Ankara Üniversitesi
SBF Dergisi,
Cilt 80, No. 2, 2025, s. 327-358
Türkçe

Araştırma Makalesi / Research Article
DOI

STRATEJİK KÜLTÜR VE KURUMLARIN CAYDIRICILIK STRATEJİSİ ÜZERİNDEKİ ETKİLERİ: OBAMA VE TRUMP YÖNETİMLERİNİN SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRMALI ANALİZİ *

Emre İnan
Milli Savunma Üniversitesi
ORCID: 0000-0001-9804-0382
ROR ID: ror.org/010t24d82

● ● ●

Öz

Zorlayıcı diplomasinin bir aracı olan caydırıcılık stratejisi, Soğuk Savaş dönemi güç ilişkilerinde belirleyici etkiye sahip olmuştur. Dolayısıyla alana ilişkin çalışmalar, bu döneme dair nükleer silah ve güç dengesi gibi yapısal faktörlerinden önemli ölçüde etkilenmiştir. Bununla birlikte yakın dönemde karşılaşılan siber tehditlere karşı yürütülen caydırıcılık stratejilerini anlamak için güç dengesi ilişkilerine ilaveten 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 başvurulan çalışmada, vaka analizi ve süreç takibi yöntemleri uygulanmıştır. Örnek vaka olarak ABD siber caydırıcılık politikaları ele alınmış ve Barack Obama ve 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 Sözcükler: Caydırıcılık, Neoklasik realizm, Siber tehditler, Dış politika gelenekleri, Kongre

Effects of Strategic Culture and Institutions on Deterrence Strategy: A Comparative Analysis of Cybersecurity Policies of Obama and Trump Administrations

Abstract

Deterrence strategy, as an instrument of coercive diplomacy, played a pivotal role in the power dynamics of the Cold War. Consequently, deterrence studies became largely shaped by the defining features of that era—namely, nuclear weapons and the balance of power. However, to comprehend deterrence strategies in response to contemporary cyber threats, it is essential to incorporate internal variables into foreign policy analysis. This study investigates the role of strategic culture and institutions in shaping cyber deterrence strategies. Anchored in the theoretical framework of neoclassical realism, the research employs case analysis and process tracing methods. The United States' cyber deterrence policies serve as the case study, with a comparative analysis of cyber strategies during the Obama and Trump administrations. The findings reveal that while structural factors such as power distribution and threat perception offer a general orientation for security policy, internal variables—particularly strategic culture and institutions—lead to divergent deterrence approaches within similar structural contexts. This study contributes to the field by demonstrating how internal and structural variables can be jointly applied in foreign policy analysis, offering a refined understanding of cyber deterrence strategy.

Keywords: Deterrence, Neoclassical realism, Cyber threats, Foreign policy traditions, Congress

---

* Makale geliş tarihi / Received date: 28.01.2025
Makale kabul tarihi / Accepted date: 05.05.2025
Erken görünüm tarihi / Published online: 13.05.2025

Yazar email: emreinan123@gmail.com

Stratejik Kültür ve Kurumların Caydırıcılık Stratejisi Üzerindeki Etkileri: Obama ve Trump Yönetimlerinin Siber Güvenlik Politikalarının Karşılaştırmalı Analizi

Giriş

Siber tehditler karşısında caydırıcılık stratejisinin uygulanabilirliği, son yıllarda akademik yazında artan bir ilgiyle ele alınmaktadır. Ancak mevcut literatürde, devletlerin benimsediği caydırıcılık stratejilerinin analizinde ağırlıklı olarak güç dengesi gibi yapısal değişkenlere odaklanıldığı; liderlik, kurumlar ve stratejik kültür gibi içsel değişkenlerin göz ardı edildiği görülmektedir. Oysa içsel dinamiklerin dış politika karar alma süreçlerindeki belirleyici rolü, son dönemdeki birçok çalışmanın merkezinde yer almaktadır. Bu makale benzer bir yaklaşımla, caydırıcılık stratejisini bir dış güvenlik politikası aracı olarak ele alarak iç değişkenlerin etkisini test etmeyi amaçlamaktadır.

Çalışmanın kuramsal çerçevesini, yapısal ve içsel değişkenlerin dış politika üzerindeki etkisini birlikte ele alan Neoklasik Realizm oluşturmaktadır. Neoklasik Realizm, güç dağılımı ve tehdit algısı gibi uluslararası sistemin sunduğu fırsat ve kısıtların, devletler tarafından içsel faktörler aracılığıyla farklı biçimlerde yorumlandığını ve bunun dış politika tercihlerine yansıdığını savunur.

Bu çerçevede, 2009-2021 yılları arasında ABD'nin yürüttüğü siber caydırıcılık stratejisi vaka analizi olarak seçilmiştir. Siber tehditlerin tercih edilme nedeni ise; bu tehditlerin klasik anarşi düzenine dayalı güvenlik yaklaşımlarının ötesine geçerek, aktör odaklı iç değişkenlerin etkisine daha açık bir güvenlik alanı oluşturmasıdır.

Makalenin ilk bölümünde, literatürdeki yapısal değişken odaklı caydırıcılık yaklaşımları incelenmiş ve bu çalışmalarda iç değişkenlerin yeterince ele alınmadığı tespit edilmiştir. İkinci bölümde kuramsal tartışma kapsamında Neoklasik Realizme yer verilmiş, ardından araştırma tasarımı açıklanmıştır. Çalışmada vaka analizi ve süreç izleme yöntemleri kullanılmış; Obama ve Trump dönemlerinde uygulanan caydırıcılık stratejileri karşılaştırmalı olarak analiz edilmiştir.

Dördüncü bölümde, ABD'nin siber güvenlik politikalarının güç dağılımı ve tehdit algısıyla nasıl şekillendiği değerlendirilmiş ve yapı-aktör ilişkisi analiz edilmiştir. Beşinci bölümde, 2009-2021 dönemine ait resmi güvenlik belgeleri analiz edilerek her iki başkan döneminde tercih edilen caydırıcılık yöntemleri ortaya koyulmuştur.

Son bölümde, bu yöntemlerin arkasındaki stratejik kültür ve kurumların etkileri değerlendirilmiştir. Bu kapsamda; Mead'in ABD dış politika gelenekleri çalışmasından yararlanılarak başkanların karar alma profillerini şekillendiren stratejik kültürler analiz edilmiş; bu kültürlerin siber güvenlik politikalarıyla ilişkisi irdelenmiştir. Kurum değişkeninde ise Kongre'nin yasama ve denetleme mekanizmaları yoluyla caydırıcılık stratejilerine etkileri incelenmiştir.

Elde edilen bulgular, siber güvenlik stratejilerinin başkanların benimsediği stratejik kültürlerin doğal bir uzantısı olduğunu ve farklılaşan caydırıcılık yöntemlerinin bu kültürler doğrultusunda şekillendiğini göstermektedir. Kongre'nin ise caydırıcılık stratejisine katkı ve yön verme kapasitesine sahip olduğu ancak bu etkinin genellikle partizanlık engelinin aşıldığı koşullarda ortaya çıkabildiği sonucuna ulaşılmıştır.

1. Caydırıcılık Kuramının Evrimi ve Siber Tehditler Bağlamında Güncel Yaklaşımlar

Caydırıcılık, bir aktörün belirli bir davranış biçimini benimsemesi halinde ciddi maliyetlerle karşılaşacağına dair bir beklenti oluşturarak bu davranışın engellenmesini amaçlayan stratejik bir yaklaşımdır (Paul vd., 2009). 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 (Lilli, 2021, s. 163).

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 klasik güç dengesi anlayışının öngördüğü karşılıklı şeffaflık ve hesap verebilirlik ilkelerini ihlal etmektedir. Bu yönüyle siber caydırıcılık, nükleer caydırıcılığın topyekûn engelleme mantığından ayrılarak, tehditlerin yoğunluğunu ve sıklığını minimize etmeye odaklanan bir stratejiye evrilmiştir (Lilli, 2021, s. 166).

Caydırıcılık kuramının tarihsel gelişimi, Jervis (1979) tarafından üç teorik dalga altında sınıflandırılmıştır. İlk dalga, nükleer silahların güvenlik stratejilerine etkisini açıklamaya çalışan öncü çalışmaları içermektedir. İkinci dalga, Rasyonel Caydırıcılık Teorisinin kuramsal temellerini inşa etmiştir. Bu yaklaşım, aktörlerin kararlarını rasyonel fayda-maliyet analizine göre verdikleri varsayımına dayanır. Thomas Schelling, Herman Kahn ve Glenn Snyder gibi isimlerin öncülüğünde geliştirilen bu modelde, caydırıcılığın başarısı üç temel bileşene bağlanır: kapasite, inandırıcılık ve etkili iletişim (Kahn, 1962; Schelling, 1966; Snyder, 1961). Ancak Jervis, bu çerçevenin yetersiz kaldığını savunarak caydırıcılık stratejilerinin psikolojik boyutuna dikkat çekmiştir. Ona göre; bir tehdit yalnızca ilan edilmiş olmasıyla değil karşı tarafta nasıl algılandığı ile anlam kazanmaktadır. Bu nedenle yanlış anlamalar ve ön yargılar caydırıcılığın başarısını etkileyen unsurlardır (Jervis, 1976). Rasyonel Caydırıcılık Teorisinin statik doğasına ve Jervis'in psikolojik odaklı analizine yapısal bir alternatif sunmayı amaçlayan Frank Zagare ve Marc Kilgour Mükemmel Caydırıcılık Teorisini (*Perfect Deterrence Theory*) geliştirmiştir. Oyun Teorisi temelli bu yaklaşıma göre; tehditlerin büyüklüğünden çok karşı tarafta inandırıcı ve karşılanabilir görülmesi önemlidir (Zagare & Kilgour, 2004). Diğer taraftan statükoyu bozma veya boyun eğme davranışı tek seferlik bir karar olmayıp aktörlerin birbiri ardına uyguladıkları etkileşimsel bir süreçtir.

Üçüncü dalga ise George ve Smoke'un (1974) ampirik temelli çalışmalarıyla şekillenmiş, karar vericilerin sınırlı rasyonaliteye sahip olduğunu savunan eleştirel yaklaşımlarla derinleşmiştir (Achen & Snidal, 1989; Lebow & Stein, 1989). Mearsheimer (1983), caydırıcılığın yalnızca nükleer değil konvansiyonel tehdit ortamlarında da geçerli olduğunu göstererek farklı tehdit ortamlarına dair çalışmaların kapısını aralamıştır. Soğuk Savaş'ın sona ermesiyle birlikte, Jeffrey Knopf yeni bir dördüncü dalgadan söz ederek devlet dışı aktörlerin, asimetrik savaş biçimlerinin ve siber tehditlerin caydırıcılık kuramı içine dahil edilmesi gerektiğini vurgulamıştır (Knopf, 2010).

Bu bağlamda, güncel literatür caydırıcılığı sadece devlet merkezli değil çok aktörlü bir güvenlik ortamında değerlendirmektedir. Bununla birlikte, caydırıcılık stratejisini siber tehditler özelinde inceleyen yakın dönem çalışmaların ampirik yaklaşımdan uzaklaşarak yeniden başarılı olma koşullarına odaklanan teorik bir anlayış benimsediği görülmektedir (Iasiello, 2014; Lilli, 2021; Wilner, 2019). Ayrıca bu çalışmalar caydırıcılığın başarı durumunu sorgularken bunu sağlayacak siber kapasite inşasını ve etkileyen iç koşulları ele almamaktadır. Siber kabiliyetler gibi kapasite bileşeninin verili olarak kabul edilemeyeceği, ofansif/defansif kabiliyetlerin halen inşa aşamasında olduğu bir tehdit ortamında iç bileşenleri hesaba katmamak eksik bir çerçeve sunmaktadır. Bu çalışma; söz konusu boşluğu doldurmayı amaçlamakta ve caydırıcılığın

başarısı yerine, uygulanan caydırıcılık modelinin içsel koşullarla nasıl şekillendiğini analiz etmeyi hedeflemektedir.

2. Neoklasik Realizm: Yapı, İç Dinamikler ve Dış Politika Karar Alma Süreci

Neoklasik Realizm, Uluslararası İlişkiler disiplininde dış politika analizine yönelik teorik bir çerçeve sunarak yapısal faktörler ile devlete özgü iç değişkenleri birlikte ele alan bütüncül bir yaklaşım geliştirmiştir. Gideon Rose'un öncülüğünde (Rose, 1998) sistematik hale gelen kuram, devletlerin dış politika davranışlarının temel itici gücünün uluslararası sistemdeki güç dağılımı olduğunu kabul etmekte ve bu yönüyle Neorealist gelenekle ortak bir zeminde konumlanmaktadır. Anarşi, rekabet, hayatta kalma ve güç maksimizasyonu gibi kavramlar, her iki teorik yaklaşımın merkezi unsurları arasındadır. Bununla birlikte Neoklasik Realizm, yalnızca yapısal değişkenlerin devlet davranışını açıklamakta yetersiz kaldığını ileri sürerek, analitik düzlemini iç siyasal ve toplumsal değişkenlerle genişletmektedir (Ripsman vd., 2009).

Neorealizm, özellikle Kenneth Waltz'ın ortaya koyduğu biçimiyle, devletlerin uluslararası sistemin yapısal mantığına göre davranacağını ve benzer yapısal koşullar altında benzer dış politika tercihlerinde bulunacaklarını varsaymaktadır (Waltz, 1979). Buna karşılık Neoklasik Realizm sistemik baskıların devlet davranışını ancak devletin içsel kapasitesi ve algı süreçleri aracılığıyla etkileyebileceğini ileri sürer (Zakaria, 1998). Bu doğrultuda devletlerin neden aynı yapısal koşullar altında farklı dış politika stratejileri benimsediklerini açıklamayı hedefler.

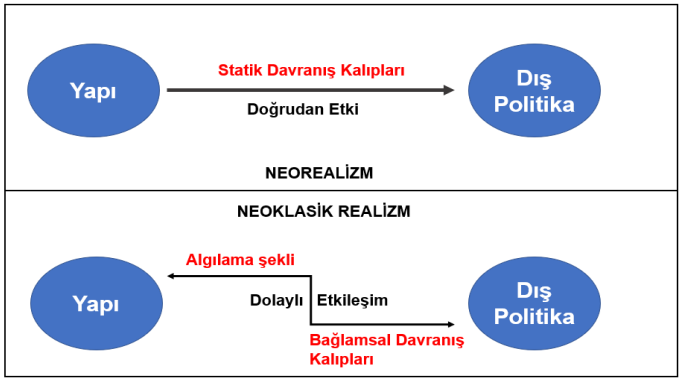
Neoklasik Realizme göre, dış politika karar alma sürecini anlamak için iki temel analitik aşama izlenmelidir. İlk aşamada, devletin uluslararası sistemdeki göreli konumu ve bu konumun yarattığı fırsatlar ile sınırlılıklar analiz edilir. Bu analiz, devletin karşı karşıya olduğu dışsal baskıları ve stratejik 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 (Ripsman vd., 2016).

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 (Johnston, 1995). 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 (Dueck, 2006; Snyder, 1977).

Rose'a göre "ara değişken" işlevi gören kurumlar liderin tehdit algılamasını ve dış politika kararlarını etkileme kapasitesine sahip bürokratik unsurlardır (Rose, 1998). Bürokratik yapıların etkinliği, karar alıcıların yetki alanları ve iç siyasal rekabetin düzeyi gibi unsurlar, uluslararası sistemden gelen baskıların devlete nasıl yansıdığını belirleyen kritik faktörlerdir (Rathbun, 2008). 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 (Schweller, 2004). 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 (Taliaferro, 2006). 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 (Ripsman vd., 2009, s. 147).

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.



Yapı-Dış Politika İlişkisi Bakımından Neorealizm/Neoklasik Realizm Karşılaştırması

3. Araştırma Tasarımı ve Metodoloji

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:

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

Hipotezin testinde yöneltilen her soru, farklı bir değişkeni analiz etmek için tasarlanmıştır. İlk 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.

Yapısal koşulların irdelendiği ilk bölümde ABD'nin güç dağılımındaki yeri ve tehdit algılaması sorgulanmaktadır. ABD'nin içinde bulunduğu uluslararası bağlamın ortaya konulması, güvenlik stratejilerine yön veren çerçevenin belirlenmesi açısından önemlidir. Karşılaştırmalı vaka analizine başvurulan sonraki bölümde, bağımlı değişkende bir farklılaşma olup olmadığını ortaya koymak için öncelikle bu değişkenin aldığı değerler ortaya çıkarılmıştır. Zira uygulanan caydırıcılık stratejileri verili olmayıp siber güvenlik politikalarının caydırıcılık çerçevesinde yorumlanması sonucu ortaya çıkmaktadır. Bu kapsamda; 2009-2021 yılları arasında yayımlanan ulusal güvenlik belgeleri, siber güvenlik belgeleri ve Başkanlık İcra Emirleri gibi siber güvenlik ile ilgili 25 adet birincil kaynak analiz edilmiştir. Analizde belgelerin siber güvenlikle ilgili ağırlık noktası, amaçları ve bu amaçlara hangi araçlar ile erişmeyi planladığı sorgulanmıştır. Ortaya konulan araçlar caydırıcılık stratejisi kapsamında yorumlanmış ve izlenen metot ortaya çıkarılmıştır. Uygulanan caydırıcılık stratejisinin başarılı olup olmadığı çalışmanın kapsamı dışındadır. Bağımlı değişken olan caydırıcılık stratejisi iki ayrı nominal değer ile ölçeklendirilmiştir: İkna/dayanıklılık yoluyla caydırıcılık metodu ve ceza yoluyla caydırıcılık metodu.

İkna yoluyla caydırıcılık metodunda, rakibin amacına ulaşma ve fayda elde etme kabiliyetini fiziksel olarak imkânsız hale getirmek hedeflenir (Snyder,

1959, s. 38). Rakibe verilen mesaj, istenmeyen davranışı uygulaması durumunda vermiş olduğu kararın kendine büyük maliyetler/zararlar doğuracağıdır (Schelling 1966, s. 78-79). Dayanıklılık, maruz kalınan bir saldırı sonrasında iyileşebilme ve mevcut koşullara adapte olarak gelecek muhtemel tehditlerin zararlarından kaçınma becerisidir (Lasconjarias, 2017, s. 2). Amaç saldırının öngörülen etkileri doğurmadığını rakibe göstererek 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 resmi güvenlik belgesi vasıtasıyla rakibe dolaylı olarak iletildiğinden ötürü ikna ve dayanıklılık yoluyla caydırıcılık stratejisi kapsamında değerlendirilmiştir. Öte yandan analiz edilen belgelerde geçen ve rakibe bedel ödetme anlayışına dayanan ofansif tedbirler ise ceza yoluyla caydırıcılık metodu olarak yorumlanmıştır.

Çalışmanın son bölümünde, iki dönemde görülen farklı caydırıcılık metotları ile stratejik kültür ve kurum değişkenleri arasındaki nedensellik bağı incelenmiştir. Burada süreç takibi metoduna başvurulmuştur. Süreç takibi metodu nedensel ilişkilerin açıklanmasını sağlayan etkin bir araçtır (George & Bennett, 2005, s. 268). İncelemeye konu nedensel ilişkiyi tespit etmek için sebepten sonuca giden sürecin açığa çıkarılması gerekmektedir (Collier, 2011, s. 824).

Veri analizi sonucunda, ilgili başkanlık dönemine dair saptanan caydırıcılık metodunu mümkün kılan resmi belgenin bizzat başkanlık makamı tarafından yayımlanması caydırıcılık stratejisi ve başkan arasında eylemsel ilişkiyi ortaya koymaktadır. Bu bulgu, hipotezin geçerliliği için gerekli bir şart olmakla birlikte tek başına caydırıcılık stratejisi üzerindeki stratejik kültür etkenini ispatlamak için yeterli değildir. Zira başkan söz konusu belgeyi kurumlar, muhalefet baskısı veya dış tehdit gibi farklı bağlamsal koşullar etkisinde 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 bağını güçlendirecek bir yeter şarttır. Burada liderin benimsediği stratejik kültür çerçevesi olarak Mead'in dış politika gelenekleri (Mead, 2001) kavramından faydalanılmıştır. Bu geleneklerden Jeffersoncılık Başkan Obama ile, Jacksoncılık ise Trump ile ilişkilendirilmiştir. Müteakiben bu geleneklerin

karakteristik özellikleri bağlamında caydırıcılık stratejilerinde farklılığa yol açan ana belgeler incelenmiştir. Son olarak, bu belgelerde tespit edilen yaklaşımlar ile başkanların diğer ofansif kabiliyet kullanımı içeren dış politika kararları karşılaştırılarak birbirleri ile uyumluluğu incelenmiştir.

Kurum değişkeninin incelendiği son bölümde ABD Kongresinin siber güvenlikle ilgili yasama ve denetim faaliyetleri incelenmiştir. Bu kapsamda yasa tasarılarının onaylanma durumları ve komisyon faaliyetleri doğrultusunda başkanların izledikleri caydırıcılık stratejilerine etkileri ortaya koyulmuştur.

4. ABD'nin Güç Dağılımındaki Yeri ve Siber Politikalara Etkileri

ABD'nin Soğuk Savaş sonrasında elde ettiği mutlak güç üstünlüğünü 2000'li yıllardan itibaren kaybettiği görülmektedir. Singer, Bremer ve Stuckey'nin geliştirdiği Ulusal Kabiliyet Bileşik Endeksi bu göreceli gerilemeyi ortaya koymaktadır. Askeri harcama, nüfus, asker sayısı gibi değişkenler esas alınarak hesaplanan endekse göre 2000 yılında Çin'in ABD karşısındaki güç katsayısı 1.13 iken, bu oran 2010'da 1.42'ye, 2016'da ise 1.73'e yükselmiştir. Bu bulgular; Çin'in küresel güç dengesinde dengeleyici bir rakip olarak öne çıktığını göstermektedir (Singer, 2021).

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	455908000	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

ABD, Çin ve Rusya Ulusal Kabiliyet Bileşik Endeks Puanları (Singer, 2021)

Tehdit algılaması açısından da benzer bir yönelim izlenmektedir. 2002 Ulusal Güvenlik Stratejisi Belgesi'nde Çin, "potansiyel bir ortak" olarak tanımlanırken; 2006'da askeri kapasitesi ve otoriter uygulamaları eleştirilmiş, 2010 ve 2015'te Güney Çin Denizi'ndeki "statükoyu tehdit eden bölgesel aktör" olarak betimlenmiştir. 2017 belgesinde ise ilk kez "revizyonist" bir tehdit olarak nitelendirilmiştir. Rusya ise 2002'de "ortak", 2006'da eleştirel bir bakışla değerlendirilen bir aktör olarak görülmüş; 2015'te "tehdit", 2017'de ise "revizyonist aktör" olarak tanımlanmıştır.

Söz konusu dönüşüm, siber güvenlik alanında da karşılık bulmaktadır. Maness ve Valeriano'nun verilerine göre ABD, 2009-2020 arasında 125 siber saldırıya uğramış olup bunların 49'u Çin, 37'si Rusya kaynaklıdır (Maness vd., 2022). Eurepoc'un Avrupa Siber Olay Deposu verilerine göre ise aynı dönemde ABD'ye yönelik 288 saldırının 62'si Çin, 37'si Rusya tarafından gerçekleştirilmiştir (Eurepoc, 2024). Buna göre; ABD'nin küresel güç dağılımında nispeten gerilediği, Çin'in dengeleyici bir rakip olarak ortaya çıktığı, Rusya ve Çin'in statüko bozucu eylemlerinin arttığı görülmektedir. Söz konusu rekabet ortamının siber uzayda da karşılık bulduğu ve ABD'nin iki devlet tarafından saldırılara maruz kaldığı görülmektedir. Dolayısıyla siber güç kapsamında tespit edilecek ABD ulusal menfaatlerinin ve caydırıcılık stratejisinin rekabet ortamına uygun biçimde şekillenmesi anarşi ortamında beklenen bir davranıştır.

5. Obama ve Trump Başkanlık Dönemlerindeki Siber Güvenlik Düzenlemelerinin Caydırıcılık Stratejisi Açısından Analizi

Bu bölümde çalışmanın ikinci sorusuna cevap aranmaktadır: "Benzer yapısal faktörler altında caydırıcılık stratejileri farklılık gösterebilir mi?" Bu doğrultuda farklı lider dönemlerinde farklı siber caydırıcılık stratejilerinin tespit edilmesi, nedensel ilişkinin varlığının incelenmesi için uygun zemini hazırlayacaktır.

Vaka analizine başvurulan bölümde ABD siber güvenlik politikaları ele alınmıştır. Bunlardan bir caydırıcılık metodu çıkarımı yapmak için siber güvenliği konu alan ulusal güvenlik belgeleri, siber güvenlik belgeleri ve başkanlık icra emirleri gibi birincil kaynaklardan meydana gelen bir veri havuzu oluşturulmuştur. Ağırlık noktası, amaçlar, araçlar ve caydırıcılık metodu başlıkları doğrultusunda elde edilen veri, 2009-2016 yılları arasındaki Barack Obama ve 2017-2021 Donald Trump başkanlık dönemleri olmak üzere boylamsal olarak ikiye ayrılıp karşılaştırılmıştır.

Belge Adı	Yılı	Yayımlayan Kurum	Ağırlık Noktası	Amaçlar	Araçlar	Caydırıcılık Metodu
BARACK OBAMA DÖNEMİ						
Siber Uzay Politika Değerlendirmesi: Güvenilir ve Dayanıklı Bilgi ve İletişim Altyapısının Oluşturulması	2009	Beyaz Saray	Mevcut tehditler, içinde bulunulan durum ve muhtemel hareket tarzlarını ortaya koyan bir durum tespiti	*Siber alandaki stratejik vizyon eksikliğini gidermek * Kamu ve özel sektörün iş birliğine dayalı, belirli standartları bulunan bir güvenlik ekosistemi yaratılması	* Beyaz Saray Siber Güvenlik Koordinatörlüğü makamının teşkili * Bu yetkilinin kurumlar arası eş güdümden ve belirlenen stratejilerin doğru bir şekilde uygulanmasından sorumlu olması * Koordinatör tarafından özel sektörde siber tehlikelere dair durumsal farkındalık artırıcı temaslarda bulunulması	İkna ve Dayanıklılık
Ulusal Güvenlik Stratejisi	2010	Beyaz Saray	Ulusal ve uluslararası düzeyde iş birliği	Bilişim tabanlı stratejik altyapı tesislerinin korunması için güvenli ve dayanıklı ağların oluşturulması.	Savunma yöntemleri geliştirici ARGE yatırımlarının artırılması. Durumsal farkındalık ve dijital okuryazarlık geliştirici idari adımlar	İkna ve Dayanıklılık
Siber Uzayda Harekât Strateji Belgesi	2011	Savunma Bakanlığı	Siber tehditlerin dört boyutunda angajman: 1. Dış tehditler 2. İçTehditler 3. Tedarik zinciri hassasiyetleri 4. Bakanlığın operasyonel kabiliyetlerine yönelik tehditler	Siber uzayın kendine özgü hassasiyetlerine uygun (gizlilik, kişisel özgürlük hakları vb.) operasyonel kabiliyete erişmek	* Siber uzayı ayrı bir harekât alanı olarak tanımlamak * Yeni Ağ İşletim Konseptleri * Kamu-Özel sektör iş birliğini esas alan bir güvenlik stratejisi * ABD müttefikleri ile yardımlaşma, kolektif güvenlik * Siber iş gücü kapasite artırımı	İkna ve Dayanıklılık
Siber Uzay Politika Raporu	2011	Savunma Bakanlığı	Farklı nitelikteki tehditlere göre şekillenen kapsamlı caydırıcılık anlayışının uygulanış biçimi ayrıntılarını sunmaktadır	* Uluslararası aktörler ile ofansif siber kuvvet kullanım normları oluşturmak * Kritik altyapı güvenliğini artırmak * Kamufle olan saldırganları belirleyip cezalandırmak	Sadırgan aktörlerin tespitinde Ulusal Güvenlik Ajansı, Kritik Altyapıların korunmasında diğer kamu kuruluşları ve normların tesisinde diğer devletler ile iş birliği	İkna ve Dayanıklılık Ceza
Siber Uzay Uluslararası Stratejisi	2011	Beyaz Saray	Siber tehditlerin uluslararası toplumu bir bütün olarak tehdit etmesi ve buna karşı kolektif çabanın gerekliliği	Siber uzayda istikrar ve güvenliğin sağlanması	Temel hak ve özgürlüklerin korunması, meşru müdafaa hakkı gibi normların siber uzaya adapte edilmesi doğrultusunda diyalog platformları oluşturulması. ABD'nin bu alanda öncülük etmesi	Normlar
Siber Uzayda Güvenilir Kimlikler için Ulusal Strateji	2011	Beyaz Saray	Bireysel kullanıcı seviyesinde internet güvenliği	Kişisel veri ve kimlik hırsızlığına karşı emniyetli bir internet ekosisteminin kurulması	* Birlikte çalışabilirlik standartları, risk modellerini ve mahremiyet haklarını ortaya koyan Kullanıcı Ekosistemi Çerçevesi Belgesi *Çerçeve metninde kamu ve özel sektör paydaşlarına verilen sorumlulukların takibi ile görevli akreditasyon komitesi	İkna ve Dayanıklılık
Başkanlık Siyaset Direktifi-20	2012	Beyaz Saray	Siber etki operasyonlarının tanımı, etkileri ve sınırlandırma yolları	Ofansif siber operasyonların sonuçlarının bütün devletleri etkileyeceği, bu nedenle bu operasyonların kullanım ve etkilerinin azaltılması	* Egemenlik hakkı normuna uyum * Siber harekât için çok paydaşlı planlama ve başkana ait nihai karar yetkisi * Siber etki yerine diplomatik ve ekonomik yaptırımlar	Ceza (Ofansif kabiliyetler sınırlandırılmıştır. Alan dışı yaptırımlar ve norm inşasına öncelik verilmiştir)
Savunma Bilimi Kurulu Raporu: Dayanıklı Askeri Sistemler ve Gelişmiş Siber Tehdit	2013	Savunma Bakanlığı	Siber tehditlerin teknik niteliği, askeri faaliyetlere yönelttiği tehditler ve çözüm için önerilen yaklaşımlar	Siber uzayın saldırgan aktörlere sunduğu avantajlar doğrultusunda reaktif tedbirlerin yerine proaktif bir savunma ve caydırıcılık iş birliği	* Konvansiyonel ve nükleer yaptırım seçeneklerinin incelenmesi * İstihbarat temin ve analiz kabiliyetlerini geliştirme * Ofansif siber kabiliyetleri geliştirmek	Ceza
İcra Emri-13636	2013	Beyaz Saray	Kritik altyapı güvenliği	Kritik Altyapı Tesislerini siber saldırılara karşı güvenli ve dayanıklı hale getirmek	* 16 adet kritik altyapı sektörünün tanımlanması ve her birine sorumlu bir bakanlık atanması * Kritik Altyapı güvenliğinde takip edilecek adımları belirleyen Siber Güvenlik Çerçevesi Belgesi	İkna ve Dayanıklılık
İcra Emri-13687	2015	Beyaz Saray	Sony Yapım Şirketi'ne yönelik siber saldırıları gerçekleştiren Kuzey Kore'ye uygulanacak yaptırımlar	İlk kez bir devleti hedef göstererek yaptırımları ortaya koymak; gelecekteki muhtemel benzer girişimleri caydırmak	Kuzey Kore hükümet yetkililerinin ve parti bağlantılı kurumların ABD'deki mal varlıklarına Hazine Bakanlığınca bloke konulması	Ceza (Alan Dışı)
Ulusal Güvenlik Stratejisi	2015	Beyaz Saray	Siber uzay, "ortak alanlara erişim" başlığı altında ele alınmaktadır. Siber saldırıların tüm devletleri etkileyen yapısı ve ABD menfaatlerine yansımaları	Açık, güvenli ve erişilebilir bir internet ortamının muhafazasının sağlanması, kritik altyapılarının korunması	* Diğer devletlerle diyalog; ortak davranış biçimlerinin belirlenmesi * Siber Güvenlik Çerçeve Belgesinin uygulanması * Saldırgan kişilere yönelik adli süreçler	* Normlar * İkna ve Dayanıklılık * Ceza (Alan dışı)
İcra Emri-13691	2015	Beyaz Saray	Kamu-özel sektör iş birliği	Siber Tehditlere karşı tüm paydaşların koordinasyon ve iş birliği içerisinde olduğu bir anlayışı hakim kılmak	* Koordinasyonun İç Güvenlik Bakanlığınca sağlanması * Bilgi paylaşımı ve analizi kurumlarının oluşturulması * Özel sektörün iş birliğinde gönüllülük ve mahremiyet esası	* İkna ve Dayanıklılık
İcra Emri- 13694	2015	Beyaz Saray	Kötü amaçlı siber faaliyetlerle ilgili şahısların mal varlıklarının bloke edilmesi	ABD ulusal güvenliğine ve ekonomik istikrarına zarar veren siber eylemlere girişen şahıs ve kurumların Hazine Bakanlığınca cezalandırılması	ABD vatandaşı olmayan ve ikamet etmeyen kişilere yönelik yasal boşluğu doldurmak için suç teşkil eden eylemler belirlenmiştir	Ceza (Alan Dışı)
Siber Strateji Belgesi	2015	Savunma Bakanlığı	Siber uzaydaki tehditlere yönelik Savunma Bakanlığı faaliyetleri yol haritası	ABD menfaatlerine yönelen siber tehditlere karşı gerekli kuvvet kapasitesini oluşturmak; çatışma ortamını şekillendirmek ve Bakanlık ağlarını korumak	* Tehditlerin gerekirse gerçekleşmeden imhası * İstihbarat birimleri ile yoğun iş birliği * Kuvvet komutanlıklarının siber kabiliyetlerinin birleştirilmesi	Ceza İkna ve Dayanıklılık
İcra Emri- 13718	2016	Beyaz Saray	Siber Güvenliği Geliştirme Komisyonu	* Siber güvenlik tedbirlerini artırıcı uzman görüşlerine başvurmak * Toplumun bütün paydaşlarında siber güvenliğe ilişkin durumsal farkındalığı geliştirmek	Yönetim hizmetleri, kritik altyapı güvenliği, siber kabiliyet AR-GE faaliyetleri, siber iş gücünün inşası, kimlik tanımlama ve durumsal farkındalık konularında uzmanları içeren komisyonun sene sonunda başkana bir rapor sunması	İkna ve Dayanıklılık
Başkanlık Siyaset Direktifi-41	2016	Beyaz Saray	Maruz kalınan siber etkilere verilecek tepkiler	Tehdit-odaklı reaksiyon, birim-odaklı reaksiyon ve istihbarat paylaşımı olmak üzere üç farklı boyutta kurumlar arası eş güdümün sağlanması	* Birleşik Siber Koordinasyon Grubunun teşkili * Adalet Bakanlığı, İç Güvenlik Bakanlığı ve İstihbarat Başkanlığı'na verilen yaptırım yetkileri	İkna ve Dayanıklılık Ceza (Alan dışı)

Belge Adı	Yılı	Yayımlayan Kurum	Ağırlık Noktası	Amaçlar	Araçlar	Caydırıcılık Metodu
DONALD TRUMP DÖNEMİ						
İcra Emri- 13800	2017	Beyaz Saray	Kritik altyapıların korunmasında federal kurumların etkinliği	Kritik altyapıların güvenlik tedbirlerinin artırılmasında kamu kurumlarını daha aktif hale getirmek, takip ve kontrol mekanizmasını geliştirmek	* Milli Siber Güvenlik Çerçeve belgesinin kamu kurumları tarafından uygulanmasının zorunlu hale getirilmesi * Belirlenen kurum yöneticilerinin siber güvenlik risk yönetiminde başkana karşı doğrudan sorumlu ve hesap verir hale getirilmesi	İkna ve Dayanıklılık
Ulusal Güvenlik Stratejisi	2017	Beyaz Saray	Caydırıcılığa ilişkin yeni yönetimin temel yaklaşımları	Siber uzayın ortaya koyduğu hassasiyetlere tedbir almak için reaktif durumdan proaktif yaklaşıma geçmek. Tehditler kadar fırsatların da farkına varmak.	* Risk yönetiminin caydırıcılığın temeline oturtulması; sektörel tehdit önceliklendirmeleri * Saldırgan davranışlara ani ve etkin karşılık verilmesi * Bilgi teknolojileri aygıtlarının modernize edilmesi * Özel sektör ile kapsamlı iş birliği	İkna ve Dayanıklılık Ceza
Ulusal Güvenlik Başkanlık Memorandumu-13	2018	Beyaz Saray	Ofansif siber operasyonların yetkilendirme durumu	Siber Komutanlığın elinde bulundurduğu ofansif kabiliyetleri etkin bir şekilde kullanmak	Obama döneminde siber harekât için düzenlenen çok paydaşlı karar alma ve başkan onayı mekanizması iptal edilerek yetki Siber Komutanlığa devredilmiştir.	Ceza
Siber Strateji Belgesi	2018	Savunma Bakanlığı	Savunma Bakanlığının siber güvenliğin sağlanması ile ilgili ana fikir ve yaklaşımlarının ortaya koyulması	İlerde savunma ve sürekli angajmana dayalı aktif bir siber caydırıcılık anlayışının hakim kılınması	* AR-GE ile desteklenen daha öldürücü bir Siber kuvvet inşası * Siber tehditlere karşı siber ve askeri kabiliyetlerin ortak bir misilleme aracı olarak kullanımı * Siber kuvveti oluşturan insan kapasitesinin doğru seçimi ve doğru şekilde eğitilmesi * Yalnızca kendi açıklarını düzeltme anlayışının ötesinde siber uzayda sürekli keşif ve muhtemel tehditlerin yerinde yok edilmesi	Ceza
Ulusal Siber Strateji	2018	Beyaz Saray	Rusya, Çin, Kuzey Kore ve İran'ın doğrudan hedef gösterilmesi; bu aktörlerin siber uzayda egemenlik şemsiyesi altında gerçekleştirdiği saldırgan davranışlara karşı yenilikçi bir güvenlik anlayışının gerekliliği	* Amerikan halkı, Amerikan yaşam tarzı ve refahının korunması * Saldırgan davranışların kuvvet yoluyla önlenmesi * Siber uzayda ABD etkinliğinin geliştirilmesi	* Misillemelerin hızlı ve şeffaf olması, diğer aktörlere net mesajlar vermesi * Kritik altyapıların korunmasında İç Güvenlik Bakanlığına kurumlar arası koordinasyon sağlayan ve reaksiyon sürelerini kısaltan yetkilerin tanınması * Teknolojik altyapının tedariğinde özel sektör merkezli planlama ve bürokratik engellerin ortadan kaldırılması * Uluslararası siber güvenlik standart ve normlarının inşası ve tehditlere karşı müttefiklerle kolektif yaptırım için sürekli diyalog zeminlerinin işletilmesi	İkna ve Dayanıklılık Ceza
İcra Emri - 13870	2019	Beyaz Saray	Siber güvenlik iş gücünün istihdamı, eğitimi ve değerlendirilmesi	Siber güvenlik iş gücünün güvenlik gereksinimlerini karşılayacak nitelikte teşkil edilmesi, bu süreçte etkin eğitim süreçleri ve kariyer olanaklarının ortaya koyulması	* İç Güvenlik Bakanlığının siber iş gücünün temini, eğitim müfredatının belirlenmesi ve uygulanması konularında yetkilendirilmesi * İş gücü verimliliği konusunda kurum liderlerinin sorumluluğunun artırılması	İkna ve Dayanıklılık
İcra Emri - 13873	2019	Beyaz Saray	Bilgi-İletişim teknolojileri ile tedarik zinciri emniyeti	Bilgi teknolojilerine erişimi olan kurum ve şahısların erişikleri hassas bilgileri yabancı devletler ile paylaşmasının önüne geçilmesi	* Hasım bir devlete ait ve kritik altyapılara zarar verme potansiyeli olan yazılım, donanım ve hizmetlere dair işlemlerin yasaklanması * İç Güvenlik Bakanlığına bağlı Kritik Altyapı Güvenlik Ajansı tarafından 80 gün içinde istismar edilebilecek hassasiyetleri içeren bir rapor hazırlanması	İkna ve Dayanıklılık
İcra Emri - 13942 ve 13943	2020	Beyaz Saray	TikTok ve Wechat uygulamalarının kullanımı	Çin tarafından gerçekleştirilen siber casusluk ve veri hırsızlığını engellemek	* ABD vatandaşları, kurum ve şirketlerinin; uygulama sahipleri ByteDance ve Tencent Şirketleri ile herhangi bir ticari ilişki içine girmesi yasaklanmıştır. * Uygulamaların reklam alması ve AppStore'da yer alması engellenmiştir.	İkna ve Dayanıklılık
İcra Emri - 13984	2021	Beyaz Saray	Bulut bilişim hizmeti hassasiyetleri	Bulut hizmeti üzerinden veri hırsızlığını önlemek	Bulut bilişim hizmet modelinde servis sağlayan şirketlerin müşterilerine ait kullanıcı hesaplarının incelenerek yabancı kullanıcı profillerinin Ticaret Bakanlığı ile paylaşılması zorunluluğu getirilmesi	İkna ve Dayanıklılık

Obama ve Trump Dönemi Siber Güvenlik Belgelerinin Caydırıcılık Metodu Kapsamında Analizi

Obama ve Trump dönemlerine ait güvenlik belgeleri (EK) incelendiğinde, caydırıcılık stratejisinin hem ikna hem de ceza yoluyla uygulandığı görülmektedir. Özellikle savunma tedbirlerine dayanan ikna yoluyla caydırıcılık yöntemine dair her iki başkan döneminde önemli adımlar atıldığı dikkat

çekmektedir. Bu kapsamda, her iki başkanın siber güvenliğe ilişkin yayımladığı ilk icra emirleri olan 13636 ve 13800 numaralı belgeler, kritik altyapı tesislerinin siber saldırılara karşı korunmasını önceleyen düzenlemelerdir. Bu emirlerin doğrudan başkan inisiyatifi ile yayımlanması, konunun ulusal güvenlik açısından taşıdığı önemin göstergesidir.

Obama döneminde yayımlanan icra emirleri, kritik altyapıların tanımlanması, sorumluluk dağılımı, uzmanlardan oluşan komisyonlar aracılığıyla savunma tedbirlerinin belirlenmesi ve özel sektörle bilgi paylaşımını teşvik eden uygulamaları içermektedir. Trump döneminde yayımlanan belgeler ise federal kurumların etkinliğini artırmaya, yöneticilerin sorumluluklarını belirginleştirmeye ve teknik kabiliyetleri geliştirmeye odaklanmıştır. Bu farklılıklara rağmen her iki dönemde de savunmaya yönelik ortak bir iradenin olduğu anlaşılmaktadır. Özellikle bu düzenlemelerin resmî belgeler aracılığıyla kamuoyuna sunulması, caydırıcılığın mesaj bileşenine katkı sağlamakta ve potansiyel saldırgan aktörlerin risk algısını artırmaktadır.

Siber caydırıcılığın tesis edilmesi kapsamında Çin gibi devletleri doğrudan hedef alan yaptırımların yanında bütün devletleri kapsayıcı kuralların oluşturulması dikkate alınması gereken bir konudur. Zira siber uzay coğrafi sınırlar ile kısıtlanmayan ve aktörlerin birbirleriyle sürekli angajman halinde olduğu bir alandır. Bu alanda meydana gelen etkiler uluslararası toplumun tamamında yansımalar bulabilmektedir. Bu tehdide işaret eden Joseph Nye ve Tim Stevens gibi araştırmacılar normların bir caydırıcılık aracı olarak kullanılabileceğini ve devletlerin siber güvenliğe ilişkin birlikte çalışması gerektiğini savunmaktadır (Nye, 2017; Stevens, 2012). Söz konusu kolektif çabalara dair iki başkan döneminde önemli gelişmeler görülmektedir. Bu bağlamda, Birleşmiş Milletler Hükümet Uzmanları Grubu (UNGGE) oluşumu önemlidir. UNGGE devletlerin siber uzaydaki davranışlarını düzenlemeye yönelik diyalog zemini tesis eden ve devletleri temsilen konu uzmanlarının oluşturduğu bir platformdur. ABD'nin Obama ve Trump yönetimleri dönemlerinde UNGGE sürecine yaklaşımları, norm geliştirme çabalarının doğası ve kapsamı açısından farklılıklar göstermektedir.

Obama yönetimi, uluslararası hukukun siber alana uygulanmasını savunan çok taraflı bir norm oluşturma stratejisi benimsemiştir. 2011 tarihli "Uluslararası Siber Uzay Stratejisi", açık, güvenli ve uluslararası hukukla uyumlu bir dijital ortamı teşvik etmeyi amaçlamıştır (Beyaz Saray, 2011). Bu yaklaşım doğrultusunda; 2013 UNGGE raporunda devletler, uluslararası hukukun siber faaliyetlere de uygulanabilir olduğunu kabul etmiş; 2015 raporunda ise barış zamanında kritik altyapıya saldırmama gibi gönüllü normlar belirlenmiştir (Birleşmiş Milletler 2013, 2015).

Trump yönetimi ise siber uzayda egemenlik ve ulusal çıkarları önceleyen daha tek taraflı bir yaklaşım benimsemiştir. 2018 tarihli Ulusal Siber Strateji, ABD'nin çıkarlarını korumak için bağımsız hareket etme ilkesini vurgulamıştır (Beyaz Saray, 2018). Bu dönemde, ABD'nin UNGGE içindeki uzlaşıya dayalı norm geliştirme çabalarına bağlılığı azalmış; uluslararası hukukun siber uzaya uygulanması konusundaki geniş yorumlara direnç gösterilmiştir (Maurer, 2018). 2017–2018 UNGGE oturumunun başarısızlıkla sonuçlanması, bu yaklaşım değişiminin bir yansıması olarak değerlendirilebilir. Diğer taraftan Savunma Bakanlığı Siber Strateji Belgesi ile benimsenen "sürekli angajman" ve "ileriden savunma" stratejileri, aktif siber operasyonların meşrulaştırılması yönünde normatif bir kaymaya işaret etmiştir (Savunma Bakanlığı, 2018)

Norm inşası yaklaşımının saldırgan tespiti (attribution) sorununda da etkiler doğurduğu görülmektedir. Birçok araştırmacı siber uzaydaki saldırganların botnet ve zararlı yazılımlarla kimliğini gizlediğini ve saldırganın tespit edilememesinden dolayı etkili bir caydırıcılık tesis edilemeyeceğini savunmaktadır (Wilner, 2019, s. 253). Diğer taraftan David Blagden ve Jon Lindsay saldırgan tespiti konusunun gereğinden fazla üzerinde durulduğunu, ciddi derecede zarar veren bir siber saldırı sonrasında saldırganın bu çaptaki bir eylemi gerçekleştirebilecek sınırlı sayıdaki aktörlerden biri olacağını ve aynı zamanda saldırıdan menfaat sağlama durumunun saldırgan tespiti için ilave bir kolaylaştırıcı etken olduğunu ifade etmektedir (Lindsay, 2015; Blagden, 2020). Diğer taraftan Emilio Iasiello Çin'in siber yollarla saldırı, veri hırsızlığı ve espiyonaj faaliyetlerinin bilinmesine rağmen caydırıcı bir tedbir alınmadığına işaret ederek asıl sorunun saldırgan tespiti olmadığını savunmaktadır (Iasiello, 2014). Konuya ilişkin başkanların farklı politikaları göze çarpmaktadır. Bu kapsamda Obama yönetimi 2013 yılında artan Çin siber saldırıları sonrası Çin'i, 2014 yılında Sony Yapım Şirketi'ni hedef alan siber saldırılar sonrası Kuzey Kore'yi doğrudan kamuoyu önünde işaret etmemesi saldırgan tespiti konusundaki ılımlı ve yatıştırıcı tavrını ortaya koymaktadır (Sanger, 2018, s. 117; Waters, 2014). Buna karşın benzer siber saldırılar sonrası Trump yönetimin Kuzey Kore ve Rusya'yı kamuoyu önünde suçlaması dikkat çekicidir (Geller, 2017; Sheth, 2018).

Ceza yoluyla caydırıcılık açısından bir değerlendirme yapmak için ceza mekanizmasını gerçekleştirecek ofansif kabiliyetlere yaklaşımı irdelemek gerekir. Siber uzayda saldırgan aktörlere karşı cezai uygulama tehdidi oluşturabilecek unsur ofansif siber kabiliyetlerdir. Bu kabiliyetlere ilişkin kapasite artırıcı adımlar dikkat çekicidir. Siber Komutanlık bünyesinde yetiştirilen 6200 personelli 133 Siber Misyon Timinin muharebeye hazır halde teşkili, ofansif siber kabiliyetlerin bir ceza aracı olarak kullanılmasına ilişkin ciddiyeti göstermektedir (Sanger, 2018).

Siber Komutanlığın eriştiği bu kabiliyetler caydırıcılık açısından incelendiğinde, kabiliyet ve mesaj bileşenleri açısından belirgin niteliktedir. Bununla birlikte inandırıcılık bileşeni açısından iki başkan döneminde farklılıklar mevcuttur. Söz konusu fark Siber Komutanlığın ofansif harekâtta kullanım kararlılığından kaynaklanmaktadır. Bu farkı anlamak için Obama'nın 20'nci Başkanlık Siyaset Direktifi (PPD-20) ve Trump'ın 13'üncü Ulusal Güvenlik Başkanlık Memorandumu (NSPM-13) belgelerinin incelenmesi gerekmektedir.

2012 yılında yayımlanan PPD-20, defansif ve ofansif siber etki operasyonlarını tanımlayarak başlamakta ve siber ofansif harekâtın yetkilendirme durumunu ele almaktadır (National Security Archive, 2012). Belgenin tehdit algılaması siber uzayın küreselliği üzerinedir. Belgede ofansif siber harekâtın gizlilikle yapılması durumunda bile hedeflenen coğrafyanın ötesinde etkiler yaratabileceği ve bu durumun ABD menfaatlerini zedeleyeceği savunulmaktadır (Beyaz Saray, 2012). Söz konusu menfaatlerin ABD Kritik Altyapı Tesisleri güvenliği olduğu anlaşılmaktadır. Direktifin zamanı ve kapsamı Stuxnet saldırısı sonrası Kritik Altyapı Tesislerini hedef alacak tehditlere karşı hassasiyeti göstermektedir. Zira 2009 yılında ortaya çıkan Stuxnet saldırısı ofansif siber harekâtın etkilerinin erişebileceği boyutlar açısından önemlidir. ABD ve İsrail ortak kabiliyetleri ile yürütüldüğü iddia edilen Stuxnet saldırısı İran'ın Natanz nükleer zenginleştirme tesisini hedef almıştır. Stuxnet, siber tehditlerin somut fiziksel alanlarda tahribatlar yaratabilme kabiliyetini göstermesi bakımından önemlidir (Lilli, 2020, s. 277). Natanz Nükleer tesisinin Merkezi Denetleme Kontrol sistemine sızdırılan zararlı yazılım, uranyum zenginleştirme işleminde kullanılan santrifüjlerin yer değiştirmesini sağlayarak İran nükleer programını sekteye uğratmıştır.

PPD-20, ABD menfaatlerini hedef alacak benzer tehditlere karşı uluslararası topluma sunulan bir iyi niyet adımı olarak nitelendirilebilir. Zira bu belge ile Obama yönetimi ofansif siber harekâtın uygulama prosedürlerini ciddi anlamda sıkılaştırmıştır. Belgede ofansif bir operasyon için askeri istihbaratın yeterlilik kriteri aranmakta ve siber operasyonlara dair askeri yeteneklerin kullanımı sivil iradenin onayına tabi kılınmaktadır (Healey, 2019, s. 3). Ofansif harekât onaylama yetkisi Siber Komutanlıktan alınarak içerisinde farklı bakanlık ve kurumların bulunduğu çok paydaşlı bir mekanizmaya verilmiştir. Bu mekanizmadan geçen harekât tasarısı, nihai onay için Başkana sunulmaktadır. Görüldüğü üzere; PPD-20, ofansif siber harekâtın icrası öncesinde bürokratik işleyişi bir zorunluluk haline getirerek bir kendini sınırlandırma işlevi görmüştür.

2018 yılında Trump Başkanlık döneminde yayımlanan NSPM-13 belgesi, PPD-20'nin bürokratik sınırlandırmalarını tersine çevirir niteliktedir. Obama uygulamalarını "hantal" ve "fazla bürokratik" bulan Trump, imzalamış olduğu

memorandum ile 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 (Department of Defense, 2020; Smalley, 2022; Washington Post, 2018). Söz konusu karar sonrası Siber Komutanlık ofansif siber harekât konusunda çok daha aktif bir duruma gelmiştir. Memorandumun yürürlüğe girmesi ile Trump dönemi ilk iki senesinde yapılan siber harekât sayısı Obama'nın toplam sekiz yıllık döneminde gerçekleştirilen saldırı sayısını aşmıştır (Dilanian, 2019). ABD Siber Komutanı ve Ulusal Güvenlik Ajansı Direktörü General Paul Nakasone, NSPM-13 sonrası dönemde ofansif siber kabiliyetlerin etkin şekilde kullanıldığını ve önceki dönemde benimsenen saldırılara karşı pasif tutumun terk edildiğini vurgulamaktadır (Dilanian, 2019).

Ceza bileşeninin kullanımına ilişkin yaklaşımların kabiliyet geliştirme açısından da farklılık gösterdiği ifade edilebilir. Bunun en göze çarpan örneği Siber Komutanlık gelişimidir. 2009 yılında ayrı bir komutanlık olarak kurulan ABD Siber Komutanlığı, Ulusal Güvenlik Ajansı (NSA) ile birlikte Fort Meade yerleşkesinde konuşlandırılmıştır. Bu dönemde, mevcut yeteneklerin etkin kullanımını sağlamak amacıyla, Siber Komutanlık ve NSA çift başlı bir yapıda, aynı direktör tarafından komuta edilmiştir. Emir-komuta zincirinde ise Siber Komutanlık, ABD Stratejik Komutanlığı'na bağlanmıştır. Stratejik Komutanlık esasen nükleer caydırıcılıktan sorumlu olmakla birlikte, bu kurumsal yerleşim, Obama yönetiminin siber tehditleri caydırıcılık doktrini bağlamında değerlendirdiğini göstermektedir. Ayrıca Siber Komutanlık ile NSA arasındaki kurumsal sınırların net olarak ayrıştırılmaması, Obama döneminin çok katmanlı denetim ve sivil bürokratik kontrol ilkeleriyle uyumludur.

Başkan Trump, Ağustos 2017'de yayımladığı başkanlık memorandumu ile Siber Komutanlığı bağımsız bir Birleşik Muharip Komutanlık statüsüne yükseltmiştir (Gibbons-Neff & Nakashima, 2017). Bu adım, ABD yönetiminin siber alanı bağımsız bir operasyonel ortam olarak tanıdığının açık bir göstergesidir. Günümüzde ABD Savunma Bakanlığı'na bağlı 11 Birleşik Muharip Komutanlık bulunmakta olup, her biri kendi coğrafi ya da fonksiyonel alanında doğrudan operasyonel faaliyet yürütmektedir.

Trump yönetimi bu yapısal değişikliğin üç temel amaca hizmet edeceğini belirtmiştir:

1. Müttefiklere güven vererek ve rakipleri caydırarak ABD'nin siber tehditlere karşı kararlılığını göstermek,
2. Operasyonel karar alma ve uygulamada çevikliği artırmak,
3. Siber operasyonlar için daha fazla kaynak aktarımını kolaylaştırmak.

Bu reform, ABD'nin siber alanı yalnızca destekleyici bir yetenek değil bağımsız bir muharebe sahası olarak konumlandırma stratejisinin önemli bir parçasıdır.

İki başkanlık dönemine ilişkin siber güvenlik politikaları caydırıcılık metodu açısından incelendiğinde en somut farklılığın ceza yoluyla caydırıcılık metodunda oluştuğu görülmektedir. Bu doğrultuda çalışmanın bağımlı değişkeni ceza yoluyla caydırıcılık, değişkenin aldığı nominal değerler ise cezai yaptırıma ilişkin "aktif" ve "pasif" yaklaşımlardır. Her iki başkan döneminde ABD ofansif siber kabiliyetleri etkin bir düzeye ulaşmış olmasına rağmen bu kabiliyetlerin bir "cezai" yaptırım olarak kullanılması noktasında Obama döneminde temkinli ve sınırlı davranıldığı, Trump döneminde ise yaptırımların fiili kullanımı için alan açıldığı görülmektedir. Bu doğrultuda, Trump döneminde ceza yoluyla caydırıcılık metodu bakımından çok daha etkin bir caydırıcılık stratejisinin benimsendiği ifade edilebilir.

Sonraki bölümde iki başkanlık dönemi arasındaki tespit edilen farklılığın nedenleri stratejik kültür başlığı altında incelenmiştir. Bu noktada siber güvenlik kültürünün söz konusu dönemlerde nasıl şekillendiğini kısaca hatırlatmak faydalı olacaktır. Obama yönetimi henüz ilk senesinde yayımlamış olduğu Siber Güvenlik Politika Değerlendirmesi Belgesi ile siber güvenliği ulusal güvenliğin temel bir unsuru olarak konumlandırmıştır. Kritik altyapı güvenliğinin sağlanması için özel sektörle bilgi paylaşımını teşvik etmiştir. 13636 sayılı İcra Emri ile kritik altyapıların korunması tedbirlerini standart hale getiren Siber Güvenlik Çerçevesini (Cyber Security Framework) oluşturmuştur. Bu doğrultuda Obama döneminde siber tehditlerin ciddiyetle ele alındığı, caydırıcılığın tesisinde özel sektör hassasiyetlerinin gözetildiği, çok paydaşlı bir diyalog zeminin yaratıldığı ve tedbirlerin standardize edildiği bir siber güvenlik kültürünün oluştuğundan söz edilebilir. Trump döneminde ise Ticaret ve İç Güvenlik Bakanlıkları tarafından ortaklaşa yayımlanan "Botnet ve Diğer Otomatik Dağıtık Tehditlere Karşı İnternet ve İletişim Ekosisteminin Dayanıklılığını Artırmak" konulu rapor, özel sektör ve akademinin rehberliğinde toplumun tamamında farkındalık yaratan teknik ve idari düzenlemeleri içermektedir. Öte yandan Trump döneminde daha çok devlet düzeyinde müdahalelerin ön plana çıktığı, "ileriden savunma" ve "sürekli angajman" prensipleri gereği daha agresif tedbirlerin benimsendiği, kritik altyapı savunmasında önceliğin savunmadan çok misillemeye kaydığı bir siber güvenlik kültürünün ortaya çıktığı görülmektedir.

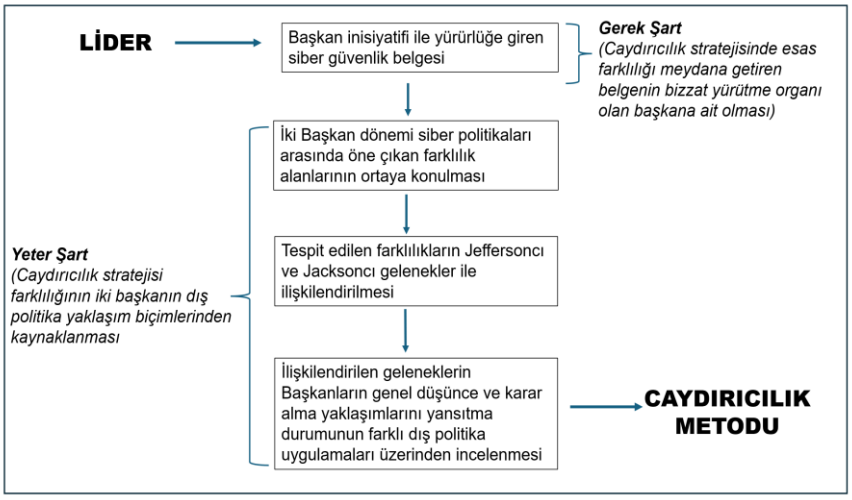
6. Caydırıcılık Stratejisinde Stratejik Kültür Etkisi

Bu bölümde, çalışmanın üçüncü araştırma sorusu olan "Caydırıcılık stratejisindeki farklılaşmada stratejik kültür etkisi nedir?" sorusuna yanıt aranmaktadır. İki başkanlık döneminde ceza yoluyla caydırıcılık stratejilerinin farklılık göstermesi, başkan ve caydırıcılık stratejisi arasındaki ilişkiyi incelemeye değer kılmaktadır. Bu bağlamda, stratejik kültürün etkisini ortaya koymak amacıyla süreç takibi yöntemi kullanılmıştır. Süreç takibinde gerek ve yeter şartların karşılanması, nedensel ilişkiyi destekleyici niteliktedir (Collier, 2011; Mahoney, 2012, s. 573).

Bu analizde gerek şart, caydırıcılıktaki değişimin doğrudan başkan inisiyatifiyle gerçekleşmesidir. Çünkü Kongre etkisinin analize dahil edilmesi, liderin stratejik kültürünün etkisini izole etmeyi güçleştirecektir. Önceki bölümde ifade edildiği gibi, Obama tarafından yürürlüğe konan PPD-20 ve Trump tarafından yayımlanan NSPM-13, başkanın tek taraflı yetkisiyle hayata geçirilmiş olup stratejideki değişimin lider inisiyatifiyle gerçekleştiğini göstermektedir. Bu nedenle, hipotezin testinde gerek şart karşılanmaktadır.

Yeter şart olarak ise liderin benimsediği stratejik kültürün, belirlenen caydırıcılık stratejileriyle örtüşme düzeyi değerlendirilmiştir. Bu kapsamda, Walter Russell Mead'in (2001) ortaya koyduğu dört dış politika geleneği – Wilsoncılık, Hamiltoncılık, Jeffersoncılık ve Jacksoncılık – temel alınmıştır. Bu gelenekler, liderlerin dış politika tercihlerini analiz etmek için son dönem literatürde sıkça başvurulan bir çerçeve sunmaktadır (Bentley ve Holland, 2016; Clarke ve Ricketts, 2017a, 2017b; Dimitrova, 2018; Mead, 2017; Rolf, 2021).

Bu bağlamda, PPD-20 belgesi Jeffersoncı; NSPM-13 belgesi ise Jacksoncı gelenek doğrultusunda değerlendirilmiştir. PPD-20, ofansif siber operasyonları çok paydaşlı ve bürokratik onay süreçlerine bağlayarak, iş birliğine açık ve çatışmadan kaçınan bir yaklaşımı temsil etmektedir. Buna karşılık, NSPM-13, angajman yetkisini doğrudan Siber Komutanlığa devrederek bürokratik süreci azaltmış, daha merkezi ve çatışmacı bir yaklaşımı benimsemiştir. Bu belgeler arasında özellikle "bürokrasi ve iş birliği" ile "çatışmaya yaklaşım" kriterleri açısından belirgin farklar gözlenmektedir.



Stratejik Kültür - Caydırıcılık Metodu İlişkisinin Nedensellik Analizinde Süreç Takibi Aşamaları

Son olarak, stratejik kültür ile caydırıcılık metodu arasındaki bağın güçlendirilmesi amacıyla başkanların diğer ofansif kapasite kullanımı örnekleri – Suriye'ye yönelik hava taarruzu kararları ve Silahlı İnsansız Hava Aracı (SİHA) operasyonları – analiz 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.

6.1. Bürokrasi ve İş Birliğine Bakış Açıları:

ABD'nin kuruluş yıllarında federal sisteme ilişkin tartışmalarda güçlü bir merkezi sistemin varlığına karşı duran Jeffersoncı geleneğe göre güç ve otoritenin tek bir merkezde toplanması hak ve özgürlükler açısından sakıncalar barındırmaktadır (Clarke & Ricketts, 2017b, s. 499). Dolayısıyla bu gelenekte paydaşların birbirini denetlediği ve gücün dengeli dağıldığı bir bürokratik yönetim tercih edilmektedir.

Halkın iradesini ön planda tutan Jacksoncı gelenekte ise bürokrasinin çeşitli kademelerinde bulunan elitlere kuşku ile bakılmaktadır. Bu zümrelerin yozlaşmış olduğu ve halka gerçeği söylemediği düşünülmekte, çoklu karar alma ve denetim mekanizmalarına mesafeli durulmaktadır (Mead, 2017). Yetki sahibi bürokratik kesimin sayısı azaldıkça ve yönetim merkezileştikçe karar alma işlevinin daha başarılı olacağı kabul edilmektedir (Mead, 2001, s. 238).

İş birliği ve Bürokrasiye Bakış Kapsamında Jeffersoncı ve Jacksoncı Gelenek

6.2. Çatışmaya Yönelik Tavır

Jeffersoncı gelenekte hâkim olan anlayış uluslararası ortamda maruz kalınan tehditlere karşı asgari tedbirleri alarak tehdidi bertaraf etmek ve vakit kaybetmeden iç işleyişteki ekonomik ve hukuksal problem sahalarına dönmektir (Mead, 2017). Çatışmacı ve tırmandırıcı davranışlardan kaçınılmaktadır. Sorunların çözümünde askeri güç en son opsiyon olarak değerlendirilmektedir (Mead, 2001, s. 188-189). Topyekûn güç kullanımından ziyade sınırlı güç kullanımı tercih edilir.

Jacksoncı yaklaşım, menfaatlere yönelik gerçekleşen saldırılara karşı askeri gücü ana opsiyon olarak görmektedir. Başvurulan sert gücün niteliğinin saldırgan aktörlerin gelecekteki davranış biçimlerini şekillendireceği kabul edilir (Mead, 1999, s. 21). Dolayısıyla sınırlı güç kullanımından ziyade misli ile mukabele tercih edilir. Askeri kabiliyetlere önem verilir ve bu harcamalar kabul görür (Mead, 1999, s. 14-16). Çatışma sürecinde gerginlik artırıcı askeri tedbirlerin kullanımından kaçınılmaz (Mead, 2001, s. 250-251).

Çatışmaya Yönelik Tavır Kapsamında Jeffersoncı ve Jacksoncı Gelenek

Görüldüğü üzere, PPD-20 çatışma ve iş birliğine yaklaşım kriterleri açısından Jeffersoncı dış politika geleneğini; NSPM-13 ise Jacksoncı geleneğin

anlayışını yansıtmaktadır. Söz konusu anlayışların 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 karar almayı gerektiren örneklerle karşılaştırılmıştır. Bu örnekler Suriye rejimine yönelik yaptırımlar ve SİHA kullanımıdır.

6.3. Suriye Rejimine Yönelik Yaptırım Kararı

Arap Baharı sürecinde Suriye iç çatışması ile ilgili Obama yönetiminin en fazla tartışılan kararı, kimyasal silah ültimatomunun yerine getirilmemesidir. Esad'ın elindeki kimyasal silah stokunun farkında olan Beyaz Saray, bu silahların sivil halk üzerinde kullanımını bir "kırmızı çizgi" olarak tanımlamış ve cezai sonuçları olacağını net bir şekilde dile getirmiştir (Kessler, 2013). Buna karşın 2013 yılında başkent Şam yakınlarında rejim güçleri tarafından muhalif güçlere karşı sarin gazı kullanılmış ve 1500 sivilin ölümüyle sonuçlanmıştır (Kaplan, 2015).

Uyguladığı zorlayıcı diplomasinin başarısızlığı karşısında Başkan Obama beklentilere rağmen askeri müdahale seçeneğini değerlendirmemiştir. Bunun yerine, Rus yönetimi ile diyaloğa girilerek Esad'ın elinde bulunan kimyasal silah stokunun Rusya'ya devredilmesi kararı alınmıştır. Verilen sert ültimatomun bu şekilde yumuşak bir çözüm ile geçiştirilmesi 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 askeri yaptırım kararı alınmış, saldırıyı gerçekleştiren savaş uçaklarının kalktığı Şayrat havaalanı 63 saat sonra Tomahawk füzeleri ile vurulmuştur (Da Vinha, 2021, s. 64). Obama'nın Suriye politikasında koymuş olduğu kırmızı çizgileri uygulamamasını bir "küçük düşme" (Rolf, 2021, s. 674) olarak niteleyen Trump, benimsemiş olduğu çatışmacı tavırla ceza yoluyla caydırıcılığı ön plana çıkaran adımlar atmıştır.

6.4. SİHA Saldırıları

SİHA saldırılarının önleyici bir güvenlik tedbiri olarak kullanımı büyük ölçüde Obama yönetimi ile özdeşleşmiştir. Bu dönemde Yemen, Pakistan ve Somali'de toplam 506 saldırıda 3040 terörist ve 391 sivil hayatını kaybetmiştir (Zenko, 2016). Sivil ölümlere yönelik kamuoyu eleştirilerine karşı duyarlılık gösteren Obama yönetimi, 2013 yılında yayımlanan Başkanlık Siyaset Rehberi ile sivil zayiatın önlenmesine yönelik bir dizi prosedür geliştirmiştir. Bu rehbere göre, tehdit değerlendirmesi sırasında sivil kaybının yaşanmayacağı "neredeyse kesin" olacak ve saldırı kararı öncesi Ulusal Güvenlik Konseyi'nin onayı alınacaktır (Beyaz Saray, 2013; Savage, 2016). Ayrıca, 13732 sayılı Başkanlık İcra Emri ile Ulusal İstihbarat Ajansı'na, sivil zaiyatlara ilişkin Kongre'ye yıllık rapor sunma yükümlülüğü verilmiştir.

Trump yönetimi ise SİHA operasyonlarının sayısını artırmakla kalmamış, aynı zamanda Obama döneminin kısıtlayıcı prosedürlerinden uzaklaşmıştır (BBC, 2024). CIA ve Pentagon'a daha geniş operasyonel yetkiler tanınmış, saha operatörlerine daha fazla inisiyatif verilmiştir (Savage & Schmitt, 2017; Savage, 2021). 13862 sayılı İcra Emri ile sivil kayıplara dair raporlama yükümlülüğü kaldırılmıştır (Federal Register, 2019). Bu uygulamalar, Obama'nın Jeffersoncı temkinli yaklaşımını, Trump'ın ise Jacksoncı doğrudan ve çatışmacı tarzını yansıttığını göstermektedir. Dolayısıyla caydırıcılık stratejisindeki farklar, liderlerin benimsediği stratejik kültürlere dayanmaktadır.

7. Kongre Değişkeninin Caydırıcılık Stratejisine Etkileri

Yasama organı olan Kongre'nin misyonu, yürütmede önemli ölçüde pay sahibi olacak şekilde tasarlanmıştır. Başkanın yönetimde sınırsız güç sahibi olmasını önlemek maksadıyla dizayn edilen bu misyon, anayasanın mimarlarından biri olan James Madison tarafından "hırsa karşı koyma hırsı" olarak nitelendirilmiştir (Hamilton, 2005, s. 281). Nitekim anayasanın tasarlanması aşamasında Başkan ve Kongre arasındaki güç dengesi gözetilerek mutlak gücün tek bir elde toplanmaması için çaba gösterildiği ifade edilebilir. Kongre, yasa koyma ve uygulanacak politikaların bütçesini onaylama gibi yetkiler dahilinde güvenlik politikalarına doğrudan etki edebilmektedir.

7.1. Obama Dönemi Siber Güvenlik Politikalarında Kongre Etkisi

Obama'nın ilk kez siber güvenliği bir ana ulusal güvenlik sorunu olarak tanımlaması ve göreve geldikten hemen sonra başlattığı altmış günlük durum değerlendirme süreci onun siber güvenlik konusundaki hassasiyetini göstermektedir. Bu doğrultuda 2010-2012 yılları arasında Kongre'nin her iki kanadında siber güvenliğin çeşitli boyutlarını ele alan yasama teklifleri gündeme gelmiştir. Ancak bu adımlar genel itibariyle başarısız olmuştur.

Yasa Teklifi Adı	Tarih	Teklif Makamı	Konusu	Onaylanma Durumu
Siber Güvenlik Geliştirme Yasası (H.R.4061)	2010	Temsilciler Meclisi	Siber Güvenlik İş Gücü kaynak artırımı ve ArGe çalışmalarının geliştirilmesi	Yürürlüğe girdi
Siber Güvenlik Yasası (S.771)	2010	Senato	Kritik altyapıların savunmasında başkana acil eylem yetkileri (internete erişimin sınırlandırılması vb) tanıma	Yürürlüğe girmedi
Siber Uzayı Bir Ulusal Varlık Olarak Koruma Yasası (S.3480)	2010	Senato	Kritik altyapıların savunmasında başkana acil eylem yetkileri tanıma (bir önceki yasa tasarısına kıyasla başkanın yetki kullanım koşulları detaylı bir şekilde belirlenmiştir	Yürürlüğe girmedi
Siber Uzay ve İnternet Özgürlük Yasası (S.413)	2011	Senato	Kritik Altyapıların Savunmasında İç Güvenlik Bakanlığı yetki artırımı	Yürürlüğe girmedi
Siber Güvenlik ve Bilgi Paylaşımı Etkinliğini Geliştirme Yasası (H.R.3674)	2012	Temsilciler Meclisi	Siber güvenliğin geliştirilmesinde kamu ve özel sektör diyalog kanallarının geliştirilmesi	Yürürlüğe girmedi
Siber Güvenlik Yasası (S.2105)	2012	Senato	İç Güvenlik Bakanlığı sorumluluğunda bir kamu-özel sektör siber güvenlik diyalog platformu kurmak	Yürürlüğe girmedi

Obama Dönemi Kongre'nin Siber Güvenlik Yasama Çalışmaları

2010-2012 yılları arasında Kongre'nin yasama faaliyetleri incelendiğinde, yürütme organının siber güvenlik alanındaki ihtiyaçlarına cevap verecek olgunlukta bir yasal çerçevenin oluşmadığı görülmektedir. Bu başarısızlığın temelinde, devlet-özel sektör ilişkilerinde yaşanan güvensizlikler ve kritik altyapıları elinde bulunduran özel şirketlerin, yürütmeye tanınacak keyfi müdahale hakkı konusunda duyduğu endişeler yer almaktadır (Federal News, 2014). Bu endişelerin zaman zaman partizan saiklerle manipüle edildiği ve yasama sürecinin aksadığı gözlemlenmiştir. Örneğin, özel sektörün gönüllülük esasına dayalı katılımını hedefleyen Siber Güvenlik Yasası teklifi, Senato'daki Cumhuriyetçi üyeler tarafından engellenmiştir.

Kongre'nin etkisizliği üzerine Başkan Obama, yürütmeye ait tek taraflı yetkilerini kullanarak 12 Şubat 2013'te iki belge yayımlamıştır: İcra Emri 13636 ve Başkanlık Siyaset Memorandumu 21. Bu belgeler, kritik altyapıların siber tehditlere karşı korunması için özel sektörün aktif katılımını teşvik eden bir çerçeve sunmuştur (Shackleford vd., 2015). Bu kapsamda İç Güvenlik Bakanlığı koordinatör olarak görevlendirilmiş; risk temelli ortak bir çerçevenin geliştirilmesi, örnek uygulamaların belirlenmesi, teşvik mekanizmalarının oluşturulması ve kişisel hakların gözetilmesi hedeflenmiştir. Ticaret Bakanlığı'na bağlı Ulusal Standart ve Teknoloji Enstitüsü (NIST) liderliğinde çok paydaşlı bir süreçle Siber Güvenlik Çerçevesi oluşturulmuş; bu yaklaşım, Obama'nın çok taraflılık ilkesini ve özel sektör hassasiyetlerine duyarlılığını yansıtmıştır (Margulies, 2017). Takip edilen süreçte siber uzay güvenliğinin bir paydaşı haline gelen özel sektörün bu alana yönelik güvenlik girişimlerinde daha fazla sorumluluk almaya başladığı gözlemlenmiştir (Knake, 2015).

İç Güvenlik Bakanlığı koordinesinde yürütülen müteakip saha adımları bu altyapıların güvenliğinde diyalog ve standardizasyon zeminini güçlendirerek ikna ve dayanıklılık yoluyla caydırıcılığı güçlendirmiştir. Süreç içerisinde önce Kongre'nin iç işleyişi takip edilerek beklenilmiş, ancak yasama organından yapıcı hamlelerin gelmemesi neticesinde Başkan Obama tarafından tek taraflı icra emri yayımlama yolu seçilmiştir.

7.2. Trump Dönemi Siber Güvenlik Politikalarında Kongre Etkisi

Trump'ın ofansif siber harekâtlara yeniden öncelik tanıması, ABD siber caydırıcılık politikası açısından kritik bir dönüm noktasıdır. Buna yönelik Kongre tutumunu değerlendirmek için aynı hafta yayımlanan 2018 Ulusal Güvenlik Yetkilendirme Yasası'na (NDAA) başvurmak anlamlıdır (Congress, 2018). Savunma bütçesini onaylayan ve Kongre'nin savunma önceliklerini belirleyen bu yasa, aynı zamanda siber güvenliğe dair önemli düzenlemeler içermektedir. NDAA'nın 1632. maddesi, siber harekâtların "geleneksel askeri operasyon" kapsamına alınmasını öngörerek istihbarat ve askeri kurumlar arası yetki belirsizliklerini ortadan kaldırmış; başkanın Kongre üyelerini bilgilendirme yükümlülüğünü sınırlamıştır. 1642. madde ise Çin, Kuzey Kore, İran ve Rusya'yı hedef alarak, bu ülkelerden gelen tehditlerin tespiti hâlinde bozucu ve caydırıcı siber faaliyetlere yetki vermektedir.

Bu hükümler, Trump'ın ceza yoluyla caydırıcılık yaklaşımıyla örtüşmektedir. Bürokratik kısıtlamaların azaltılması ve Siber Komutanlık yetkilerinin genişletilmesi bu çerçevede değerlendirilmelidir. Kongre, yürütme

ve Savunma Bakanlığı tarafından koordineli biçimde atılan bu adımlar, siber caydırıcılık stratejisinde kurumsal uyumu pekiştirmiştir.

NDAA kapsamındaki en önemli gelişmelerden biri, Siber Solaryum Komisyonu'nun (CSC) kurulmasıdır. 1652. madde ile kurulan bu yapı, Kongre'nin siber güvenliği partiler üstü bir ulusal öncelik olarak değerlendirdiğini göstermektedir. Cumhuriyetçi ve Demokrat iki eş başkan tarafından yönetilen CSC, denetim, strateji geliştirme ve politika üretim işlevleri üstlenmiştir.

CSC'nin 2020 tarihli raporunda öne çıkan önerilerden biri, Ulusal Siber Direktör makamının oluşturulmasıdır. Bu öneri, Trump döneminde kapatılan Beyaz Saray Siber Güvenlik Koordinatörlüğü'ne yönelik eleştirel bir duruşu yansıtmaktadır. Oluşturulan makamın doğrudan Senato onayı ile atanması, Ulusal Güvenlik Konseyi üyeliği, bağımsız bütçe ve 75 kişilik personel yönetimi gibi geniş yetkilerle donatılması öngörülmüştür (Chesney, 2020).

CSC raporu ayrıca, Obama döneminde kurulan ve siber tehditlerin istihbarat analizine odaklanan Siber Tehdit İstihbaratı Entegrasyon Merkezi'nin kaynak ve yetki bakımından güçlendirilmesini tavsiye etmektedir. Bu öneri, saldırıların kaynağını tespit etme sorununa çözüm getirmeyi amaçlamaktadır. Ek olarak, Kritik Altyapı Güvenlik Ajansı'na (CISA) ".gov" uzantılı ağlarda tehdit devriyesi yapma ve güvenlik açıkları hakkında yasal işlem başlatma yetkisi verilmesi önerilmiştir.

Bu önerilerin 2021 NDAA ile yasalaşması, Kongre'nin siber güvenlik politikasında etkin bir rol üstlendiğini göstermektedir. Kongre, Trump'ın ceza temelli caydırıcılık stratejisini desteklerken; koordinasyon ve hesap verebilirlik ekseninde çok taraflı yapılar aracılığıyla bu yaklaşımı dengelemiştir. Böylece, Obama döneminde pasif konumda kalan Kongre, Trump döneminde hem ceza hem de ikna yoluyla caydırıcılık stratejilerinde daha aktif bir aktör hâline gelmiştir.

Sonuç

Bu çalışma, caydırıcılık stratejisinde stratejik kültür ve kurumların etkilerini inceleyerek, siber güvenlik politikalarında Obama ve Trump dönemlerini karşılaştırmıştır. Neoklasik Realizmin varsayımlarına uygun şekilde analiz edilen bulgular, yapısal faktörlerin güvenlik politikalarına yön verdiğini; ancak iç değişkenlerin devletlerin bağlamı farklı yorumlamasına olanak tanıyarak farklı stratejiler benimsemelerine yol açtığını ortaya koymuştur. ABD'nin Çin ve Rusya gibi rakiplere karşı önlem alma yönelimi her iki dönemde de gözlenmiş, ancak Trump döneminde ceza temelli, ofansif bir caydırıcılık

stratejisi uygulanmıştır. Bu farklılık, Obama'nın Jeffersoncı, Trump'ın ise Jacksoncı stratejik kültür yaklaşımlarından kaynaklanmaktadır.

Kongre'nin rolü dönemsel farklılık göstermektedir. Obama döneminde sınırlı etki gösteren Kongre, Trump döneminde ceza yoluyla caydırıcılığın uygulanmasında doğrudan ve etkili bir aktör hâline gelmiştir. Bu bulgular, dış politika analizinde stratejik kültürün belirleyici bir ara değişken olduğunu ve kurumların ortak bir tutum benimsediği ölçüde etkili olabildiğini göstermektedir.

Neoklasik Realizm, yapısal koşullara ek olarak iç değişkenleri de dikkate alarak dış politika analizine önemli bir kuramsal katkı sunmaktadır. Bu çalışma, nükleer caydırıcılık ekseninde gelişen caydırıcılık stratejisini siber güvenlik özelinde açıklayarak literatüre katkı sağlamaktadır.

Modelin, gri alan ve dezenformasyon gibi diğer hibrit tehditlere de uyarlanabilirliği bulunmaktadır. Bu tehditler, güç dağılımının sunduğu yapısal koşulları belirsizleştirdiğinden, iç değişkenlerin ve liderlik gibi etkenlerin önemi daha da artmaktadır. Son olarak, siber tehditlerin yeni olması ve başarı ölçümüne dair verilerin sınırlılığı nedeniyle analizde caydırıcılığın yöntemi bağımlı değişken olarak tercih edilmiştir.

Ek: Veri Analizinde Başvurulan Resmi Güvenlik Belgeleri

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)

Kaynakça

Achen, C., & Snidal, D. (1989). Rational deterrence theory and comparative case studies. *World Politics, 41*(2), 143–169.

BBC. (2019, March 7). Trump revokes Obama rule on reporting drone strike deaths. *BBC News*. https://www.bbc.com/news/world-us-canada-47480207

Beyaz Saray. (2011). *Siber uzay için uluslararası strateji*. https://nsarchive.gwu.edu/document/20843-04

Beyaz Saray. (2013). *Remarks by the President at the National Defense University*. https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university

Beyaz Saray. (2018). *Ulusal siber strateji*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Birleşmiş Milletler. (2013). *Bilgi ve telekomünikasyon alanındaki gelişmeler bağlamında uluslararası güvenlik raporu (A/68/98)*. https://digitallibrary.un.org/record/3964709?ln=en&v=pdf

Birleşmiş Milletler. (2015). *Bilgi ve telekomünikasyon alanındaki gelişmeler bağlamında uluslararası güvenlik raporu (A/70/174)*. https://digitallibrary.un.org/search?ln=en&p=A%2F70%2F174

Blagden, D. (2020). Deterring cyber coercion: The exaggerated problem of attribution. *Survival, 62*(1), 131–148.

Chesney, R. (2020). The NDAA's National Cyber Director: Justifications, authorities and lingering questions. *Lawfare*. https://www.lawfaremedia.org/article/ndaas-national-cyber-director-justifications-authorities-and-lingering-questions

Clarke, M., & Ricketts, A. (2017a). Donald Trump and American foreign policy: The return of the Jacksonian tradition. *Comparative Strategy, 36*(4), 366–379.

Clarke, M., & Ricketts, A. (2017b). Shielding the republic: Barack Obama and the Jeffersonian tradition of American foreign policy. *Diplomacy & Statecraft, 28*(3), 494–517.

Collier, D. (2011). Understanding process tracing. *Political Science & Politics, 44*(4), 823–830.

Congress. (2018). *John S. McCain National Defense Authorization Act for Fiscal Year 2019*. https://www.congress.gov/bill/115th-congress/senate-bill/2987

Da Vinha, L. (2021). A tale of two red lines: Managing foreign policy crises in the Obama and Trump administrations. *Comparative Strategy, 40*(1), 63–85.

Department of Defense. (2020). DOD General Counsel remarks at U.S. Cyber Command Legal Conference. https://www.defense.gov/News/Speeches/ Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

Dilanian, K. (2019). Under Trump, U.S. military ramps up cyber offensive against other countries. *NBC News*. https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281

Dimitrova, A. (2018). Trump's "America First" foreign policy: The resurgence of the Jacksonian tradition? *L'Europe en Formation, 382*(1), 33–46.

Dueck, C. (2006). *Reluctant crusaders: Power, culture and change in American grand strategy*. Princeton University Press.

Eurepoc. (2024). *Global dataset of cyber incidents*. https://eurepoc.eu/database/

Federal News Network. (2014). Collateral damage of Snowden leaks being felt in cyber, public trust. https://federalnewsnetwork.com/defense/2014/07/collateral-damage-of-snowden-leaks-being-felt-in-cyber-public-trust/

Federal Register. (2019). *EO 13862, revocation of reporting requirement*. https://www.federalregister.gov/presidential-documents/executive-orders/donald-trump/2019

Geller, E. (2017). Trump administration blames North Korea for global WannaCry cyberattack. *Politico*. https://www.politico.eu/article/trump-administration-blames-north-korea-for-global-wannacry-cyberattack/

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

George, A., & Smoke, R. (1974). *Deterrence in American foreign policy: Theory and practice*. Columbia University Press.

Gibbons-Neff, T., & Nakashima, E. (2017). President Trump announces move to elevate Cyber Command. *The Washington Post*. https://www.washingtonpost.com/news/checkpoint/wp/2017/08/18/president-trump-announces-move-to-elevate-cyber-command/

Haffa, R. P. (2018). The future of conventional deterrence: Strategies for great power competition. *Strategic Studies Quarterly, 12*(4), 94–115.

Hamilton, A., Madison, J., Jay, J., & Pole, J. R. (2005). *The Federalist*. Hackett Publishing Company.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity, 5*(1), 1–15.

Holland, J. (2016). Obama as modern Jeffersonian. In M. Bentley & J. Holland (Eds.), *The Obama doctrine: A legacy of continuity in US foreign policy?* (pp. 40–53). Routledge.

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security, 7*(1), 54–67.

Jervis, R. (1976). *Perception and misperception in international politics*. Princeton University Press.

Jervis, R. (1979). Deterrence theory revisited. *World Politics, 31*(2), 289–324.

Johnston, A. (1995). Thinking about strategic culture. *International Security, 19*(4), 32–64.

Kahn, H. (1962). *Thinking about the unthinkable*. Avon Books.

Kaplan, F. (2015). The president in practice. *Foreign Affairs*. https://www.foreignaffairs.com/united-states/obamas-way

Kessler, G. (2013). President Obama and the 'red line' on Syria's chemical weapons. *The Washington Post*. https://www.washingtonpost.com/news/fact-checker/wp/2013/09/06/president-obama-and-the-red-line-on-syrias-chemical-weapons/

Knake, R. (2015). Private sector and government collaboration on cybersecurity: The Home Depot model. *Council on Foreign Relations*. https://www.cfr.org/blog/private-sector-and-government-collaboration-cybersecurity-home-depot-model

Knopf, J. (2010). The fourth wave in deterrence research. *Contemporary Security Policy, 31*(1), 1–33.

Lasconjarias, G. (2017). Deterrence through resilience: *NATO*, the nations and the challenges of being prepared (Eisenhower Paper No. 7). *NATO Defence College Research Division*.

Lebow, R., & Stein, J. (1989). Rational deterrence theory: I think, therefore I deter. *World Politics, 41*(2), 208–224.

Lilli, E. (2020). President Obama and US cyber security policy. *Journal of Cyber Policy, 5*(2), 265–284.

Lilli, E. (2021). Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence. *Contemporary Security Policy, 42*(2), 163–188.

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity, 1*(1), 53–67.

Mahoney, J. (2012). The logic of process tracing tests in the social sciences. *Sociological Methods & Research, 41*(4), 570–597.

Maness, R. C., Valeriano, B., Hedgecock, K., Jensen, B. M., & Macias, J. M. (2022). *The Dyadic Cyber Incident and Campaign Dataset*. https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV

Margulies, P. (2017). Global cybersecurity, surveillance, and privacy: The Obama administration's conflicted legacy. *Indiana Journal of Global Legal Studies, 24*(2), 459.

Maurer, T. (2018). *Cyber mercenaries*. Cambridge University Press.

Mead, W. R. (1999). Jacksonian tradition and American foreign policy. *The National Interest, 58*(Winter), 5–25.

Mead, W. R. (2001). *Special providence: American foreign policy and how it changed the world*. Knopf.

Mead, W. R. (2017). American populism and the liberal order. *Foreign Affairs*. https://www.foreignaffairs.com/united-states/jacksonian-revolt-populism-donald-trump

Mearsheimer, J. J. (1983). *Conventional deterrence*. Cornell University Press.

National Security Archive. (2012). *Barack Obama, Presidential Policy Directive/PPD-20, subject: U.S. cyber operations policy. National Security Archive*. https://nsarchive.gwu.edu/document/21533-document-2-9

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Paul, T. V., Morgan, P., & Wirtz, J. (2009). *Complex deterrence: Strategy in the global age*. University of Chicago Press.

Quinn, A. (2010). *US foreign policy in context: National ideology from the founders to the Bush doctrine*. Routledge.

Rathbun, B. (2008). A rose by any other name: Neoclassical realism as the logical and necessary extension of structural realism. *Security Studies, 17*(2), 294–321. https://doi.org/10.1080/09636410802098917

Ripsman, N. M., Taliaferro, J. W., & Lobell, S. E. (2009). *Neoclassical realism, theory and the state*. Cambridge University Press.

Ripsman, N. M., Taliaferro, J. W., & Lobell, S. E. (2016). *Neoclassical realist theory of international politics*. Oxford University Press.

Rolf, J. N. (2021). Donald Trump's Jacksonian and Jeffersonian foreign policy. *Policy Studies, 42*(5–6), 62–81. https://doi.org/10.1080/01442872.2021.1972014

Rose, G. (1998). Review: Neoclassical realism and theories of foreign policy. *World Politics, 51*(1), 144–172. https://doi.org/10.1017/S0043887100007814

Sanger, D. E. (2018, June 17). Pentagon puts cyberwarriors on the offensive, increasing the risk of conflict. *The New York Times*. https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html

Savage, C. (2016). U.S. releases rules for airstrike killings of terror suspects. *The New York Times*. https://www.nytimes.com/2016/08/07/us/politics/us-releases-rules-for-airstrike-killings-of-terror-suspects.html

Savage, C. (2021). Trump's secret rules for drone strikes outside war zones are disclosed. *The New York Times*. https://www.nytimes.com/2021/05/01/us/politics/trump-drone-strike-rules.html

Savage, C., & Schmitt, E. (2017). Trump poised to drop some limits on drone strikes and commando raids. *The New York Times*. https://www.nytimes.com/2017/09/21/us/politics/trump-drone-strikes-commando-raids-rules.html

Savunma Bakanlığı. (2018). *Savunma Bakanlığı siber stratejisi*. https://sepub-prod-0001-124733793621-us-gov-west-1.s3.us-gov-west-1.amazonaws.com/s3fs-public/ documents/DoD%2BCYBER_STRATEGY_SUMMARY_FINAL%2B09-2018.pdf?VersionId=yMYWnmLD86vTpHIqSLIFhzA6B7P.1Vy

Schelling, T. C. (1966). *Arms and influence*. Yale University Press.

Schweller, R. L. (2004). Unanswered threats: A neoclassical realist theory of underbalancing. *International Security, 29*(2), 159–201. https://doi.org/10.1162/0162288042879975

Shackleford, S., Proia, A., Martell, B., & Craig, A. (2015). 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*, (291).

Sheth, S. (2018). Trump blames Russia for NotPetya cyberattack. *Business Insider*. https://www.businessinsider.com/trump-russia-notpetya-cyberattack-2018-2

Singer, D. J. (1972). Capability distribution, uncertainty, and major power war, 1820–1964 (6th version). In D. J. Singer, S. Bremer, & J. Stuckey (Eds.), *Peace, war, and numbers* (pp. 19–48). SAGE Publications.

Smalley, S. (2022). Biden administration is studying whether to scale back Trump-era cyber authorities at DOD. *CyberScoop*. https://cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/

Snyder, G. (1959). *Deterrence by denial and punishment*. Center of International Studies.

Snyder, G. (1961). *Deterrence and defense: Toward a theory of national security*. Princeton University Press.

Snyder, J. L. (1977). *The Soviet strategic culture: Implications for limited nuclear operations*. Rand Corporation Reports.

Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy, 33*(1), 148–170. https://doi.org/10.1080/13523260.2012.659586

Taliaferro, J. W. (2006). State building for future wars: Neoclassical realism and the resource-extractive state. *Security Studies, 15*(3), 464–495. https://doi.org/10.1080/09636410601028206

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.

Washington Post. (2018). The Cybersecurity 202: Trump just gave the military a lot more leeway to launch cyber operations. *The Washington Post*. 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/

Waters, R. (2014). US struggles to find response to hack attack on Sony. *Financial Times*. https://www.ft.com/content/70a160b4-893c-11e4-ad5b-00144feabdc0

Wilner, A. (2019). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies, 43*(2), 245–280. https://doi.org/10.1080/01402390.2019.1570141

Zagare, F. C., & Kilgour, M. (2004). *Perfect deterrence*. Cambridge University Press.

Zakaria, F. (1998). *From wealth to power*. Princeton University Press.

Zenko, M. (2016). Obama's embrace of drone strikes will be a lasting legacy. *The New York Times*. https://www.nytimes.com/roomfordebate/2016/01/12/reflecting-on-obamas-presidency/obamas-embrace-of-drone-strikes-will-be-a-lasting-legacy