek "Haçlı" ifadesini kullanmaktadır.

²⁹⁹ Burada da benzer şekilde "vaadedilmiş toprak" ifadesi yer almaktadır.

³⁰⁰ Michael Clarke ve Anthony Ricketts, "Donald Trump and American Foreign Policy: The Return of the Jacksonian Tradition", *Comparative Strategy* 36, sayı: 4 (08 Ağustos 2017): 366, <https://doi.org/10.1080/01495933.2017.1361210>.

³⁰¹ Michelle Bentley ve Jack Holland, ed., *The Obama Doctrine: A Legacy of Continuity in US Foreign Policy?*, 1. bs (New York : Routledge, 2016. | Series: Routledge studies in US foreign policy: Routledge, 2016), 2-4, <https://doi.org/10.4324/9781315731346>.

³⁰² A.g.e., 2-4

ortamın materyal gerekliliklerinin ötesinde, karar vericilerinin entelektüel bakış açılarının bir ürünüdür.³⁰³ Dolayısıyla başkanın benimsemiş olduğu dış politika geleneği, uygulanacak strateji ve uygulamalara yol gösterecek entelektüel bir kılavuz niteliğindedir. Her ne kadar başkanların bahse konu olan dış politika geleneklerin birini benimsemiş olduğu verili olarak kabul edilemese de söylem ve uygulamalarından yola çıkılarak kendileri ile iliştilen gelenekler ABD'nin belirli bir döneme ait dış politika uygulamalarını anlamlandırmak için kullanışlı bir analiz çerçevesi sunmaktadır. Söz konusu analiz çerçevesi son dönemde özellikle Barack Obama ve Donald Trump Başkanlık dönemlerini konu alan çalışmalarda sıklıkla kullanılmaktadır.³⁰⁴ Bahse konu olan çalışmalara bakıldığında Obama dönemi dış politika uygulamalarının Jeffersoncu yaklaşım ile, Trump dönemi uygulamalarının ise Jacksoncu yaklaşım ile ilişkilendirildiği görülmektedir. Bu doğrultuda, adı geçen iki geleneğin ihtiva ettiği yaklaşım ve uygulama biçimleri bir sonraki başlıkta ayrıntılı olarak ele alınmıştır.

3.3.2.1. Jeffersoncu Gelenek

ABD'nin üçüncü başkanı olan Thomas Jefferson, aynı zamanda Amerikan Bağımsızlık Bildirgesinin yazarıdır. Kişisel hak ve özgürlüklerin etkin bir savunucusu olan Jefferson, düzenli ordunun kurulması ve güçlü bir merkezi yönetimin tesisinde Alexander Hamilton ile sıklıkla karşı karşıya gelmiş, bireyin haklarını ihlal edeceği gerekçesiyle devlete minimalist bir görev alanı çizilmesini öngören çalışmalar yapmıştır.³⁰⁵ Jefferson'ın bireyi ön planda tutan ve temel hak ve özgürlükler anlamında bir model ulus olmayı öngören yaklaşımı doğrultusunda, güçlü bir merkezi otorite tehdit olarak görülmüş ve esas yetkilerin yerel eyaletlerde kalması savunulmuştur.³⁰⁶

³⁰³ Adam Quinn, *US Foreign Policy in Context: National Ideology from the Founders to the Bush Doctrine*, Routledge Studies in US Foreign Policy (London ; New York: Routledge, 2010), 23.

³⁰⁴ Clarke ve Ricketts, "Donald Trump and American Foreign Policy"; Jan Niklas Rolf, "Donald Trump's Jacksonian and Jeffersonian Foreign Policy", *Policy Studies* 42, sy 5-6 (02 Kasım 2021): 662-81, <https://doi.org/10.1080/01442872.2021.1934431>; Michael Clarke ve Anthony Ricketts, "Shielding the Republic: Barack Obama and the Jeffersonian Tradition of American Foreign Policy", *Diplomacy & Statecraft* 28, sayı: 3 (03 Temmuz 2017): 494-517, <https://doi.org/10.1080/09592296.2017.1347448>; Bentley ve Holland, *The Obama Doctrine*; Dimitrova, "Trump's 'America First' Foreign Policy"; Walter Russell Mead, "American Populism and the Liberal Order", *Foreign Affairs*, Mart 2017.

³⁰⁵ Mead, *Special Providence*, 177.

³⁰⁶ Clarke ve Ricketts, "Shielding the Republic", 499.

Wilsoncu ve Hamiltoncu geleneğin aksine Amerikan dış müdahalelerine karşı mesafeli duran Jeffersoncu gelenek minimal realist bir dış politika yaklaşımını benimsemektedir. Buna göre amaçlar ve araçlar birbirine uyumlu olmalı, dış politikada izlenecek millî menfaatler mütevazî bir çerçevede tanımlanmalı ve ortaya konulan hedeflere mümkün olan en kısıtlı askerî güç kullanımı ile erişilebilmelidir.³⁰⁷

Mead'e göre Jeffersoncu gelenek dış politikada meydana gelen gelişmelere karşı oldukça temkinlidir. Karşılaşılan olaylara “fırsat” yerine “tehdit” gözlüğünden bakılır.³⁰⁸ Dolayısıyla aktif ve cüretkâr politikalara nadiren rastlanılmaktadır. Mead, İkî Dünya Savaşı arasında ABD'nin izlediği izolasyoncu dış politikayı Jeffersoncu geleneğin o dönemki baskınlığına atfetmektedir.³⁰⁹

Jeffersoncu gelenekte takip edilen dış politika stratejilerine körü körüne bir bağlılık söz konusu değildir. Alternatif durumlar için her zaman açık bir kapı bırakılır ve kamuoyu algısı buna göre şekillendirilir. 1970'lerde Vietnam'dan askerî varlığın geri çekilişi, küçük düşürücü bir mağlubiyetten ziyade merkezi otoritenin kontrolsüz yetkilerinin Jeffersoncu ademimerkeziyetçi mantıkla yeniden gözden geçirilmesi ve anayasal düzene dönüş olarak lanse edilmiştir.³¹⁰

Mead'e göre Jeffersoncu gelenek savaşı, merkezi otoritenin kontrolünü ve baskısını artırdığı gerekçesiyle mesafeli durmaktadır. Ayrıca askerî ve istihbarat kurumlarının üstünde sivil kontrolü üzerinde hassasiyetle durulan bir konudur.³¹¹ Askerî yatırımlar daha çok bütçede meydana gelen açıklar açısından değerlendirilmektedir. Bu doğrultuda savaşı en son seçenek olarak gören Jeffersoncu gelenek karşılaştığı provokasyonlara cevap vermekte hantal davranmaktadır. Ekonomik yaptırımlar her zaman fiziksel çatışmaya tercih edilmektedir.³¹² Çatışma kaçınılmaz olduğu noktada bile tırmandırma basamakları takip edilmekte ve bir anda topyekûn saldırıya girilmemektedir.

³⁰⁷ Walter Russell Mead, “Jacksonian Tradition and American Foreign Policy”, *The National Interest* 58 (1999): 17.

³⁰⁸ Mead, *Special Providence*, 183.

³⁰⁹ Mead, 196.

³¹⁰ Mead, 217.

³¹¹ Mead, 195-96.

³¹² Mead, 188-89.

Jeffersoncu geleneğin bir diğere öne çıkan karakteristiğı ise diplomatik kanalların etkin kullanılmasıdır. Öngörülen dış politika hedeflerine ulaşmak ve muhtemel askeri tırmandırma senaryolarının önüne geçebilmek için diğere devletler ile diyalog kanalları sürekli açık bulundurulmaktadır. Barış ve silahsızlanma antlaşmaları Jeffersoncu geleneğin önemle üzerinde durduğu dış politika araçlarıdır.³¹³ Tek taraflı dış politika girişimleri yerine çok taraflılık olgusu tercih edilir.

Jeffersoncu gelenek bireysel hak ve özgürlükler nazarında ABD'yi bir model ülke haline getirmeyi amaçlamakta, bu süreçte dış politika sorunları ile ilgili minimal bir angajman yaklaşımı taşımaktadır. Bu doğrultuda karşılaşılan sorunların çözümüne ilişkin anahtar kavram “yük paylaşımıdır”. ABD'nin tüm uluslararası sorunları tek başına çözemeyeceğı veya çözmemesi gerektiğı ön kabulünden yola çıkan bu anlayışa göre diğere uluslar ile yapıcı diyaloglar esastır. İş birliğinin geliştirilmesi için yazılı anlaşmalar ve normların üretilmesine çaba harcanır.

Jeffersoncu dış politika geleneğinde dış politikaya ilişkin karar verme süreci sıkı bir fayda/maliyet analizine tabidir. Muhtemel risk faktörleri detaylı bir şekilde ele alınır. Benimsenen politikalara körü körüne bağlılıktan ziyade işler yolunda gitmediğinde duruma göre karar ve uygulama biçimleri değiştirilebilir. Kamuoyu algısı farklı yönde şekillendirilir. Jeffersoncu gelenekte fiziksel çatışma bir son çare aracı olarak görülmektedir. Bu geleneğe göre savaşlar askeri harcamaları ve dolayısıyla bütçe açıklarını artırır. Diğere taraftan ordu üzerinde sivil denetimini güçleştirir. Buradan hareketle yaptırım aracı olarak öncelikle diplomatik, hukuki ve ekonomik tedbirlere başvurulur. Girişilen fiziksel çatışmada esas yaklaşım asgari maliyet ile azami sonucu elde etmektir. İnsan kaybını azaltmak için teknolojik üstünlüğün imkanlarından faydalanılır. Herhangi bir çatışmanın topyekûn savaşa evrilmesinden kaçınılır. Bu suretle tırmandırma basamakları çok dikkatli takip edilerek çatışmanın sınırlı şekilde kalmasına gayret edilir.

3.3.2.3. Jacksoncu Gelenek

Mead'e göre eğer bir karşılaştırma yapmak gerekiyorsa Jeffersoncu gelenek Amerikan aydınlanma çağının ideolojik rehberiyken, Jacksoncu gelenek için orta sınıfın temel

³¹³ Mead, 190.

ideolojisi yansıtan bir düşünce kalıbıdır.³¹⁴ Zira, ABD'nin 7. Başkanlığını yapan Andrew Jackson'ın en önemli politik adımlarından biri erkek nüfusu için oy verme hakkını ülkenin tamamına genişletmesi ve halkı ilk kez politikanın içine davet etmesidir.

Mead'e göre, her iki gelenek bireyin hak ve özgürlükleri ile yakından ilgilidir. Bununla birlikte söz konusu hak ve özgürlükler bakımından farklılıkları bulunmaktadır. Jeffersoncu gelenek ifade özgürlüğü, seçme seçilme hakkı gibi özgürlüklerin yanında yer alırken Jacksoncu gelenek ise bireysel silahlanma hakkını savunmaktadır.³¹⁵

Jacksoncu geleneğe göre yönetim biçimi ne kadar basit ve doğrudan olursa o derece etkindir.³¹⁶ Kariyer diplomatlarına ve elitlere olan güven azdır. Jacksoncu popülist kültür, yozlaşmanın idarenin doğal bir sonucu olduğu ve bürokratik düzeylerdeki yetkililerin bu yozlaşma sebebiyle halkı kandırma eğiliminde olduğu görüşündedir. Buna göre meseleleri karmaşık ifadeler ile dile getirmek elitlerin gerçeği halktan gizlemek için kullandığı bir yöntemdir.³¹⁷

Jacksoncu gelenek uluslararası hukuk ve uluslararası kurumlara en az itibar eden dış politika geleneğidir. Mütakabiliyet ilkesi yazılı hukuk kurallarına tercih edilmektedir.³¹⁸ Eğer rakip kabul edilebilir rekabet koşulları çerçevesinde hareket ediyorsa saygıyı hak etmektedir, ancak birtakım hilelere ve kabul görmeyen yollara başvuruyorsa ona aynı şekilde karşılık verilmelidir. Millî çıkarların tehlike altında olduğuna kanaat getirildiğinde çok hızlı, çok kapsamlı ve tek taraflı olarak harekete geçmekten çekinilmez.³¹⁹ Önleyici savaş da millî menfaatlerin korunmasında takip edilecek seçenekler arasındadır.³²⁰

Jacksoncu gelenek uluslararası düzeni realizm odaklı bir perspektifle anarşik olarak kabul etmektedir. Kendine yardımın temel ilke olduğu bu rekabet ortamında askerî

³¹⁴ Mead, "Jacksonian Tradition and American Foreign Policy", 9.

³¹⁵ Mead, 9.

³¹⁶ Mead, 14-16.

³¹⁷ Mead, 14-16.

³¹⁸ Mead, 18-19.

³¹⁹ Mead, *Special Providence*, 260.

³²⁰ Dimitrova, "Trump's 'America First' Foreign Policy", 41.

yatırım bir hükümetin yapabileceği en olumlu yönetim davranışıdır.³²¹

Jacksoncı gelenek için onur temel bir kavramdır. Bu yaklaşımı savunanlar ABD'nin uluslararası ortamda itibar görmesini oldukça önemsemektedirler. Söz konusu itibar eksikliğinde savaşa bile başvurmayı göze almaktadırlar.

Uluslararası hukuk kuralları ve kurumlara duyulan güvenin en az seviyede olduğu Jacksoncı gelenek kendine yardım ilkesini benimser ve dolayısıyla tek taraflı yaptırımlara karşı oldukça ılımlıdır. Askerî müdahale için millî menfaatlerin tehlikede olduğu inancı esas motivasyon sebebidir. Söz konusu motivasyon sağlandığında önleyici savaş dahil olmak üzere her türlü tek taraflı yaptırıma girişilebilir; uluslararası kamuoyu nezdinde bir haklılık gereksinimi veya savaş için etik bir gerekçe gözetmez.³²² Bahse konu olan bakış açısı yalnızca uluslararası düzeyde sınırlı kalmamaktadır. Dış politikaya ilişkin önemli kararların alınmasında çok taraflı diyalog ile yetkili kişi ve kurumların tartışma ortamından ziyade olabildiğince basit, tek kişi tarafından verilen ve uygulanan kararlar tercih edilir. Mead'in deyiimiyle 'Yönetim ne kadar basit ve doğrudan olursa, sonuçlar o kadar iyi olacaktır.'³²³

Jacksoncı gelenekte dış politikada verilen sözlerin tutulması büyük önem taşımaktadır. Zira üstün bir yaptırım gücünün bulunmadığı uluslararası ortamda davranışlar karşılıklı müteakabiliyet çerçevesinde şekillenmektedir. Tutarlı bir ABD imajının sürdürülmesi büyük önem arz etmektedir. Çünkü başkalarına karşı benimsenen davranışın adil/hileli veya sert/yumuşak oluşu aynı doğrultuda benzer davranış biçimleri ile karşılaşılmasını sağlar.³²⁴ Tavizkar politikalar onursuz ve yararsız kabul edilir, zorbaya karşı zorbaca hareket edilmelidir.³²⁵ Jacksoncı gelenekte sınırlı savaş uzak durulan bir kavramdır. Savaş bir kez başladığında sınırlandırılmamalı ve millî menfaatlere ulaşınca kadar bütün imkanlarla sürdürülmelidir. Savaşlar topyekûn olmalı, kesin zaferle sonuçlanmalıdır.³²⁶ Realizmin temel varsayımlarına en yakın bakış açılarını yansıtan

³²¹ Mead, "Jacksonian Tradition and American Foreign Policy", 14-16.

³²² Mead, 18-19.

³²³ Mead, 14-16.

³²⁴ Mead, 21.

³²⁵ Mead, *Special Providence*, 250-51.

³²⁶ Mead, "Jacksonian Tradition and American Foreign Policy", 23.

Jacksoncı gelenekte millî menfaatler tehdit edildiğinde başvurulacak temel enstrüman askerî güçtür. Bu gelenekte askeri kurumlara olan güven üst seviyededir ve idarenin yapabileceği en yapıcı yönetsel adım askerî güce yatırım yapmaktır.³²⁷

3.2.3.3. İki Dış Politika Geleneği Arasındaki Farklılıklar

Jeffersoncu ve Jacksoncu dış politika gelenekleri devletin güvenlik politikalarına ilişkin ulusal ve uluslararası düzeyde takip edilmesi öngörülen farklı fikirler bütünü temsil etmektedir. İki geleneğin karakteristik özellikleri ele alındığında söz konusu farklılıkların genel olarak işbirliği ve çatışmaya yönelik yaklaşımları etrafında kümelendiği ifade edilebilir. Zira gerek ulusal/uluslararası aktörler ile etkileşim biçimleri, gerekse kuvvet kullanım durumları iki gelenek arasında belirgin farklılıklar sunan ve geleneğin genel güvenlik anlayışını resmeden iki parametre görevi görmektedir.

Bürokrasi ve iş birliğine bakış açıları: Mead'in çalışmasında Jefferson ve Jacksoncu yaklaşımın gerek uluslararası ilişkilerde gerekse dış politikanın oluşturulmasındaki bürokratik süreçte iş birliği bakımından farklı noktalarda olduğu görülmektedir. Jeffersoncu gelenekte dış politikada karşılaşılan sorunların çözümünde ele alınacak tedbirler için anahtar kelime "yük paylaşımıdır". Dış müdahalecilikte minimalist bir anlayışın ağırlıkta olduğu bu gelenekte müttefiklerle diyalog ve iş birliği esastır. Söz konusu iş birlikçi yaklaşımın bir tezahürü de devletin iç bürokratik kademelerindedir. Daha ABD'nin kuruluş yıllarında federal sisteme ilişkin tartışmalarda güçlü bir merkezi sistemin varlığına karşı duran Jeffersoncu geleneğe göre, güç ile otoritenin tek bir merkezde toplanması hak ve özgürlükler açısından sakıncalar barındırmaktadır. Dolayısıyla bu gelenekte paydaşların birbirini denetlediği ve gücün dengeli dağıldığı bir bürokratik yönetim tercih edilmektedir.

Jacksoncu gelenek, tıpkı Jeffersoncu gelenek gibi dış müdahaleciliğe uzak bir duruş sergilemekle birlikte, varlığına veya çıkarlarına yönelik tehditler meydana geldiğinde tek taraflı askerî yaptırımlara başvurabilmektedir. Bu geleneğin uluslararası iş birliğine yönelik bakış açısı realizm ile doğrudan örtüşmektedir. Zira dış politikanın temel motivasyon kaynağı çıkarlar olup hayatta kalmak için kendine yardım ilkesi esastır. Bu doğrultuda iş birliği kavramı menfaatlerin ortak olduğu bazı bağlamsal koşullarda mümkün olmakla birlikte hâkim olan anlayış çıkarlar doğrultusunda kendi başına

³²⁷ Mead, *Special Providence*, 240.

hareket etmektedir. İş birliğine ilişkin benzer durum iç karar alma mekanizmalarında da görülmektedir. Halkın iradesini ön planda tutan bu gelenekte bürokrasinin çeşitli kademelerinde bulunan elitlere kuşku ile bakılmaktadır. Karar alıcı kesim merkezileştikçe, söz sahibi bürokratik kesimin sayısı azaldıkça ve yönetim merkezileştikçe karar alma işlevinin daha fazla başarılı olacağı kabul edilmektedir.



Şekil 4: İş Birliği ve Bürokrasiye Bakış Açısından Jeffersoncu/Jacksoncu Gelenek

Çatışmaya Yönelik Tavır: Jeffersoncu gelenekte hâkim olan anlayış uluslararası ortamda maruz kalınan tehditlere karşı asgari tedbirleri alarak tehdidi bertaraf etmek ve vakit kaybetmeden iç işleyişteki ekonomik, hukuki problem sahalarına dönmektir. Çatışma tırmandırıcı davranışlardan kaçınılır. Başvurulacak tedbirler uzun bir fayda/maliyet analizine tabi tutulur ve çatışmaya müdahil olma durumu ancak faydalar maliyetlerin üzerindeyse tercih edilir. Sorunların çözümünde askerî güç en son opsiyon olarak değerlendirilir. Daha çok ekonomik ve diplomatik yaptırımlar tercih edilir. Askerî gücün kullanımına mesafeli yaklaşılmaktadır. Bir askerî çatışmaya girilmesi zaruri ise tırmandırma basamakları dikkatle takip edilir. Topyekûn güç kullanımından ziyade sınırlı güç kullanımı tercih edilir ve karşı tarafın reaksiyonuna göre güç artırımına başvurulabilir. Çatışma alanlarına en sınırlı müdahale ile en fazla faydayı sağlamayı hedefleyen pragmatik bakış açısı dış politika sorunlarının çözümünde ağırlıklı felsefedir.

Jacksoncu yaklaşımda uluslararası hukuk kurallarına ve uluslararası örgütlerin düzenleyici rolüne inanç zayıftır. Karşılıklı ilişkilerin mütekabiliyet ilkesine dayandığı kabul edilir. Bu doğrultuda uğranılan saldırılara karşı kuvvet kullanımı esastır. Başvurulan sert gücün niteliğinin saldırgan aktörlerin gelecekteki davranış biçimlerini şekillendireceği kabul edilir. Bu yüzden sınırlı güç kullanımından ziyade misli ile mukabele tercih edilir. Askerî kabiliyetlere önem verilir ve bu yönde harcamalar kabul görür. Askeri kabiliyetler tehditler karşısında başvurulacak temel amaçtır. Çatışma süreci

kesin zafer elde edilinceye kadar sürdürülür. Bu süreçte gerginlik artırıcı askerî tedbirlerin kullanımından kaçınılmaz.



Şekil 5: Çatışmaya Yönelik Tavir Açısından Jeffersoncu/Jacksoncu Gelenek

3.3.3. Obama ve Trump Dönemlerinde Takip Edilen Stratejik Kültürün Farklı Dış Politika Kararları Üzerinden İncelenmesi

İki Başkan dönemine ait siber güvenlik belgeleri arasından caydırıcılık metodunu belirgin bir şekilde etkileyen ve genel siber güvenlik yaklaşımına yön veren iki belge PPD-20 ve NSPM-13'tür.

PPD-20, elde bulundurulmuş ofansif siber kabiliyetlerin ikinci bir aktör üzerinde kullanılması öncesinde çok basamaklı ve çok paydaşlı bir onay mekanizması getirmektedir. NSPM-13 ise söz konusu bürokratik süreci kısaltarak angajman yetkisini siber komutanlık direktörüne devretmektedir. Bürokrasi ve iş birliği açısından PPD-20'nin karar öncesi çok paydaşlı istişareyi kapsayan bürokratik bir işleyişi yansıttığı, NSPM-13'ün ise planlamadan ziyade icraya yönelen ademimerkeziyetçi pratik bir yapı barındırdığı görülmektedir. Çatışma kriteri açısından bakıldığında ise PPD-20'nin ofansif siber kabiliyetlerin kullanımını zorlaştıran, siber uzayda tırmanmadan kaçınarak farklı yaptırımları önceleyen bir yaklaşım benimsediği; buna karşın NSPM-13'ün ofansif siber kabiliyetlerin zamanında ve aktif kullanımını teşvik eden çatışmacı bir anlayışı yansıttığı ifade edilebilir.

Bu değerlendirmeler doğrultusunda PPD-20'nin hem çatışma hem de iş birliğine yaklaşım kriterleri açısından Jeffersoncu dış politika yaklaşım düşünce yapısını; NSPM-13'ün ise Jacksoncu anlayışı yansıttığı sonucuna varılmaktadır. Bu noktada akları gelen soru PPD-20 belgesinin Obama dönemi, NSPM-13'ün ise Trump dönemi genel caydırıcılık anlayışını yansıtır yansıtmadığıdır. Başka bir deyişle bu belgelerin temsil ettiği geleneklerin başkanlık dönemine ilişkin birer anomali olmaması ve genel güvenlik politikaları ile uyumlu olması elde edilen bulguyu anlamlı hale getirecektir. Söz konusu

yaklaşımların başkanların diğer dış politika kararları ile paralellik göstermesi bahse konu olan caydırıcılık stratejisi farklılaşmasının liderin takip ettiği stratejik kültür biçiminden kaynaklı doğal ve mantıksal bir tercih olduğunu ortaya koyacaktır. Bu doğrultuda, çatışma ve iş birliği yaklaşım pratiklerinin izleri, benzer koşullar altında gerçekleşen ve her iki lider döneminde de ofansif kabiliyetlerin kullanımına ilişkin kararlar almayı gerektiren örneklerle karşılaştırılmıştır. Bu örnekler Suriye rejimine yönelik yaptırımlar ve dron kullanımlarıdır.

3.3.3.1. Suriye Rejimine Yönelik Yaptırım Kararı

Arap Baharı sürecinde Suriye iç çatışması ile ilgili olarak Obama yönetiminin en fazla tartışılan kararı, kimyasal silah ultimatunun yerine getirilmemesidir. Esad'ın elindeki kimyasal silah stoğunun farkında olan Beyaz Saray, söz konusu silahların sivil halk üzerinde kullanımını bir “kırmızı çizgi” olarak tanımlamış, bu silahlara başvurulmasının cezai sonuçları olacağını net bir şekilde dile getirmiştir.³²⁸ Buna karşın 2013 yılında başkent Şam yakınlarında rejim güçleri tarafından muhalif güçlere karşı sarin gazı kullanılmış ve 1500 sivilin ölümü meydana gelmiştir.³²⁹

Uyguladığı zorlayıcı diplomasinin başarısızlığı karşısında Başkan Obama beklentilere rağmen askerî müdahale seçeneğini değerlendirmemiştir. Bunun yerine Rus yönetimi ile diyaloga girilerek Esad'ın elinde bulunan kimyasal silah stoğunun Rusya'ya devredilmesi kararı alınmıştır. Verilen sert ultimatunun bu şekilde yumuşak bir çözüm ile geçirilmesi ABD dış politika saygınlığını zedelediği gerekçesiyle eleştirilere maruz kalmıştır.

2017 yılında Trump liderliğindeki ABD yönetimi çok benzer bir gelişme ile karşılaştığında tepkisi sert ve hızlı olmuştur. Suriyeli muhaliflerin kontrolündeki Han Şeyhun kentine yapılan kimyasal saldırı, seksen sivilin ölümü ile neticelenmiştir. Bu durum karşısında vakit kaybedilmeden askerî yaptırım kararı alınmış, saldırıyı gerçekleştiren savaş uçaklarının kalktığı Şayrat havaalanı 63 saat sonra Tomahawk

³²⁸ Glenn Kessler, “President Obama and the ‘red line’ on Syria’s chemical weapons - The Washington Post.pdf”, *Washington Post*, 06 Eylül 2013, <https://www.washingtonpost.com/news/fact-checker/wp/2013/09/06/president-obama-and-the-red-line-on-syrias-chemical-weapons/>.

³²⁹ Fred Kaplan, “The President in Practice”, *Foreign Affairs*, Şubat 2015, <https://www.foreignaffairs.com/united-states/obamas-way>.

füzeleri ile vurulmuştur.³³⁰ Obama'nın Suriye politikasında koymuş olduğu kırmızı çizgileri uygulamamasını bir "küçük düşme"³³¹ olarak niteleyen Trump, benimsemiş olduğu çatışmacı tavırla ceza yoluyla caydırıcılığı ön plana çıkaran adımlar atmıştır.

3.3.3.2. Dron Saldırıları

Dron saldırılarının bir önleyici güvenlik tedbiri olarak kullanımı Obama yönetimi ile özdeşleştirilen bir konudur. Obama'nın başkanlık döneminde Yemen, Pakistan, ve Somali'de toplam 506 adet dron saldırısı düzenlenmiş, bu saldırılarda 3040 terörist ve 391 sivil öldürülmüştür.³³² Buna karşın meydana gelen sivil ölümleri eleştirilerine karşı kamuoyunu ikna çabası altı çizilmesi gereken bir noktadır. 2013 yılında yayımlanan Başkanlık Siyaset Rehberi sivil zayıatın önüne geçilmesi için birtakım kuralları karara bağlamıştır. Buna göre; tehdit değerlendirmesi esnasında sivil ölümlerin olmayacağı "neredeyse kesin" olacak ve Pentagon'un operasyon kararı öncesi Ulusal Güvenlik Konseyinin onayı alınacaktır.³³³ Aynı şekilde 2016 yılında yayımlanan 13732 sayılı Başkanlık İcra Emri sivil ölümlerinin araştırılması konusunda devlete bağlı kurumları harekete geçirmiş, Ulusal İstihbarat Ajansına bu konuda Kongreye senelik rapor sunma görevi vermiştir. Bu doğrultuda Obama'nın dron saldırılarını aktif bir güvenlik tedbiri olarak konumlandırmakla birlikte bunların etkilerini sınırlandırıcı tedbirler aldığı görülmektedir.

Her ne kadar dron saldırıları Başkan Obama ile birlikte sıklıkla anılsa da bu yönteme Trump döneminde daha fazla başvurulmuştur.³³⁴ Bununla birlikte Trump dönemine dair altı çizilmesi gereken nokta niceliksel artıştan ziyade bu operasyonların işleyiş tarzı ve denetim mekanizmaları ile ilgilidir. Zira Trump, dron kullanımını Obama döneminin

³³⁰ Luis Da Vinha, "A Tale of Two Red Lines: Managing Foreign Policy Crises in the Obama and Trump Administrations", *Comparative Strategy* 40, sayı: 1 (02 Ocak 2021): 64, <https://doi.org/10.1080/01495933.2021.1853441>.

³³¹ Rolf, "Donald Trump's Jacksonian and Jeffersonian Foreign Policy", 674.

³³² Micah Zenko, "Obama's Embrace of Drone Strikes Will Be a Lasting Legacy", *Haber, New York Times*, 12 Ocak 2016, <https://www.nytimes.com/roomfordebate/2016/01/12/reflecting-on-obamas-presidency/obamas-embrace-of-drone-strikes-will-be-a-lasting-legacy>.

³³³ Charlie Savage, "U.S. Releases Rules for Airstrike Killings of Terror Suspects", *The New York Times*, 06 Ağustos 2016, <https://www.nytimes.com/2016/08/07/us/politics/us-releases-rules-for-airstrike-killings-of-terror-suspects.html>.

³³⁴ BBC, "Trump revokes Obama rule on reporting drone strike deaths", 07 Mart 2024, <https://www.bbc.com/news/world-us-canada-47480207>.

sınırlandırıcı prosedürlerinden arındırmıştır. Saldırı öncesi hükümet yetkililerinin onayını içeren prosedür yerine CIA ve Pentagon’a geniş yetki alanları tanımıştır.³³⁵ Terörizme karşı alınan tedbirlerin hızlı ve efektif olmasını savunan Trump, dron kullanımında saha operatörlerine operasyonun icrası konusunda önemli yetkiler tanımıştır.³³⁶ Buna ek olarak, 2019 yılında yayımlamış olduğu Başkanlık İcra Emri 13862 ile Obama döneminde yürürlüğe konulan sivil zayıat durum raporlarının kongreye sunulması uygulamasını yürürlükten kaldırmıştır.³³⁷

Ofansif kabiliyetlerin kullanımında bürokrasi ve çatışmaya yönelik tavırları gösteren bu iki örnek, Obama döneminde Jeffersoncu geleneğin, Trump döneminde ise Jacksoncu geleneğin hâkim olduğunu göstermektedir. Dolayısıyla siber güvenlik politikaları özelinde görülen farklı yaklaşımların birer anomali olmadığı, başkanların genel karar alma çerçevelerinin birer uzantısı olduğu görülmektedir. Bu doğrultuda ceza yoluyla caydırıcılık stratejisi bakımından Trump ve Obama döneminde görülen farklı uygulamaların doğrudan ilgili başkanların benimsemiş olduğu stratejik kültürlerden kaynaklandığı ifade edilebilir.

3.3.4. Jeffersoncu ve Jacksoncu Dış Politika Geleneklerinin Siber Caydırıcılık Politikalarına Etkileri

Obama ve Trump dönemlerinin dış politika uygulamaları farklı çatılar altında karakterize edilebilen yaklaşım pratiklerini yansıtmaktadır. Mead’in Amerikan dış politika gelenekleri doğrultusunda Obama’nın dış politika sorunlarına ilişkin ifade, karar ve uygulamaları Jeffersoncu gelenek özelliklerini yansıtırken diğer taraftan Trump döneminde Jacksoncu gelenekle örtüşen başkan davranışları gözlemlenmektedir. Mead’in her iki geleneğe dair farklılıkları genel çerçevede toplayan iki bileşene bakıldığında iki başkanın sorunları ele alış bakımından ne kadar farklı noktada olduğu görülebilir. İş birliği ve bürokrasiye bakış açısı bakımından Obama, uluslararası alanda diyalog kanallarını işleten, diplomasi ve örnek olma yoluyla norm oluşturma çabası

³³⁵ Charlie Savage ve Eric Schmitt, “Trump Poised to Drop Some Limits on Drone Strikes and Commando Raids”, *The New York Times*, 21 Eylül 2017, <https://www.nytimes.com/2017/09/21/us/politics/trump-drone-strikes-commando-raids-rules.html>.

³³⁶ Charlie Savage, “Trump’s Secret Rules for Drone Strikes Outside War Zones Are Disclosed”, *The New York Times*, 01 Mayıs 2021, <https://www.nytimes.com/2021/05/01/us/politics/trump-drone-strike-rules.html>.

³³⁷ Beyaz Saray, “İcra Emri 13862”, 06 Mart 2019, <https://www.federalregister.gov/presidential-documents/executive-orders/donald-trump/2019>.

gösteren ve çok taraflı iş birliğini savunan bir yaklaşım göstermektedir. Bürokrasi yönünden karar alma süreçlerinde uzman görüşlerine değer veren benzer bir yaklaşım göstermektedir. Aynı değişken kapsamında Trump'ın ise uluslararası ittifak ve anlaşmalara yönelik güvensiz duruşu benzer şekilde iç politikada elit görüşlerine değer vermemesi ile benzerlik göstermektedir. Bu doğrultuda Trump'ın uluslararası siyasette benimsediği kendine yardım prensibinin bürokratik anlamda da merkeziyetçi uygulamalar olarak yansıma bulduğu ifade edilebilir. Kısaca İş birliği ve bürokrasiye bakış değişkeni bakımından Obama'ya “yardımlaşmacı”, Trump'a ise “merkeziyetçi” değerlerini atfetmek yanlış olmaz.

Çatışmaya yönelik tavır değişkeni açısından Obama'nın askerî tedbirler yerine farklı kabiliyetleri öncelemesi, askerî kabiliyetin geliştirilmesi ve denetimi anlamında gösterdiği sınırlandırıcı yaklaşımlar ve çatışmaları sınırlı seviyede tutmaya çalışması Jeffersoncu yaklaşım ile paralellik içerisindedir. Jacksoncu geleneğin izlerini taşıyan Trump uygulamaları ise maruz kalınan saldırılara karşı askerî sert reaksiyonları öngörmekte, verilecek reaksiyonun niteliğinin mütekabiliyet ilkesi gereği ABD imajıyla doğrudan bağlantılı olduğunu savunmaktadır. Bu doğrultuda kontrollü ve sınırlı bir angajman yerine kesin ve cezalandırıcı askerî tedbirlerin kullanımını benimsemektedir. Bu çerçevede söz konusu değişken bakımından Obama'yı “sınırlandırıcı”, Trump'ı ise “çatışmacı” olarak özetlemek mümkündür.

	İşbirliği ve Bürokrasiye Bakış	Çatışmaya Yönelik Tavır
Barack Obama	Yardımlaşmacı	Sınırlandırıcı
Donald Trump	Merkeziyetçi	Çatışmacı

Tablo 5: İş Birliği-Bürokrasi ve Çatışmaya Yönelik Tavır Bileşenleri Kapsamında Obama ve Trump Karakteristikleri

Stratejik kültür doğrultusunda benimsenen farklı yaklaşımlar caydırıcılık stratejilerine doğrudan etki etmektedir. Burada karşı aktörlere karşı uygulanacak ceza bileşeninin kullanım durumuna dair somut farklılıklar göze çarpmaktadır. Dolayısıyla Ceza yoluyla caydırıcılık metodu iki başkan dönemi arasındaki caydırıcılık stratejilerinin en bariz farklılık noktasını teşkil etmektedir. Obama döneminde Savunma Bakanlığı ve Siber Komutanlık caydırıcılık stratejilerinin uygulanmasında arka planda kalmış, bu birimler

tarafından icra edilecek ofansif siber kabiliyetler sınırlandırılmış ve yerini askerî olmayan tedbirlere bırakmıştır. Bu doğrultuda söz konusu dönemde gerek cezai yaptırımlar bakımından gerekse saldırgan aktörlere verilecek mesajın ciddiyeti bakımından yumuşak bir ceza yoluyla caydırıcılığın benimsendiği görülmektedir. Diğer taraftan Trump döneminde ise Siber Komutanlığın siber uzaydaki tehditlerin cezalandırılması sürecinde esas aktör olduğu, askerî kabiliyet gelişimi ve bu kabiliyetlerin kullanımı konusunda rakiplere inandırıcı mesajlar verildiği net bir ceza yoluyla caydırıcılık metodunun ortaya konulduğu görülmektedir. Bahse konu olan farklılığın arkasında yatan ana faktör Obama'nın sınırlandırıcı ve Trump'ın çatışmacı dış politika yaklaşımını benimsemesidir. Aşağıda örnekleri sunulduğu üzere, çatışmaya yönelik tavır değişkeni bağlamında iki başkanın benimsediği sınırlandırıcı ve çatışmacı davranış biçimleri farklı dış politika sorunlarında askerî tedbirlerin bir cezai yaptırım olarak kullanılış düzeylerini belirlemiştir. Farklı örnekler ile desteklenen çatışmaya yönelik tavır değişkeninin belirleyiciliği ceza yoluyla caydırıcılık metodunun farklılığını açıklamada da etkilidir. Söz konusu değişkenin üç düzeyde belirleyici olduğu ve bu düzeylerde sunulan başkanlık uygulamalarının ceza yoluyla caydırıcılık metodundaki farklılığa sebebiyet verdiği görülmektedir:

- Alan içi ve alan dışı yaptırımlar
- Yetkilendirme durumu
- Kabiliyet geliştirme

Ceza yoluyla caydırıcılığın tesisinde saldırgan aktör statükoyu bozmaması için mesaj yoluyla uyarılır. Bu mesajlar yazılı veya sözlü olabildiği gibi benzer olaylarda gösterilen yaptırımlar ilerideki muhtemel saldırgan davranış için uyarı niteliği taşır. Söz konusu yaptırımlar sıkı bir mütekabiliyet ilkesi çerçevesinde gerçekleştiğinde askerî nitelikli saldırılara karşı askerî güç kullanımı görülmektedir. Bununla birlikte tırmanmayı önleyici hassasiyetler doğrultusunda zaman zaman karşılaşılan askerî tehditlere karşı askerî olmayan tedbirler de ortaya konulabilir. Bu durum alan içi ve alan dışı tedbirlerin kullanımı şeklinde adlandırılmaktadır. Siber uzay ortamında değerlendirildiğinde, maruz kalınan siber saldırılara karşı benimsenen cezai yaptırımların ofansif siber kabiliyetlerden meydana gelmesi alan içi yaptırımları ifade ederken, ilgili tehditler karşısında diplomatik, ticari, hukuksal yaptırımlara başvurulması alan dışı yaptırım anlayışına işaret etmektedir. Barack Obama'nın başkanlık döneminde

takip edilen sınırlandırıcı yaklaşım doğrultusunda fiziksel çatışma alanlarına mesafeli yaklaşıldığı, askerî kabiliyetlerin kullanımından kaçınılarak alan dışı tedbirlere öncelik verildiği, kullanılan askeri tedbirlerin ise kısıtlandığı görülmektedir. Söz konusu duruma dair örnekler Suriye ve Libya gibi Obama döneminde müdahil olunan çatışma alanlarından sunulabilir.

Suriye’de rejim güçleri ve muhalifler arasında süren çatışmalarda kimyasal silah kullanımı konusunda Esad yönetimi bizzat Başkan Obama tarafından uyarılmış ve söz konusu davranış sonucunda askerî yaptırımlar olacağı ifade edilmiştir. Buna rağmen arzu edilen caydırıcılık sağlanamamış ve kimyasal silah kullanım eşiği aşılmıştır. Bahse konu olan durum karşısında beklenen askerî müdahale gerçekleşmeyerek alternatif çözüm arayışlarına girilmiş ve sonuç olarak Rusya’nın arabuluculuk önerdiği kimyasal silah stoğunun devredilmesi seçeneği benimsenmiştir. Söz konusu çözüm kuşkusuz istenen statüko durumunun bozulmasına yol açacak saldırgan aktör davranışlarının caydırılmasına yönelik zayıflatıcı bir nitelik taşımaktadır. Zira diplomasi yoluyla başvurulmuş bu alan dışı yaptırım caydırıcılık konusunda ABD yönetimin inandırıcılığını sekteye uğratmıştır. Bahse konu olan süreçte Başkan Obama kimyasal saldırının gerçekleşmesi sonrasında beklenen hava taarruzu emrini vermemiş ve karar sorumluluğunu Kongreye bırakmıştır. Kongrede de belirleyici bir kararın çıkmaması doğrultusunda yaşanan süreçte Rusya’nın teklifi bir kurtarıcı olarak görülmüştür. Bu doğrultuda teklif edilen diplomatik yaptırımın cezai niteliğine bakılmaksızın alan dışı tedbir kullanılarak çatışma ortamına fiziksel müdahaleden kaçınılmıştır.

Obama yönetiminin çatışma alanlarına fiziksel olarak müdahil olunduğu durumlarda da askerî gücü kısıtlayıcı tedbirler geliştirdiği görülmektedir. Arap Baharı sürecinin etkilediği bir diğer ülke olan Libya’da Kaddafi yönetimine karşı girişilecek insani müdahale seçeneğinde Obama tarafından önceki ABD uygulamalarıyla bağdaşmayan “geriden liderlik” kavramının ortaya atılması ve gerçekleşen hava harekâtında önemli derecede alanın Fransa ve İngiltere yeteneklerine bırakılması çatışma alanlarındaki askerî varlığa ilişkin sınırlandırma anlayışının bir başka örneğidir. Örneği verilen dış politika sorunlarına benzer şekilde siber uzayda da karşılaşılan tehditlere karşı bizzat Başkan Obama’nın imza atmış olduğu diplomatik diyalog ve İcra Emirleri doğrultusunda sınırlandırma davranışına gidilmiş, ofansif siber kabiliyetlerin cezai niteliğine başvurulmamıştır.

2012-2016 yılları arasında ABD'ye bağılı çeşitli kurum ve şirketlerin Çin, İran ve Kuzey Kore gibi aktörler tarafından ciddi siber saldırılara maruz kalması neticesinde muhtemel gelecek saldırıları caydırmak için bir ceza tesis edilmek istenmiştir. Ancak sınırlandırma hassasiyetinin bir parçası olarak bahse konu olan saldırılara yönelik siber-askerî misilleme yoluna gidilmemiştir. Dolayısıyla ceza yoluyla caydırıcılık stratejisinin ceza bileşeni alan içerisinde seçilmemiştir. Bunun yerine alan dışı ceza arayışına gidilerek saldırıların arkasında bulunan devletleri doğrudan cezalandırmak yerine saldırıyı gerçekleştiren kişi, kurum ve bağlılarına münferit olarak bedel ödetilmiştir. Söz konusu cezaların çeşidi ise yargısal ve ticari niteliktedir. Bu süreçte Adalet Bakanlığı ve Ticaret Bakanlığı ile koordineli bir şekilde hareket eden Obama yönetimi, sınırlandırma prensibi ile hareket ettiği münferit cezalarda söz konusu kişi ve kurumları sınır dışı etme, mahkûmiyet cezası verme ve mal varlıklarına el koyma gibi tedbirlere yönelmiştir.

Doğrudan Başkan Obama inisiyatifi ile yürürlüğe giren İcra Emri-13687, onun bu konudaki caydırıcılık stratejisine bakış açısını yansıtmaktadır. Sony Yapım Şirketi'ne yapılan siber saldırı sonucu açık bir şekilde Kuzey Kore hükümetini hedef alan belge, caydırıcılık mesajını net bir şekilde vermekle birlikte ceza bileşeni olarak ticari yaptırımlara yönelmiştir. Obama'nın bu yaklaşımının ilk sinyallerini göreve geldikten kısa bir süre sonra yayımladığı Ulusal Güvenlik Strateji Belgesinde görmek mümkündür. Bir önceki yönetimin güç kullanım pratiklerine üstü kapalı göndermede bulunan belgede kuvvete başvurmadan önce diğer bütün seçeneklerin uygulanacağı ifade edilmektedir.³³⁸

Ghalehdar'a göre Obama, kuvvet kullanımını bir inandırıcılık unsuru olarak tercih etmemektedir. Obama'nın Libya, Suriye ve Afganistan'daki kuvvet kullanım pratiklerini inceleyen Ghalehdar, söz konusu uygulamaların pragmatik hedeflere yöneldiğini ve rakibe gözdağı verme amaçlı herhangi bir mesaj kaygısı amacıyla yürütülmediğini savunmaktadır.³³⁹ Bu açıdan bakıldığında, dönemin sınırlandırma yaklaşımına da uygun olarak Başkan Obama Çin, İran ve Kuzey Kore gibi devletlere

³³⁸ Henderson, "The 2010 United States National Security Strategy and the Obama Doctrine of 'Necessary Force'", 418.

³³⁹ Payam Ghalehdar, "The Purpose of Military Force and the Obama Doctrine: No Fighting for Face", *International Relations*, 31 Ocak 2023, 004711782311519, <https://doi.org/10.1177/00471178231151907>.

siber güç kullanımı yoluyla gözdağı verme yolunu tercih etmemiştir. Bundan ziyade tesis etmeye çalıştığı cezalandırıcı caydırıcılığın ceza bileşenini hukuki ve ticari alan dışı tedbirlerden seçme yoluna gitmiştir. Alan dışı yaptırımlara ilişkin çatışmaya yönelik tavır bağlamında Trump dönemindeki örneklerin ise tamamen farklı olduğu görülmektedir. Obama döneminin reaksiyon göstermekte etkisiz kaldığı Esad rejimi kimyasal silah kullanımı örneğinin tekrar yaşandığı 2017 yılında, aynı koşullarda Trump yönetimi 63 saat gibi kısa bir sürede hava taarruzu emri vererek askerî yaptırımı uygulamıştır. Trump'ın çatışmacı yaklaşımının caydırıcılığın mesaj ve inandırıcılık bileşenlerine verdiği önem başvurduğu askerî kabiliyetin niteliğinden anlaşılabılır. Afganistan'daki küçük bir IŞİD hücreğine karşı “tüm bombaların anası” olarak bilinen ABD ordusunun en büyük nükleer olmayan bombasının kullanılması kuşkusuz hedefin fiziken yok edilmesinin ötesinde saldırgan aktörlere çatışmadan hiçbir seviyede kaçınılmayacağına dair net bir mesaj niteliğindedir.³⁴⁰

Trump'ın diğer askerî sorunlara ilişkin göstermiş olduğu çatışmacı yaklaşım siber uzayda karşılık bulmuş, siber uzayda meydana gelen tehditlere karşı siber ofansif kabiliyetlere başvurulmuştur. Ulusal Güvenlik Danışmanı John Bolton'ın siber uzayda hedef aradıklarını ve artık av değil avcı olacakları söylemi ve düzenlenen ofansif siber operasyon sayılarındaki ciddi artış, çatışmacı yaklaşımın Amerikan siber güvenlik politikalarına bu dönemdeki iz düşümü niteliğindedir.³⁴¹ Geliştirilen kabiliyetlerin ofansif siber kabiliyetlere evrilmesinin önünü açan temel unsur ise yetkilendirme konusudur.

Obama ve Trump başkanlık dönemlerindeki ceza yoluyla caydırıcılık metodu farklılaşmasına dair en önemli belirleyici nokta Siber Komutanlığın yetkilendirme konusudur. Bu kapsamda doğrudan başkan imzalı olan 20. Başkanlık Siyaset Direktifi (PPD-20) ve 13. Ulusal Güvenlik Başkanlık Memorandumu (NSPM-13) önemli kilometre taşlarıdır. Bu iki belge ofansif siber operasyon düzenleme yetkisi konusunda farklı yaklaşımları ihtiva etmektedir. PPD-20 ofansif siber operasyon düzenleme yetkisini Siber Komutanlık direktöründen alarak bunu başkanın nihai onaylayıcı olduğu

³⁴⁰ Clarke ve Ricketts, “Donald Trump and American Foreign Policy”, 374.

³⁴¹ Michael Farrell, Tim Starks, ve Gavin Bade, “Trump Is Rattling Sabers in Cyberspace — but Is the U.S. Ready?”, Politico.com, 13 Temmuz 2019, <https://www.politico.com/story/2019/07/13/trump-cybersecurity-defense-1415650>.

ve birçok kurumun müdahil olduğu çok paydaşlı bir mekanizmanın iradesine bırakmaktadır. Trump dönemi belgesi olan NSPM-13 ise uygulamayı tersine çevirerek planlama ve icra yetkisini doğrudan Siber Komutanlık Direktörüne vermektedir. İki belge arasındaki farklılık başkanlara dair çatışmaya yönelik tavır ve iş birliği/bürokrasiye bakış konumlanmasını özetler niteliktedir. Obama uygulamalarını “hantal” ve “fazla bürokratik” bulan Trump, imzalamış olduğu başkanlık memorandumunu ile birlikte ofansif siber harekât karar alma sürecindeki çoklu yapıyı devre dışı bırakmış ve siber tehlikelerin “zamana karşı hassas” durumuna dayanarak karar alma yetkisini siber komutanlığa devretmiştir.³⁴² PPD-20’nin ortaya koyduğu çok paydaşlı bürokrasi temelli karar mekanizması operasyonel faaliyetlerin onaylanma sürecini hantallaştırarak sınırlandırma davranışına hizmet etmektedir. Diğer taraftan NSPM-13 yoluyla karar yetkisinin alt kademedeki icracı komutana tek merkezli bir şekilde devredilmesi operasyonel faaliyetlerin önünü açan çatışmacı yaklaşım ile eş güdüm içerisindedir. İcra edilen ofansif siber operasyon rakamları her ne kadar gizli tutulsa da Siber Komutanlık direktörlerinin açıklamalarından operasyonel anlamda Trump döneminde çok daha aktif bir Siber Komutanlık rolü bulunduğu açık bir şekilde görülmektedir. ABD Siber Komutanı ve Ulusal Güvenlik Ajansı Direktörü General Paul Nakasone’un NSPM-13 öncesi ve sonrası siber uygulamaları değerlendiren aşağıdaki ifadeleri dikkat çekicidir:

“Yetki, siyaset ve strateji açısından son 18 ayda muazzam değişiklikler yaşandı...Geçtiğimiz 10 yıl içerisinde maruz kaldığımız siber saldırılara karşı neredeyse hiçbir şey yapmadık...Artık pasif durumda değiliz.”³⁴³

Nakasone’un bu açıklamaları bir taraftan ofansif siber kabiliyetlerin kullanımına yönelik yönetimler arası anlayış farklılıklarına işaret ederken diğer taraftan

³⁴² Suzanne Smalley, “Biden Administration Is Studying Whether to Scale Back Trump-Era Cyber Authorities at DOD”, CyberScoop.com, 31 Mart 2022, <https://cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/>; Savunma Bakanlığı, “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference U.S. Department of Defense Speech”, 02 Mart 2020, <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>; Washington Post, “The Cybersecurity 202: Trump just gave the military a lot more leeway to launch cyber operations”, Haber, 17 Ağustos 2018, <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/17/the-cybersecurity-202-trump-just-gave-the-military-a-lot-more-leeway-to-launch-cyber-operations/5b75a7551b326b7234392972/>.

³⁴³ Dilanian, “Under Trump, U.S. Military Ramps up Cyber Offensive against Other Countries”.

caydırıcılığın mesaj ve inandırıcılık bileşenlerinin geliştirilmesine yönelik Trump yönetimi tarafından izlenen siber caydırıcılık stratejisine somut bir şekilde hizmet etmektedir. Bu durum, Trump'ın Ulusal Güvenlik Danışmanı John Bolton'un kaleme almış olduğu anılarında açıklıkla anlaşılmaktadır. Obama dönemi siber politikalarını pasif ve etkisiz olarak niteleyen Bolton, Trump döneminde benimsenen Siber Stratejinin bu eksikliğe cevap verdiğini ancak süreç içerisinde alınan karar ve başvurulmuş uygulamaların gerektirdiği gizlilik prensibi doğrultusunda rakiplere gözdağı vermekte sıkıntı yaşandığını dile getirmektedir. Bu yüzden Nakasone gibi üst düzey yetkililere ABD'nin ulaşmış olduğu siber ofansif yetenekler hakkında kamuoyunu bilgilendirici üstü kapalı açıklamalar yapılması talimatı verildiğini ifade etmektedir.³⁴⁴ Kamuoyu açıklamaları üzerinden muhtemel saldırgan aktörlere iletilen mesajlar ABD'nin siber ofansif kabiliyetlerinin üst düzeye eriştiğini ve söz konusu kabiliyetlerin kullanımında bir tereddüt bulunmadığını aktarma niyetindedir. Obama dönemi bürokratik sınırlandırmaların geride bırakıldığını özenle vurgulayan açıklamalar, kuvvet kullanımının herhangi bir engel veya limite bağlı kalmaksızın uygulanacağını dile getirmektedir.

Yetkilendirmeye ilişkin bürokratik/merkeziyetçi, sınırlandırıcı/çatışmacı yaklaşım farklılıkları siber uzaya mahsus değildir. Benzer durum dron saldırılarının kullanımında da görülmektedir. Obama döneminin önemli askerî kabiliyetlerinden olan dron saldırılarının Afganistan'da birçok sivil ölümüne yol açtığı eleştirisi sonrası hedef belirleme kriterinin çok paydaşlı mekanizmaya bırakılması ve icra edilen operasyonlara ilişkin Kongreye rapor verme zorunluluğu Obama dönemi bürokratik-sınırlandırıcı yaklaşımı gösterirken, Trump döneminde operasyonel icrada Pentagon ve CIA'nın tam yetkili kılınması ve Kongreye rapor zorunluluğuna son verilmesi merkeziyetçi-çatışmacı yaklaşımı gözler önüne sermektedir.

Ceza yoluyla caydırıcılık metodundaki farklılaşmaya ilişkin bir diğer belirleyici ise askerî kabiliyetlerin geliştirilmesine ilişkin tutumlardır. Obama dönemi hâkim dış politika anlayışı olan Jeffersoncu geleneğe uygun şekilde askerî harcamaların azaltılması ve asker üzerinde etkin bir sivil kontrolü gerek genel güvenlik politikasında gerekse Siber caydırıcılık stratejisinde yansımalar bulmuştur. Obama'nın başkanlık döneminde

³⁴⁴ John Bolton, *The Room Where It Happened: A White House Memoir* (New York: Simon and Schuster, 2020), 161-69.

askeri harcamalar %15’lik azalışla 750 milyar dolardan 640 milyar dolara kadar gerilemiştir. İki bölgesel savaşı aynı anda sürdürebilme hedefinden vazgeçilerek yönünü Çin’e dönen ve bu süreçte askeri harcamalardaki düşüşün gerekliliklerini savunan Obama, sonraki on yıl için de önemli ölçüde askerî harcama kesintisi tablosu çizmiştir.³⁴⁵ Askerî kabiliyetlere ilişkin sınırlı vizyon aynı dönemde siber kabiliyetler özelinde de yansıma bulmaktadır. 2009 yılında kurulan Siber Komutanlık, kendine özgü ayrı kabiliyetleri geliştirmektense Ulusal Güvenlik Ajansı ile aynı yerleşkede konuşlandırılmış, iki birimin ortak kabiliyet havuzunu kullanması öngörülmüştür. Söz konusu adım, askerî ve istihbari operasyonların istihbari yeteneklere zorunlu kılması diğer taraftan sivil bir kurum olan Ulusal Güvenlik Ajansı tarafından Siber Komutanlık operasyonlarının yakın denetimini mümkün kılmıştır.

Siber Komutanlığın Savunma Bakanlığı hiyerarşisindeki yeri ve idari büyüklüğü de askerî yeteneklere ilişkin sınırlandırıcı yaklaşımın izlerini barındırmaktadır. Savunma Bakanlığına bağlı Stratejik Komutanlığın bir alt birimi olarak konumlandırılan Siber Komutanlık esas itibariyle nükleer caydırıcılıktan sorumlu bir birime hesap verir halde teşkil edilmiştir. Söz konusu yaklaşım ofansif siber kabiliyetlere bakış açısına dair çarpıcı ipuçları sunmaktadır. Siber Komutanlığın askerî hiyerarşide yükselerek doğrudan Savunma Bakanlığı’na bağlı hale getirilmesi Trump döneminde meydana gelmiştir. 2009 yılında kurulan ve Stratejik Komutanlık bünyesinde bir alt birim olarak faaliyet gösteren Siber Komutanlık, 2018 yılı itibariyle Başkan Trump tarafından Muharip Komutanlık seviyesine çıkarılmıştır.³⁴⁶ Diğer kuvvet komutanlıkları ile eş seviyeye ulaşan birim, doğrudan Savunma Bakanlığı’na bağlı hale gelmiş, kaynak ve faaliyet alanı olarak kayda değer bir ilerleme kaydetmiştir.

2019 yılı başında Siber Komutanlık, diğer kuvvet komutanlıklarının siber unsurlarının bir çatı altında toplandığı 4406 personelin görev yaptığı ciddi bir planlama ve uygulama kademesi haline gelmiştir.³⁴⁷ Obama dönemi ofansif hareket sınırlandırmaları sebebiyle

³⁴⁵ “Obama Unveils New Defence Strategy with Greater Emphasis on Asia”, *The Guardian*, 05 Ocak 2012, <https://www.theguardian.com/world/2012/jan/05/obama-unveils-defence-strategy-asia>.

³⁴⁶ Lisa Ferdinando, “Cybercom to Elevate to Combatant Command”, Savunma Bakanlığı Resmi Web Sayfası, 03 Mayıs 2018, <https://www.defense.gov/News/News-Stories/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/>.

³⁴⁷ Jon R. Lindsay, “Cyber Conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem”, *Intelligence and National Security*, 2020, 9, <https://doi.org/10.1080/02684527.2020.1840746>.

sıkletinin çok altında yumruk atan bir boksör analojisini hatırlatan Siber Komutanlığın ulaşmış olduğu kapasite ABD tarafından gerçekleştirilecek muhtemel ofansif siber hareketin etkilerine dair bir fikir sunabilir.³⁴⁸ Fischerkeller, Trump döneminin “ileride savunma” doktrininin Siber Komutanlık tarafından kısa sürede pratiğe konulduğunu ve benimsenen proaktif yaklaşımın üç önemli başarıya imza attığını ifade etmektedir:³⁴⁹

- 2018 ABD ara seçimlerinin dış müdahalelere karşı korunması
- ABD’nin RQ-4 Global Hawk insansız hava aracına karşı İran tarafından gerçekleştirilen saldırı sonrası İran’ın radar sistemlerinin siber saldırıya maruz bırakılması
- IŞİD’in internette yürüttüğü propaganda faaliyetlerini engellemek amacıyla yürütülen Glowing Symphony Harekâtı

Bu üç örnek olay arasından İran’a yönelik siber müdahaleyi vurgulamak gerekir. Çünkü fiziksel bir saldırı karşısında siber yaptırımlara başvurulması bakımından Trump döneminde siber ofansif kabiliyetlerin eriştiği noktayı ve bu gücün kullanım yaklaşımını somut bir şekilde örneklemektedir. Söz konusu olayda Hürmüz Boğazı yakınlarında iki sivil yük gemisine İran güçleri tarafından saldırılması ve müteakiben bölgede konuşlu ABD insansız hava aracının düşürülmesi neticesinde hava saldırısı dahil olmak üzere birçok askerî yaptırım seçeneği masada iken Trump siber kabiliyetlere başvurmayı tercih etmiş; İran Devrim Muhafızlarına bağlı birçok keşif, komuta kontrol ve istihbarat unsuru seri siber saldırılara maruz bırakılmıştır.³⁵⁰ Jacksoncı geleneğin muhafazakar bakış açısı ile aynı çizgiyi paylaşan *The Federalist* dergisinde Trump’ın siber saldırı kararına atfen “Pearl Harbor” göndermesi yapılması ve ABD Siber gücünün İran kritik altyapılarında yaratabileceği hasara işaret edilerek İranlı yetkililerin üstü kapalı olarak uyarılması ceza yoluyla caydırıcılık kapsamında ABD’nin siber saldırı kapasitesinin araçsallaştırılmasına örnek teşkil etmektedir.³⁵¹

³⁴⁸ Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, 52; Wilner, “US cyber deterrence: Practice guiding theory”, 18-20.

³⁴⁹ Michael P Fischerkeller, “The Cyberspace Solarium Commission Report and Persistent Engagement”, *Lawfare*, 23 Mart 2020, <https://www.lawfaremedia.org/article/cyberspace-solarium-commission-report-and-persistent-engagement>.

³⁵⁰ Jacob Shively, “Cybersecurity Policy and the Trump Administration”, *Policy Studies* 42, sayı: 5-6 (02 Kasım 2021): 748, <https://doi.org/10.1080/01442872.2021.1947482>.

³⁵¹ Sean T. Lawson, *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*, 1. bs (New York: Routledge, 2019), 278, <https://doi.org/10.4324/9781315505619>.

2018 yılında Savunma Bakanlığı'na doğrudan bağlı 11 muharip komutanlıktan biri haline getirilen Siber Komutanlık Trump'ın deyimiyle önemli maddi kaynaklara kavuşurken, ABD yönetiminin siber caydırıcılığa ilişkin ciddiyeti açısından rakiplere net mesajlar vermiştir. Ofansif siber kabiliyetlerin geliştirilmesine yönelik bu adım, kuşkusuz Trump dönemi Jacksoncı geleneğin bir özelliği olan askeri kabiliyetlere yatırımın somut bir örneği niteliğindedir. Söz konusu adım yalnızca siber kabiliyetler nazarında kalmamış, Obama döneminde %16'lık küçülme ile 640 milyar dolara gerileyen yıllık savunma harcamaları Trump döneminde %20'lik büyüme ile 806 milyar dolara çıkmıştır.

Genel olarak bakıldığında, önceki başlıklarda ceza yoluyla caydırıcılık metoduna ilişkin iki dönem arası farklılıkların başkanların benimsemiş olduğu dış politika geleneği farklılıklarından kaynaklandığı görülmektedir. Bir tarafta Obama'nın bizzat yaptığı açıklamalar, yürüttüğü diplomatik ilişkiler ve imzaladığı icra emirleri ile ofansif askerî yeteneklerin bir ceza unsuru olarak kullanımını kısıtlarken, diğer tarafta Trump emriyle harekete geçilen kapasite artırımı ve ofansif harekât yetkilendirmeleri Siber Komutanlık ofansif kabiliyetlerini esas cezai yaptırım olarak konumlandırmıştır.

Siber komutanlığına yönelik yetki devri ve hiyerarşik kademe artırımı adımları ile bunun akabinde gerçekleştirilen kuvvet kullanımını içeren proaktif uygulamalar kuşkusuz Schelling'in ceza yoluyla caydırıcılık metoduna dair kullandığı "belirsizlik" ve "irrasyonelitenin rasyonelitesi" kavramlarını akıllara getirmektedir. Sivil iradenin de dahil olduğu geniş kapsamlı bir karar alma yapısından karar alıcı ve uygulayıcının bir arada bulunduğu "sahadaki lidere komuta devri" bir taraftan cezalandırmanın eşiği ve zamanına dair bir belirsizlik yaratırken diğer taraftan kontrol mekanizmalarının azaldığı bir tırmandırma yaklaşımını ortaya koymaktadır. Bu açıdan bakıldığında Jacksoncı gelenek izlerinin temel karakteristikleri olan merkeziyetçi ve çatışmacı yaklaşımların cezai yaptırımların araçsallaştırılmasında kökten belirleyici olduğu ifade edilebilir. Dolayısıyla iki başkanın takip ettiği Jeffersoncu ve Jacksoncu yaklaşım pratikleri; askerî müdahalenin sertliği, operasyonel planlamada karar çevikliği ve askerî kabiliyetlerin geliştirilmesi anlamında farklı uygulamalara yol açarak ceza yoluyla caydırıcılık metodunun icrasından somut bir farklılaşmanın sebebi olmuştur.

3.3.5. Kongre Değişkeni

ABD örneği, güvenlik politikalarının şekillenmesinde kurum etkisini inceleyen bir araştırma için çok uygun bir vaka sunmaktadır. Bunun sebebi yasama ve yürütme faaliyetlerinde Kongrenin sahip olduğu ağırlıktır. Zira yasama organı olan Kongrenin misyonu, yürütmeye önemli ölçüde pay sahibi olacak şekilde tasarlanmıştır. Başkanın yönetimde sınırsız güç sahibi olmasını önlemeye yönelik olarak dizayn edilen bu misyon, anayasanın mimarlarından biri olan James Madison tarafından “hırsa karşı koyma hırsı” olarak nitelendirilmiştir.³⁵² Gerçekten de anayasanın tasarlanması aşamasında Başkan ve Kongre arasındaki güç dengesi gözetilerek mutlak gücün tek bir elde toplanmaması için çaba gösterildiği ifade edilebilir.

Yürütmenin başı olan Başkan, ayrıca Silahlı Kuvvetler Başkomutanlığı görevini üstlenmektedir. Kongre tarafından hayata geçirilen yasaların uygulanmasını tatbik eden Başkan, yürütme görevini 15 ayrı departmandan oluşan federal hükümet ile gerçekleştirmektedir. Başkan Kongrenin aldığı yasa kararlarını imzalama veya veto etme, diğer devletler ile ilişkilerde bulunma, anlaşma imzalama gibi yetkilere sahiptir.³⁵³

Yasama faaliyetinden sorumlu olan Kongre, Temsilciler Meclisi ve Senato olmak üzere iki ayrı birimden oluşmaktadır. Temsilciler Meclisinde eyaletler nüfusları ile orantılı olacak şekilde temsil edilirken, Senatoda nüfusa bakılmaksızın her eyalet için iki temsilci bulunmaktadır.³⁵⁴ 435 Temsilcinin bulunduğu ve hangi yasama çalışmasının oylamaya sunulacağını belirleyen Temsilciler Meclisine kıyasla Senatonun yetki alanının daha geniş olduğu ifade edilebilir. Zira 100 üyeden teşkil olan yasama organı, kanunları onaylama veya veto etme, başkan tarafından yapılan üst düzey atamaları değerlendirme ve başkan için açılan güvenoyu sürecinde araştırma yapma gibi önemli yetkilere haizdir.³⁵⁵

³⁵² Alexander Hamilton vd., ed., *The Federalist* (Indianapolis: Hackett Pub. Co, 2005), 281.

³⁵³ Beyaz Saray Resmi Web Sayfası, “The Executive Branch”, erişim 14 Eylül 2023, <https://www.whitehouse.gov/about-the-white-house/our-government/the-executive-branch/>.

³⁵⁴ Beyaz Saray Resmi Web Sayfası, “The Legislative Branch”, erişim 14 Eylül 2023, <https://www.whitehouse.gov/about-the-white-house/our-government/the-legislative-branch/>.

³⁵⁵ BBC, “How does the US political system work”, erişim 15 Eylül 2023, <https://www.bbc.co.uk/bitesize/articles/zjpxjsg>.

Başkana verilmiş olan veto yetkisi yasama süreci için önemli bir sınırlandırmadır. Diğer taraftan veto edilen bir kanun tasarısı, her iki yasama organı tarafından üçte iki çoğunlukla tekrar onaylanırsa yürürlüğe girebilmektedir.³⁵⁶

ABD kurucu babaları tarafından gücün eşit bir şekilde dağılımı için titizlikle yaratılan sistemin zaman içerisinde başkan lehine değiştiğini belirtmek yanlış olmaz.³⁵⁷ Örneğin 1863 yılında Yüksek Mahkemenin aldığı kararla, Kongre tarafından bir savaş ilanının yapılmadığı durumlarda bile ABD'nin müdahil olduğu bir askeri çatışma kapsamında Başkana Başkomutanlık yetkilerini kullanma hakkı tanınmıştır.³⁵⁸ Başkan lehine bozulan dengeye Kongrenin bizzat kendisinin hizmet ettiği dönemler bulunmaktadır. Nitekim Anayasaya göre bütçenin hazırlanmasında tam yetkili olan Kongre, 1921 yılında çıkarmış olduğu yasa ile Başkana bütçeye ilişkin Kongreye bir ilk taslak sunma hakkı tanımıştır.³⁵⁹ Healy'e göre Başkanın artan yetki alanı ABD'nin bir kıta devletinden küresel güce dönmesi ile ilişkili bulunmaktadır.³⁶⁰ Özellikle Soğuk Savaş döneminde çift kutuplu dünya düzeninin getirdiği rekabet koşullarında Kongrenin Başkana karşı alan açıcı bir yaklaşım benimsediği ifade edilebilir. Bu yaklaşımın en somut örneklerinden biri Kore Savaşı'dır. Başkan Truman'ın herhangi bir Kongre onayı aramaksızın Amerikan askerlerini Kore Yarımadasına konuşlandırması Başkan-Kongre ilişkilerinde çarpıcı bir eşik aşımı niteliği taşımaktadır.³⁶¹ 21'inci yüzyılın başında ABD'nin kendi topraklarında uğradığı saldırı sonrasında "Teröre karşı Savaş" ve beraberinde meydana gelen teyakkuz durumu, başkana neredeyse tek taraflı bir idare ortamı sunmuş ve "Emperyal Başkanlık" söylemlerine sahne olmuştur.³⁶² Çatışma ve savaş kavramlarının anlam bakımından muğlak hale gelmesi, olası bir teyakkuz

³⁵⁶ "The Legislative Branch".

³⁵⁷ Lauren Cohen Bell, "Following the Leaders or Leading the Followers? The US President's Relations with Congress", *The Journal of Legislative Studies* 10, sy 2-3 (21 Haziran 2004): 195, <https://doi.org/10.1080/1357233042000322300>.

³⁵⁸ A.g.e., 195

³⁵⁹ A.g.e., 195

³⁶⁰ Gene Healy, *The Cult of the Presidency: America's Dangerous Devotion to Executive Power* (Washington, D.C: Cato Institute, 2008), 9.

³⁶¹ Healy, 89.

³⁶² Andrew Rudalevige, *The New Imperial Presidency: Renewing Presidential Power after Watergate*, 1. paperback ed., [Nachdr.], Contemporary Political and Social Issues (Ann Arbor: Univ. of Michigan Pr, 2006), 5.

durumda başkanlara esnetebileceği alanlar yaratarak yürütme yetkisine hareket alanı açmıştır.³⁶³

Burada şunu eklemek gerekir ki; askerî yetkilerin kullanımında Başkanın Kongreye karşı elde etmiş olduğu kazanımlar bu idare ilişkisini Başkan lehine tek taraflı mutlak bir yönetim biçimine çevirmemiştir. Kongrenin yürütmeyi denetleme ve bütçe onaylama yetkisi halen bu kuruma önemli bir kontrol ve yaptırım yeteneği sunmaktadır. Örneğin 2007 yılında Irak'taki mezhepçi çatışmalara son vermek maksadıyla 21.500 ilave ABD askerinin Irak'a konuşlandırılması için Kongreye öneride bulunan Başkan George W. Bush, her iki parti tarafından protestoya maruz kalmış ve teklifi reddedilmiştir.³⁶⁴ Başkan Obama'nın Guantanamo Hapishanesinin kapatılması uğraşında karşılaştığı Kongre engeli ve Suriye'de kimyasal silah kullanımı sonrası harekât için Kongre onayının aranması, dış politikada Kongrenin kayda değer bir ağırlığının bulunduğunu gösteren örneklerdir.³⁶⁵

Bu örnekler doğrultusunda, her ne kadar başkana karşı etki alanı zaman içerisinde farklılık gösterse de, Kongrenin ABD güvenlik politikalarının oluşturulması ve uygulanmasında yadsınamaz bir etkisi olduğu ifade edilebilir. Söz konusu etkiyi vaka analizinde test etmek için öncelikle Başkanlık İcra Emirlerine yer verilmiştir. Bu emirlerin fonksiyonlarının aydınlatılması yürütmeye esas olacak yasama prosedürlerinin işletilmesinde Başkan-Kongre ilişkisini anlamak için önemlidir. Çünkü söz bu emirler yasama faaliyetlerinin tıkanıp durumlarda başkana yasa statüsünde düzenlemeler yapma yetkisi tanımaktadır. Müteakiben analize konu olan dönemlere ait Kongre temsiliyet durumları ortaya konulmuştur. Kongrenin iki kanadı olan Temsilciler Meclisi ve Senatodaki parti çoğunlukları başkanın yürütmeyi arzuladığı güvenlik politikaları ile iş birliği veya çatışma durumuna dair ipuçları verebilir. Son olarak Kongrenin siber güvenlik alanına ilişkin yürüttüğü yasama faaliyetleri faaliyetleri incelenmiştir. Bu kapsamda yasa tasarıları, tasarıların kapsamları, tekliflerin yasalaşma durumları ve bütçe kanunlarının siber güvenlikle ilgili doğurduğu sonuçlar incelenmiştir.

³⁶³ Hugh Liebert, Gary L. McDowell, ve Terry L. Price, ed., *Executive Power in Theory and Practice* (New York: Palgrave Macmillan US, 2012), 165, <https://doi.org/10.1057/9781137014450>.

³⁶⁴ James M. McCormick, Traci Traci Crowell, ve Mary Malley, ed., *The Domestic Sources of American Foreign Policy: Insights and Evidence*, Seventh edition (Lanham: Rowman & Littlefield, 2018), 219-21.

³⁶⁵ Ryan C. Hendrickson, *Obama at War: Congress and the Imperial Presidency* (Lexington, Kentucky: The University Press of Kentucky, 2015), 111-22.

3.3.5.1. Başkanlık İcra Emirleri

Yürütme ve yasama kanatları arasındaki güç ilişkilerinde yürütmeye avantaj sağlayan en önemli araçlardan biri başkanlara tanınan İcra Emri yayımlama yetkisidir. İcra emirleri, yürütme yetkililerini yasaların nasıl yorumlanacağı ve uygulanacağı konusunda bilgilendiren yazılı başkanlık direktifleridir.³⁶⁶ Anayasada herhangi bir tanımı veya uygulanış biçimi bulunmayan bu direktif türü, George Washington’dan itibaren başkanların kullandığı bir tür yasama yetkisi olarak varlığını sürdürmüştür. Byers’a göre söz konusu direktif başkana anayasa ile verilen yürütme yetkisinin birtakım belirsizlikler ihtiva etmesi sonucu ortaya çıkmıştır.³⁶⁷ Bu direktifler ağırlıklı olarak Anayasanın ikinci maddesinde yer alan yürütme yetkileri ile ilişkilendirilmektedir. Bahse konu olan maddede başkana verilen “yasaların doğru bir şekilde uygulanmasının sağlanması” görevi İcra Emirlerine bir uygulama alanı açmıştır.³⁶⁸ Kongre tarafından çıkarılan yasaların uygulamada kolaylaştırılması amacını taşıyan İcra Emirleri, zaman içerisinde başlı başına birer yasa işlevi görecektir şekilde kullanılmaya başlanmıştır. Thomas Jefferson’ın Louisiana’yı satın alma yoluyla ABD topraklarına katması, Abraham Lincoln’un İç Savaş sırasında kölelerin özgürlüğünü ilan etmesi veya teröre karşı savaşta göz altına alınan şüphelilerin askerî mahkemelerce yargılanması geçmişten günümüze İcra Emri yoluyla gerçekleştirilen önemli uygulamaların örnekleridir.³⁶⁹

ABD Başkanlarının İcra Emirlerini bir yasa alternatifi olarak kullanma nedeninin pragmatik olduğu ifade edilebilir. Yürürlüğe girmek için Temsilciler Meclisi, Senato ve Başkanın onayından geçmesi gereken yasaların aksine İcra Emirleri Başkanlık tasarrufları ile hayata geçebilmektedir. Her ne kadar Kongrenin bu direktifleri sonradan iptal etme yetkileri bulunsa da bu amaç için takip edilmesi gereken bürokratik adımların

³⁶⁶ Alexander Bolton ve Sharece Thrower, *Checks in the Balance: Legislative Capacity and the Dynamics of Executive Power*, Princeton Studies in American Politics: Historical, International, and Comparative Perspectives (Princeton, New Jersey: Princeton University Press, 2022), 129.

³⁶⁷ Jason S. Byers, Jamie L. Carson, ve Ryan D. Williamson, “Policymaking by the Executive: Examining the Fate of Presidential Agenda Items”, *Congress & the Presidency* 47, sayı: 1 (02 Ocak 2020): 8-9, <https://doi.org/10.1080/07343469.2019.1631905>.

³⁶⁸ Bell, “Following the Leaders or Leading the Followers?”, 203.

³⁶⁹ Bell, 203.

zorluğu İcra Emirlerini efektif bir yasama aracı haline getirmektedir.³⁷⁰ Kongrenin partizan yapısı ve hantal işleyişi göz önünde bulundurulduğunda İcra Emirleri belirli bir konuda yürütme çerçevesini dizayn eden hızlı ve etkili bir alternatif olarak göze çarpmaktadır. Başkanın doğrudan tek taraflı müdahalesini içermesi ve meydana getirdiği hukuki etkiler bakımından değerlendirildiğinde, İcra Emirleri Anayasa tarafından belirlenen Yasama-Yürütme dengesinde yürütmeye avantajlar sunan bir inisiyatif durumundadır.³⁷¹ Bu niteliği dolayısıyla Dış Politikaya yön veren Başkan-Kongre ilişkilerinde göz ardı edilmemesi gereken bir siyaset belgesidir. İlerleyen bölümde görüleceği üzere Kongre ile düşülen anlaşmazlıklarda bu yetki ile başkanlar takip ettikleri güvenlik politikalarında bağlayıcı kararlar alabilmektedir.

3.3.5.2. Barack Obama ve Donald Trump Başkanlık Dönemlerinde Kongre Temsilîyet Durumları

Başkanların yürütmeye esas olacak yasaların çıkarılmasındaki gücünü araştıran Neustadt'a göre başkanın asıl gücü ikna kabiliyetinden gelmektedir.³⁷² Söz konusu ikna kabiliyeti ile ifade edilmek istenen, yürütmeye esas teşkil edecek olan yasaların onaylanması için Kongrenin her iki kanadındaki delegeleri istenilen yönde harekete geçirebilme becerisidir. Kuşkusuz, bu becerinin Beyaz Saray ve Kongrenin çift partili siyasi sistemde aynı parti tarafından elde bulundurulduğu siyasal konjonktürü tasvir eden birleşik hükümet modelinde daha kolay uygulanabildiği düşünülebilir. Başkan ve Kongre ilişkilerinin yasama faaliyetlerine etkilerini inceleyen birçok çalışma birleşik hükümet modelinde yasama organının çok daha aktif çalıştığı bulgusuna varmıştır.³⁷³

³⁷⁰ Healy, *The Cult of the Presidency*, 100-102.

³⁷¹ Andrew Rudalevige, "Executive Branch Management and Presidential Unilateralism: Centralization and the Issuance of Executive Orders", *Congress & the Presidency* 42, sayı: 3 (02 Eylül 2015): 346, <https://doi.org/10.1080/07343469.2015.1077484>.

³⁷² Todd M. Schaefer, *Presidential Power Meets the Art of the Deal: Applying Neustadt to the Trump Presidency* (Cham: Springer International Publishing, 2021), 24, <https://doi.org/10.1007/978-3-030-56029-4>.

³⁷³ Andrew W. Barrett ve Matthew Eshbaugh-Soha, "Presidential Success on the Substance of Legislation", *Political Research Quarterly* 60, sayı: 1 (Mart 2007): 107, <https://doi.org/10.1177/1065912906298605>; Daniel Paul Franklin ve Michael P. Fix, "The Best of Times and the Worst of Times: Polarization and Presidential Success in Congress", *Congress & the Presidency* 43, sayı: 3 (Eylül 2016): 390, <https://doi.org/10.1080/07343469.2016.1206638>; John J. Coleman, "Unified Government, Divided Government, and Party Responsiveness", *American Political Science Review* 93, sy 4 (Aralık 1999): 832, <https://doi.org/10.2307/2586115>; Byers, Carson, ve Williamson, "Policymaking by the Executive", 14.

Öte yandan Bölünmüş Hükümet adı verilen yasama ve yürütme organlarının farklı partiler tarafından kontrol edildiği senaryoda yasama faaliyetleri daha sert pazarlıklar ve çıkmazlara sahne olabilmektedir.

İKİ BAŞKAN DÖNEMİNDEKİ KONGRE TEMSİL DURUMLARI							
Kongre Kanadı	Parti	BARACK OBAMA				DONALD TRUMP	
		2009	2011	2013	2015	2017	2019
SENATO	Demokrat Parti	57	51	53	44	46	45
	Cumhuriyetçi Parti	41	47	45	54	52	53
TEMSİLCİLER	Demokrat Parti	257	193	201	188	194	235
MECLİSİ	Cumhuriyetçi Parti	178	242	234	247	241	199

Tablo 6: İki Başkan Dönemindeki Kongre Temsiliyet Durumları 374

Tablo-10’da Obama ve Trump başkanlık dönemlerine ait seçimler sonrasında yasamanın her iki kanadında meydana gelen parti delege durumları sunulmuştur. Her iki başkan yalnızca başkanlık dönemlerinin ilk iki senesinde birleşik hükümet avantajını yaşayabilmiş, sonraki dönemlerde yasamanın el değiştirmesiyle bölünmüş hükümet durumu ortaya çıkmıştır. Zira Obama döneminin ilk ara seçimleri olan 2010 yılında Temsilciler Meclisinde Cumhuriyetçi Parti çoğunluğu ele geçirmiş, ikinci dönem başkanlığının ilk safhasında mevcut durum devam etmiş, son ara seçimlerin yapıldığı 2014 yılında ise yasamanın her iki kanadında da Cumhuriyetçi Parti çoğunluğu elde etmiştir. Diğer taraftan Trump döneminin ara seçimlerinin yapıldığı 2018 senesinde Temsilciler Meclisinde Demokrat Partinin çoğunluğu elde ettiği görülmektedir.

Yasama ve yürütme organları ilişkisinde tek belirleyici unsur temsilci sayısı değildir. Bu konuda delegeler arasındaki partizanlık ve kutuplaşma durumu da yasama faaliyetlerini etkileyen önemli bir değişkendir. ABD siyasal konjonktüründeki partizanlık ilişkilerini konu edinen çalışmalar geçmişe kıyasla partiler arası kutuplaşmanın giderek daha keskin bir hal aldığına ve bölünmüş hükümet senaryosunda

³⁷⁴ “Election and voting information”, Federal Election Commission, erişim 15 Eylül 2023, <https://www.fec.gov/introduction-campaign-finance/election-and-voting-information/>.

başkanın işini oldukça zorlaştırdığına işaret etmektedir.³⁷⁵ Bununla birlikte başkanın kongre ile ilişkileri ve ikna yeteneği birleşik hükümet modeli senaryosunda bile belirleyiciliğini korumaktadır.

Trump'ın başkanlık dönemine ait ses getiren ilk yasama çalışması olan *ObamaCare*³⁷⁶ yasası iptali ve Meksika sınırına duvar inşası için ekonomik kaynak aktarımı adımlarında reddedilen teklifler Başkan-Kongre uyumsuzluklarının önemli örnekleridir. Bu uyumsuzlukları Başkanın Kongre ile olan iletişimsel hatalarına bağlayan Schaefer, özellikle *ObamaCare* yasası iptali sürecinde Trump'ın John McCain başta olmak üzere Cumhuriyetçi delegeleri kışkırtan ifadeleri nedeniyle Cumhuriyetçi Parti ağırlıklı bir kongrede oylamayı kaybettiğini ifade etmektedir.³⁷⁷ Bu açıdan bakıldığında yasama organında parti lehine görülen sayısal avantajın doğrudan başkan lehine değerlendirilemeyeceği çıkarımı yapılabilir. Yürütmeye esas olacak yasama işlemi, başkanın ilişkileri, gündem maddesinin niteliği, kongrenin kontrolü ve polarizasyon derecesi gibi birçok değişkenin bir arada bulunduğu ve vaka özelinde değerlendirilmesi gereken bir süreç niteliği taşımaktadır.

3.3.5.3. Barack Obama'nın Siber Güvenlik Politikası ve Kongre

Franklin ve Fix'e göre, görev süresinin ilk aşamasında bulunan Başkanlar, görev süresi sona yaklaşan başkanlara göre destekledikleri yasaları Kongreden geçirme konusunda daha başarılıdır.³⁷⁸ Obama'nın başkanlık döneminin ilk senesinde oluşan Demokrat Parti kontrolündeki Kongre göz önüne alındığında başkanın önceliklerini içine alan yasa tasarılarının daha kolay onaylanacağı öngörülebilir. Hendrickson Başkanlık döneminin ilk sürecindeki bu uyumu Obama'nın Afganistan politikası üzerinden analiz etmektedir. Adaylık kampanyası boyunca Afganistan'daki ABD askerî varlığını eleştiren

³⁷⁵ Jon R. Bond, Richard Fleisher, ve Jeffrey E. Cohen, "Presidential-Congressional Relations in an Era of Polarized Parties and a 60-Vote Senate", içinde *American Gridlock*, ed. James A. Thurber ve Antoine Yoshinaka, 1. bs (Cambridge: Cambridge University Press, 2015), 137, <https://doi.org/10.1017/CBO9781316287002.008>; Bell, "Following the Leaders or Leading the Followers?", 198.

³⁷⁶ Resmi Adı: Ekonomik Sağlık Bakımı Yasası (Affordable Care Act). 2010 yılında yürürlüğe giren ve sağlık sisteminde sigorta kapsamı, bakım ücretleri ve önleyici sağlık hizmetlerinde kapsamlı düzenlemeler içeren yasa.

³⁷⁷ Schaefer, *Presidential Power Meets the Art of the Deal*, 44-45.

³⁷⁸ Franklin ve Fix, "The Best of Times and the Worst of Times", 390.

Obama'nın beklenmedik şekilde 21000 kişiyi kapsayan büyük bir takviye ile bölgedeki askerî varlığı güçlendirme kararına Kongrenin herhangi bir itiraz sunmaması; Afganistan-Pakistan hudut hattının kontrolü için Pakistan hükümetine beş yıl boyunca yıllık 1.5 milyar dolarlık kaynak aktarımının Temsilciler Meclisinde büyük çoğunlukla, Senatoda ise oy birliği ile kabul edilmesi bu dönemde Obama'ya verilen Kongre desteğini göstermektedir.³⁷⁹

Obama'nın ilk kez siber güvenliği bir ana ulusal güvenlik sorunu olarak tanımlaması ve göreve gelişinden itibaren başlattığı 60 günlük durum değerlendirme süreci onun bu konudaki hassasiyetini göstermektedir. Söz konusu dönemdeki Başkan-Kongre uyumu doğrultusunda, siber uzaya dair güvenlik artırıcı yasama faaliyetlerinin ivme kazanması beklenebilir. Gerçekten de 2010-2012 yılları arasında Kongrenin her iki kanadında siber güvenliğin çeşitli boyutlarını ele alan yasama teklifleri gündeme gelmiştir. Buna rağmen bahse konu olan adımların nihayet kazanmada her zaman başarılı olduğu ifade edilemez. Söz konusu yasama tekliflerini şu şekilde sıralamak mümkündür:

- Siber Güvenlik Geliştirme Yasası³⁸⁰ – H.R.4061³⁸¹ (2010)
Temsilciler Meclisi üyesi Dan Lipsman (Demokrat Parti) tarafından verilen kanun teklifi siber güvenlik iş gücünü geliştirmek için kaynak artırımını ve bu alandaki araştırma-geliştirme faaliyetlerinin artırılması tedbirlerini içermektedir. Kongrenin her iki kanadında onaylanan kanun teklifi 18 Aralık 2010 tarihinde Başkan Obama tarafından imzalanarak yürürlüğe girmiştir.

³⁷⁹ Hendrickson, *Obama at War*, 26-29.

³⁸⁰ ABD Kongresi Resmi Sayfası “H.R.4061 - 111th Congress (2009-2010) Cybersecurity Enhancement Act of 2010”, , erişim 18 Eylül 2023, <https://www.congress.gov/bill/111th-congress/house-bill/4061/text/eh>.

³⁸¹ Yasa tekliflerinin sonunda kullanılan kısaltma ve numaralardan oluşan kelimeler, teklifin Kongrenin hangi kanadında işlem gördüğünü ve yasama işlem numarasını göstermektedir. H.R.: Temsilciler Meclisi (House of Representatives); S: Senato (Senate)

- Siber Güvenlik Yasası³⁸² – S.771 (2010)

Senatör John Rockefeller (Demokrat Parti) tarafından teklife sunulmuştur. Kamu kurumlarına uyum ve raporlama sorumlulukları getirmeyi, başkan tarafından ulusal çapta bir siber güvenlik acil durum eylem planı oluşturulmasını ve böyle bir durumda internete erişimin başkan tarafından kontrollü bir şekilde kısıtlanmasını öngörmektedir. Özellikle başkana verilen yetkilerin aşırı bulunduğu ve kontrolsüz kamu harcaması artışına neden olacağı eleştirilerine maruz kalan yasa teklifi hazırlama komisyonunda kalmış, oylama safhasına geçmeyi başaramamıştır.³⁸³

- Siber Uzayı Bir Ulusal Varlık Olarak Koruma Yasası³⁸⁴ - S.3480 (2010)

Senatör Joe Lieberman (Demokrat Parti), Tom Carper (Demokrat Parti) ve Susan Collins (Cumhuriyetçi Parti) tarafından gündeme getirilen yasa teklifi siber uzayı ve kritik altyapıları etkileyen büyük çaplı bir siber saldırı durumunda bir acil durum tedbiri olarak ABD Başkanına internet bağlantısına erişimi belirli bir süre veya sınırsız olacak şekilde kısıtlama imkânı veren bir yetkiyi önermektedir. Daha önce Komiteden geçemeyen ve acil durum yetkileri kapsamında benzer yetkileri esas alan Siber Güvenlik Yasa teklifinden farklı olarak bu girişimde başkanın acil durum yetkilerini kullanacağı durumlar³⁸⁵ daraltılarak detaylandırılmıştır.³⁸⁶ Yürütme organının internet üzerinde keyfi bir idare taşımayacağı açıklamaları ve söz konusu acil durumların belirli alanlarla kısıtlanmasına rağmen bir önceki kanun teklifiyle kamuoyunda meydana gelen

³⁸² ABD Kongresi Resmi Sayfası, “S.773 - 111th Congress (2009-2010) Cybersecurity Act of 2010”, 18 Eylül 2023, <https://www.congress.gov/bill/111th-congress/senate-bill/773/summary/00>.

³⁸³ Jeremy Kaplan ve Fox News, “New Cybersecurity Act Eliminates Internet Kill Switch”, Haber, FoxNews, 18 Mart 2010, <https://www.foxnews.com/tech/new-cybersecurity-act-eliminates-internet-kill-switch>.

³⁸⁴ ABD Kongresi Resmi Sayfası “S.3480 - 111th Congress (2009-2010) Protecting Cyberspace as a National Asset Act of 2010”, erişim 18 Eylül 2023, <https://www.congress.gov/bill/111th-congress/senate-bill/3480>.

³⁸⁵ 1. Bir yıllık bir süre içerisinde 25 milyar dolardan fazla hasara sebep olan siber saldırılar

2. 2500 ABD vatandaşının ölümüne sebebiyet veren siber saldırılar

3. Zorunlu olarak kitlesel tahliyelere sebebiyet veren siber saldırılar

³⁸⁶ Scott M. Ruggiero, “Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch”, *Science and Technology Law Review* 15, sayı: 2 (2017): 246.

endişeler giderilememiştir. Medyada internetin kısıtlanmasına olanak tanıyan yetkiye verilen “öldürme düğmesi”³⁸⁷ benzetmesi kamuoyunda söz konusu yasa tasarısına karşı oluşan olumsuz algıyı yansıtmaktadır. Sonuç olarak, özel sektör temsilcileri tarafından yoğun bir eleştiriye maruz kalan kanun teklifi her iki yasama organında da oylamaya tabi tutulmadan iptal edilmiştir.

- Siber Uzay ve İnternet Özgürlük Yasası³⁸⁸ – S.413 (2011)

Senatör Joseph Liberman (Demokrat Parti) tarafından sunulan yasa teklifi Beyaz Saray’da bir siber uzay yönetim merkezi kurulmasını, kritik altyapı işletmecilerinin uğranılan siber saldırılar konusunda İç Güvenlik Bakanlığına rapor vermesini ve İç Güvenlik Bakanlığı tarafından kritik altyapıların uyması gereken risk yönetimi yaklaşımını siber tedbirlerin belirlenmesini öngörmektedir. Teklif, gerek Kongrede yaşanan parti çekişmesi, gerekse siber güvenlik tedbirleri ile kişisel özgürlükler arasındaki hassas dengeyi gözetemediği gerekçesiyle hukukçu çevrelerden eleştiri alması sonucu oylama seviyesine gelemeyen iptal edilmiştir.

- Siber Güvenlik ve Bilgi Paylaşımı Etkinliğini Geliştirme Yasası³⁸⁹ – H.R.3674 (2011-2012)

Temsilciler Meclisi üyesi Dan Lungren (Cumhuriyetçi Parti) tarafından teklif edilen yasa tasarısı devlet ve özel sektör arasında bilgi paylaşım kanallarının kurulmasını öngörmektedir. Kişisel hak savunucuları tarafından söz konusu yasa teklifi, yürütme organı tarafından elde edilen kişisel bilgilerin keyfi kullanımına belirgin sınırlandırmalar getirmediği gerekçesiyle muhalif görüşler ile karşılanmış ve oylamaya sunulmadan iptal edilmiştir.

³⁸⁷ “Kill switch”

³⁸⁸ ABD Kongresi Resmi Sayfası , “S.413 - 112th Congress (2011-2012) Cybersecurity and Internet Freedom Act of 2011”, erişim 18 Eylül 2023, <https://www.congress.gov/bill/112th-congress/senate-bill/413>.

³⁸⁹ ABD Kongresi Resmi Sayfası “H.R.3674 - 112th Congress (2011-2012)_ PRECISE Act of 2012”, erişim 18 Eylül 2023, <https://www.congress.gov/bill/112th-congress/house-bill/3674/text>.

- Siber Güvenlik Yasası³⁹⁰ – S.2105 (2012)

Senatör Joseph Lieberman (Demokrat Parti) tarafından sunulan yasa teklifi İç Güvenlik Bakanlığının koordinesinde kritik altyapıların korunması için gönüllülük çerçevesinde bir özel sektör-kamu diyalogu oluşturmayı öngörmektedir. Özel sektörün görüşlerinin merkeze alındığı bir altyapı güvenlik çerçevesi oluşturulması planlanmaktadır. Başkan Obama'nın çok taraflılık ve kişisel özgürlüklere saygı yaklaşımlarını yansıtan ve Beyaz Saray tarafından açıkça desteklenen yasa tasarısı Senator John McCain'in liderlik ettiği Cumhuriyetçi Parti muhalif oyları nedeniyle yasa niteliğine kavuşmamıştır.³⁹¹ McCain liderliğindeki Cumhuriyetçi kanat, teklifin başarıya ulaşmaması için mevzuat üzerinde bir tartışma ortamı yaratarak en az 60 lehte oyun gerektiği bir yasama prosedürünü tetiklemiştir. Yasama faaliyetini engellemeye yönelik bu partizan yaklaşım, lehte oy sayısının 52'de sınırlı kalması ile Kongredeki parti merkezli yaklaşımların yasama faaliyetlerindeki önemini ortaya koymuştur.³⁹² Kritik altyapı güvenliğine dair önemli bir çerçeve belgesi olması beklenen tasarının senatodan geçememesi Beyaz Saray tarafından bir "hayal kırıklığı" olarak nitelendirilmiştir.³⁹³

2010-2012 yılları arasındaki Kongre yasama faaliyetleri incelendiğinde, Başkanın siber caydırıcılığın uygulanması açısından önem verdiği tedbirlere zemin hazırlayacak yasaların olgunluğa erişmediği görülmektedir. Bu dönem içerisinde gerek Temsilciler Meclisinde gerekse Senatoda kritik altyapı güvenliği başta olmak üzere siber güvenliğin farklı boyutları her ne kadar yasama gündemini yoğun bir şekilde işgal etmiş olsa da yasa niteliği kazanmamıştır. Bu tekliflerin başarısızlığı arkasındaki temel neden devlet-

³⁹⁰ ABD Kongresi Resmi Sayfası , "S.2105 - 112th Congress (2011-2012)_ Cybersecurity Act of 2012 _ Congress.gov _ Library of Congress.pdf", erişim 18 Eylül 2023, <https://www.congress.gov/bill/112th-congress/senate-bill/2105?q=%7B%22search%22%3A%22cybersecurity%22%7D&s=4&r=7>.

³⁹¹ Michael S Schmidt, "Republicans Block Bill on Cybersecurity", Haber, The Boston Globe, 03 Ağustos 2012, <https://www.bostonglobe.com/news/nation/2012/08/02/republicans-block-vote-cybersecurity-bill/XN4yYtGWUD5maxCv1EE3vI/story.html>.

³⁹² Michael S. Schmidt, "Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster", Haber, The New York Times, 02 Ağustos 2012, <https://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html>.

³⁹³ Jennifer Rizzo, Pm Edt, ve Thu August, "Cybersecurity Bill Fails in Senate", Haber, CNN, 02 Ağustos 2012, <https://edition.cnn.com/2012/08/02/politics/cybersecurity-act/index.html>.

özel sektör ilişkisinde yaşanan güvensizlikler ve kritik altyapıları kontrol eden özel şirketler tarafından duyulan yürütme organına keyfi müdahale hakkı tanınması endişesidir. Bununla birlikte söz konusu endişelerin zaman zaman partizan amaçlarla manipüle edilerek yasama sürecinin aksadığı da görülmektedir. Şöyle ki özel sektörü doğrudan planlama modeline paydaş haline getirmeyi ve gönüllülük esasına dayalı bir katılımı betimleyen Siber Güvenlik Yasası teklifi Senatodaki Cumhuriyetçi Parti temsilcileri tarafından engellenmiştir. İki yıllık bir yasama faaliyetleri verimsizliği sonrasında ilgili paydaşların hassasiyetlerini göz önünde bulunduracak şekilde hazırlanan ve kritik altyapıların korunmasında ihtiyaç duyulan adımları ihtiva eden tasarının kabul edilmemesi büyük çapta eleştiri uyandırmıştır.³⁹⁴

Siber güvenliğe ilişkin Başkan Obama'nın hassas yaklaşımı ortadayken yasama organının bu yaklaşıma ayak uyduramaması Beyaz Saray tarafından atılacak tek taraflı adımların habercisi olmuştur. Obama'nın yasama organı işlevsizliklerine karşı sarf ettiği şu sözler bu konuda başvuracağı idari tedbirleri açıklar niteliktedir:

*“Bir kalemim ve bir telefonum var. Bu kalemle İcra Emirlerini imzalayabilir ve bütün Amerikalıları birleştirecek adımların atılması için kabinemi arayarak yasama dışındaki alternatiflerimizi değerlendirebilirim.”*³⁹⁵

12 Şubat 2013 tarihinde Başkan Obama tarafından imzalanarak yürürlüğe giren iki yürütme belgesi (İcra Emri-13636 ve Başkanlık Siyaset Memorandumu-21) kritik altyapıların siber tehditlere karşı korunmasında somut adımları barındırmaktadır. Söz konusu inisiyatifle birlikte öne çıkan düzenlemeler şu şekildedir:³⁹⁶

- Risk yönetimi bazlı kriter ve tedbirlerin oluşturulmasında özel sektör paydaşlarının aktif katılımını teşvik etmek. Bu konuda İç Güvenlik

³⁹⁴ ABC News, “Congress’ Profound Failure on Cybersecurity - ABC News.pdf”, 12 Ağustos 2012, <https://abcnews.go.com/Business/congress-profound-failure-cybersecurity-care/story?id=16979814>.

³⁹⁵ Bolton ve Thrower, *Checks in the Balance*, 125.

³⁹⁶ Scott Shackleford vd., “Toward a Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices”, *Legal Studies Research Paper Series*, sy 291 (2015): 26-40.

Bakanlığı'nın koordinatör olarak görevlendirilmesi³⁹⁷

- Risk yönetimi esaslı ortak bir tedbir temel çerçevesinin oluşturulması ve uygulanması
- Uygulanacak çerçevenin oluşturulmasında örnek uygulama tarzlarının ortaya konulması. Bunlar ışığında standartlar üretilmesi; sürecin Ulusal Standart ve Teknoloji Enstitüsü Müdürü tarafından koordine edilmesi
- İç Güvenlik Bakanlığı, Hazine Bakanlığı ve Ticaret Bakanlığı'nın programa katılmayı özendirecek teşviklerin yaratılması ile görevlendirilmesi
- Kişisel hak ve özgürlüklerin korunmasına yönelik hassasiyetlerin her aşamada gözetilmesi
- Meydana getirilecek temel çerçevenin icrasında benimsenmesi gereken birtakım somut uygulama hedeflerinin ortaya konulması.

Beyaz Saray tarafından kaleme alınan bu iki belge, bir taraftan mevcut siber tehditlere karşı tedbir geliştirmeye çalışırken diğer taraftan özel sektör hassasiyetlerine dikkat etmektedir. Bu şekilde etkin ve dengeli bir güvenlik çerçevesi sunmaktadır. Söz konusu belgeler sayesinde kritik altyapıların savunmasını geliştirecek tedbirlerin yasal zemini atılmıştır. İç Güvenlik Bakanlığı koordinesinde yürütülen müteakip saha adımları bu altyapıların güvenliğinde diyalog ve standardizasyon zeminini güçlendirerek ikna ve dayanıklılık yoluyla caydırıcılığı güçlendirici basamaklar olmuştur. Caydırıcılık tedbirlerinin ortaya konulmasında önce Kongrenin iç işleyişi takip edilerek beklenilmiştir. Fakat yasama organından herhangi bir yapıcı hamle gelmemesi neticesinde Başkan Obama tarafından tek taraflı icra emri yayımlama yolu seçilmiştir.

İcra Emri sonrasında kamu-özel sektör bilgi paylaşımını geliştirecek yasal prosedürlerin arayışı devam etmiştir. Bu doğrultuda Senato tarafından 2015 yılında onaylanarak yürürlüğe giren Siber Güvenlik Bilgi Paylaşımı Kanunu³⁹⁸ önemli adımlar arasındadır. Başkan Obama'nın desteklediği kanun, devlet kurumlarının elde etmiş olduğu bilgilerin kullanım alanlarını düzenlemektedir. Ayrıca bilgi paylaşımı yapan

³⁹⁷ Bu kapsamda İç Güvenlik Bakanlığı tarafından, kritik altyapıları işleten özel sektör şirketlerinin doğrudan işletme alanına ilişkin bakanlıklar ile koordinasyonunu öngören Kritik Altyapı Siber Güvenlik Topluluğu Gönüllülük Programı yürürlüğe girmiştir.

³⁹⁸ ABD Kongresi Resmi Sayfası, "S.754 - 114th Congress (2015-2016)_ To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.", erişim 19 Eylül 2023, <https://www.congress.gov/bill/114th-congress/senate-bill/754?q=%7B%22search%22%3A%22s.754%22%7D&s=1&r=2>.

özel sektör paydaşlarını birtakım yasal sorumluluk ve yüklerden arındırmaktadır. 2013 yılı öncesinde siber güvenlik konularında uzlaşmasız bir tutum sergileyen Kongrenin böyle önemli bir tasarıyı kolaylıkla geçirmesi, Obama'nın göstermiş olduğu kararlı duruş, icra emri ve veto yetkilerini etkili bir şekilde kullanma pratiklerine bağlanmaktadır.³⁹⁹

3.3.5.4. Donald Trump'ın Siber Politikası ve Kongre

Donald Trump başkanlığının ilk yılı olan 2017 yılı aynı zamanda Cumhuriyetçi Partinin Kongrenin her iki kanadında çoğunluğunu elde ettiği birleşik hükümet dönemine sahne olmuştur. Bu açıdan bakıldığında Trump'ın siber politikalarının yasama organı tarafından desteklendiği bir durum öngörülebilir. Trump'ın siber güvenlik politikalarında benimsediği yaklaşımın en belirgin özelliklerinden biri çatışmacı tavrıdır. Bu doğrultuda Obama döneminin birtakım norm oluşturucu ve yatıştırıcı adımlarının takip edilmeyi bırakıldığı, hatta tersine çevrildiği görülmektedir. Bu gelişmelerin en fazla ses getiren adımı 20. Başkanlık Siyaset Direktifi (PPD-20)'nin sınırlandırıcı düzenlemelerini ortadan kaldıran 13. Ulusal Güvenlik Başkanlık Memorandumudur.

PPD-20, Obama döneminin ofansif siber operasyonlara karşı “sınırlandırıcı” bakış açısını yansıtan bir düzenlemedir. Bu düzenleme ile birlikte Stuxnet saldırısı ile aşılan siber kuvvet kullanım eşiğinin tekrar tesis edilmesi hedeflenmiş ve ofansif siber operasyonlara birtakım sınırlamalar getirilmiştir. Takip eden süreçte ofansif siber operasyonları geri planda tutan Obama yönetimi kritik altyapı tesislerinin savunması konusuna ağırlık vermiştir. Bu doğrultuda ceza yoluyla caydırıcılıktan ziyade ikna ve dayanıklılık yoluyla caydırıcılık yaklaşımının benimsendiği ve alınan tedbirlerin takibi için merkezi kurum olarak İç Güvenlik Bakanlığının atandığı görülmektedir.

Trump'ın NSPM-13 aracılığıyla PPD-20 düzenlemelerini iptal ederek ofansif siber harekâtın tekrar önünü açması ABD siber caydırıcılık politikasının en önemli dönüm noktalarından biri olarak kabul edilebilir. Tesis edilen çok taraflı karar verme sürecini hantal ve işlevsiz bulan Trump, ofansif siber harekât yetkisini tekrar Siber Komutanlığa

³⁹⁹ Peter Margulies, “Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy”, *Indiana Journal of Global Legal Studies* 24, sayı: 2 (2017): 467-70, <https://doi.org/10.2979/indjglolegstu.24.2.0459>.

devrederek siber uzayda daha aktif ve müdahaleci bir yaklaşım benimseyeceğinin mesajını vermiştir.⁴⁰⁰ Ceza yoluyla caydırıcılığın önünü açan bu adım aynı zamanda siber kuvvet kullanımını uygulayacak olan Savunma Bakanlığını tekrar caydırıcılık stratejisinin merkezine oturtmaktadır. Söz konusu adım Trump'ın Jacksoncı çatışmacı ve merkeziyetçi yaklaşımının siber güvenliğe yansımasıdır.

Caydırıcılık stratejisinde önemli değişiklikler yaratan bu adıma ilişkin Kongre tepkisini ölçmek için aynı hafta içinde yayımlanan Ulusal Güvenlik Yetkilendirme Yasası'na⁴⁰¹ (NDAA) bakmak uygun olacaktır. Ulusal Güvenlik Yetkilendirme Yasası yıllık olarak Kongrenin her iki kanadında oylanan, yürütmenin kullanacağı savunma harcamalarını inceleyip buna yönelik bütçeyi onaylayan bir yasama belgesidir. Daha da önemlisi, bu belge savunma politikalarına ilişkin olarak Kongre önceliklerini ifade etmektedir. 2018 yılı ağustos ayında yayımlanan NDAA'nın siber güvenliğe ilişkin öne çıkan düzenlemeleri şu şekildedir:

- Ofansif siber harekâta ilişkin ABD Kanunu Başlık-10/Başlık-50 ikilemine son verilmiştir. Daha açıklayıcı bir ifadeyle, ABD Kanununda askerî faaliyetler Başlık-10'da, istihbarat faaliyetleri Başlık-50'de konumlandırılmaktadır. Siber Komutanlığın kurulması ile birlikte siber harekâta askerî personelin yer alması, ofansif siber operasyonların hangi başlık altında konumlandırılacağı sorunsalına yol açmış, askerî ve istihbarat kanat arasında anlaşmazlıklara sebep olmuştur.⁴⁰² İstihbarat operasyonları ulusal güvenlik istihbarat komitesi ve Kongre üyelerinin başkan tarafından bilgilendirilmesi gibi birtakım yasal zorunlulukları içerirken, geleneksel askerî operasyonlar bu yasal kapsama girmemektedir. Ofansif siber hareketin gizliliğini, inkâr edilebilirliğini ve etkinliğini zedeleyen söz konusu yasal ikileme ilişkin olarak NDAA'nın 1632'nci maddesi, siber harekâtın “geleneksel bir askerî harekât olarak değerlendirileceği” hükmü ile kurumlararası yetki karmaşasına son vermiştir.

⁴⁰⁰ Geller, “Trump scraps Obama rules on cyberattacks, giving military freer hand”; Borghard ve Loneragan, “What Do the Trump Administration’s Changes to PPD-20 Mean for U.S. Offensive Cyber Operations”.

⁴⁰¹ “National Defense Authorization Act for Fiscal Year 2019”, ABD Kongresi Resmi Sayfası, 16 Ağustos 2018, <https://www.congress.gov/bill/115th-congress/senate-bill/2987?q=%7B%22search%22%3A%22national+defense+authorization+act%22%7D&s=5&r=11>.

⁴⁰² Robert Chesney, “The Law of Military Cyber Operations and the New NDAA”, Lawfare, 26 Temmuz 2012, <https://www.lawfaremedia.org/article/law-military-cyber-operations-and-new-ndaa>.

- NDAA'nın 1642'nci maddesi, ofansif siber operasyonlara dair bürokratik engelleri azaltmaya yöneliktir. Söz konusu maddede açık bir şekilde dört devlet (Çin, Kuzey Kore, İran ve Rusya) tanımlanmış; bu devletlerden herhangi biri tarafından ABD menfaatlerine zarar verici bir siber saldırı ihtimalinin tespit edilmesi durumunda ABD Başkanı ve Savunma Bakanı onayıyla ilgili devlete karşı bozucu ve caydırıcı siber faaliyetlerin yürütülmesine yetki tanınmıştır.

NDAA'nın siber güvenlikle ilgili iki maddesi, Trump'ın caydırıcılık yaklaşımı ile örtüşür niteliktedir. Şöyle ki bir taraftan ofansif siber operasyonlara yönelik bürokratik süreçler azaltılırken diğer taraftan bu yaptırımı gerçekleştirecek olan Siber Komutanlığın yetkisi ve rolü güçlendirilmektedir. Bu doğrultuda Başkan Trump döneminde benimsenen ceza yoluyla caydırıcılık stratejisinin Cumhuriyetçi Parti kontrolündeki Kongre tarafından destek bulduğu ifade edilebilir. Lonergan'a göre Savunma Bakanlığı siber kabiliyetlerinin bir cezalandırıcı araç olarak kullanılması birbirini izleyen üç adımda gerçekleşmiştir: İlerde Savunma Konseptini barındıran Savunma Bakanlığı Siber Stratejisi, ofansif siber operasyonların geleneksel askerî harekât sınıflandırmasına tabi olduğunu ifade eden 2019 Ulusal Güvenlik Yetkilendirme Yasası ve Siber Komutanlığın operasyonel karar alma alanını genişleten NSPM-13.⁴⁰³ Savunma Bakanlığı, Kongre ve ABD başkanı eliyle ortaya konulan bu adımlar ceza yoluyla caydırıcılığın tesisinde yasama ve yürütmenin eş güdüm içerisinde çalıştığını göstermektedir.

NDAA'nın siber uzaya dair göze çarpan düzenlemeleri yalnızca Siber Komutanlık ofansif operasyonları ile sınırlı değildir. Belgenin en dikkat çeken uygulaması Siber Solaryum Komisyonunun (CSC) kurulmasıdır. 1652'nci maddede yer bulan CSC Kongrenin siber güvenlik konusuna yalnızca yasa yapmanın ötesinde, tarafsız bir şekilde müdahil olmasını öngörmektedir. Yeni stratejiler üretme, yürütme organı siber politikalarını denetleme ve teklifler sunma gibi görevler verilen CSC'nin yapısı biri Cumhuriyetçi, diğeri ise Demokrat Parti temsilcisi olmak üzere iki eş başkan tarafından yönetilecek şekilde dizayn edilmiştir. Komisyonun kadro yapılanmasına bakıldığında aynı şekilde eşit dağılıma dikkat edildiği görülmektedir. Bu adım, Kongrenin ilk kez

⁴⁰³ Erica D. Lonergan ve Shawn W Lonergan, "To Defend Forward, the U.S. Must Strengthen the Cyber Mission Force", *Lawfare*, 13 Mart 2020, <https://www.lawfaremedia.org/article/defend-forward-us-must-strengthen-cyber-mission-force>.

siber güvenliği bir ulusal öncelik olarak kabul ettiği ve partiler üstü bir sorun olarak tanımladığı bir bakış açısını yansıtmaktadır.

Komisyon, 2019 yılı itibariyle hayata geçmesinden itibaren aktif bir şekilde çalışmalarına başlamıştır. Bu kapsamda, komisyonun yıllık olarak geniş kapsamlı bir rapor yayımladığı ve söz konusu raporda yürütmenin siber güvenlik politikalarını değerlendirdiği, incelemiş olduğu konu başlıklarına ilişkin hükümete öneri ve eleştirilerde bulunduğu görülmektedir. Komisyonun ilk çalışması olan 2020 yılı raporundaki⁴⁰⁴ “ileride savunma” doktrini ifadeleri dikkat çekicidir. İlk kez 2018 yılı Savunma Bakanlığı Siber Strateji belgesinde yer alan ve müteakip dönemde caydırıcılık stratejisinin anahtar ifadesi olan “ileride savunma” kavramının aynı yıl hazırlanan Ulusal Siber Strateji Belgesinde yer almadığına dikkat çeken rapor, bu konuda söz konusu kavrama gerekli atfın yapıldığı yeni bir ulusal siber strateji belgesinin gerekliliğini savunmaktadır.⁴⁰⁵ Raporun diğer bir önemli katkısı “katmanlı caydırıcılık” kavramıdır. Siber uzaydaki tehdit ve aktörlerin çeşitliliğine dikkat çeken belgede ilgili tehditlere karşı kabiliyetlerin de çeşitlendirilmesi görüşü söz konusu kavramın savunduğu esas noktadır. Bu kapsamda, katmanlı caydırıcılık anlayışının ifade ettiği üç katman aslında doğrudan caydırıcılığın üç metoduna ilişkindir. İlk katmanda uluslararası düzeyde sorumlu davranış normları oluşturma, ikinci katmanda bilişim ağlarını siber saldırılara karşı daha az geçirgen kılma ve üçüncü katmanda maruz kalınan saldırılar karşısında bedel ödetme araçlarının tamamının uyumlu bir şekilde kullanılması öngörülmektedir.

Siber Solaryum Komisyonu, kapsamlı caydırıcılık kavramı ile birlikte üç caydırıcılık metodunun her birinde önemli geliştirme önerileri sunmakla birlikte bunlar arasında uygulamada en fazla sonuç doğuran önerileri ikna ve dayanıklılık yoluyla caydırıcılık ile ilgilidir. Bu öneriler; Ulusal Siber Direktörlüğü makamının kurulması, kritik altyapı sektörlerinin belirlenmesi ve Kritik Altyapı ve Savunma Ajansının yetkilendirilmesidir.

Siber Solaryum Komisyonu 2020 yılı raporunun en fazla göze çarpan önerisi Ulusal Siber Direktör makamının teşkil edilmesidir. Hatırlanacağı üzere, benzer işleyişte bir makam olan Beyaz Saray Siber Güvenlik Koordinatörlüğü makamı Obama döneminde

⁴⁰⁴ “Cyberspace Solarium Commission Report-2020” (ABD Kongresi, Mart 2020), <https://www.solarium.gov/>.

⁴⁰⁵ Patrick J. Murphy ve Erica Borghard, “To Defend Forward, US Cyber Strategy Demands a Cohesive Vision”, *Cyber Defense Review*, 2020, 19.

tesis edilmiş, 2018 yılında Trump başkanlığında söz konusu makama yeni görevlendirme yapılmayarak söz konusu birim rafa kaldırılmıştır. Raporun bu makamın kurulmasına ilişkin önerisi, kapatılan kadroya ilişkin Trump’a yöneltilen eleştirilerin Kongre tarafından resmiyete dökülmüş hali olarak değerlendirilebilir. Dahası, komisyonun önermiş olduğu Siber Direktörlük makamının, önceki versiyonundan farklı olacak şekilde doğrudan Senato tarafından onaylanma, Ulusal Güvenlik Komisyonu üyesi olma, kendine özgü bir bütçesi ve 75 kişilik bir ekibi yönetme gibi yetki ve haklarla donatılması öngörülmüştür.⁴⁰⁶ Bahse konu olan öneri; siber güvenlik stratejilerinin kurumsallaşmaması, etkin şekilde denetlenmemesi ve başkana gerekli danışmanlığın yapılmaması gibi sorun noktalarına işaret etmektedir. Bu açıdan bakıldığında Kongrenin söz konusu alandaki siber güvenlik politikalarına dair duymakta olduğu endişelerin ürünüdür. İkna ve dayanıklılık yoluyla caydırıcılık pratikleri açısından ele alındığında, bu atama ile birlikte Trump dönemi merkeziyetçi yaklaşımlarının bir kenara bırakılarak bilişim ağlarının kuvvetlendirilmesinde yardımlaşma ve çok taraflılık prensibinin tekrar tesis edilmesi amaçlanmaktadır.

Komisyonun bir diğer öne çıkan önerisi Kritik Altyapı Tesislerinin siber saldırılara karşı korunmasına ilişkindir. Obama’nın 13636 sayılı Başkanlık İcra Emrinden itibaren kritik altyapıların barındırdığı bilişim ağlarının siber saldırılara karşı geçirgenliğinin azaltılması konusu ikna ve dayanıklılık yoluyla caydırıcılığın esas ilgi alanlarının başında gelmektedir. Bununla birlikte, söz konusu kavramın sunduğu kapsayıcı nitelik hangi hizmet ve tesisin kritik olduğu noktasında karmaşa meydana getirmektedir. Jhangiani ve Kennis’e göre “kritik altyapı” kavramı birçok alan ve sektörü işaret edecek şekilde sıklıkla kullanıldığından ötürü anlamını yitirmiştir.⁴⁰⁷ Buna ilaveten yazarlar, Obama’nın 13636 sayılı İcra Emrinin 16 adet kritik altyapı tesisi tanımlamasını yapıcı bir adım olarak değerlendirmekle birlikte söz konusu belgede bilişim sektörünün yer almamasını ve zaman içerisinde ilgili sektörlerden çok sektörde faaliyet gösteren özel sektör teşebbüslerine odaklanmanın zafiyetler meydana getirdiğini savunmaktadır.⁴⁰⁸

⁴⁰⁶ Robert Chesney, “The NDAA’s National Cyber Director: Justifications, Authorities and Lingering Questions”, *Lawfare*, 07 Aralık 2020, <https://www.lawfaremedia.org/article/ndaas-national-cyber-director-justifications-authorities-and-lingering-questions>.

⁴⁰⁷ Tasha Jhangiani ve Graham Kennis, “Protecting the Critical of Critical: What Is Systemically Important Critical Infrastructure?”, 15 Haziran 2021, <https://www.lawfaremedia.org/article/protecting-critical-critical-what-systemically-important-critical-infrastructure>.

⁴⁰⁸ A.g.e

Bu eleştirilere dair tedbir niteliği taşıyan komisyonun önerisi doğrultusunda “Sistemik Olarak Önemli Kritik Altyapı” kavramı geliştirilerek bilişim, ulaştırma, enerji ve bankacılık gibi “gerçekten kritik” sektörlerin tespiti öngörülmektedir. Ayrıca söz konusu sektörlerin bilişim ağlarının güçlendirilmesi kapsamında federal bütçeden kaynak aktarımı yapılması önerilmektedir.

Raporda bilişim ağlarının korunmasına ilişkin farklı uzmanlık alanlarında faaliyet gören birimlere ilişkin geliştirici tedbirler dikkat çekicidir. Örnek olarak, 2015 yılında Obama’nın Başkanlık Memorandumu ile kurulan Siber Tehdit İstihbaratı Entegrasyon Merkezi (CTIIC)’nin kaynak ve yetki bakımından kuvvetlendirilmesi önerilmektedir. Söz konusu geliştirmenin siber tehditlerde saldırganı tespit etme sorununa yardımcı olacağı düşünülmektedir. Diğer taraftan Kritik Altyapı Güvenlik Ajansı (CISA) önemli idari ve hukuksal yetkiler ile donatılmaktadır. Şöyle ki kuruma “.gov” uzantılı federal bilişim ağlarında tehdit devriyesinde bulunma görevi verilirken, diğer taraftan kritik altyapı güvenliğine ilişkin olarak, bu tesisleri etkileyebilecek bir bilişimsel güvenlik açığına sahip federal veya federal olmayan sistem ve ağlar hakkında mahkeme kararı çıkartma yetkisi CISA’nın siber güvenlikteki aktif rolünü pekiştirecek niteliktedir.

Siber Solaryum Komisyonunun 2020 tarihli raporundaki siber güvenlik geliştirme önerilerinin sunulduğu yukarıdaki düzenlemeleri sadece öneri boyutunda kalmayarak 2021 Ulusal Güvenlik Yetkilendirme Yasası ile birlikte kanunlaşmıştır. Bu durum Kongrenin komisyon eliyle siber güvenlik tedbirlerine önemli şekilde müdahil olduğunu göstermektedir. Siber Solaryum Komisyonu ve Ulusal Güvenlik Yetkilendirme Yasası marifetiyle Trump döneminde siber güvenliğe ilişkin önemli idari tedbirlerde rolü görülen Kongrenin uygulamaları caydırıcılık stratejisi açısından ele alındığında Trump uygulamalarını bazı boyutlarda pekiştirdiği, bazı boyutlarda ise değiştirdiği gözlemlenmektedir. Nitekim Trump döneminin en belirgin caydırıcılık metodu olan ceza yoluyla caydırıcılık stratejisinde ofansif siber operasyonlara dair hesap verilebilirlik kısıtını rahatlatan yetkilendirme yasaları, özellikle Çin, Kuzey Kore, İran ve Rusya’ya yönelik siber saldırıların önünü açan düzenlemeler ve siber uzayda agresif proaktif tedbirlerin alınmasını öngören “ilerden savunma” kavramının desteklenmesi bu dönemde takip edilen ceza yoluyla caydırıcılık pratiklerini sağlamlaştıran bir etki taşımaktadır. Buna karşın ikna ve dayanıklılık yoluyla caydırıcılık metoduna ilişkin Kongrenin bulunduğu çizgi Başkan Trump’tan farklılık arz etmektedir. Zira Trump’ın

en fazla ses getiren adımlarından biri olan Beyaz Saray Siber Güvenlik Koordinatörü makamının Kongre eliyle bu sefer daha güçlü bir şekilde tekrar tesis edilmesi, Obama döneminde kurulan farklı siber güvenlik merkezlerinin güçlendirilerek daha aktif yetkiler ile donatılması Trump'ın merkezîyetçi yaklaşımı ile ters düşmektedir. Obama döneminde siber güvenliğe ilişkin pasif bir rol oynayan kongrenin, Trump döneminde yukarıda sunulan adımlarla ön plana çıkması ve düzenleyici tedbirler geliştirmesi özellikle koordinatörlük makamının iptali sonrasında tek taraflı yaptırımlara karşı Kongrenin bir reaksiyonu olarak yorumlanabilir.

3.3.5.5. Kongrenin Caydırıcılık Stratejileri Kapsamında Etkilerinin Değerlendirilmesi

Başkanın uygulayacağı politikalara yasal zemin sağlaması ve söz konusu uygulamaları denetlemesi açısından Kongrenin ABD dış politikasında önemli bir ağırlığa sahiptir. Bununla birlikte söz konusu etkinin partisel temsiliyet durumları ile her zaman doğrusallık taşımadığı, kendi bağlamsal koşulları çerçevesinde incelenmesi gerektiği görülmektedir. Bahsedilen bağlamsal koşullar içinde başkan ile kongre ilişkileri önemli bir yer tutmaktadır. Obama döneminde takip edilen ikna ve dayanıklılık yoluyla caydırıcılık stratejisini güçlendirici yasama adımlarının atılmasında etkisiz bir Kongre rolü başkanı tek taraflı uygulamalara yöneltmiştir. Söz konusu etkisiz tutum Başkan tarafından İcra Emirleri yoluyla aşılmıştır. Müteakiben Kongrenin bahse konu olan güvenlik politikalarına zemin hazırlama konusunda daha aktif olduğu gözlemlenmiştir. Diğer taraftan Trump döneminde Kongrenin izlenen ceza yoluyla caydırıcılığın geliştirilmesi için aktif bir şekilde çalıştığı görülmektedir. Bu alana yönelik başkan ile eş güdüm içinde olan Kongre ceza bileşeninin tesisindeki sınırlamaların kaldırılmasında oldukça etkin olmuştur. Bununla birlikte güvenlik paydaşlarının geri plana atılarak merkezîyetçi uygulamaların arttığı Trump döneminde Kongrenin bu sefer başkana muhalif bir şekilde ön plana çıkarak başkan uygulamalarını denetleyici ve değiştirici bir rol oynadığı görülmektedir. Böylece Kongrenin Trump döneminde ceza yoluyla caydırıcılık stratejisi uygulamalarını güçlendirdiği, ikna yoluyla caydırıcılık uygulamalarının ise merkezîyetçi yaklaşımını değiştirdiği ifade edilebilir. Sonuç olarak; güvenlik politikalarının uygulanmasında başkan lehine ağır basan başkan-kongre ilişkisinin siber caydırıcılık politikasında da benzer şekilde geliştiği çıkarımı yapılabilir. Kongrenin işlevsiz kaldığı durumlarda başkanlar yasama yetkilerini kullanarak caydırıcılık stratejilerine hizmet edecek zeminleri yaratabilmektedir. Bununla birlikte

başkanların merkeziyetçi uygulamalarının arttığı dönemlerde Kongrenin reaktif davranarak yürütmeye müdahil olan ve caydırıcılık stratejilerini değiştirebilen bir etkide bulunabildiği de gözden kaçırılmamalıdır.

Araştırmanın vaka analizi olan bu bölümde siber tehditlere karşı caydırıcılık stratejisi farklılaşması, yapısal faktör ve iç bileşen etkileri sorularına cevap aranmıştır. Bu kapsamda öncelikle ABD'nin yapısal faktörler karşısındaki durumu ele alınmıştır. Güç dağılımı koşulları ve tehdit algılaması olarak nitelendirilen bu faktörler siber uzay düzleminde ABD yönetimini tedbir almaya davet etmektedir. Zira gerek konvansiyonel güç dağılımındaki göreceli düşüş, gerekse siber uzayda sürekli saldırılara maruz kalma durumu ABD'yi güvenliksiz bir alana itmektedir.

Söz konusu durum ABD yönetimini güvenlik artırıcı tedbirlere yöneltmektedir. Fakat bir yapısal dönüştürücü olan siber uzayın belirsiz durumu söz konusu tedbirlerin niteliği bakımından dikte edici mesajlar yerine yönetimin kendi oluşturacağı seçeneklere alan açmaktadır. Söz konusu seçeneklerin, başka bir deyişle caydırıcılık stratejilerinin, karşılaştırılan başkanlık dönemlerinde farklılaşma durumunu incelemek için resmi güvenlik belgelerine başvurulmuştur. Ağırlık noktası, amaçlar ve araçlar bakımından incelenen bu belgelerin beraberinde getirmiş olduğu güvenlik düzenlemelerinin hangi caydırıcılık metoduna tekabül ettiği yorumlanmış ve sonuç olarak başkan dönemlerinin genelini yansıtan bir caydırıcılık stratejisi resmi oluşturulmuştur. Bu kapsamda ceza yoluyla caydırıcılık metodu bakımından iki dönem arasında ciddi farklılık tespit edilmiştir. Bu farklılık, özellikle PPD-20 ve NSPM-13 belgeleri ile belirginlik kazanan ofansif siber harekâtı etkin bir misilleme unsuru olarak kullanma seçiminden kaynaklanmaktadır. Nitekim Trump döneminde çok daha etkin bir ceza yoluyla caydırıcılık metodunun takip edildiği bulgusuna varılmıştır. Bu bulgu doğrultusunda söz konusu farklılaşmanın sebepleri için iç değişkenler ele alınmıştır. Bu değişkenler stratejik kültür ve kurum bileşenleridir. Yapılan süreç takibinde gerek Obama dönemi caydırıcılık stratejisindeki işbirlikçi ve çatışmaya uzak tavrın, gerekse Trump dönemi merkeziyetçi ve çatışmacı yaklaşımın birer istisna olmadığı tespit edilmiştir. Bu yaklaşımlar iki başkan döneminde sırasıyla benimsenen Jeffersoncu ve Jacksoncu stratejik kültürün yansımalarıdır. Zira söz konusu geleneklerin benzer karakteristik özellikleri ilgili başkanların ofansif yaptırım kararı içeren diğer dış politika

uygulamalarında görülmektedir. Bu doğrultuda stratejik kültür değişkeni ile caydırıcılık stratejisi arasında bir nedensellik bağından söz etmek olağandır.

Çalışmanın ikinci iç değişkeni olan kurum bileşeninin vakadaki örneği ABD Kongresidir. Tarihsel süreçte Kongrenin güvenlik politikalarındaki etkinliğinin farklılık gösterdiği görülmektedir. Söz konusu durum siber caydırıcılık stratejisini içeren politikalarda benzerlik göstermektedir. Bu durumu izah etmek için güvenlik politikalarındaki ağırlığı bakımından Başkan-Kongre dengesini Başkan lehine değiştiren İcra Emirlerine yer verilmiştir. Bu belgeler Başkana Kongre prosedürlerine bağlı kalmaksızın yasa gücünde düzenlemeler yapma yetkisi tanımaktadır. Nitekim Obama'nın bu yetkiye başvurarak sonuç vermeyen Kongre çalışmaları karşısında tek yollu idari düzenlemelere gittiği görülmektedir. Obama'nın bu hamlesi ile uygulanması öngörülen ikna yoluyla caydırıcılık stratejisinin geliştirilmesi için gerekli yasal altyapı hazırlanmıştır. Dikkate değer bir şekilde söz konusu düzenlemenin yürürlüğe girmesi sonrasında siber güvenliğe ilişkin yasama faaliyetlerinde Kongrenin çok daha aktif işlemeye başladığı görülmüştür. Bu durum Kongre etkinliğinin parti temsil çoğunluğu durumundan ziyade başkan uygulamaları ile ilgili olduğunu göstermektedir. Trump döneminde ise siber güvenlik politikalarında çok daha aktif bir Kongre göze çarpmaktadır. Kongrenin ofansif siber harekât önündeki prosedürleri azaltıcı ve saldırgan devletlere karşı misilleme tedbirlerini kolaylaştırıcı yasama çalışmaları Trump dönemi ceza yoluyla caydırıcılık stratejisi etkinliğini ciddi biçimde geliştirmiştir. Diğer taraftan Siber Güvenlik Koordinatörü makamının tesisi, çeşitli kurumsal yapıların siber güvenliğin farklı boyutları ile görevlendirilmesi gibi adımlar Trump dönemi merkeziyetçi uygulamalarını tersine çevirir niteliktedir. Özellikle bu dönemde Siber Solaryum Komisyonu yoluyla siber güvenlik uygulamalarına bilfiil müdahil olan Kongre ikna-dayanıklılık yoluyla caydırıcılığın tesisinde oldukça aktif bir rol oynamıştır.

Bu doğrultuda kongre değişkeni ve caydırıcılık stratejisi arasında nedensel bir bağın varlığından söz etmek mümkündür. Bununla birlikte söz konusu bağın niteliği başkan okuması ile birlikte anlamlı hale gelmektedir. Zira partizanlık durumunun Kongreyi işlevsiz kıldığı senaryolarda bile başkan tek taraflı yasama yetkilerini kullanarak Kongre yerine kararlar alabilmektedir. Bu adım Kongreyi güvenlik ile ilgili tasarılarının yasalaşması konusunda teşvik etmektedir. Diğer taraftan başkanın merkeziyetçi ve tek

tarafli uygulamalarının arttıđı durumlarda Kongre takip edilen stratejiden farklı yasama kararları alabilmekte ve kurmuş olduđu komisyonlar aracılıđı ile bu kararların pratiđe konulmasında belirleyici olabilmektedir.





Bu çalışma, farklılaşan caydırıcılık stratejilerinde stratejik kültür ve kurumlar gibi iç bileşenlerin etkin olup olmadığı sorusu etrafında şekillendirilmiştir. Bu soruya cevap aramak için yapılan analiz iki açıdan önem arz etmektedir: Birincisi, caydırıcılık alan yazınında ağırlıklı kullanılan rasyonel aktör varsayımı ve Neorealizm teorisi etkisinin ötesine geçilerek Neoklasik Realizmin geçerliliği bu alanda test edilmiştir. Stratejik kültür ve kurum iç değişkenlerinin yapısal faktörler ile birlikte dış politika analizinde bir arada kullanımı caydırıcılık çalışmalarına örnek bir model sunarak kuramsal bir katkı sağlamaktadır. İkincisi, Neorealizmin öngördüğü rekabet ve taklit yoluyla şekillenen devlet davranışlarının aksine, siber uzay yapısal dönüştürücü fonksiyonu aracılığıyla devletlerin güvenlik kararlarında iç bileşenlerin etkilerine alan açmıştır. Bu ortamda stratejik kültür ve kurum değişkenleri etkisiyle şekillenen siber kapasite inşası, daha önce siber güvenliği bir vaka olarak ele alan caydırıcılık çalışmalarında gözardı edilen kabiliyet bileşeninin nasıl oluşturulduğu konusunda kavramsal bir katkı sağlamaktadır.

Araştırma sorusu doğrultusunda oluşturulan hipotez, benzer yapısal koşullar altında devletlerin dış politika tercihlerinin stratejik kültür ve kurum değişkenleri doğrultusunda farklılık gösterebildiğidir. Çalışma sonuçları stratejik kültür ve kurum değişkenlerinin caydırıcılık stratejisi üzerindeki etkisini açıkça ortaya koymuştur. Zira elde edilen bulgular, başkanların güvenlik politikası kararlarında takip etmiş oldukları stratejik kültürün belirleyici olduğunu, kurumların ise bu kararların uygulanmasında destekleyici veya değiştirici fonksiyon üstlenebildiğini göstermektedir. Bu kapsamda analiz sonucunda günümüzün karmaşık güvenlik ortamında, caydırıcılık stratejisi örneğinin göstermiş olduğu şekilde, dış politika kararlarının yalnızca yapısal faktörlerce açıklanamayacağı, bunun için yapısal ve aktör merkezli değişkenlerin birarada ele alındığı kapsamlı analiz çerçevelerine ihtiyaç duyulduğu tespitine varılmıştır.

Araştırma hipotezinin test edilmesi maksadıyla yöneltilen üç alt sorunun her biri farklı bir değişkenin durumunu ortaya koyarak somut bulguların elde edilmesine imkan

sağlamıştır. Bu kapsamda, “Güç dağılımı ve tehdit algılaması koşullarının siber tehditlere karşı caydırıcılık stratejisinin benimsenmesinde etkileri nelerdir?” sorusu, açıklayabilme kabiliyeti bakımından dış politika analizine iç bileşenleri bir yenilik olarak getiren, ancak yapısal faktörlerin önceliğini yadsımayan Neoklasik Realizm analiz çerçevesinin doğru bir şekilde uygulanması açısından önemlidir. Bu soruya yönelik yapılan analizde konvansiyonel güç dağılımındaki göreceli düşüşün yanı sıra siber uzayda sürekli saldırılara maruz kalma durumunun ABD’yi güvenliksiz bir alana ittiği görülmüştür. Söz konusu durumun ABD yönetimini güvenlik artırıcı tedbirlere yönelttiği ancak siber uzayın kendine has koşulları sonucu güvenlik tedbirlerinin niteliği bakımından dikte edici mesajlar yerine yönetimin kendi oluşturacağı seçeneklere alan açtığı tespit edilmiştir.

Yapısal faktörlerin caydırıcılık stratejisi tedbirlerine yönelttiği, fakat bu tedbirlerin kapsamının bilinmediği durum, çalışmanın ikinci sorusunu davet etmiştir. Bu soru, benzer yapısal koşullar altında devletlerin siber caydırıcılık stratejilerinin farklılık gösterip göstermediğidir. Caydırıcılık stratejisinin somut olarak gözlemlenemeyen bir zorlayıcı diplomasi ürünü olması ve başvurulacak güvenlik tedbirlerinin belirli bir çerçevede yorumlanması sonucu ortaya çıkarılması, yöneltilen bu soruyu önemli kılmaktadır. Zira sorunun cevabı için yapılan belge analizi daha önce münferit söylem ve uygulamalar doğrultusunda yorumlanan başkanlık dönemi siber güvenlik politikalarını kapsayıcı bir tespite dönüştürmektedir. Bu doğrultuda çalışmanın ortaya koymuş olduğu bulguların en önemlilerinden biri Trump döneminde çok daha etkin bir ceza yoluyla caydırıcılık stratejisinin uygulanmış olduğudur. Siber Komutanlığın yetkilerini artıran, kaynak artırımına giden ve onu bürokratik engellerden arındıran Trump yönetimi ofansif siber kabiliyetleri gerçek anlamda bir misilleme aygıtı olarak kullanarak ceza yoluyla caydırıcılığın tanımına uygun şekilde hareket etmiştir. Diğer taraftan Obama döneminde Siber Komutanlığın ofansif siber harekât düzenleme yetkisinin sınırlandırıldığı ve siber uzayda gerginlik tırmandırıcı davranışlardan kaçınarak misillemelerin daha çok hukuki ve ekonomik olmak üzere alan dışı tedbirlerden seçildiği tespit edilmiştir.

Yapısal faktörlerin belirleyici olmadığı, caydırıcılık stratejisinde ise farklılaşmanın tespit edildiği durum çalışmanın üçüncü sorusunu beraberinde getirmiştir. Bu soru caydırıcılık stratejileri arasındaki farkların oluşumunda stratejik kültür ve kurum

değişkenleri etkilerinin neler olduğudur. Bu soru çalışmanın bir diğer önemli bulgusuna aracılık etmiştir. Bahsedilen bulgu, caydırıcılık stratejisinde stratejik kültürün doğrudan, kurum değişkeninin ise bağlamsal koşullar altında belirleyici olduğudur. Özellikle Trump döneminde izlenen etkin ceza yoluyla caydırıcılık stratejisinin oluşumunda Jacksoncı dış politika geleneğinin doğrudan etkisi bulunduğu görülmüştür. Yapılan süreç takibinde gerek Obama dönemi caydırıcılık stratejisindeki işbirlikçi ve çatışmaya uzak tavrın, gerekse Trump dönemi merkeziyetçi ve çatışmacı yaklaşımın birer istisna olmadığı tespit edilmiştir. Bu yaklaşımlar iki başkan döneminde sırasıyla benimsenen Jeffersoncı ve Jacksoncı stratejik kültürün yansımalarıdır. Zira söz konusu geleneklerin benzer karakteristik özellikleri, ilgili başkanların ofansif yaptırım kararı içeren diğer dış politika uygulamalarında görülmektedir. Bu doğrultuda stratejik kültür değişkeni ile caydırıcılık stratejisi arasında bir nedensellik bağından söz etmek olağandır. Diğer taraftan kongre değişkeni ve caydırıcılık stratejisi arasındaki nedensel bağın niteliği başkan okuması ile birlikte anlamlı hale gelmektedir. Zira partizanlık durumunun Kongreyi işlevsiz kıldığı senaryolarda bile başkan tek taraflı yasama yetkilerini kullanarak Kongre yerine kararlar alabilmektedir. Bu adım Kongreyi güvenlik ile ilgili tasarılarının yasalaşması konusunda teşvik etmektedir. Diğer taraftan başkanın merkeziyetçi ve tek taraflı uygulamalarının arttığı durumlarda Kongre, takip edilen stratejiden farklı yasama kararları alabilmekte ve kurmuş olduğu komisyonlar aracılığı ile bu kararların pratiğe konulmasında belirleyici olabilmektedir. Kısaca ifade etmek gerekirse, Başkan ve Kongre kıyaslamasında Başkanın caydırıcılık stratejisi üzerindeki belirleyiciliğinin çok daha fazla olduğu, bu etkiye yön veren düşünsel altyapının ise stratejik kültür olduğu tespit edilmiştir.

Yapısal koşullara ilaveten devletlere ait iç değişkenleri dış politika analizine dahil eden Neoklasik Realizm, farklılaşan dış politika uygulamalarını açıklayabilme yeteneği bakımından Uluslararası İlişkiler disiplinine önemli katkılar sağlamaktadır. Söz konusu iç değişkenlerin kullanım biçimine dair eleştiriler bulunmakla birlikte kurama dayalı modellerin farklı vakalarda test edilmesi, Neoklasik Realizmin geçerlilik durumunu geliştirecektir. Bu çalışma, caydırıcılık stratejisi gibi nükleer silahların meydana getirdiği güç dengesi koşulları ekseninde gelişen bir dış politika stratejisini Neoklasik Realizm çerçevesinde açıklayarak akademik yazına kuramsal bir katkı sunmaktadır. Zira vaka örneğinde yapısal faktörlerin devleti güvenlik kararları bağlamında belirli bir yöne sevk ettiği ancak bu kararların niteliği konusunda yol gösterici olmadığı

görülmektedir. Dolayısıyla rasyonel aktör varsayımına dayanan ve yalnızca yapısal faktörleri analiz kapsamına alan bir araştırma metodu açıklayıcılık bakımından eksik bir çerçeve sunacaktır. Bu doğrultuda Neoklasik Realizmin özellikle siber tehditler gibi yeni tehdit koşullarında başvurulmuş caydırıcılık stratejisine ilişkin çok daha açıklayıcı bir perspektif sunduğu aşıkardır.

Diğer taraftan siber tehditlerin bir vaka olarak seçilmesi ile çalışma sonucunda elde edilen bulguların kurama kazandırdığı katkıların altı çizilmesi gerekir. Bu katkılardan biri kuramın yapı-aktör etkileşimine ilişkin varsayımlarının eksiksiz bir şekilde örneklendirilmesidir. Neoklasik Realizme göre yapı her devlete eşit şekilde etki etmemektedir. Bu ilişkide yapısal dönüştürücü, açıklık ve stratejik çevre kavramları farklı etkileşimler meydana getirebilmektedir. Siber tehditlerin halen nispeten bilinmeyen doğası, zayıf devletlerin güçlü devletleri hedef alabilmesi, uluslararası çatışma sınırlandırmalarının bulunmaması ve günlük hayatın bilişim altyapısının bir silah olarak kullanılabilmesi yapı-aktör etkileşiminde göze çarpan bir örnek sunmaktadır. Zira bu özelliklerinden dolayı siber tehditler bir yapısal dönüştürücüdür. Bu yapısal dönüştürücü özellik, devletler için örnek davranış kalıplarının bulunmadığı belirsiz ve açık olmayan bir ortam yaratmaktadır. Söz konusu ortam yapısal faktörlerin genel olarak yönlendirici olduğu ancak belirleyicilik açısından iç değişkenlere alan açan serbest bırakıcı bir stratejik çevre yaratmaktadır. Bu şekilde kuramın ortaya koymuş olduğu fakat vaka örneklerinin kısıtlı olduğu yapısal dönüştürücü, açıklık ve stratejik çevre etkenlerinin tamamına tek bir vakada yer verilmiştir.

Çalışmanın kurama yaptığı bir diğer katkı da iç değişkenlerin kullanımına yöneliktir. Alan yazında kurama yöneltile en sık eleştirilerden biri iç değişkenlerin gelişigüzel kullanımıdır. Bu doğrultuda çalışmada söz konusu değişkenler sistematik bir biçimde tamamlayıcı faktör olarak kullanılmıştır. Nitekim önce güç dağılımı ve tehdit algılaması değişkenleri incelenerek yapısal koşulların hiyerarşik üstünlüğü kabul edilmiştir. Müteakiben yapısal koşulların yönlendirici olduğu ancak belirleyici olmadığı tespiti neticesinde iç değişkenlere yönelinmiştir. Bu kapsamda öncelikle stratejik kültür değişkeni ele alınmış müteakiben kurum değişkenine yer verilmiştir. Stratejik kültür değişkeni dış politika kararlarında lideri doğrudan etkilemektedir. Kurum değişkeninin test edildiği Kongre örneğinde ise bu değişkenin etkisinin bağlamsal olduğu tespit edilmiştir. Dolayısıyla Neoklasik Realizm kuramsal çerçevesini kullanarak ABD dış

politika analizi yapacak alıřmalar iin bu iki i deęiřken arasındaki hiyerarři yol gsterici bir rol oynayabilir.

Son olarak alıřmanın sunmuř olduęu kabiliyet bileřeni inceleme modelinin drdnc dalga alıřmalarında grlen caydırıcılıęın bařarılı olma durumlarını esas alan ğretici epistemolojik yaklařımdan farklı bir noktada konumlanması nemlidir. Zira bu dalga alıřmalarında caydırıcılıęın siber tehditlere karřı nasıl bařarılı olabileceęini tartıřan bir yaklařım sz konusudur. Bu alıřma ise siber kabiliyetlerin inřa srecine odaklanarak olması gerekenden ziyade mevcut durumu ortaya koymaktadır. Bu aıdan alıřmanın sunduęu test edilebilir ve gzlemlenebilir bulgular nemlidir. Sz konusu kabiliyetlerin oluřturulma sreci yasal ve idari dzenlemeler aısından ele alınmıřtır. İlerleyen alıřmalarda bu kabiliyetlerin teřkilat ve donanım gibi boyutları ile birlikte incelenmesi siber tehditlere karřı inřa edilen kabiliyetleri ok daha somut bir řekilde ortaya koyabilir.

Kurama dayalı oluřturulan model, gri alan ve dezenformasyon faaliyetleri gibi dięer hibrit tehditlere uyarlanabilir. Zira konvansiyonel olmayan bu tehdit ortamları, g daęılımı aısından yapının aktre sunmuř olduęu kořulları belirsizleřtirmektedir. Yapısal kořulların aktr tarafından yorumlanması nem arz ettięi dıř politika analizlerinde lider karakteri ve kamuoyu desteęi gibi dięer i deęiřkenlerin rol de arařtırılabilir.

Siber tehditlerin nispeten yeni olması arařtırma iin kısa olarak kabul edilebilecek 12 yıllık bir dnemin incelenmesine sebep olmuřtur. Dięer taraftan bu tehditler doęrultusunda gerekleřtirilen saldırıların ne kadarının bařarılı olduęu veya ne kadarının caydırıldıęına iliřkin bir veri bulunmamaktadır. Bu durum, analize tabi olan verilerin caydırıcılık akademik yazını doęrultusunda yorumlanmasını gerektiren tespitleri beraberinde getirmiřtir. Takip eden alıřmalarda baęımsız deęiřkenin gzlemlenebilir verileri barındıracak řekilde tayin edilmesi bulguların kesinlięi aısından daha faydalı olacaktır.

Nkleer silahların ortaya ıkması ile kavramsallařan caydırıcılık stratejisi gnmze kadar olan srete kullanılan aralar, ngrlen tehditler ve bařvurulan taktikler olmak zere birok aıdan geliřerek derin bir alıřma alanı haline gelmiřtir. Bu alıřma ilk bařta nkleer silahlar ile zdeřleřen ve yalnızca “ceza yoluyla caydırıcılık” olarak algılanan caydırıcılık stratejisinin tehdit algılaması paralelindeki deęiřimine ıřık

tutmaktadır. Silahlı kuvvetlerin esas vazifesi olan, bunun yanında gerektiğinde devletin her türlü milli güç unsurunun kullanıldığı caydırıcılık konusu gelecekte de önemini korumaya devam edecektir. Yakın dönem farklılaşan tehdit ortamının örneklerinden biri olan siber tehditlere karşı caydırıcılık stratejisinin nasıl uygulandığını ve bu süreçte hangi etkenlerin belirleyici olduğunu gösteren bu çalışmanın caydırıcılık stratejisinin günümüzdeki durumunu göstermesi ve gelecekteki muhtemel pratiklerine dair projeksiyon sağlaması açısından okuyuculara faydalı olması temenni edilmektedir.



KAYNAKÇA

ABC News. "Congress' Profound Failure on Cybersecurity - ABC News.pdf". Haber, 12 Ağustos 2012. <https://abcnews.go.com/Business/congress-profound-failure-cybersecurity-care/story?id=16979814>.

ABD Adalet Bakanlığı. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", 19 Mayıs 2014. <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

ABD Başkanlık İcra Ofisi. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009.

———. "National Cyber Strategy-2018". Beyaz Saray, Eylül 2018. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

———. "National Security strategy". Beyaz Saray, 2010.

———. "National Security Strategy 2017". Beyaz Saray, Aralık 2017. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

ABD Kongresi Resmi Sayfası. "H.R.3674 - 112th Congress (2011-2012)_ PRECISE Act of 2012". Erişim 18 Eylül 2023. <https://www.congress.gov/bill/112th-congress/house-bill/3674/text>.

ABD Kongresi Resmi Sayfası. "H.R.4061 - 111th Congress (2009-2010) Cybersecurity Enhancement Act of 2010". Erişim 18 Eylül 2023. <https://www.congress.gov/bill/111th-congress/house-bill/4061/text/eh>.

ABD Kongresi Resmi Sayfası. "National Defense Authorization Act for Fiscal Year 2019", 16 Ağustos 2018. <https://www.congress.gov/bill/115th-congress/senate-bill/2987?q=%7B%22search%22%3A%22national+defense+authorization+act%22%7D&s=5&r=11>.

ABD Kongresi Resmi Sayfası. "S.413 - 112th Congress (2011-2012) Cybersecurity and Internet Freedom Act of 2011". Erişim 18 Eylül 2023. <https://www.congress.gov/bill/112th-congress/senate-bill/413>.

ABD Kongresi Resmi Sayfası. "S.754 - 114th Congress (2015-2016)_ To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes." Erişim

19 Eylül 2023. <https://www.congress.gov/bill/114th-congress/senate-bill/754?q=%7B%22search%22%3A%22s.754%22%7D&s=1&r=2>.

ABD Kongresi Resmi Sayfası. “S.773 - 111th Congress (2009-2010) Cybersecurity Act of 2010”, 18 Eylül 2023. <https://www.congress.gov/bill/111th-congress/senate-bill/773/summary/00>.

ABD Kongresi Resmi Sayfası. “S.2105 - 112th Congress (2011-2012)_ Cybersecurity Act of 2012 _ Congress.gov _ Library of Congress.pdf”. Erişim 18 Eylül 2023. <https://www.congress.gov/bill/112th-congress/senate-bill/2105?q=%7B%22search%22%3A%22cybersecurity%22%7D&s=4&r=7>.

ABD Kongresi Resmi Sayfası. “S.3480 - 111th Congress (2009-2010) Protecting Cyberspace as a National Asset Act of 2010”. Erişim 18 Eylül 2023. <https://www.congress.gov/bill/111th-congress/senate-bill/3480>.

ABD Savunma Bakanlığı. “DoD Cyber Strategy-2018”, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

“ABD Siber Komutanlığı Vizyon Belgesi”. ABD Siber Komutanlığı, Nisan 2018. <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.

ABD Ticaret Bakanlığı. “A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats”. ABD Ticaret Bakanlığı, Mayıs 2018. <https://www.commerce.gov/data-and-reports/reports/2018/05/report-president-enhancing-resilience-against-botnets>.

Abrams, Abigail. “Here’s What We Know So Far About Russia’s 2016 Meddling”. Time, 18 Nisan 2019. <https://time.com/5565991/russia-influence-2016-election/>.

Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown and Company, 1971.

Allyn, Bobby. “Trump Signs Executive Order That Will Effectively Ban Use Of TikTok In the U.S. _ NPR.pdf”. NPR.Org., 06 Ağustos 2020. <https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s>.

Almog, Doron. “Cumulative Deterrence and the War on Terrorism”. *Parameters* 34, no 3 (2004): 4-19.

Axelrod, Robert M. *The Evolution of Cooperation*. Rev. ed. New York: Basic Books, 2006.

- Bagby, Laurie M. Johnson. "Thucydidean Realism: Between Athens and Melos". *Security Studies* 5, sy 2 (Aralık 1995): 169-93. <https://doi.org/10.1080/09636419508429266>.
- Barrett, Andrew W., ve Matthew Eshbaugh-Soha. "Presidential Success on the Substance of Legislation". *Political Research Quarterly* 60, sy 1 (Mart 2007): 100-112. <https://doi.org/10.1177/1065912906298605>.
- Bentley, Michelle, and Jack Holland, eds. *The Obama Doctrine: A Legacy of Continuity in US Foreign Policy?* 1st ed. New York: Routledge, 2016. <https://doi.org/10.4324/9781315731346>.
- Beyaz Saray. "İcra Emri 13800: Federal Ağların ve Kritik Altyapıların Siber Güvenliğini Güçlendirmek." Mayıs 2017. <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
- . "İcra Emri 13862." 6 Mart 2019. <https://www.federalregister.gov/presidential-documents/executive-orders/donald-trump/2019>.
- Beyaz Saray Resmi Web Sayfası. "The Executive Branch." Erişim 14 Eylül 2023. <https://www.whitehouse.gov/about-the-white-house/our-government/the-executive-branch/>.
- . "The Legislative Branch." Erişim 14 Eylül 2023. <https://www.whitehouse.gov/about-the-white-house/our-government/the-legislative-branch/>.
- Bolton, Alexander, and Sharece Thrower. *Checks in the Balance: Legislative Capacity and the Dynamics of Executive Power*. Princeton Studies in American Politics: Historical, International, and Comparative Perspectives. Princeton, New Jersey: Princeton University Press, 2022.
- Bolton, John. *The Room Where It Happened: A White House Memoir*. New York: Simon and Schuster, 2020.
- Bond, Jon R., Richard Fleisher, and Jeffrey E. Cohen. "Presidential-Congressional Relations in an Era of Polarized Parties and a 60-Vote Senate." In *American Gridlock*, edited by James A. Thurber and Antoine Yoshinaka, 133–51. 1st ed. Cambridge: Cambridge University Press, 2015. <https://doi.org/10.1017/CBO9781316287002.008>.
- Borghard, Erica, and Shawn Lonergan. "What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?" *Council on Foreign Relations*, 10 Eylül 2018. <https://www.cfr.org/blog/what-do>

[trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations.](#)

Boulding, Kenneth E. *Conflict and Defense: A General Theory*. Lanham, MD: University Press of America, 1988.

Brewster, Thomas, and Forbes Staff. "U.S. Accuses 7 Iranians Of Cyberattacks On Banks And Dam." *Forbes*, 24 Mart 2016. [https://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/?sh=6e7a30c37255.](https://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/?sh=6e7a30c37255)

Brodie, Bernard. *The Absolute Weapon: Atomic Power and World Order*. New York: Yale University Institute of International Studies, 1946.

Byers, Jason S., Jamie L. Carson, and Ryan D. Williamson. "Policymaking by the Executive: Examining the Fate of Presidential Agenda Items." *Congress & the Presidency* 47, no. 1 (January 2, 2020): 1–31. [https://doi.org/10.1080/07343469.2019.1631905.](https://doi.org/10.1080/07343469.2019.1631905)

Cavelty, Myriam Dunn, and Andreas Wenger. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41, no. 1 (2020): 5–32.

Chesney, Robert. "The Law of Military Cyber Operations and the New NDAA." *Lawfare*, July 26, 2012. [https://www.lawfaremedia.org/article/law-military-cyber-operations-and-new-ndaa.](https://www.lawfaremedia.org/article/law-military-cyber-operations-and-new-ndaa)

———. "The NDAA's National Cyber Director: Justifications, Authorities and Lingering Questions." *Lawfare*, December 7, 2020. [https://www.lawfaremedia.org/article/ndaas-national-cyber-director-justifications-authorities-and-lingering-questions.](https://www.lawfaremedia.org/article/ndaas-national-cyber-director-justifications-authorities-and-lingering-questions)

Chesney, Robert, James Shires, and Max Smeets, eds. *Cyberspace and Instability*. Edinburgh: Edinburgh University Press, 2023.

Clarke, Michael, and Anthony Ricketts. "Donald Trump and American Foreign Policy: The Return of the Jacksonian Tradition." *Comparative Strategy* 36, no. 4 (August 8, 2017): 366–79. [https://doi.org/10.1080/01495933.2017.1361210.](https://doi.org/10.1080/01495933.2017.1361210)

———. "Shielding the Republic: Barack Obama and the Jeffersonian Tradition of American Foreign Policy." *Diplomacy & Statecraft* 28, no. 3 (July 3, 2017): 494–517. [https://doi.org/10.1080/09592296.2017.1347448.](https://doi.org/10.1080/09592296.2017.1347448)

- Coetzee, Eben. "No Rest for the Weary: Competition and Emulation in International Politics. A Waltzian Perspective." *Politikon* 46, no. 1 (January 2, 2019): 1–19. <https://doi.org/10.1080/02589346.2018.1486527>.
- Coleman, John J. "Unified Government, Divided Government, and Party Responsiveness." *American Political Science Review* 93, no. 4 (December 1999): 821–35. <https://doi.org/10.2307/2586115>.
- Collier, David. "Understanding Process Tracing." *PS: Political Science & Politics* 44, no. 4 (October 2011): 823–30. <https://doi.org/10.1017/S1049096511001429>.
- Crandall, Matthew, and Collin Allan. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Contemporary Security Policy* 36, no. 2 (May 4, 2015): 346–68. <https://doi.org/10.1080/13523260.2015.1061765>.
- Cyberspace Solarium Commission. *Cyberspace Solarium Commission Report*. U.S. Congress, March 2020. <https://www.solarium.gov/>.
- Da Vinha, Luis. "A Tale of Two Red Lines: Managing Foreign Policy Crises in the Obama and Trump Administrations." *Comparative Strategy* 40, no. 1 (January 2, 2021): 63–85. <https://doi.org/10.1080/01495933.2021.1853441>.
- Danilovic, Vesna. *When Stakes Are High*. Ann Arbor: University of Michigan Press, 2002.
- Department of Defense. *Dayanıklı Askeri Sistemler ve Gelişmiş Siber Tehdit*. Defense Science Board, 2013. <https://dsb.cto.mil/reports.htm>.
- . "Defense.gov News Article: Lynn: Cyber Strategy's Thrust is Defensive," n.d.
- Delpech, Thérèse. *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy*. Pittsburgh: RAND Corporation, 2012.
- DeNardo, James. *The Amateur Strategist: Intuitive Deterrence Theories and the Politics of the Nuclear Arms Race*. New York: Cambridge University Press, 1995.
- Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, 2011.
- Dilanian, Ken. "Under Trump, U.S. Military Ramps Up Cyber Offensive against Other Countries." *NBC News*, June 23, 2019. <https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281>.

- Dimitrova, Anna. "Trump's 'America First' Foreign Policy: The Resurgence of the Jacksonian Tradition." *L'Europe En Formation* 382, no. 1 (February 6, 2018): 33–46. <https://doi.org/10.3917/eufor.382.0033>.
- European Repository of Cyber Incidents (Eurepoc). *Global Dataset of Cyber Incidents*, 2024. <https://doi.org/10.5281/zenodo.11108195>.
- Farrell, Michael, Tim Starks, and Gavin Bade. "Trump Is Rattling Sabers in Cyberspace — but Is the U.S. Ready?" *Politico*, July 13, 2019. <https://www.politico.com/story/2019/07/13/trump-cybersecurity-defense-1415650>.
- Federal Election Commission. "Election and Voting Information." Accessed September 15, 2023. <https://www.fec.gov/introduction-campaign-finance/election-and-voting-information/>.
- Ferdinando, Lisa. "Cybercom to Elevate to Combatant Command." U.S. Department of Defense Official Website, May 3, 2018. <https://www.defense.gov/News/News-Stories/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/>.
- Finnemore, Martha. *National Interests in International Society*. Ithaca, NY: Cornell University Press, 1996.
- Fischerkeller, Michael P. "The Cyberspace Solarium Commission Report and Persistent Engagement." *Lawfare*, March 23, 2020. <https://www.lawfaremedia.org/article/cyberspace-solarium-commission-report-and-persistent-engagement>.
- Foster, Dennis M., and Jonathan W. Keller. "Leaders' Cognitive Complexity, Distrust, and the Diversionary Use of Force." *Foreign Policy Analysis* 10, no. 3 (July 2014): 205–23. <https://doi.org/10.1111/fpa.12019>.
- Foulon, Michiel. "Neoclassical Realism: Challengers and Bridging Identities." *International Studies Review*, September 2015. <https://doi.org/10.1111/misr.12255>.
- Foulon, Michiel, and Gustav Meibauer. "Realist Avenues to Global International Relations." *European Journal of International Relations* 26, no. 4 (December 2020): 1203–29. <https://doi.org/10.1177/1354066120926706>.
- Foulon, Michiel, and Gustav Meibauer. "How cyberspace affects international relations: The promise of structural modifiers." *Contemporary Security Policy*. 45(3) (2024): 426–458 <https://doi.org/10.1080/13523260.2024.2365062>

- Franklin, Daniel Paul, and Michael P. Fix. "The Best of Times and the Worst of Times: Polarization and Presidential Success in Congress." *Congress & the Presidency* 43, no. 3 (September 2016): 377–94. <https://doi.org/10.1080/07343469.2016.1206638>.
- Freedman, Lawrence. "Deterrence: A Reply." *Journal of Strategic Studies* 28, no. 5 (2005): 789–801. <https://doi.org/10.1080/01402390500393944>.
- Gaddis, John L. "Long Peace: Elements of Stability in the Postwar International System." *International Security* 10, no. 4 (1986): 99–142.
- Gambino, Lauren, and Sabrina Siddiqui. "Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking." *The Guardian*, December 30, 2016. <https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack>.
- Geller, Eric. "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand." *Politico*, August 16, 2018. <https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095>.
- George, Alexander L. "The Operational Code: A Neglected Approach to the Study of Political Leaders and Decisionmaking." *International Studies Quarterly* 13, no. 2 (1969): 190–222.
- George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press, 2005.
- Ghalehdar, Payam. "The Purpose of Military Force and the Obama Doctrine: No Fighting for Face." *International Relations*, January 31, 2023. <https://doi.org/10.1177/00471178231151907>.
- Gibbons-Neff, Thomas, and Ellen Nakashima. "President Trump Announces Move to Elevate Cyber Command." *The Washington Post*, August 18, 2017. <https://www.washingtonpost.com/news/checkpoint/wp/2017/08/18/president-trump-announces-move-to-elevate-cyber-command/>.
- Götz, Elias. "Neoclassical Realist Theories, Intervening Variables, and Paradigmatic Boundaries." *Foreign Policy Analysis* 17, no. 2 (February 16, 2021): oraa026. <https://doi.org/10.1093/fpa/oraa026>.
- Grigsby, Alex. "The End of Cyber Norms." *Survival* 59, no. 6 (November 2, 2017): 109–22. <https://doi.org/10.1080/00396338.2017.1399730>.
- Hamilton, Alexander, James Madison, John Jay, and J. R. Pole, eds. *The Federalist*. Indianapolis: Hackett Publishing Co, 2005.

- Hammer, Ann E., Trisha H. Miller, and Eva C. Uribe. "Cyber Resilience as a Deterrence Strategy." New Mexico: Sandia National Laboratories, 2020.
- Hassan, Oz, ve Christopher Featherstone. "Trump's Low Conceptual Complexity Leadership and the Vanishing 'Unpredictability Doctrine'." *Cambridge Review of International Affairs* 34, no. 3 (May 4, 2021): 407–29. <https://doi.org/10.1080/09557571.2020.1853054>.
- Healey, Jason. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity* 5, no. 1 (January 1, 2019): 1–15. <https://doi.org/10.1093/cybsec/tyz008>.
- Healy, Gene. *The Cult of the Presidency: America's Dangerous Devotion to Executive Power*. Washington, D.C.: Cato Institute, 2008.
- Henderson, C. "The 2010 United States National Security Strategy and the Obama Doctrine of 'Necessary Force'." *Journal of Conflict and Security Law* 15, no. 3 (December 1, 2010): 403–34. <https://doi.org/10.1093/jcsl/krq025>.
- Hendrickson, Ryan C. *Obama at War: Congress and the Imperial Presidency*. Lexington, Kentucky: The University Press of Kentucky, 2015.
- Henriksen, Thomas H. *Cycles in US Foreign Policy since the Cold War*. Cham: Springer International Publishing, 2017. <https://doi.org/10.1007/978-3-319-48640-6>.
- Hermann, Margaret G. "Explaining Foreign Policy Behavior Using the Personal Characteristics of Political Leaders." *International Studies Quarterly* 24, no. 1 (March 1980): 7. <https://doi.org/10.2307/2600126>.
- Hermann, Margaret G., ve Thomas Preston. "Presidents, Advisers, and Foreign Policy: The Effect of Leadership Style on Executive Arrangements." *Political Psychology* 15, no. 1 (March 1994): 75. <https://doi.org/10.2307/3791440>.
- Hlatky, Stefanie Von, ve Andreas Wenger. *The Future of Extended Deterrence*. Washington: Georgetown University Press, 2015.
- Hobson, John M. *The State ve International Relations*. New York: Cambridge University Press, 2003.
- Hoffman, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, 2007.
- Holland, Steve, and Matt Spetalnick. "Obama Vows U.S. Response to North Korea over Sony Cyber Attack." Reuters, December 19, 2014. <https://www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141219>.

- Huth, Paul, ve Bruce Russett. "What Makes Deterrence Work? Cases from 1900 to 1980." *World Politics* 36, no. 4 (1984): 496–526.
- Iasiello, Emilio. "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2014): 54–67.
- Jackson, Nicole J. "Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO." *Journal of Military and Strategic Studies* 19, no. 4 (2019): 104–25.
- Jackson, Van. "Beyond Tailoring: North Korea and the Promise of Managed Deterrence." *Contemporary Security Policy* 33, no. 2 (2012): 289–310. <https://doi.org/10.1080/13523260.2012.693795>.
- Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30, no. 2 (1978): 167–214.
- "Deterrence Theory Revisited." *World Politics* 31, no. 2 (1979): 289–324. <https://doi.org/10.2307/2009945>.
- *Perception and Misperception in International Politics*. New ed. Princeton, NJ: Princeton University Press, 2017.
- *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell University Press, 1989.
- Jhangiani, Tasha, ve Graham Kennis. "Protecting the Critical of Critical: What Is Systemically Important Critical Infrastructure?" June 15, 2021. <https://www.lawfaremedia.org/article/protecting-critical-critical-what-systemically-important-critical-infrastructure>.
- Johnson, Alex. "Trump Eliminates Job of National Cybersecurity Coordinator." NBC News, May 15, 2018. <https://www.nbcnews.com/politics/white-house/trump-eliminates-job-national-cybersecurity-coordinator-n874511>.
- Johnston, Alastair, "Thinking about Strategic Culture", *International Security*, Sayı:19 (4): (1995)
- Joint Chiefs of Staff. *JP 3-12 Cyberspace Operations*. 2018.
- Joint Chiefs of Staff. *JP 3-13 Information Operations*. 2012.
- Kahn, Herman. *On Thermonuclear War*. London: Transaction Publishers, 2007.
- Kahn, Herman. *Thinking about the Unthinkable*. New York: Avon Books, 1962.

- Kaplan, Fred. "The President in Practice." *Foreign Affairs*, February 2015.
<https://www.foreignaffairs.com/united-states/obamas-way>.
- Kaplan, Jeremy. Fox News. "New Cybersecurity Act Eliminates Internet Kill Switch."
Fox News, March 18, 2010. <https://www.foxnews.com/tech/new-cybersecurity-act-eliminates-internet-kill-switch>.
- Kaufman, Robert G. "E. H. Carr, Winston Churchill, Reinhold Niebuhr, and US: The Case for Principled, Prudential, Democratic Realism." *Security Studies* 5, no. 2 (December 1995): 314–53.
<https://doi.org/10.1080/09636419508429270>.
- Kaufmann, William. *Requirements of Deterrence*. Princeton, NJ: Princeton University Press, 1954.
- Kaur Chahal, Jasmeen, Abhinav Bhandari, ve Sunny Behal. "Distributed Denial of Service Attacks: A Threat or Challenge." *New Review of Information Networking* 24, no. 1 (January 2, 2019): 31–103.
<https://doi.org/10.1080/13614576.2019.1611468>.
- Keohane, Robert. *Neorealism and Its Critics*. New York: Columbia University Press, 1986.
- Kessler, Glenn. "President Obama and the 'Red Line' on Syria's Chemical Weapons." *Washington Post*, September 6, 2013.
<https://www.washingtonpost.com/news/fact-checker/wp/2013/09/06/president-obama-and-the-red-line-on-syrias-chemical-weapons>.
- Kissinger, Henry A. "Domestic Structure and Foreign Policy." *Daedalus* 95, no. 2 (1966): 503–29.
- Kitchen, Nicholas. "Systemic Pressures and Domestic Ideas: A Neoclassical Realist Model of Grand Strategy Formation." *Review of International Studies* 36, no. 1 (January 2010): 117–43.
<https://doi.org/10.1017/S0260210509990532>.
- Knopf, Jeffrey W. "The Fourth Wave in Deterrence Research." *Contemporary Security Policy* 31, no. 1 (2010): 1–33.
<https://doi.org/10.1080/13523261003640819>.
- Kramer, Franklin D., Stuart H. Starr, ve Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: Potomac Books, 2011.
<https://doi.org/10.2307/j.ctt1djmhj1>.

- Lasconjarias, Guillaume. "Deterrence Through Resilience: NATO, the Nations and the Challenges of Being Prepared." *NATO Defense College Eisenhower Paper*, no. 7 (May 2017).
- Lawson, Sean T. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. 1st ed. New York: Routledge, 2019.
<https://doi.org/10.4324/9781315505619>.
- Lebow, Richard Ned. "Thucydides and Deterrence." *Security Studies* 16, no. 2 (2007): 163–88. <https://doi.org/10.1080/09636410701399440>.
- Legro, Jeffrey W. ve Andrew Moravcsik. "Is Anybody Still a Realist?" *International Security* 24, no. 2 (October 1999): 5–55.
<https://doi.org/10.1162/016228899560130>.
- Lehto, Martti, ve Pekka Neittaanmaki, eds. *Cybersecurity: Critical Infrastructure Protection*. Cham: Springer, 2022.
- Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.
- Liebert, Hugh, Gary L. McDowell ve Terry L. Price, eds. *Executive Power in Theory and Practice*. New York: Palgrave Macmillan US, 2012.
<https://doi.org/10.1057/9781137014450>.
- Lilli, Eugenio. "President Obama and US Cyber Security Policy." *Journal of Cyber Policy* 5, no. 2 (May 3, 2020): 265–84.
<https://doi.org/10.1080/23738871.2020.1778759>.
- . "Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence." *Contemporary Security Policy* 42, no. 2 (February 5, 2021): 163–88.
<https://doi.org/10.1080/13523260.2021.1882812>.
- Lin, Herbert ve Amy Zegart. *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington, DC: Brookings Institution Press, 2018.
- Lindsay, Jon R. "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem." *Intelligence and National Security*, 2020.
<https://doi.org/10.1080/02684527.2020.1840746>.
- . "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (2013): 365–404.

- , "Tipping the scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack." *Journal of Cybersecurity*, 1(1) (2015): 53–67.
- Lonergan, Erica D. ve Shawn W. Lonergan. "To Defend Forward, the U.S. Must Strengthen the Cyber Mission Force." *Lawfare*, March 13, 2020. <https://www.lawfaremedia.org/article/defend-forward-us-must-strengthen-cyber-mission-force>.
- Luijff, Eric. "Understanding Cyber Threats and Vulnerabilities." In *Critical Infrastructure Protection*, edited by Javier Lopez, Roberto Setola, and Stephen D. Wolthusen, 52–67. Lecture Notes in Computer Science 7130. Berlin: Springer, 2012. https://doi.org/10.1007/978-3-642-28920-0_4.
- Lupovici, Amir. "Cyber Warfare and Deterrence: Trends and Challenges in Research." *Military and Strategic Affairs* 3, no. 3 (2011): 49–62.
- . "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives*, 2014, 1–21. <https://doi.org/10.1111/insp.12082>.
- . "The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda." *International Studies Quarterly* 54 (2010): 705–32.
- Mahoney, James. "The Logic of Process Tracing Tests in the Social Sciences" *Sociological Methods & Research* 41(4) (2012): 570-597
10.1177/0049124112437709
- Mallory, King. *New Challenges in Cross-Domain Deterrence*. Santa Monica, CA: RAND Corporation, 2018. <https://www.rand.org/pubs/perspectives/PE259.html>.
- Maness, Ryan C., Brandon Valeriano, Kathryn Hedgecock, Benjamin M. Jensen, and Jose M. Macias. "The Dyadic Cyber Incident and Campaign Dataset." July 2022. <https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV>.
- Martel, William C. ve Paul L. Savage. *Strategic Nuclear War: What the Super Powers Target and Why*. New York: Greenwood Press, 1986.
- Martellini, Maurizio, ed. *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*. Springer Briefs on Computer Science, 2013. <https://doi.org/10.1007/978-3-319-02279-6>.

- McCormick, James M., Traci Crowell ve Mary Malley, eds. *The Domestic Sources of American Foreign Policy: Insights and Evidence*. 7th ed. Lanham: Rowman & Littlefield, 2018.
- McDougall, Walter A. *Promised Land, Crusader State*. Boston: Houghton Mifflin, 1997.
- McFall, Caitlin ve Jake Gibson. "FBI Charges Three Iranians in Cyber Attacks Targeting Local US Governments, Power Companies." *Fox News*, September 14, 2022. <https://www.foxnews.com/politics/fbi-charges-three-iranians-cyber-attacks-targeting-local-us-governments-power-companies>.
- McGraw, Gary. "Cyber War Is Inevitable (Unless We Built Security In)." *Journal of Strategic Studies* 36, no. 1 (2013): 109–19. <https://doi.org/10.1080/01402390.2012.742013>.
- Mead, Walter Russell. "American Populism and the Liberal Order." *Foreign Affairs*, March 2017.
- . "Jacksonian Tradition and American Foreign Policy." *The National Interest* 58 (1999): 5–25.
- . *Special Providence: American Foreign Policy and How It Changed the World*. 1st ed. New York: Knopf, 2001.
- Mears, Alan ve Joe Mariani. "The Temporal Dimension of Defending Forward." *The Cyber Defense Review* 5, no. 1 (November 2019): 55–74.
- Mearsheimer, John J. "Back to the Future: Instability in Europe after the Cold War." *International Security* 15, no. 1 (1990): 5–56.
- . *Conventional Deterrence*. Ithaca: Cornell University Press, 1983.
- Meibauer, Gustav. "Interests, Ideas, and the Study of State Behaviour in Neoclassical Realism." *Review of International Studies* 46, no. 1 (January 2020): 20–36. <https://doi.org/10.1017/S0260210519000214>.
- . "Neorealism, Neoclassical Realism and the Problem(s) of History." *International Relations*, n.d.
- Meibauer, Gustav, Linde Desmaele, Tudor Onea, Nicholas Kitchen, Michiel Foulon, Alexander Reichwein, and Jennifer Sterling-Folker. "Forum: Rethinking Neoclassical Realism at Theory's End." *International Studies Review* 23, no. 1 (March 4, 2021): 268–95. <https://doi.org/10.1093/isr/viaa018>.

- Meredith, R., Sarkees ve Frank W. Wayman. *Resort to War: A Data Guide to Inter-State, Extra-State, Intra-State, and Non-State Wars, 1816–2007*. Washington: CQ Press, 2010.
- Moran, Michael, Martin Rein ve Robert E. Goodin, eds. *The Oxford Handbook of Public Policy*. The Oxford Handbooks of Political Science. Oxford: Oxford University Press, 2006.
- Morgan, Patrick M. *Deterrence: A Conceptual Analysis*. London: SAGE Publications, 1977.
- . "The State of Deterrence in International Politics Today." *Contemporary Security Policy* 33, no. 1 (2012): 85–107.
- Morgenthau, Hans J. "The Mainsprings of American Foreign Policy: The National Interest vs. Moral Abstractions." *American Political Science Review* 44, no. 4 (December 1950): 833–54. <https://doi.org/10.2307/1951286>.
- Murphy, Patrick J. ve Erica Borghard. "To Defend Forward, US Cyber Strategy Demands a Cohesive Vision." *Cyber Defense Review*, 2020, 15–29.
- Nakashima, Ellen. "Iran Blamed for Cyberattacks on U.S. Banks and Companies." *Washington Post*, September 21, 2012. https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html.
- Narang, Vipin. *Nuclear Strategy in the Modern Era*. Oxford: Princeton University Press, 2014.
- National Strategy for Trusted Identities in Cyberspace. Beyaz Saray, April 2011.
- New York Times. "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity." May 14, 2021. <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>.
- Nicole, Jackson. "Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO", *Journal of Strategic Studies*, 19 (4), 104-125, 2019.
- Nye, Joseph S. "Nuclear Learning and U.S.-Soviet Security Regimes." *International Organization* 41, no. 3 (1987): 371–402.
- Nye, Joseph. S. "Deterrence and Dissuasion in Cyberspace". *International Security*, 41(3), (2017):44–71. https://doi.org/10.1162/ISEC_a_00266
- Obama, Barack. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World: (688502011-001)*. American

- Psychological Association, 2011. <https://doi.org/10.1037/e688502011-001>.
- Onea, Tudor. "Putting the 'Classical' in Neoclassical Realism: Neoclassical Realist Theories and US Expansion in the Post-Cold War." *International Relations* 26, no. 2 (June 2012): 139–64. <https://doi.org/10.1177/0047117811430674>.
- Palmer, Glenn, Roseanne W. McManus, Vito D'Orazio, Michael R. Kenwick, Mikaela Karstens, Chase Bloch, Nick Dietrich, Kayla Kahn, Kellan Ritter, and Michael J. Soules. "The MID5 Dataset, 2011–2014: Procedures, Coding Rules, and Description." *Conflict Management and Peace Science* 39, no. 4 (July 2022): 470–82. <https://doi.org/10.1177/0738894221995743>.
- Pape, Robert A. "Coercion and Military Strategy: Why Denial Works and Punishment Doesn't", *The Journal of Strategic Studies*, Vol.15, No.4 (December 1992), sf.423-475
- Perlroth, Nicole ve David E. Sanger. "White House Eliminates Cybersecurity Coordinator Role." *New York Times*, May 15, 2018. <https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html>.
- Peter Margulies. "Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy." *Indiana Journal of Global Legal Studies* 24, no. 2 (2017): 459. <https://doi.org/10.2979/indjglolegstu.24.2.0459>.
- Peterson, Andrea. "The Sony Pictures Hack, Explained." *The Washington Post*, December 18, 2014. <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>.
- Presidential Memorandum for the Secretary of Defense. Beyaz Saray, August 18, 2017. <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-secretary-defense/>.
- Press, Daryl G. "The Credibility of Power: Assessing Threats during the 'Appeasement' Crises of the 1930s." *International Security* 29, no. 3 (2005): 136–69.
- Putnam, Robert D. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42, no. 3 (1988): 427–60. <https://doi.org/10.1017/S0020818300027697>.
- Quackenbush, Stephen L. *Understanding General Deterrence*. New York: Palgrave Macmillan, 2011.

- Quinn, Adam. *US Foreign Policy in Context: National Ideology from the Founders to the Bush Doctrine*. Routledge Studies in US Foreign Policy. London; New York: Routledge, 2010.
- Rathbun, Brian. "A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism." *Security Studies* 17, no. 2 (May 22, 2008): 294–321. <https://doi.org/10.1080/09636410802098917>.
- Realism, Gideon Rose. Reviewed work(s): *The Perils of Anarchy: Contemporary International Security* by Michael E. Brown, *Useful Adversaries: Grand Strategy, Domestic Mobilization, and Sino-American Conflict, 1947–1958* by Thomas J. Christensen, *Deadly Imbalances: Tripolarity, and ... Hitler's Strategy of World Conquest* by Randall L. "Review: Neoclassical Realism and Theories of Foreign Policy." *World Politics* 51, no. 1 (1998): 144–72.
- Ripsman, Norrin M., Jeffrey W. Taliaferro, and Steven E. Lobell. *Neoclassical Realist Theory of International Politics*. New York: Oxford University Press, 2016.
- Rizzo, Jennifer. "Cybersecurity Bill Fails in Senate." CNN, August 2, 2012. <https://edition.cnn.com/2012/08/02/politics/cybersecurity-act/index.html>.
- Roberts, Dan. "Obama Imposes New Sanctions against North Korea in Response to Sony Hack." *The Guardian*, January 2, 2015. <https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview>.
- Rolf, Jan Niklas. "Donald Trump's Jacksonian and Jeffersonian Foreign Policy." *Policy Studies* 42, no. 5–6 (November 2, 2021): 662–81. <https://doi.org/10.1080/01442872.2021.1934431>.
- Rublee, Maria Rost ve Avner Cohen. "Nuclear Norms in Global Governance: A Progressive Research Agenda." *Contemporary Security Policy* 39, no. 3 (July 3, 2018): 317–40. <https://doi.org/10.1080/13523260.2018.1451428>.
- Rudalevige, Andrew. "Executive Branch Management and Presidential Unilateralism: Centralization and the Issuance of Executive Orders." *Congress & the Presidency* 42, no. 3 (September 2, 2015): 342–65. <https://doi.org/10.1080/07343469.2015.1077484>.
- . *The New Imperial Presidency: Renewing Presidential Power after Watergate*. 1st paperback ed. Contemporary Political and Social Issues. Ann Arbor: University of Michigan Press, 2006.

- Ruggiero, Scott M. "Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch." *Science and Technology Law Review* 15, no. 2 (2017): 241–69.
- Ryan, N. J. "Five Kinds of Cyber Deterrence." *Philosophy & Technology* 31, no. 3 (September 2018): 331–38. <https://doi.org/10.1007/s13347-016-0251-1>.
- Sagan, Scott D. "The Perils of Proliferation: Organization Theory, Deterrence Theory and the Spread of Nuclear Weapons." *International Security* 18, no. 4 (1994): 66–107.
- . "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb." *International Security* 21, no. 3 (1996): 54. <https://doi.org/10.2307/2539273>.
- Sanger, David E. "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict." *The New York Times*, June 17, 2018. <https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html>.
- Savage, Charlie. "Trump's Secret Rules for Drone Strikes Outside War Zones Are Disclosed." *The New York Times*, May 1, 2021. <https://www.nytimes.com/2021/05/01/us/politics/trump-drone-strike-rules.html>.
- . "U.S. Releases Rules for Airstrike Killings of Terror Suspects." *The New York Times*, August 6, 2016. <https://www.nytimes.com/2016/08/07/us/politics/us-releases-rules-for-airstrike-killings-of-terror-suspects.html>.
- Savage, Charlie ve Eric Schmitt. "Trump Poised to Drop Some Limits on Drone Strikes and Commando Raids." *The New York Times*, September 21, 2017. <https://www.nytimes.com/2017/09/21/us/politics/trump-drone-strikes-commando-raids-rules.html>.
- Savunma Bakanlığı. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference U.S. Department of Defense Speech." March 2, 2020. <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.
- . "Savunma Bakanlığı Siber Stratejisi-2015." April 2015. <https://nsarchive.gwu.edu/document/21384-document-25>.
- . "Savunma Bakanlığı Siber Uzay Politika Raporu." November 2011.

- Schaefer, Todd M. *Presidential Power Meets the Art of the Deal: Applying Neustadt to the Trump Presidency*. Cham: Springer International Publishing, 2021.
<https://doi.org/10.1007/978-3-030-56029-4>.
- Schelling, Thomas C. *Arms and Influence*. 2008 Edition. London: Yale University Press, 1966.
- Schmidt, Michael S. "Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster." *The New York Times*, August 2, 2012.
<https://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html>.
- . "Republicans Block Bill on Cybersecurity." *The Boston Globe*, August 3, 2012.
<https://www.bostonglobe.com/news/nation/2012/08/02/republicans-block-vote-cybersecurity-bill/XN4yYtGWUD5maxCv1EE3vI/story.html>.
- Schweller, Randall L. "Unanswered Threats: A Neoclassical Realist Theory of Underbalancing." *International Security* 29, no. 2 (2004): 159–201.
- Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. 2nd ed. New York: PublicAffairs, 2017.
- Shackleford, Scott, Andrew Proia, Brenton Martell ve Amanda Craig. "Toward a Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices." *Legal Studies Research Paper Series*, no. 291 (2015).
- Shively, Jacob. "Cybersecurity Policy and the Trump Administration." *Policy Studies* 42, no. 5–6 (November 2, 2021): 738–54.
<https://doi.org/10.1080/01442872.2021.1947482>.
- Singer, David J., Stuart Bremer ve John Stuckey. "Capability Distribution, Uncertainty, and Major Power War, 1820–1964 (6th version)." In *Peace, War, and Numbers*, 19–48. Beverly Hills: SAGE Publications, 2021.
<https://correlatesofwar.org/data-sets/national-material-capabilities/>.
- Siniver, Asaf ve Christopher Featherstone. "Low-Conceptual Complexity and Trump's Foreign Policy." *Global Affairs* 6, no. 1 (January 1, 2020): 71–85.
<https://doi.org/10.1080/23340460.2020.1734953>.
- Smalley, Suzanne. "Biden Administration Is Studying Whether to Scale Back Trump-Era Cyber Authorities at DOD." *CyberScoop.com*, March 31, 2022.
<https://cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/>.

- Smeets, Max. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. London: Hurst & Co. Publishers, 2022.
- Smith, Nicholas Ross. "Can Neoclassical Realism Become a Genuine Theory of International Relations? Squandered Opportunity: Neoclassical Realism and Iranian Foreign Policy. By Thomas Juneau. Stanford, CA: Stanford University Press, 2015. EU and NATO Relations with Russia: After the Collapse of the Soviet Union. By Glenn Diesen. Abingdon: Routledge, 2016. Neoclassical Realist Theory of International Politics. By Norrin M. Ripsman, Jeffrey W. Taliaferro, and Steven E. Lobell. Oxford: Oxford University Press, 2016." *The Journal of Politics* 80, no. 2 (April 2018): 742–49. <https://doi.org/10.1086/696882>.
- Smoke, Richard ve Alexander George. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press, 1974.
- Snyder, Glenn. *Deterrence and Defense: Toward a Theory of National Security*. Princeton, NJ: Princeton University Press, 1961.
- . *Deterrence by Denial and Punishment*. Princeton, NJ: Center of International Studies, 1959.
- . "The Balance of Power and the Balance of Terror." In *The Balance of Power*, edited by Paul Seabury. San Francisco: Chandler Books, 1965.
- . "Process Variables in Neorealist Theory." *Security Studies* 5, no. 3 (March 1996): 167–92. <https://doi.org/10.1080/09636419608429279>.
- Snyder, Jack. *Myths of Empire: Domestic Politics and International Ambition*. Ithaca, NY: Cornell University Press, 1993.
- Soesanto, Stefan. "The Evolution of US Defense Strategy in Cyberspace." Zurich: Center for Security Studies, 2019.
- Sönmezoğlu, Faruk. *Uluslararası Politika ve Dış Politika Analizi*. 6th ed. İstanbul: Der Yayınları, 2014.
- Starks, Tim. "Ramifications of Trump Revoking Obama's Cyber Offense Order." *Politico.com*, August 17, 2018. <https://www.politico.com/newsletters/morning-cybersecurity/2018/08/17/ramifications-of-trump-revoking-obamas-cyber-offense-order-320741>.
- Steff, Reuben. *Strategic Thinking, Deterrence and the US Ballistic Missile Defense Project: From Truman to Obama*. Surrey: Ashgate Publishing Limited, 2013.

- Stein, Janice Gross. "Deterrence and Reassurance." In *Behavior, Society and Nuclear Weapons*, edited by Philip E. Tetlock, Jo L. Husbands, Robert Jervis, Paul C. Stern, and Charles Tilly, 31–76. New York: Oxford University Press, 1991.
- Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (April 2012): 148–70. <https://doi.org/10.1080/13523260.2012.659597>.
- Taliaferro, Jeffrey W. "State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State", *Security Studies*, Sayı:15 (3), 2006
- Tang, Shiping. "Reputation, Cult of Reputation and International Conflict." *Security Studies* 14, no. 1 (2005): 34–62.
- The Guardian. "Obama Unveils New Defence Strategy with Greater Emphasis on Asia." January 5, 2012. <https://www.theguardian.com/world/2012/jan/05/obama-unveils-defence-strategy-asia>.
- Thompson, Mark. "Iranian Cyber Attack on New York Dam Reveals Future of War." *Time*, March 24, 2016. <https://time.com/4270728/iran-cyber-attack-dam-fbi/>.
- Ullah, Haroon K. *Digital World War*. New Haven: Yale University Press, 2017.
- "Ulusal Güvenlik Stratejisi-2015." ABD Başkanlık Makamı, February 2015. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.
- "University of Maryland Cyber Attacks Database." University of Maryland. Accessed February 24, 2023. <https://cissm.liquifiedapps.com/#charts>.
- Walker, Stephen G., Akan Malici, and Mark Schafer, eds. *Rethinking Foreign Policy Analysis: States, Leaders, and the Microfoundations of Behavioral International Relations*. New York: Routledge, 2011.
- Waltz, Kenneth N. "Emerging Structure of International Politics." *International Security* 18, no. 2 (1993): 44–79.
- . "Nuclear Myths and Political Realities." *American Political Science Review* 84, no. 3 (September 1990): 731–45.
- . "Structural Realism after the Cold War." *International Security* 25, no. 1 (2000): 5–41.

- . "The Spread of Nuclear Weapons: More May Be Better." *Adelphi Papers*, no. 171 (1981).
- . *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979.
- Washington Post. "The Cybersecurity 202: Trump Just Gave the Military a Lot More Leeway to Launch Cyber Operations." August 17, 2018. <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/17/the-cybersecurity-202-trump-just-gave-the-military-a-lot-more-leeway-to-launch-cyber-operations/5b75a7551b326b7234392972/>.
- Wendt, Alexander E. "The Agent-Structure Problem in International Relations Theory." *International Organization* 41, no. 3 (1987): 335–70. <https://doi.org/10.1017/S002081830002751X>.
- Whyte, Christopher ve Brian Mazanec. *Understanding Cyber Warfare*. New York: Routledge, 2023.
- Wilner, Alex. "Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation." *Comparative Strategy* 36, no. 4 (2017): 309–18.
- . "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43, no. 2 (2020): 245–80. <https://doi.org/10.1080/01402390.2018.1563779>.
- Winterfeld, Steve ve Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Syngress Basics Series. Amsterdam: Syngress/Elsevier, 2013.
- Wohlstetter, Albert. "The Delicate Balance of Terror." *Survival: Global Politics and Strategy*, no. 1 (1959): 8–17.
- Yalçınkaya, Haldun. *Savaş: Uluslararası İlişkilerde Güç Kullanımı*. Ankara: İmge Kitabevi, 2008.
- Yang, Y. E. "Leaders' Conceptual Complexity and Foreign Policy Change: Comparing the Bill Clinton and George W. Bush Foreign Policies toward China." *The Chinese Journal of International Politics* 3, no. 4 (December 1, 2010): 415–46. <https://doi.org/10.1093/cjip/poq015>.
- Zagare, Frank C. ve Mark D. Kilgour. *Perfect Deterrence*. New York: Cambridge University Press, 2004.
- Zakaria, Fareed. *From Wealth to Power*. Princeton, NJ: Princeton University Press, 1998.

Zarate, Robert ve Henry Sokolski, eds. *Nuclear Heuristics: Selected Writings of Albert and Roberta Wohlstetter*. Carlisle, PA: Strategic Studies Institute, 2009.

Zenko, Micah. "Obama's Embrace of Drone Strikes Will Be a Lasting Legacy." *New York Times*, January 12, 2016.

<https://www.nytimes.com/roomfordebate/2016/01/12/reflecting-on-obamas-presidency/obamas-embrace-of-drone-strikes-will-be-a-lasting-legacy>.

Zetter, Kim. "How Close Did Russia Really Come to Hacking the 2016 Election." *Time*, December 26, 2019. <https://time.com/5565991/russia-influence-2016-election/>.



VERİ ANALİZİNDE BAŞVURULAN RESMİ GÜVENLİK BELGELERİ

1. Siber Uzay Politika Değerlendirmesi: Güvenilir ve Dayanıklı Bilgi ve İletişim Altyapısının Oluşturulması – 2009 (Cyberspace Policy Review: Assuring A Trusted and Resilient Information and Communications Infrastructure)
2. Ulusal Güvenlik Stratejisi – 2010 (National Security Strategy)
3. Siber Uzayda Harekât Strateji Belgesi – 2011 (Department of Defense Strategy for Operating in Cyberspace)
4. Siber Uzay Politika Raporu – 2011 (Cyberspace Policy Report)
5. Siber Uzay Uluslararası Stratejisi – 2011 (International Strategy for Cyberspace)
6. Siber Uzayda Güvenilir Kimlikler için Ulusal Strateji – 2011 (National Strategy for Trusted Identities in Cyberspace)
7. Başkanlık Siyaset Direktifi 20 – 2012 (Presidential Policy Directive)
8. Savunma Bilimi Kurulu Raporu: Dayanıklı Askeri Sistemler ve Gelişmiş Siber Tehdit Raporu – 2013 (Department of Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat)
9. İcra Emri 13636 – 2013 (Executive Order 13636)
10. İcra Emri 13687 – 2015 (Executive Order 13687)
11. Ulusal Güvenlik Stratejisi – 2015 (National Security Strategy)
12. İcra Emri 13691 – 2015 (Executive Order 13691)
13. İcra Emri 13694 – 2015 (Executive Order 13694)
14. Siber Strateji Belgesi – 2015 (Department of Defense Cyber Strategy)
15. İcra Emri 13718 – 2016 (Executive Order 13718)
16. Başkanlık Siyaset Direktifi 41 – 2016 (Presidential Policy Directive 41)
17. İcra Emri 13800 – 2017 (Executive Order 13800)
18. Ulusal Güvenlik Stratejisi – 2017 (National Security Strategy)
19. Ulusal Güvenlik Başkanlık Memorandumu 13 – 2018 (National Security Presidential Memorandum)
20. Siber Strateji Belgesi – 2018 (Department of Defense Cyber Strategy)
21. Ulusal Siber Strateji – 2018 (National Cyber Strategy of the United States of America)
22. İcra Emri 13870 – 2019 (Executive Order 13870)
23. İcra Emri 13873 – 2019 (Executive Order 13873)
24. İcra Emri 13942 / 13943 – 2020 (Executive Order 13942/13943)
25. İcra Emri 13984 – 2021 (Executive Order 13984)



TEZDEN ÜRETİLMİŞ YAYINLAR

Emre İnan, “Stratejik Kültür Ve Kurumların Caydırıcılık Stratejisi Üzerindeki Etkileri: Obama ve Trump Yönetimlerinin Siber Güvenlik Politikalarının Karşılaştırmalı Analizi”, *Ankara Üniversitesi SBF Dergisi*, Cilt 80, No. 2, 2025, s. 327-358, <https://doi.org/10.33630/ausbf.1628859>

