SDE AKADEMİ DERGİSİ
THE JOURNAL OF SDE ACADEMY

Cilt 6 • Sayı: 3 • Eylül 2026 • ss. 409-442
Geliş Tarihi: 16.08.2026 • Kabul Tarihi: 07.09.2026
Araştırma Makalesi • DOI: 10.58375/sde.2019865

TÜRKİYE'NİN KRİTİK ALTYAPI GÜVENLİĞİ BAĞLAMINDA SİBER CAYDIRICILIK STRATEJİLERİ

Kübra Betül BİÇEN GÖREN*

Öz

Bu çalışmanın temel amacı, Türkiye'nin kritik altyapı güvenliği bağlamındaki siber caydırıcılık kapasitesini kuramsal yaklaşımlar ve ulusal politika belgeleri ışığında çok boyutlu bir perspektiften analiz etmektir. Dijitalleşme süreçlerinin hızlanmasıyla birlikte enerji, finans, ulaştırma, sağlık ve telekomünikasyon gibi kritik sektörlerde artan dijital bağımlılık, siber tehditlerin ulusal güvenlik mimarisindeki stratejik önemini büyük ölçüde artırmıştır. Çalışma, bu bağlamda uluslararası siber caydırıcılık literatüründeki temel modelleri (ceza, reddetme ve normatif caydırıcılık) Türkiye'nin özgün koşulları çerçevesinde değerlendirmektedir. Yöntem olarak doküman analizi kullanılmıştır. Türkiye'nin ulusal siber güvenlik strateji belgeleri, Siber Güvenlik Kanunu ve kurumsal yapılanmaları (USOM, SOME ve Siber Güvenlik Başkanlığı) sistematik biçimde incelenmiştir. Elde edilen bulgular, Türkiye'nin "reddetme ağırlıklı hibrit caydırıcılık" modeli çerçevesinde, kurumsal düzenlemeler, yerli teknik kapasite gelişimi ve merkezi koordinasyon aracılığıyla siber savunma kapasitesini önemli ölçüde güçlendirdiğini göstermektedir.

Anahtar Kelimeler: *Siber Güvenlik, Siber Caydırıcılık, Kritik Altyapılar, Ulusal Güvenlik, Türkiye*

* Dr. Öğr. Üyesi, Polis Akademisi, Güvenlik Bilimleri Enstitüsü Uluslararası Güvenlik Anabilim Dalı, E-posta: betulbicen@hotmail.com, ORCID: 0000-0002-1145-7642
Bu makaleye atıf için: Biçen Gören, Kübra Betül. (2026). Türkiye'nin Kritik Altyapı Güvenliği Bağlamında Siber Caydırıcılık Stratejileri, SDE Akademi Dergisi, 6(3), 409-442

SDE AKADEMİ DERGİSİ
THE JOURNAL OF SDE ACADEMY

Volume 6 • Issue: 3 • September 2026 • pp. 409-442
Received: 16.08.2026 • Accepted: 07.09.2026
Research Article • DOI: 10.58375/sde.2019865

CYBER DETERRENCE STRATEGIES IN THE CONTEXT OF TÜRKİYE'S CRITICAL INFRASTRUCTURE SECURITY

Kübra Betül BİÇEN GÖREN

Abstract

The primary objective of this study is to analyze Türkiye's cyber deterrence capacity within the context of critical infrastructure security from a multidimensional perspective, guided by theoretical approaches and national policy documents. Accelerated digitalization and the subsequent increase in digital dependency across critical sectors—such as energy, finance, transportation, healthcare, and telecommunications—have significantly elevated the strategic importance of cyber threats within the national security architecture. In this regard, the study evaluates the fundamental models established in international cyber deterrence literature (deterrence by punishment, deterrence by denial, and normative deterrence) within the framework of Türkiye's unique circumstances. Document analysis was employed as the research methodology. Türkiye's national cybersecurity strategy documents, the Cybersecurity Law, and its institutional structures (USOM, SOME, and the Presidency of Cybersecurity) were systematically examined. The findings demonstrate that Türkiye has substantially enhanced its cyber defense capabilities through institutional frameworks, the development of domestic technical capacity, and centralized coordination, operating under a "denial-oriented hybrid deterrence" model.

Keywords: *Cybersecurity, Cyber Deterrence, Critical Infrastructure, National Security, Türkiye*

Giriş

Dijitalleşme süreçlerinin küresel ölçekte hız kazanması; enerji, finans, ulaştırma, sağlık ve iletişim gibi kritik altyapı sektörlerinin bilgi ve iletişim teknolojilerine olan bağımlılığını kaçınılmaz bir boyuta taşımıştır (Vesić & Bjelajac, 2023: 77). Bu yapısal dönüşüm, siber güvenliği salt teknik bir koruma alanı olmaktan çıkararak ulusal güvenlik politikalarının merkezi haline getirmiştir (Cavelty & Egloff, 2019: 38). Kritik altyapıların işleyişinde meydana gelebilecek olası bir siber kesinti veya manipülasyon, dijital hizmetlerin aksamasına yol açabileceği gibi aynı zamanda ekonomik sürekliliğin kırılmasına, kamu düzeninin bozulmasına ve doğrudan toplumsal güvenlik zafiyetlerine yol açabilecek stratejik bir tehdit potansiyeli barındırmaktadır (Geers, 2010: 298). Siber alanın yapısal niteliklerinden kaynaklanan anonimlik, düşük giriş maliyeti, coğrafi sınır tanımama ve çok aktörlü asimetrik yapı gibi temel özellikler, bu altyapıların korunmasını geleneksel askeri ve fiziki güvenlik mekanizmalarına kıyasla çok daha karmaşık ve dinamik bir düzleme taşımaktadır (Betz & Stevens, 2011:730).

Bu karmaşık tehdit ekosisteminde siber caydırıcılık, devletlerin saldırgan aktörlerin motivasyonlarını ve fayda-maliyet analizlerini etkileyerek kritik altyapıların sürdürülebilirliğini korumak amacıyla başvurduğu en temel stratejik yaklaşımlardan biri haline gelmiştir (Freedman, 2017: 47). Ancak siber uzayın doğası, Soğuk Savaş döneminde şekillenen ve rasyonel aktör varsayımına dayanan klasik ceza temelli nükleer caydırıcılık kuramının bu alana doğrudan uyarlanmasını yapısal olarak engellemektedir (Schelling, 1966:220). Uluslararası siber güvenlik literatüründe uzun süredir tartışılan ceza, reddetme ve normatif caydırıcılık modellerinin her biri, dijital ortamda farklı avantajlar ve operasyonel sınırlılıklar üretmektedir (Nye, 2017: 44-71). Bu bağlamda, bir ülkenin siber caydırıcılık kapasitesinin ve stratejik yöneliminin bütüncül olarak anlaşılabilmesi, söz konusu teorik modellerin ülkenin kendi kurumsal yapılanması, yasal mevzuatı ve jeopolitik tehdit ortamı bağlamında analitik bir süzgeçten geçirilmesini zorunlu kılmaktadır (Libicki, 2009: 75).

Türkiye; artan dijital bağımlılığı, kritik jeopolitik konumu, bölgesel rekabet dinamikleri ve asimetrik çatışma alanlarına yakınlığı nedeniyle kü-

resel ölçekte çok çeşitli ve sofistike siber tehditlere en fazla maruz kalan ülkeler arasında yer almaktadır (Tümer & Yıldırım, 2021, s. 78). Devlet destekli gelişmiş kalıcı tehdit (APT) gruplarından organize siber suç şebekelerine, ideolojik motivasyonlu hacktivist oluşumlardan kritik tedarik zinciri zafiyetlerine uzanan geniş ve karmaşık tehdit yelpazesi (Lindsay & Gartzke, 2020: 750) Türkiye'nin ulusal kritik altyapı ekosisteminin dayanıklılığını doğrudan ve sürekli bir biçimde test etmektedir.

Bu çalışma, Türkiye'nin kritik altyapı güvenliği bağlamındaki siber caydırıcılık kapasitesini kuramsal yaklaşımlar, yasal mevzuat ve ulusal strateji belgeleri üzerinden bütüncül ve karşılaştırmalı bir yaklaşımla değerlendirmeyi amaçlamaktadır. Bu doğrultuda araştırmanın temel sorusu şu şekilde belirlenmiştir: Türkiye'nin mevcut siber caydırıcılık kapasitesini şekillendiren, güçlendiren ve sınırlayan ulusal/uluslararası unsurlar nelerdir ve bu kapasite kritik altyapı güvenliği ekseninde stratejik olarak nasıl konumlanmaktadır?

Siber caydırıcılık literatüründeki "ileri savunma" doktrinlerine ve inandırıcı bir cezalandırma tehdidinin inşasına odaklanmaktadır (Fischerkeller & Harknett, 2018: 381). Bu baskın ceza merkezli paradigmalar; siber alandaki atıf belirsizliği, Proxy aktör kullanımı ve gri alan faaliyetlerinin sürekliliği gibi kısıtlar nedeniyle devletler için siber caydırıcılığın pratikte oldukça sınırlı veya işlevsiz olduğu sonucuna varmaktadır (Rid & Buchanan, 2015: 4). Ancak bu karamsar yaklaşım, siber alanda devasa bir saldırgan misilleme kapasitesine sahip olmayan veya bu tür tırmandırma politikalarını siyasi/jeopolitik riskleri nedeniyle tercih etmeyen orta ölçekli devletlerin siber güvenlik davranışlarını ve stratejik mantıklarını açıklamakta yetersiz kalmaktadır.

İşte bu noktada Türkiye örneği, literatürdeki söz konusu analitik boşluğu doldurabilecek alternatif bir stratejik rasyonaliteye işaret etmektedir. Türkiye; cezalandırma tehdidinin inşasından ziyade, potansiyel saldırganın başarı olasılığını ve operasyonel maliyetini sistematik olarak yükseltmeyi amaçlayan; teknik dayanıklılık, kurumsal koordinasyon ve normatif entegrasyonun eş zamanlı işletildiği çok katmanlı bir güvenlik mimarisi geliştir-

mektedir (Özker, 2022). Çalışmada "reddetme ağırlıklı hibrit caydırıcılık" olarak kavramsallaştırılan bu model, siber caydırıcılığı dar bir askeri misilleme çerçevesinden çıkararak; devlet kapasitesi, siber yönetişim mekanizmaları, teknolojik yerlileşme ve kurumsal bağışıklık üzerinden işleyen genişletilmiş bir analitik perspektifle ele almaktadır (Gartzke & Lindsay, 2017: 37). Bu yönüyle model, benzer jeopolitik kısıtlara sahip diğer devletlerin siber güvenlik yaklaşımlarıyla kavramsal bir paralellik sergilemekte ve literatüre ülke odaklı özgün bir ampirik katkı sunmayı hedeflemektedir.

Çalışmanın temel katkısı, Türkiye'nin siber güvenlik yaklaşımını uluslararası caydırıcılık kuramının üç temel sacayağı (ceza, reddetme, normatif) üzerinden sistematik biçimde incelemesi, yeni kurulan Siber Güvenlik Başkanlığı (SGB) ve 7545 Sayılı Siber Güvenlik Kanunu gibi aktüel gelişmeleri kuramsal düzleme entegre etmesi ve ulusal stratejinin analitik olarak hangi modelle daha fazla örtüştüğünü ortaya koymasıdır. Böylece bu çalışma, Türkiye'nin siber güvenlik politika mimarisine açıklık getirmekte ve uluslararası politik araştırmalar literatürüne siber alanda savunmadan caydırıcılığa geçiş süreçlerini anlamlandırmaya yönelik güncel bir model sunmaktadır.

1. Kuramsal Çerçeve ve Yöntem

Bu araştırma, nitel araştırma yaklaşımı çerçevesinde tasarlanmış betimsel–analitik bir çalışmadır. Araştırmanın temel amacı, Türkiye'nin kritik altyapı güvenliği bağlamındaki siber caydırıcılık kapasitesini kuramsal yaklaşımlar ile ulusal siber güvenlik yönetişimini şekillendiren hukuki ve kurumsal belgeler üzerinden incelemektir. Çalışma, devletin siber caydırıcılık mimarisini oluşturan kurumsal yapıların, hukuki düzenlemelerin ve stratejik politika belgelerinin sistematik olarak değerlendirilmesini amaçlamaktadır.

Araştırmada temel veri toplama yöntemi olarak doküman analizi kullanılmıştır. Doküman analizi; basılı veya elektronik belgelerin sistematik biçimde incelenmesi, değerlendirilmesi ve yorumlanmasına dayanan nitel

bir araştırma yöntemidir (Creswell, 2025). Özellikle kamu politikaları, güvenlik çalışmaları ve yönetişim araştırmalarında resmî belgelerin analizinde yaygın biçimde kullanılmaktadır. Bowen (2009), doküman analizinin yalnızca mevcut belgelerin özetlenmesinden ibaret olmadığını; belgelerin araştırma soruları doğrultusunda sistematik olarak kodlanması, karşılaştırılması ve yorumlanmasını içeren analitik bir süreç olduğunu belirtmektedir (Bowen, 2009). Bu çalışma doküman analizi yaklaşımına uygun olarak dört aşamada yürütülmüştür: Veri kaynaklarının belirlenmesi, analitik kodlama çerçevesinin oluşturulması, tematik içerik analizinin gerçekleştirilmesi, bulguların kuramsal çerçeve ile karşılaştırmalı olarak yorumlanması şeklindedir.

1.1. Veri Kaynakları

Araştırmanın evrenini Türkiye'nin kritik altyapı güvenliği ve siber caydırıcılık politikalarını düzenleyen ulusal hukuki ve kurumsal belgeler oluşturmaktadır. Araştırmada olasılıklı örnekleme yerine nitel araştırmalarda yaygın olarak kullanılan amaçlı örneklem yöntemi tercih edilmiştir. Amaçlı örneklem, araştırma problemini en iyi açıklayabilecek bilgi açısından zengin veri kaynaklarının seçilmesine dayanmaktadır (Patton, 2015).

Bu kapsamda analiz edilen temel belgeler şunlardır:

- 7545 Sayılı Siber Güvenlik Kanunu (2025)
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024–2028)
- USOM ve SOME Tebliği
- Avrupa Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi)
- Siber Güvenlik Başkanlığına ilişkin mevzuat

Belgelerin seçiminde üç temel ölçüt esas alınmıştır: Türkiye'nin ulusal siber güvenlik politikasını doğrudan düzenlemesi, kritik altyapı güvenliğiyle doğrudan ilişkili olması, siber caydırıcılığın kurumsal veya hukuki boyutuna ilişkin düzenleme içermesi.

1.2. Veri Analizi

Araştırmada elde edilen veriler tümdengelimsel tematik içerik analizi yöntemiyle analiz edilmiştir. Tematik analiz, nitel veriler içerisinde tekrar eden anlam örüntülerini belirlemeyi ve bunları sistematik biçimde sınıflandırmayı amaçlayan güvenilir bir analiz tekniğidir (Braun & Clarke, 2006). Kodlama süreci araştırmanın kuramsal çerçevesinden hareketle önceden belirlenen analitik kategoriler üzerine kurulmuştur. Bu doğrultuda üç temel tema oluşturulmuştur: ceza yoluyla caydırıcılık, reddetme yoluyla caydırıcılık, normatif caydırıcılık şeklindedir.

Analiz sürecinde öncelikle seçilen hukuki ve stratejik belgeler araştırma sorusu doğrultusunda bütüncül olarak okunmuş, ardından metinlerde siber caydırıcılık kapasitesini yansıtan politika araçları, kurumsal düzenlemeler ve hukuki hükümler belirlenmiştir. Elde edilen veriler, araştırmanın kuramsal çerçevesini oluşturan ceza yoluyla caydırıcılık, reddetme yoluyla caydırıcılık ve normatif caydırıcılık temaları esas alınarak sınıflandırılmıştır. Her belge, bu üç analitik kategori bakımından karşılaştırmalı olarak değerlendirilmiştir. Benzer ve farklı yönler sistematik biçimde analiz edilerek Türkiye'nin siber caydırıcılık mimarisinin hangi kuramsal modele daha fazla yaklaştığı yorumlanmıştır. Analiz sürecinde doğrudan belge içeriklerinden hareket edilmiş, yorumlar uluslararası siber caydırıcılık literatürüyle ilişkilendirilerek bulguların kuramsal tutarlılığı sağlanmaya çalışılmıştır. Böylece çalışma, yalnızca betimleyici bir belge incelemesi olmanın ötesine geçerek kuramsal temelli karşılaştırmalı bir politika analizi niteliği kazanmıştır.

1.3. Analitik Çerçeve

Çalışmada kullanılan analiz matrisi üç temel kuramsal boyut üzerine kurulmuştur.

Analitik Boyut	Analiz Ölçütleri
Ceza Yoluyla Caydırıcılık	Misilleme kapasitesi, yaptırım araçları, stratejik sinyal verme
ReddetmeYoluyla Caydırıcılık	Teknik dayanıklılık, kritik altyapı koruması, USOM, SOME, yerli teknoloji
Normatif Caydırıcılık	Hukuki düzenlemeler, uluslararası sözleşmeler, norm üretimi, uluslararası iş birliği

Bu analiz matrisi bütün belgelerin aynı kavramsal ölçütlerle değerlendirilmesini sağlamış; farklı politika belgelerinin benzer ve ayrışan yönlerinin sistematik biçimde karşılaştırılmasına olanak vermiştir.

1.4. Geçerlilik ve Güvenirlik

Nitel araştırmalarda geçerlilik ve güvenirliği artırmak amacıyla farklı veri kaynaklarının birlikte kullanılması önerilmektedir. Doküman analizinde farklı resmî belgelerin birlikte değerlendirilmesi araştırmanın inandırıcılığını artırmaktadır (Bowen, 2009). Ayrıca araştırma sürecinin ayrıntılı biçimde raporlanması ve analiz aşamalarının açık şekilde açıklanması, çalışmanın denetlenebilirliğini güçlendirmektedir (Bowen, 2009). Bu doğrultuda araştırmada farklı belge türleri birlikte analiz edilmiş, tüm dokümanlar aynı kodlama şeması kullanılarak değerlendirilmiş ve analiz süreci ayrıntılı biçimde raporlanmıştır. Böylece araştırmanın şeffaflığı, izlenebilirliği ve metodolojik tutarlılığı artırılmıştır. Nitel araştırmanın şeffaflığı ve izlenebilirliği ilkesi gereği, çalışmanın temel analiz birimini oluşturan hukuki ve stratejik dokümanlar ile bunların analizdeki kavramsal işlevleri Tablo 1'de özetlenmiştir.

Tablo 1. Analize Dâhil Edilen Temel Dokümanlar ve Kavramsal İşlevleri

Belge Adı	Yılı	Analizdeki İşlevi ve Tematik Kodu
7545 Sayılı Siber Güvenlik Kanunu	2025	Kritik altyapı tanımı, Siber Güvenlik Başkanlığı'nın (SGB) yasal zemini, devletin müdahale kapasitesi *(Ceza ve Normatif Caydırıcılık)*
Ulusal Siber Güvenlik Stratejisi ve Eylem Planı	2024–2028	İnsan odaklı güvenlik, teknolojik egemenlik hedefleri, proaktif savunma doktrini *(Reddetme Ağırlıklı Caydırıcılık)*
Avrupa Siber Suçlar Sözleşmesi (Budapeşte)	2001	Bilişim suçlarının uluslararası uyumu, sınır aşan veri muhafazası ve adli iş birliği *(Normatif Caydırıcılık)*
USOM ve SOME Kuruluş/Çalışma Usulleri Tebliği	2013	Katmanlı siber savunma, olay müdahale süreçleri, erken tespit ve SİP koordinasyonu *(Reddetme Caydırıcılığı / Savunma Kapasitesi)*

Kaynak: Yazar tarafından oluşturulmuştur

Seçilen dokümanlar analiz sürecinde, caydırıcılık modelleri bağlamında hangi kapasite türüne (ceza, reddetme, normatif) ağırlık verdiği, kurumsal koordinasyon düzeyi ve stratejik sinyal üretme biçimi açısından değerlendirilmiştir. Bu yaklaşım, Türkiye'nin siber caydırıcılık mimarisinin yalnızca normatif beyanlar üzerinden değil, kurumsal yapı ve politika araçları üzerinden karşılaştırmalı olarak çözümlenmesine imkân sağlamıştır. Araştırmanın evreni, Türkiye'nin kritik altyapı güvenliği bağlamındaki siber güvenlik yönetişimi ve caydırıcılık mimarisi olarak tanımlanmış olup örneklem bu evreni temsil eden ulusal strateji belgeleriyle sınırlandırılmıştır.

Çalışma, ulusal güvenlik stratejilerinin siber tehditler bağlamındaki işleyişini anlamak amacıyla Uluslararası İlişkiler literatürünün temel öğelerinden biri olan caydırıcılık teorisine dayanmaktadır. Klasik caydırıcılık

anlayışı özellikle nükleer strateji ve askeri güç dengesi çerçevesinde şekillenmiş olsa da (Schelling, 1966: 220), siber alanın anonimlik, düşük maliyet, çok aktörlü tehdit yapısı ve teknik belirsizlikleri klasik modellerin uygulanmasını karmaşık hâle getirmektedir (Libicki, 2009: 91). Bu nedenle siber caydırıcılık, geleneksel kavramların dijital ortamın özgün dinamikleriyle yeniden yorumlanmasını gerektiren, hibrit ve katmanlı analizlere ihtiyaç duyan bir alana dönüşmüştür.

2. Klasik Caydırıcılık Modelleri: Ceza, Reddetme ve Normatif Yaklaşımlar

Klasik teoride ceza yoluyla caydırıcılık, saldırganın maliyetini artırmayı veya misilleme tehdidi oluşturarak saldırıyı önlemeyi hedeflemektedir (Schelling, 1966, s.221). Ancak siber saldırıların failini kesin olarak tespit etmenin güçlüğü, bu yaklaşımın siber alandaki inandırıcılığını zayıflatmaktadır (Rid, 2020). Özellikle atıf zorluğu, devletlerin açık misilleme politikalarını sınırlamakta ve ceza yoluyla caydırıcılığı pratikte uygulanabilir olmaktan uzaklaştırmaktadır (Valeriano & Jensen, 2018, s. 1132).

Reddetme yoluyla caydırıcılık ise saldırganın başarı ihtimalini düşürmeye odaklanmaktadır. Bu yaklaşım, güçlü savunma kapasitesi, ağ segmentasyonu, çok katmanlı güvenlik, olay müdahale ekipleri ve hızlı tespit mekanizmaları gibi teknik ve kurumsal tedbirleri içermektedir (Libicki, 2009). Literatürde reddetme modelinin siber alanda en uygulanabilir caydırıcılık türü olduğu ve devletlerin pratikte çoğunlukla bu modele yöneldiği belirtilmektedir (Nye, 2017: 50).

Normatif caydırıcılık ise uluslararası hukuk, davranış normları ve kurumlar arası mutabakatların devlet davranışını sınırlandırıcı etkisine dayanmaktadır (Nye, 2017: 47). Tallinn Manual gibi doktrinler devletlerin siber operasyonlarda hukuki çerçeve geliştirmesini desteklemekle birlikte, bu normların bağlayıcılık düzeyi hâlen sınırlıdır. Devlet için tamamlayıcı bir caydırıcılık mekanizması olmaktan öteye geçmemektedir (Schmitt, 2017:170).

Siber suç ekosisteminin giderek karmaşıklaşması, bu modeller arasındaki farkları daha görünür hâle getirmektedir. Veri hırsızlığı, fidye yazılımı saldırıları, kimlik bilgilerinin ticareti ve tedarik zinciri istismarları gibi tehdit türleri, bireyleri, kritik altyapıları ve ulusal güvenliği doğrudan etkilemektedir (Valeriano & Maness, 2015, s.76). Sağlık, finans, enerji ve üretim sektörlerinde ortaya çıkan saldırıların ekonomik ve toplumsal etkileri bulunmaktadır. Kritik altyapı güvenliğinin salt teknik bir sorunun ötesinde devlet kapasitesi, kurumlar arası koordinasyon ve stratejik yönetişimle yakından ilişkili bir güvenlik konusudur (Rid, 2020).

2.1. Hibrit ve Çapraz Alan Siber Caydırıcılığın Kuramsal Çerçevesi

Klasik caydırıcılık teorileri büyük ölçüde askeri güç projeksiyonu ve nükleer denge bağlamında şekillenmiştir. Bu çerçevede caydırıcılık, saldırganın rasyonel maliyet–fayda hesabını etkileyerek davranış değişikliği üretmeyi amaçlayan stratejik bir mekanizma olarak tanımlanmaktadır (Freedman, 2017: 47). Ceza ve reddetme ikiliği, bu teorik yapının merkezinde yer almaktadır. Ceza temelli caydırıcılık, saldırganın karşılaşacağı maliyetleri artırarak geri adım atmasını hedeflerken; reddetme temelli caydırıcılık saldırının başarı ihtimalini düşürerek saldırganın beklenen kazancını azaltmayı amaçlamaktadır (Snyder, 1961: 8).

Ancak siber alan, bu klasik çerçeveyi zorlayan yapısal özelliklere sahiptir. İlk olarak, siber operasyonların düşük maliyetli ve asimetrik doğası, geleneksel askeri güç dengesine dayalı caydırıcılık mantığını zayıflatmaktadır. İkinci olarak, devlet-dışı aktörlerin ve vekil yapıların etkinliği, aktör kimliğini bulanıklaştırmakta ve doğrudan misillemeye dayalı caydırıcılığı siyasal açıdan riskli hale getirmektedir (Rid & Buchanan, 2015). Üçüncü olarak ise siber alan, açık kriz anlarından ziyade sürekli düşük yoğunluklu rekabet biçiminde işlemektedir. Bu durum, klasik kriz–tırmanma–misilleme modelinin öngördüğü doğrusal stratejik döngüyü belirsizleştirmektedir (Fischerkeller & Harknett, 2018).

Bu yapısal dönüşüm karşısında literatürde "çapraz alan caydırıcılığı" yaklaşımı geliştirilmiştir. Bu modele göre, bir alandaki saldırıya verilen

karşılık aynı alanda olmak zorunda değildir. Siber bir saldırı ekonomik yaptırımlar, diplomatik izolasyon, hukuki süreçler veya askeri güç gösterisi yoluyla karşılanabilir (Nye, 2017). Böylece caydırıcılık, tekil bir askeri kapasite olmaktan çıkarak çok alanlı ve çok araçlı bir stratejik portföye dönüşmektedir.

Çapraz alan yaklaşımının temel varsayımı, saldırganın maliyet hesabının yalnızca teknik karşılık üzerinden değil, bütüncül bir güç bileşimi üzerinden etkilenebileceğidir. Bu durum, caydırıcılığı salt askeri misilleme tehdidi olmaktan çıkarıp siyasi irade, ekonomik kapasite ve diplomatik konumla birlikte değerlendirilmesi gereken çok katmanlı bir stratejik süreç haline getirmektedir (Libicki, 2009).

Bununla birlikte, siber alanın atıf sorunu ceza temelli caydırıcılığı yapısal olarak sınırlamaktadır. Teknik izlerin manipüle edilebilir olması ve operasyonların çoğu zaman örtük yürütülmesi, saldırının kesin biçimde bir devlete atfedilmesini zorlaştırmaktadır (Rid & Buchanan, 2015). Atıf belirsizliği, misillemenin meşruiyetini ve inandırıcılığını tartışmalı hale getirebilir. Bu nedenle literatürde, siber caydırıcılığın yalnızca cezaya değil, dayanıklılığa dayalı reddetme stratejilerine yaslanması gerektiği savunulmaktadır (Gartzke & Lindsay, 2017).

Bu noktada hibrit caydırıcılık kavramı teorik bir sentez sunmaktadır. Hibrit model, reddetme kapasitesini temel alırken, gerektiğinde çapraz alan karşılık opsiyonlarını stratejik bir sinyal unsuru olarak muhafaza etmektedir. Böylece caydırıcılık, teknik savunma kapasitesi, siyasi kararlılık ve normatif konumlandırmanın birlikte işlediği çok boyutlu bir yapı haline gelmektedir. Uluslararası normlar ve hukuk çerçevesi de bu yapının önemli bir bileşenidir. Zira normlar doğrudan yaptırım üretmese de, devletlerin hangi karşılıkları meşru kabul edeceğini belirleyen çerçeveyi şekillendirmektedir (Finnemore & Hollis, 2016: 430). Bu çalışmada reddetme ağırlıklı hibrit caydırıcılık, cezalandırma kapasitesini tamamen dışlamayan ancak caydırıcılığı esas olarak saldırı başarısını düşüren kurumsal ve teknik kapasite inşasına dayandıran model olarak tanımlanmaktadır

Dolayısıyla hibrit ve çapraz alan siber caydırıcılığı, klasik ceza–reddetme ikiliğinin siber alanın yapısal gerçeklikleri doğrultusunda yeniden yorumlanmış bir versiyonu olarak değerlendirilebilir. Bu yaklaşım, caydırıcılığı yalnızca askeri güç projeksiyonuna indirgemeyen; teknik kapasite, kurumsal dayanıklılık, siyasi irade ve normatif meşruiyeti birlikte ele alan genişletilmiş bir kuramsal çerçeve sunmaktadır.

2.3. Siber Alanda Caydırıcılığın Yapısal Sorunları

Siber caydırıcılık, klasik caydırıcılık teorisinin temel varsayımlarını dijital çatışma ortamına uyarlama girişiminden doğan, ancak bu uyarlamanın önemli sınırlılıklarla karşılaştığı bir alandır (Kruse et al., 2017: 3). Geleneksel caydırıcılık teorisi, Schelling'in (1966: 3–18) ortaya koyduğu biçimiyle rasyonel aktör modeline, misilleme kapasitesine ve maliyet artırma stratejilerine dayanmaktadır. Buna karşın siber uzayın dinamikleri klasik caydırıcılığın mantıksal zeminini doğrudan sarsmaktadır (Betz & Stevens, 2011: 730). Bu nedenle literatür, siber alanın caydırıcılık teorisini "basit bir aktarma" ile taşımanın mümkün olmadığı konusunda geniş bir uzlaşıya sahiptir. Rid (2020: 15), siber alanın sürekli çatışma hâli yarattığını ve bu nedenle caydırıcılığın kriz anına özgü geleneksel mantığının dijital ortama tam olarak uyarlanamayacağını savunur.

Caydırıcılık literatüründe özellikle iki temel model öne çıkmaktadır: ceza yoluyla caydırıcılık ve reddetme yoluyla caydırıcılık. Ceza yoluyla caydırıcılık, saldırgana misilleme veya siyasi, ekonomik ve teknik maliyet yükleme tehdidine dayanmaktadır. Ancak atıf güçlüğü ve çok aktörlü yapı nedeniyle bu model siber alanda sınırlı etki üretmektedir. Buna karşılık reddetme yoluyla caydırıcılık, saldırının başarı ihtimalini düşürerek caydırıcılığı güçlendirmeyi amaçlamaktadır. Çok katmanlı savunma, hızlı tespit–yanıt kapasitesi, ağ segmentasyonu ve kritik altyapıların yedekli mimarilerle korunması bu yaklaşımın temel unsurlarıdır (Libicki, 2009: 78). Literatürde reddetmenin siber alanda uygulanabilirliği konusunda güçlü bir konsensüs bulunmaktadır (Nye, 2017: 47–50). Finnemore ve Hollis (2016) ise uluslararası hukuk, norm üretimi ve devlet davranışını sınırla-

yan beklentilerin oluşturduğu "normatif caydırıcılık" yaklaşımının siber alanda teknik unsurlar kadar önemli olduğunu göstermektedir.

Kritik altyapıların dijitalleşmesi, siber caydırıcılığın yapısal sorunlarını daha görünür kılmaktadır. Enerji iletim hatları, finansal sistemler, ulaşım ağları, su yönetimi ve haberleşme altyapıları giderek daha fazla birbirine bağımlı hâle gelmekte ve bu durum çok boyutlu bir kırılganlık yaratmaktadır. Geers (2010) kritik altyapılara yönelik saldırıların yalnızca bilgi kaybı değil, fiziksel tahribat ve geniş çaplı toplumsal aksamalara neden olabileceğini vurgulamaktadır. Devlet destekli aktörlerin özellikle enerji ve finans sektörlerinde stratejik avantaj sağlamak amacıyla saldırılar düzenlemesi caydırıcılık mekanizmalarının güvenilirliğini daha da zorlaştırmaktadır (Cavelty & Egloff, 2019: 37–57). Organize suç grupları ise fidye yazılımının ekonomik ekosisteminden güç alarak ulusötesi aktörler hâline gelmiştir (Lindsay & Gartzke, 2020: 22).

Siber caydırıcılığın başarısı, devletlerin siber güç kapasitesiyle doğrudan ilişkilidir. Nye (2017: 55), siber gücü teknik kapasite, kurumsal yönetişim, insan kaynağı ve teknolojik bağımsızlık gibi çok boyutlu unsurların birleşimi olarak tanımlamaktadır. Kurumsal yönetişim; ulusal stratejiler, kriz yönetimi mekanizmaları ve kamu–özel sektör iş birliklerini içermektedir (Kuehl, 2009: 7). İnsan kaynağındaki küresel açık, caydırıcılığın sürdürülebilirliğini tehdit eden yapısal bir sorundur. Teknolojik bağımsızlık ise yabancı donanıma ve yazılıma duyulan bağımlılığı azaltarak ulusal caydırıcılık kapasitesinin güvenilirliğini artırmaktadır (Geers, 2010: 300).

Asimetrik aktörlerin düşük maliyetli teknolojilerle yüksek etki yaratabilmesi, siber caydırıcılığın en temel kırılganlıklarından biridir. Valeriano ve Maness (2015:1132), bu durumun caydırıcılığı öngörülemez hâle getirdiğini ve devletleri sürekli uyarlanabilir stratejiler geliştirmeye zorladığını belirtmektedir. Tedarik zinciri güvenliği ise reddetme yoluyla caydırıcılığın etki alanını doğrudan sınırlandırmaktadır. Trujillo (2014:50), yabancı tedarikçilere bağımlılığın arka kapılar ve zafiyet ekosistemleri üzerinden ulusal savunma mimarisini içeriden kırılganlaştırdığını ve bu nedenle teknolojik yerlileşmenin stratejik bir zorunluluk olduğunu vurgulamaktadır.

Özker (2022) ise yerli teknolojinin kritik altyapı güvenliğinde caydırıcılığı artırıcı bir faktör olduğunu göstermektedir.

Siber caydırıcılık, teknik savunma tedbirleri ve stratejik iletişim, norm üretimi, tedarik zinciri güvenliği ve teknolojik bağımsızlık gibi çok boyutlu faktörlere bağlıdır (Kolokotronis & Shiaeles, 2021). Tehditlerin karmaşıklaştığı bir ortamda, kriptografi ve bütüncül güvenlik mekanizmaları teknik birer araç olmaktan çıkıp caydırıcılığın çekirdek bileşenlerine dönüşmektedir (Vesić et al., 2023:77).

Küresel siber güvenlik mimarisinde 'atıf belirsizliği' ve asimetrik aktörlerin yükselişi geleneksel caydırıcılık teorilerini aşındırırken, bu durum özellikle stratejik fay hatları üzerinde yer alan ülkeler için benzersiz güvenlik açıkları üretmektedir. Türkiye; jeopolitik konumu, bölgesel çatışma alanlarına olan yakınlığı ve kritik altyapılarındaki yüksek dijitalleşme hızı nedeniyle, literatürde tartışılan bu yapısal krizlerin en yoğun hissedildiği aktörlerden biridir. Dolayısıyla, siber caydırıcılığın kuramsal zorlukları Türkiye bağlamında salt teorik bir sorun olmaktan çıkmakta; enerji, finans ve ulaştırma gibi sektörlerin günlük operasyonel güvenliğini ve devletin bekasını doğrudan etkileyen bir ulusal güvenlik meselesine dönüşmektedir.

3. Türkiye'nin Kritik Altyapı Ekosistemi ve Tehdit Ortamı

Türkiye, siber güvenliğin ulusal güvenliğin temel bileşeni olduğu bilinciyle 2010'lu yılların başından itibaren kurumlarını yeniden yapılandırmış ve kritik altyapıların korunmasına yönelik kapsamlı bir yönetişim modeli geliştirmiştir. Kritik altyapılar, işledikleri bilginin gizlilik, bütünlük ve erişilebilirlik ilkelerinin ihlali hâlinde fiziksel hasara, can kaybına, ekonomik çalkantıya veya kamu düzeninin bozulmasına yol açabilecek telekomünikasyon, enerji, finans, sağlık ve ulaştırma gibi sektörleri kapsamaktadır. Bu tanım uluslararası literatürle uyumludur. Örneğin Dunn Cavelty ve Suter (2009) kritik altyapıları "toplumsal işleyişi devam ettiren zorunlu sistemler" olarak tanımlamaktadır.

Türkiye'nin kurumsal siber güvenlik kapasitesi, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 2013 yılında kurulan Ulusal Siber Olaylara

Müdahale Merkezi (USOM) etrafında şekillenmiştir (Ulusal Siber Olaylara Müdahale Merkezi, 2014). USOM, ulusal ve uluslararası düzeyde Türkiye'nin siber temas noktası olarak görev yapmaktadır. Tehdit istihbaratı üretme, zafiyet tespiti yapma ve kriz anlarında koordinasyon sağlama sorumluluğunu yürütmektedir. USOM'un en kritik işlevlerinden biri, Türkiye genelinde Sektörel ve Kurumsal SOME birimlerini koordine etmesidir. Bu yapı, Libicki'nin (2009) reddetme yoluyla caydırıcılık modellerinde belirttiği üzere, etkili caydırıcılığın temelini oluşturan çok katmanlı savunma ve hızlı müdahale kapasitesiyle uyum göstermektedir.

USOM–SOME arasında güvenli veri akışını sağlamak amacıyla oluşturulan SOME İletişim Platformu (SİP), tehdit istihbaratı, zafiyetler, sıfırıncı gün açıklıkları ve güncel saldırı kampanyalarına ilişkin bilgilerin çift yönlü paylaşımını sağlamaktadır (BTK, 2013). SİP'in kapalı devre yapısı, kritik altyapıların bütünleşik bir savunma ekosistemi içinde korunmasına imkân tanımaktadır. Bu yönetişim modeli, literatürde "ulusal siber bağışıklık" olarak kavramsallaştırılan merkezî müdahale kapasitesine karşılık gelmektedir (Nye, 2017: 55).

Bu kurumsal ve stratejik gelişmeler, siber caydırıcılık literatüründeki teorik tartışmalar bağlamında değerlendirildiğinde farklı bir anlam kazanmaktadır. Türkiye'nin siber güvenlik stratejileri incelendiğinde, 2013 sonrası dönemde savunma odaklı bir kurumsal konsolidasyon sürecinin belirginleştiği görülmektedir. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve sektörel SOME yapılanmalarının yaygınlaştırılması, merkezi koordinasyon kapasitesinin artırılması ve kritik altyapı koruma mekanizmalarının kurumsallaştırılması, caydırıcılığın reddetme boyutunun sistematik biçimde inşa edildiğini göstermektedir. Bu süreç, misilleme kapasitesinin açık biçimde vurgulanmasından ziyade, saldırı yüzeyinin daraltılması ve müdahale süresinin kısaltılması üzerinden güvenlik üretme mantığına dayanmaktadır. Benzer biçimde yerli siber güvenlik ürünlerinin geliştirilmesi ve kamu ağlarında yerlilik oranının artırılması yönündeki politika tercihleri, yalnızca teknoloji politikası değil; aynı zamanda dışa bağımlılığı azaltarak yapısal kırılganlıkları düşürmeye yönelik bir caydırıcılık stratejisi

olarak okunabilir. Bu çerçevede Türkiye'nin yaklaşımı, cezalandırma tehdidinin görünür inşasından ziyade, saldırganın maliyet–fayda hesaplamasını olumsuz etkileyecek kapasite birikimine dayanmaktadır.

Verizon'un 2024 Data Breach Investigations Report'una göre doğrulanmış veri ihlallerinin %68›inde insan unsuru etkili olmaktadır. Bu bulgu, Türkiye›nin insan odaklı güvenlik kültürünü ve siber farkındalık politikalarını güçlendirmesinin kritik altyapı güvenliği açısından stratejik önem taşıdığını göstermektedir. Bu vurgu, Kuehl'ün (2009: 7) siber gücü "teknik kapasite kadar yönetişimsel kapasite ve nitelikli insan kaynağı" olarak tanımlayan yaklaşımıyla uyumludur.

Türkiye'nin kritik altyapıları, yüksek derecede dijital bağımlılık ve yoğun sektörler arası etkileşim nedeniyle çok katmanlı bir kırılganlık alanı teşkil etmektedir. Elektrik üretim ve iletiminde kullanılan SCADA sistemlerinin hedef alınması yalnızca enerji arzında kesinti yaratmakla kalmamakta; finansal sistemler, telekomünikasyon hizmetleri ve ulaştırma altyapıları zincirleme biçimde etkilenmektedir. Bu durum literatürde "kritik altyapı kümelenmesi" olarak adlandırılmakta ve modern devletlerde güvenlik risklerinin birbirini tetikleyen karakterine işaret etmektedir (Dunn Cavelty & Suter, 2009: 181).

Son yıllarda Türkiye açısından kritik öneme sahip, tedarik zinciri saldırılarıdır. SolarWinds örneği, tedarik zinciri ihlallerinin yalnızca hedef kurumu değil, onunla bağlantılı tüm dijital ekosistemi etkilediğini göstermiştir (Lindsay & Gartzke, 2020: 750). Türkiye'nin yazılım ve donanım ekosisteminde dışa bağımlı olması, arka kapı yerleştirme, manipüle edilmiş firmware bileşenleri ve güncelleme paketlerine sızma gibi riskleri artırmaktadır.

Bu çerçevede Türkiye'nin ulusal siber güvenlik politikası, teknik kapasitnin artırılması, yönetişimsel koordinasyon sağlanması ve yerli teknolojinin geliştirilmesi üzerinedir. Ağırlıklı olarak reddetme eksenli hibrit bir caydırıcılık modeli olarak değerlendirilebilir. Ancak caydırıcılığı daha dengeli ve sürdürülebilir bir yapıya kavuşturmak için iki unsur kritik görünmektedir: atıf kapasitesinin güçlendirilmesi ve misilleme stratejilerinin

görünür biçimde kurumsallaştırılması. Bu iki unsur, Türkiye'nin caydırıcılık mimarisinin gelecekte daha etkili bir stratejik bütünlük kazanmasına katkı sağlayacaktır.

4. Türkiye'nin Siber Caydırıcılık Kapasitesi: Stratejiler ve Politika Analizi

Türkiye, kritik altyapı güvenliği perspektifinden siber caydırıcılık stratejisi geliştirme sürecinde önemli kurumsal kapasite ve teknik kabiliyet inşa etmiştir. Teknik kapasite açısından Türkiye, yerli yazılım ve siber savunma araçları geliştirme yönünde stratejik bir çizgi izlemektedir. USOM tarafından geliştirilen Avcı, Azad, Kasırga, Atmaca ve Kule gibi yerli araçlar, milli kaynak kullanımını ve teknolojik bağımsızlık hedefini desteklemektedir. Erken tespit, sürekli tarama ve saldırı öncesi sinyal verme becerisini güçlendirmektedir (Ulaştırma ve Altyapı Bakanlığı, 2013).

Kurumsal ve stratejik çerçevede, Türkiye'nin Ulusal Siber Güvenlik Stratejileri ve Eylem Planları, siber caydırıcılığın kurumsal ve stratejik eksenlerini tanımlamaktadır. 2024–2028 Stratejisi, "proaktif siber savunma ve caydırıcılık" ifadesiyle insan odaklı güvenlik, teknolojik egemenlik ve uluslararası iş birliği hedeflerini vurgulamaktadır (BTK, 2013). Ancak Şenol (2016) belirttiği gibi, caydırıcılığın etkinliği devletin misilleme iradesinin görünür biçimde sinyallemesine bağlıdır. Mevcut stratejik belgeler bu iradeyi her zaman yeterince açık şekilde göstermemektedir.

Hukuki çerçeve de Türkiye'nin siber caydırıcılık kapasitesinde kritik bir rol oynamaktadır. 2025'te yürürlüğe giren Siber Güvenlik Kanunu (Kanun No. 7545), USOM ve SOME'leri yasal zemine kavuşturmuş, kritik altyapı tanımını netleştirmiş ve devletin müdahale kapasitesini güçlendirmiştir. Bu düzenleme, caydırıcılığın normatif boyutunu desteklerken, aynı zamanda hukuki yaptırım ve misilleme potansiyelini güvence altına almaktadır. Bununla birlikte, mevzuatın sahada uygulanması ve özel sektörle koordinasyon hâlâ iyileştirilmesi gereken alanlardır.

İnsan kaynağı ve kapasite geliştirme açısından Türkiye, USOM'un FETİH projesi gibi programlar aracılığıyla nitelikli siber güvenlik uzmanları

yetiştirmeyi hedeflemektedir. Üniversitelerde açılan siber güvenlik bölümleri ve araştırma merkezleri, insan kaynağı eksikliğini azaltmaya yönelik stratejik adımlar olarak öne çıkmaktadır (Çakır & Taşer, 2023). Ancak hızlı değişen tehdit ortamı karşısında uzman yetiştirme kapasitesinin yeterli olup olmadığı hâlâ kritik bir sorundur.

Siber caydırıcılık stratejisinde sürdürülebilirlik, bazı yapısal sorunlarla sınanmaktadır. Gelişmiş kalıcı tehdit (APT) gruplarının stratejik sektörlerde artan etkinliği, saldırıların uzun süreli ve tespit edilemez olmasına yol açmaktadır (CISA, 2021). Tedarik zinciri bağımlılığı ise Türkiye'nin caydırıcılık kapasitesini sınırlayan en kritik faktörlerden biridir; kamu kurumları ve özel sektör büyük ölçüde yabancı menşeli yazılım, donanım ve hizmetlere bağımlıdır. Bu durum, ulusal sertifikasyon, tedarikçi şeffaflığı ve güvenilirlik denetimlerinin kurumsallaştırılmasını zorunlu kılmaktadır.

Kamu–özel sektör iş birliği de caydırıcılığın etkinliğinde belirleyici bir unsurdur. Mevcut durumda, bilgi paylaşımı, standart uyumu ve olay müdahale süreçleri hâlâ tam anlamıyla kurumsallaşmamıştır. Bu durum hem reddetme hem de misilleme temelli caydırıcılığı sınırlandırmaktadır. Buna karşın, sektör SOME'lerinin yaygınlaşması, USOM'un merkezi koordinasyon rolü ve rehberlik dokümanları önemli ilerlemeler sağlamıştır.

Politika önerileri kapsamında, Türkiye'nin stratejik caydırıcılık kapasitesini güçlendirmek için öncelikle misilleme kapasitesinin ve stratejik sinyal verme mekanizmalarının ulusal strateji belgelerinde daha görünür hâle getirilmesi gerekmektedir. USOM ve SOME'lerin teknik kapasitesinin yanı sıra yönetişim rolünün güçlendirilmesi, özel sektör ve kritik altyapı operatörleriyle stratejik bilgi paylaşımının artırılması, caydırıcılığın etkinliğini yükseltecektir. İnsan kaynağı geliştirme stratejilerinin uzun vadeli ve sürdürülebilir biçimde planlanması, özellikle üniversite-sanayi iş birliği ile siber güvenlik eğitim ve araştırma kapasitesinin artırılması da kritik önemdedir. Türkiye'nin uluslararası norm üretimi ve diplomasi yoluyla normatif caydırıcılık kapasitesini artırması, NATO, AB ve bölgesel ortaklarla iş birliği içinde siber norm inşasına aktif katkı sunması, stratejik caydırıcılığın teknik ve diplomatik boyutunu güçlendirecektir.

Türkiye'de 2024 itibarıyla kurulan Siber Güvenlik Başkanlığı (SGB), ulusal siber güvenlik politikasının teknik savunma ekseninden çıkarılarak doğrudan stratejik caydırıcılık çerçevesine yerleştirilmesi açısından kritik bir kurumsal dönüşüme işaret etmektedir. SGB'nin tesis edilmesi, Türkiye'nin siber tehditleri yalnızca operasyonel riskler olarak değil, ulusal güvenliği etkileyen ve siyasi karşılık üretilmesi gereken stratejik tehditler olarak konumlandırdığını göstermektedir. SGB'nin kuruluşu, Türkiye'nin siber güvenlik mimarisinde operasyonel savunmadan stratejik caydırıcılığa geçişin en somut kurumsal adımıdır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). Bu yeni yapıda USOM ve SOME'ler teknik olaylara müdahale ve proaktif savunmanın merkezinde kalmaya devam ederken; SGB, devletin çapraz alan karşılık opsiyonlarını yönetecek, uluslararası aktörlere stratejik sinyalizasyon üretecek ve gerektiğinde inandırıcı bir cezalandırma iradesini koordine edecek olan 'stratejik aklı' temsil edecektir. Bu yönüyle Başkanlık, daha önce ağırlıklı olarak reddetme yoluyla caydırıcılık temelinde işleyen USOM–SOME yapısını, ceza ve normatif caydırıcılık unsurlarıyla tamamlayabilecek merkezi bir yönetişim ve karar alma mekanizması sunmaktadır.

Literatürde siber caydırıcılığın en zayıf halkalarından biri olarak değerlendirilen stratejik sinyal verme ve misilleme kapasitesi, ancak bu tür üst düzey kurumsal yapılanmalar aracılığıyla inandırıcı hâle gelebilmektedir (Libicki, 2009). SGB'nin kritik altyapı güvenliği açısından önemi ise enerji, finans, sağlık ve ulaştırma gibi sektörlerde mevcut olan parçalı yönetişim yapısını bütünleştirme ve ortak güvenlik standartlarını merkezi biçimde belirleme potansiyelinden kaynaklanmaktadır (Dunn Cavelty & Suter, 2009). Bununla birlikte, Başkanlığın caydırıcılık kapasitesine gerçek anlamda katkı sunabilmesi; yetki sınırlarının netleştirilmesine, mevcut kurumlarla (USOM, BTK) koordinasyonun açık biçimde tanımlanmasına ve özel sektörle güvene dayalı bir iş birliği modelinin kurulmasına bağlıdır (Schmitt, 2017). Bu çerçevede SGB, Türkiye'nin siber alanda savunmadan caydırıcılığa geçiş sürecinin kurumsal ön koşulu olarak değerlendirilebilir.

- **Ampirik Vaka Analizi: 2015 Finans Altyapısı Saldırıları ve Reddetme Kapasitesinin Operasyonelleşmesi**

Türkiye'nin siber güvenlik mimarisinde "reddetme ağırlıklı hibrit caydırıcılık" modelinin teorik bir hedeften operasyonel bir gerçekliğe dönüşmesi, büyük ölçüde 2015 yılının sonlarında ulusal kritik altyapılara yöneltilen ve devletin siber güvenlik aygıtı için bir "stres testi" niteliği taşıyan geniş çaplı siber saldırılarla ivme kazanmıştır. 14 Aralık 2015'te Orta Doğu Teknik Üniversitesi (ODTÜ) yönetimindeki "nic.tr" sunucularını ve ardından Türkiye'deki önde gelen kamu ve özel sektör bankalarının dijital altyapılarını hedef alan, hacmi 400 Gbps seviyelerine ulaşan Dağıtılmış Hizmet Aksatma (DRDoS/DDoS) saldırıları gerçekleştirilmiştir (Ercan vd., 2021: 28). Yaklaşık 14 gün süren ve 400.000'den fazla .tr uzantılı web sitesini çevrimdışı bırakarak perakende bankacılık hizmetlerini geçici olarak durduran bu saldırılar (Freedom House, 2016), siber alandaki atıf sorununun caydırıcılık üzerindeki kısıtlayıcı etkisini somut biçimde ortaya koymuştur. Saldırının faili olarak ulusötesi hacktivist gruplar öne çıkmış görünse de, saldırının ölçeği, senkronizasyonu ve karmaşıklığı devlet destekli aktörlerin dâhilini güçlü biçimde gündeme getirmiştir (IIJ, 2016: 5).

Bu karmaşık tehdit tablosunda, failin kesin hukuki ve teknik delillerle tespit edilememesi ve tırmandırma risklerinin yüksekliği nedeniyle klasik ceza temelli bir misilleme stratejisi uygulanamamıştır. Ancak Türkiye bu asimetrik tehdide karşı, makalede çerçevesi çizilen "reddetme kapasitesini tahkim etme" stratejisini hızla devreye sokmuştur. Kriz anında USOM'un merkezi koordinasyonunda, yurt dışı kaynaklı internet trafiği geçici olarak sınırlandırılarak ve yurt içi bankacılık işlemleri Ulusal Akademik Ağ (ULAKNET) ve yerel ağlara yönlendirilerek saldırı yüzeyi daraltılmıştır (Ercan vd., 2021: 29). Bu müdahale, devletin açık bir misilleme yapamadığı durumlarda dahi, ağ segmentasyonu ve ulusal yönlendirme mekanizmalarıyla saldırganın "beklenen faydasını" ve operasyonel başarısını sıfırlayabildiğini göstermektedir.

Saldırının hemen ardından başlayan süreçte ise reddetme stratejisi, kurumsal bir bağışıklık politikasına dönüştürülmüştür. Bankacılık Düzen-

leme ve Denetleme Kurumu (BDDK) ve BTK'nın eşgüdümlü regülatif adımlarıyla finans sektörü başta olmak üzere kritik altyapı operatörlerine çok katmanlı savunma ve veri yerelleştirme standartları zorunlu kılınmıştır. Bu durum, Türkiye›nin teknik savunma araçlarını yapısal bir «regülatif caydırıcılık» unsuruna dönüştürdüğünü kanıtlamaktadır. 2015 vakası, Türkiye'nin siber uzayda dramatik bir cezalandırma tehdidinden ziyade; saldırganın maliyetini artıran, kurumsal koordinasyonu merkeze alan ve kritik altyapıların esnekliğini önceleyen hibrit caydırıcılık modelini sahada nasıl kurumsallaştırdığını açıkça teyit etmektedir.

2015 DDoS saldırıları ağ seviyesindeki reddetme kapasitesinin inşası için bir dönüm noktası olurken, 2020 sonrası dönemde siber tehdit vektörleri yön değiştirmiş; SolarWinds vakasında küresel ölçekte tecrübe edildiği gibi doğrudan tedarik zinciri zafiyetlerine ve kritik altyapı odaklı fidye operasyonlarına kaymıştır. Türkiye'nin özellikle enerji dağıtım şebekeleri (SCADA sistemleri) ve telekomünikasyon altyapılarında kullanılan donanım ve yazılımlardaki dışa bağımlılığı, Gelişmiş Kalıcı Tehdit (APT) grupları için geniş bir saldırı yüzeyi sunmaktadır. Türkiye, dışa bağımlılığın getirdiği bu asimetrik riske karşı klasik misilleme stratejileri yerine 'regülatif caydırıcılık' aracını devreye sokmuştur. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yürürlüğe konan *Bilgi ve İletişim Güvenliği Rehberi*, kritik altyapı operatörleri için veri yerelleştirmesi, kapalı ağ mimarileri ve yerli ürün kullanımını zorunlu kılarak, makalede öngörülen hibrit caydırıcılık modelinin kurumsal bağışıklık boyutunu sahada tahkim etmiştir.

4.1. Normatif Boyut ve Hibrit Caydırıcılık: Avrupa Siber Suçlar Sözleşmesi Bağlamında Türkiye

Hibrit ve çapraz alan siber caydırıcılık yaklaşımları, caydırıcılığı yalnızca askeri veya teknik kapasiteye indirgememekte; normatif çerçeve üretimini de stratejik denklemin parçası olarak değerlendirmektedir. Siber alanın sınır aşan doğası, ulusal hukukun tek başına yeterli olmadığı bir güvenlik ortamı yaratmıştır. Bu durum, siber uzayın klasik egemenlik anlayışını zorlayan bir yapıya sahip olduğunu göstermektedir (Brenner,

2006: 189). 23 Kasım 2001 tarihinde imzaya açılan Avrupa Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi), yalnızca bir ceza hukuku metni değil; uluslararası siber düzenin normatif altyapısını oluşturan temel belgelerden biri olarak değerlendirilmektedir (Nezgitli & Benzer, 2020: 10). Sözleşmenin temel amacı, taraf devletlerin maddi ceza hukuku hükümlerini uyumlaştırmak ve sınır ötesi dijital delillere hızlı erişim sağlayacak adli iş birliği mekanizmaları kurmaktır (Aliusta & Benzer, 2018: 36). Özellikle enerji, finans, sağlık ve ulaştırma gibi ulusal sınırları aşan dijital ağlara yüksek oranda bağımlı olan kritik altyapılara yönelik saldırılarda, faillerin genellikle yabancı ülkelerde konumlanması veya uluslararası vekil sunucular kullanması atıf sorununu derinleştirmektedir. Bu noktada Budapeşte Sözleşmesi'nin sunduğu 7/24 uluslararası adli iş birliği ve hızlı veri muhafazası mekanizmaları, kritik altyapı operatörlerini hedef alan sınır ötesi organize siber suç şebekelerine karşı yürütülecek caydırıcılık stratejisinin hukuki omurgasını oluşturmaktadır. Sözleşmenin en yenilikçi yönü, dijital delillerin korunması ve hızlı veri muhafazası mekanizmasını kurumsallaştırmasıdır. Bu mekanizma, klasik adli yardımlaşma süreçlerinin yavaşlığını aşarak zamanın kritik olduğu siber soruşturmalarda operasyonel etkinlik sağlamayı hedeflemektedir (Clough, 2011). Böylece sözleşme, teknik kapasite ile hukuki iş birliği arasında kurumsal bir köprü kurmaktadır. Normatif perspektiften bakıldığında, uluslararası hukuk ve norm üretimi siber caydırıcılığın meşruiyet boyutunu şekillendirmektedir. Normlar doğrudan yaptırım üretmese de, hangi davranışların kabul edilebilir olduğuna dair ortak beklenti üretir ve devletlerin karşılık verme eşiğini belirlemektedir (Finnemore & Hollis, 2016: 430). Bu yönüyle Budapeşte Sözleşmesi, normatif caydırıcılık altyapısının önemli bir bileşeni olarak işlev görmektedir. Türkiye'nin sözleşmeye katılım süreci bu normatif boyutun somut bir örneğidir. Türkiye, sözleşmeyi 10 Kasım 2010 tarihinde imzalamış; iç hukuk onay sürecini 2014 yılında tamamlayarak 29 Eylül 2014 itibarıyla bağlayıcılık kazanmasını sağlamıştır (Aliusta & Benzer, 2018: 37). Hibrit caydırıcılık perspektifinden değerlendirildiğinde, Budapeşte Sözleşmesi Türkiye'nin siber güvenlik stratejisinin normatif ayağını güçlendiren bir unsur olarak ortaya çıkmaktadır. Türkiye'nin reddetme ağırlıklı siber gü-

venlik yaklaşımı, teknik dayanıklılık kapasitesiyle birlikte uluslararası hukuki uyum ve iş birliği mekanizmaları üzerinden desteklenmektedir. Böylece caydırıcılık, yalnızca saldırının teknik olarak engellenmesi değil; aynı zamanda sınır aşan suçların uluslararası iş birliği yoluyla soruşturulabilir ve cezalandırılabilir hale getirilmesi üzerinden de üretilmektedir. Dolayısıyla Budapeşte Sözleşmesi'ne katılım, Türkiye açısından yalnızca hukuki bir uyum süreci değil; kritik altyapıları hedef alan hibrit ve çapraz alan siber caydırıcılığın normatif boyutunun kurumsallaştırılması anlamına gelmektedir. Bu durum, siber caydırıcılığın teknik, hukuki ve diplomatik araçların bütünleştiği çok katmanlı bir stratejik yapı olduğunu göstermektedir

Sonuç

Son on yılda Türkiye, kritik altyapı güvenliği ve siber caydırıcılık alanında salt teknik bir savunma anlayışından, stratejik bir ulusal güvenlik vizyonuna doğru kapsamlı bir kurumsal dönüşüm geçirmiştir. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile Sektörel Siber Olaylara Müdahale Ekipleri (SOME) etrafında şekillenen mimari, yerli siber güvenlik teknolojilerinin teşvik edilmesi ve 2025 yılında yürürlüğe giren Siber Güvenlik Kanunu, bu dönüşümün temel yapı taşlarını oluşturmuştur. Bu stratejik adımlar, enerji, finans, sağlık ve ulaştırma gibi kritik altyapı sektörlerinde asgari güvenlik standartlarını yaygınlaştırmıştır. Erken tespit, hızlı müdahale ve kurumsal koordinasyon mekanizmalarının etkinliğini artırarak Türkiye'nin reddetme yoluyla caydırıcılık kapasitesini belirgin ölçüde tahkim etmiştir.

Çalışmada kamu kurumları, kritik altyapı işletmecileri veya siber güvenlik uzmanlarıyla görüşmeler yapılmamış, ampirik saha verileri kullanılmamıştır. Ayrıca analiz, Türkiye örneği üzerine odaklandığından elde edilen sonuçların farklı ülkelerin siber güvenlik mimarilerine doğrudan genellenmesi mümkün değildir. Siber güvenlik alanının hızla değişen yapısı nedeniyle yeni hukuki düzenlemeler, kurumsal yapılanmalar ve tehdit dinamikleri gelecekte farklı değerlendirmeleri gerekli kılabilir. Bu doğrultuda ileride gerçekleştirilecek araştırmalarda karşılaştırmalı ülke analizleri-

nin yapılması, uzman görüşmelerinin ve nicel performans göstergelerinin analize dâhil edilmesi, Türkiye›nin siber caydırıcılık kapasitesinin daha kapsamlı ve çok boyutlu biçimde değerlendirilmesine katkı sağlayacaktır.

Çalışmanın ortaya koyduğu en temel bulgu; siber alanda atıf belirsizliği, gri alan rekabeti ve sürekli düşük yoğunluklu asimetrik faaliyetler gibi yapısal kısıtların, klasik ceza temelli caydırıcılık modellerini sınırlandırdığıdır. Türkiye, dayanıklılık, kurumsal koordinasyon ve seçici çapraz alan araçları üzerinden işleyen "reddetme ağırlıklı hibrit caydırıcılık" modelini benimsemiştir. Bu yaklaşım, saldırganın cezalandırılma ihtimalinden çok, saldırının başarı olasılığının ve operasyonel maliyetinin sistematik biçimde artırılmasına dayanmaktadır. Ayrıca Avrupa Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi) gibi normatif mekanizmalara entegrasyon, bu hibrit modelin diplomatik ve hukuki meşruiyet zeminini oluşturarak sınır aşan kritik altyapı tehditlerine karşı adli iş birliği kapasitesini artırmıştır. Bu kurumsal ve stratejik evrimin en güncel kırılma noktası ise Siber Güvenlik Başkanlığı'nın (SGB) kurulmasıdır. SGB, daha önce ağırlıklı olarak operasyonel düzeyde işleyen USOM–SOME modelini; politika üretimi, stratejik eşiklerin belirlenmesi ve kurumlar arası üst düzey koordinasyonla tamamlayan bir üst yönetişim katmanı olarak sisteme dâhil olmuştur. Bu yönüyle Başkanlık, Türkiye'nin siber caydırıcılık mimarisinde eksikliği hissedilen "stratejik sinyal verme" ve gerektiğinde "cezalandırma/misilleme" kapasitesinin daha görünür ve inandırıcı hâle gelmesi için gerekli doktrinel çerçeveyi sunma potansiyeline sahiptir. Orta ve uzun vadede Türkiye'nin siber caydırıcılığını daha dengeli, bütüncül ve inandırıcı bir yapıya kavuşturabilmesi için üç temel politika eksenine odaklanması gerekmektedir: Stratejik Sinyalizasyon ve Doktrin İnşası: Siber saldırılara verilecek diplomatik, ekonomik veya karşı-siber karşılıkların eşiklerini ve araçlarını net biçimde tanımlayan, dışa dönük ve tutarlı bir stratejik iletişim doktrininin oluşturulması. Tedarik Zinciri Güvenliği: Kritik altyapılarda dışa bağımlılıktan kaynaklanan sistemik kırılganlıklara karşı, ulusal donanım/yazılım sertifikasyon süreçlerinin, düzenli denetimlerin ve güvenilir tedarikçi mekanizmalarının katı bir biçimde kurumsallaştırılması. Bütünleşik Yönetişim Modeli: Kamu ve özel sektör (kritik altyapı operatörleri) arasında

yalnızca gönüllülük esasına dayanmayan, karşılıklı hukuki yükümlülükleri ve veri paylaşım standartlarını açık biçimde tanımlayan bağlayıcı bir siber güvenlik yönetişim modelinin tesis edilmesi.

Sonuç olarak, siber alanın sürekli evrilen, çok aktörlü ve dinamik doğası, caydırıcılığın statik bir durum değil, sürekli güncellenmesi gereken bir süreç olduğunu göstermektedir. Türkiye'nin "reddetme ağırlıklı hibrit caydırıcılık" yaklaşımı, misilleme kapasitesinin görünürlüğünün sınırlı olduğu veya jeopolitik nedenlerle doğrudan tırmandırmanın tercih edilmediği asimetrik çatışma ortamlarında, kapasite inşası ve yönetişim temelli alternatif bir caydırıcılık mimarisinin teorik ve pratik olarak mümkün olduğunu kanıtlamaktadır. Bu yönüyle Türkiye deneyimi, uluslararası siber güvenlik literatürüne kavramsal ve ampirik açıdan özgün bir katkı sunmaktadır.

Kaynakça

Aliusta, C., & Benzer, R. (2018). Avrupa siber suçlar sözleşmesi ve Türkiye'nin dâhil olma süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *4*(7), 35–42. https://dergipark.org.tr/tr/pub/ubgmd/article/512829.

Avrupa Konseyi. (2001). *Convention on cybercrime* (ETS No. 185). Budapeşte. https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.

Betz, D. J., & Stevens, T. (2011). Cyberspace and the changing nature of deterrence. *Journal of Strategic Studies*,https://www.researchgate.net/publication/345705816_Cyberspace_and_the_State_Toward_a_Strategy_for_Cyber-power.

Bilgi Teknolojileri ve İletişim Kurumu (BTK). (2013). *Siber olaylara müdahale ekiplerinin kuruluş, görev ve çalışmalarına dair usul ve esaslar hakkında tebliğ*. Resmî Gazete.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, *46*(4–5), 189–206. doi:10.1007/s10611-007-9063-7.

Cavelty, M. D., & Egloff, F. (2019). *The politics of cyber security*. Oxford University Press. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf,

Center for Internet Security. (2024). *Initial access brokers: How they're changing cybercrime*. CIS Report,https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime.

Clough, J. (2010). Prıncıples of Cybercrıme. Cambridge University Press. 978-1-107-03457-0.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–

52. https://doi.org/10.1016/j.maturitas.2018.04.008.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2024). *Ulusal siber güvenlik stratejisi ve eylem planı (2024–2028)*. Resmî Gazete (Sayı: 32655).

Çakır, H., & Taşer, M. (2023). Türkiye›de yapılan siber güvenlik faaliyetlerinin ve eğitim çalışmalarının değerlendirilmesi. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C*, *11*(2), 347–366. https://doi.org/10.29109/gujsc.1165131.

Creswell, J. W. (2025). *Nitel araştırma yöntemleri: Beş yaklaşıma göre nitel araştırma ve araştırma deseni* (M. Bütün, Çev.; 8. bs.). Siyasal Kitabevi.

Dunn Cavelty, M., & Suter, M. (2009). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179–187. https://doi.org/10.1016/j.ijcip.2009.08.006.

Europol. (2025). *European Union serious and organised crime threat assessment (EU-SOCTA) 2025*. Publications Office of the European Union.

Europol. (2025). *Internet organised crime threat assessment (IOCTA 2025)*. Publications Office of the European Union.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf.

FireEye. (2020). *M-Trends 2020: Insights from the front lines*. https://cloud.google.com/blog/topics/threat-intelligence/mtrends-2020-insights-from-the-front-lines/.

Fischerkeller, M. P., & Harknett, R. J. (2018). Deterrence is not a credible strategy for cyberspace. *Orbis*, *62*(3), 381–393. https://doi.org/10.1016/j.orbis.2018.05.003.

Freedman, L. (2017). *The evolution of nuclear strategy* (3. Baskı). Palgrave Macmillan.

Gartzke, E., & Lindsay, J. R. (2017). Thermonuclear cyberwar. *Journal of Cybersecurity*, *3*(1), 37–48. https://doi.org/10.1093/cybsec/tyw017.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298–303. https://doi.org/10.1016/j.clsr.2010.03.003.

Jensen, B. M., Valeriano, B., & Maness, R. C. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, *42*(2), 212–234. https://doi.org/10.1080/01402390.2018.1559152.

Kiraz, O. Z. (2021). Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri. Journal of Management Theory and Practices Research, 2(2), 69-88, https://dergipark.org.tr/tr/download/article-file/3115090.

Kolokotronis, N., & Shiaeles, S. (Ed.). (2021). *Cyber-security threats, actors, and dynamic mitigation*. Springer. ISBN: 978-0-367-43331-4.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. F. D. Kramer, S. H. Starr, & L. K. Wentz (Ed.), *Cyberpower and national security* içinde. National Defense University Press Libicki, M. C. (2009). *Cyber deterrence and cyberwar*. RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html.

Lindsay, J. R., & Gartzke, E. (2020). Politics by many other means: The comparative strategic advantages of operational domains. *Journal of Strategic Studies*, *45*(5), 727–757. https://doi.org/10.1080/01402390.2020.1768372.

Nezgitli, S., & Benzer, R. (2020). Avrupa Birliği siber güvenlik kanunu. *Journal of Information Systems and Management Research*, *2*(1), 10–17. https://dergipark.org.tr/tr/download/article-file/1186942.

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

Özbek, M. (2015). Avrupa siber suçlar sözleşmesinin Türk ceza hukukuna etkileri. *Articleletter*, 73–88, https://www.goksusafiisik.av.tr/pdf/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf.

Özker, U. (2022). *Türkiye'de kritik altyapı ve siber güvenlik*. Konrad-Adenauer-Stiftung / EDAM, https://www.kas.de/documents/283907/283956/KAS+x+EDAM_%C3%96zker_T%C3%BCrkiye%27de+Kritik+Altyap%C4%B1+ve+Siber+G%C3%BCvenlik.pdf/d9da96b2-8bdf-36d3-96d9-012b929c9a88?version=1.1&t=1669892363991.

Resmî Gazete. (2025, 19 Mart). *Siber Güvenlik Kanunu (Kanun No. 7545)*. Resmî Gazete (Sayı: 32846).

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux, ISBN 978 1 78816 074 2.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382.

Schelling, T. C. (1966). *Arms and influence*. Yale University Press, 9780300246742.

Schmitt, M. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524.

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

Şenol, M. (2016). Siber güçle caydırıcılık ama nasıl? *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *2*(2), https://dergipark.org.tr/tr/download/article-file/290469.

Trujillo, C. (2014). The limits of cyberspace deterrence. *Joint Force Quarterly*, *75*(4), 43–52, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf.

Ulusal Siber Olaylara Müdahale Merkezi (USOM). (2024). *Kurumsal yapı ve faaliyetler*. https://www.usom.gov.tr/.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190204792.001.0001.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press. doı:10.1093/oso/9780190618094.001.0001.

Vesić, S., & Bjelajac, M. (2023). Cyber security of a critical infrastructure. *Pravo – Teorija i Praksa*, *40*(2), 77–88, doı: 10.5937/ptp2302077V.

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025.

Extended Summary

The rapid acceleration of global digitalization has deepened the reliance of critical infrastructure sectors on complex information technologies, positioning cybersecurity as a paramount pillar of national security policy. Cyberspace is characterized by anonymity, minimal barriers to entry, and an asymmetric landscape featuring multiple state and non-state actors. These unique attributes render the defense of digital infrastructures substantially more complicated than conventional physical security paradigms. Furthermore, these structural complexities fundamentally impede the direct application of classical deterrence theory, historically predicated on the rational actor model and the explicit threat of punitive retaliation. Against this backdrop, the primary objective of this research is to comprehensively analyze Türkiye's cyber deterrence capabilities concerning critical infrastructure security. Employing a multidimensional perspective, this analysis is grounded in established theoretical frameworks and is contextualized through national policy documents and the nation's distinct geopolitical realities. Given its escalating digital interdependency and strategic proximity to asymmetric conflict zones, Türkiye emerges as highly vulnerable to sophisticated global cyber threats.

Theoretical Framework and Methodology

This descriptive-analytical investigation adopts a qualitative research methodology, utilizing rigorous document analysis as the principal mechanism for data collection. Core primary sources encompass the Cybersecurity Law No. 7545 (2025), the National Cybersecurity Strategy and Action Plan (2024–2028), the foundational USOM and SOME Communiqué, and the Convention on Cybercrime. Information extracted from these legislative texts underwent deductive thematic content analysis, categorized under the theoretical paradigms of punishment, denial, and normative deterrence. Acknowledging the inherent limitations of traditional deterrence literature in the digital realm the study builds its foundation on the premise that states are increasingly gravitating toward

the "deterrence by denial" model. This paradigm strategically prioritizes defensive resilience to explicitly reduce an adversary's probability of executing a successful cyber operation.

Türkiye's Cybersecurity Architecture and Hybrid Deterrence Model

Findings reveal that rather than cultivating a posture reliant on dramatic threats of direct punishment, Türkiye has embraced a "denial-oriented hybrid deterrence" model. This approach systematically elevates operational costs for potential attackers while neutralizing their likelihood of success. The model functions through a multi-layered security architecture synchronizing technical resilience, inter-agency coordination, and normative integration. The institutional foundation of Türkiye's cyber capacity revolves around the National Computer Emergency Response Team (USOM) and various Sectoral and Corporate Computer Emergency Response Teams (SOME), operating under the Information and Communication Technologies Authority (BTK). Centralized coordination by USOM operationalizes early detection and rapid intervention, systematically fortifying the denial aspect of cyber deterrence.

Moreover, the asymmetric dynamics of cyberspace have catalyzed a "cross-domain deterrence" methodology, positing that malicious cyber activities can be countered through alternative vectors like economic sanctions or legal avenues. Empirically, during the massive 2015 DDoS attacks targeting Türkiye's financial infrastructure, obscured attribution made traditional retaliation unfeasible. However, defensive entities rapidly mitigated the attack surface utilizing aggressive network segmentation, successfully converting theoretical denial capacity into operational reality. Subsequently, regulatory mandates enforcing data localization and domestic technological product utilization were instituted against Advanced Persistent Threat (APT) groups, establishing a framework of "regulatory deterrence". Parallelly, Türkiye's active participation in the Budapest Convention has bolstered the normative foundations of its cyber deterrence strategy, ensuring streamlined access to international judicial collaboration.

The Presidency of Cybersecurity (SGB) and Institutional Transformation

A pivotal milestone in Türkiye's cyber defense evolution is the establishment of the Presidency of Cybersecurity (SGB), securing its formal legal mandate via the Cybersecurity Law No. 7545 of 2025. This signifies a profound paradigm shift, elevating national cybersecurity policy from a purely technical defense focus into the broader realm of strategic deterrence. Functioning as the designated "strategic mind" of the state, the SGB orchestrates cross-domain response options, projects deliberate strategic signaling, and coordinates credible punitive postures, supplementing the USOM-SOME framework with overarching executive governance.

Conclusion and Policy Recommendations

Ultimately, the fluid configuration of the digital domain dictates that cyber deterrence demands continuous recalibration. Through its denial-oriented hybrid model, Türkiye provides robust empirical evidence that an alternative deterrence architecture is viable in asymmetric conflict scenarios where retaliatory capabilities are constrained. To ensure this strategy remains cohesive and credible, this study recommends three primary policy axes. First, the state must develop an outward-facing doctrine for strategic signaling that unambiguously delineates thresholds for counter-responses. Second, to mitigate systemic vulnerabilities from foreign technological dependencies, it is imperative to strictly institutionalize national hardware/software certification protocols and comprehensive supply chain security mechanisms. Third, the state must forge a binding, integrated governance model that clearly articulates legal obligations and mandates standardized data-sharing protocols between public sector entities and critical infrastructure operators, transitioning beyond frameworks reliant solely on voluntary cooperation.