



TİGİN

Analytical Social Sciences Journal

Analitik Sosyal Bilimler Dergisi

ISSN 3023-5391 | 4 (2) | 2026

Research Article

Received: 12.08.2026

Accepted: 25.10.2026

Çağlar Özer*

<https://orcid.org/0000-0003-3090-4740>

Türkiye'nin Siber Güvenlik Mimarisi: NATO ve BM Çerçevelerinde Uyum Stratejilerinin Karşılaştırmalı Analizi

Türkiye's Cybersecurity Architecture: A Comparative Analysis of Compliance Strategies Within NATO and UN Frameworks

Öz

Türkiye, NATO üyesi olmasına karşın her uluslararası siber güvenlik çerçevesine aynı yoğunlukta katılmamaktadır. Bu çalışma, farklılaşmanın örneğini ve olası nedenlerini 2016-2025 dönemini kapsayan nitel karşılaştırmalı vaka analiziyle incelemektedir. Analiz, NATO zirve belgelerine, Türkiye'nin BM Açık Uçlu Çalışma Grubu (OEWG) toplantılarındaki doğrudan açıklamalarına, BM Genel Sekreterliğine sunduğu ulusal katkılara, Türkiye'nin aday ülke sıfatıyla katıldığı bir Avrupa Birliği açıklamasına ve ulusal strateji ile mevzuat belgelerine uygulanan dört kategorili bir kodlama çerçevesine dayanır. Bulgular, Türkiye'nin bağlayıcı NATO çerçevesinde kurumsal üyelikler ve zirve kararlarının benimsenmesi yoluyla operasyonel uyum gösterdiğine işaret etmektedir. BM süreçlerinde katılım daha seçici ve düşük yoğunlukludur. Türkiye'nin incelenen BM açıklamaları mevcut gönüllü norm çerçevesine karşı çıkmaz; tavsiyelerin gönüllü niteliğini ve kapasite inşasını öne çıkarır. Dijital egemenlik, verinin yurt içinde tutulması ve yerli teknoloji vurgusu ise müzakere açıklamalarından çok ulusal strateji belgelerinde ve Genel Sekreterliğe sunulan 2024 tarihli ulusal katkıda belirginleşir. Çalışma bu örneği "çift katmanlı uyum" kavramıyla adlandırır ve kavramı, Acharya'nın norm yerelleştirme yaklaşımı ile Börzel ve Risse'nin uyum tipolojisini birden fazla platformun aynı anda izlendiği durumlara uyarlayan bir analitik araç olarak önerir. Belge temelli tasarım gizli müzakereleri kapsamadığından bulgular nedensel kanıt olarak değil, kuramsal beklentilerle tutarlı bir örneği olarak okunmalıdır.

Anahtar Kelimeler: Türkiye, siber güvenlik politikası, NATO, norm uyumu, dijital egemenlik, çift katmanlı uyum

* Asst. Prof. Dr., Department of Political Science and Public Administration, Faculty of Economics, Administrative and Social Sciences, Istanbul Kent University, Türkiye, caclarozer_62@hotmail.com

Citation: Özer, Ç. (2026). Türkiye'nin siber güvenlik mimarisi: NATO ve BM çerçevelerinde uyum stratejilerinin karşılaştırmalı analizi. *Tigın Analitik Sosyal Bilimler Dergisi*, 4(2), 1-22.

Copyright, License and Responsibility Statement

© 2026 The Author(s). Copyright remains with the author(s), who grant TIGİN: Analytical Social Sciences Journal (*Analitik Sosyal Bilimler Dergisi*) the right of first publication. This article is published under the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0), permitting non-commercial use, sharing, and adaptation with appropriate attribution. The author(s) retain copyright and are solely responsible for the scientific, ethical, legal, and factual content of the article.



Abstract

Although Türkiye is a NATO member, it does not engage with all international cybersecurity frameworks at the same intensity. This study examines the pattern of this differentiation and its possible drivers through a qualitative comparative case analysis covering 2016-2025. The analysis applies a four-category coding framework to NATO summit documents, Türkiye's own statements at the UN Open-Ended Working Group (OEWG), its national submissions to the UN Secretary-General, a European Union statement with which Türkiye aligned as a candidate country, and national strategy and legal documents. The findings indicate that within the binding NATO framework Türkiye displays operational compliance through institutional memberships and the endorsement of summit decisions. Its engagement in UN processes is more selective and of lower intensity. The UN statements examined do not contest the existing voluntary norm framework; they stress the voluntary character of recommendations and capacity building. Emphasis on digital sovereignty, data localization and domestic technology appears mainly in national strategy documents and in the 2024 national submission to the Secretary-General rather than in negotiating statements. The study labels this pattern "dual-layered compliance" and proposes the concept as an analytical tool that adapts Acharya's norm localization approach and Börzel and Risse's compliance typology to settings in which several platforms are engaged at once. Because the document-based design does not cover confidential negotiations, the findings should be read as a pattern consistent with theoretical expectations rather than as causal proof.

Keywords: *Türkiye, cybersecurity policy, NATO, norm compliance, digital sovereignty, dual-layered compliance*

Giriş

Siber uzay, uluslararası siyasetin dönüşümünü belirleyen başlıca alanlardan biri hâline gelmiştir. Başlangıçta sivil iletişim altyapısı olarak tasarlanan bu alan, devletlerin güç projeksiyonu yaptığı, uluslararası normların çatıştığı ve egemenlik iddialarının yeniden üretildiği bir mücadele alanına dönüşmüştür. 2007'de Estonya'ya yönelik koordineli dağıtık hizmet engelleme saldırıları, İran nükleer santrifüjlerini devre dışı bırakan Stuxnet operasyonu ve 2020 sonunda ortaya çıkan SolarWinds tedarik zinciri ihlali farklı hedeflere ve yöntemlere sahiptir. Ortak noktaları, siber araçların casusluk, sabotaj ve devlet düzeyinde baskı için elverişli bir zemin sunduğunu göstermeleridir. Kello (2017) bu ortamı *unpeace* kavramıyla tanımlar: klasik savaş eşiğinin altında kalan ama devletlere orantısız maliyet yükleyebilen bu alanda hesap verebilirlik mekanizmaları fiilen işlemez. Rid ve Buchanan'ın (2015) belirttiği gibi saldırıların belirli bir devlete atfedilmesindeki teknik ve siyasi güçlükler uluslararası hukukun yaptırım kapasitesini zayıflatır. Normatif çerçevelerin siber uzaya nasıl uygulanacağı bu yüzden kalıcı bir gerilim noktası olarak gündemde kalmaktadır.

Bu gerilim iki ayrı çok taraflı çerçevede kurumsal karşılık bulmuştur. Kuzey Atlantik Antlaşması Örgütü (NATO), 2014 Galler Zirvesi'nde siber savunmayı kolektif savunma görevinin parçası saymış ve bir siber saldırının Washington Antlaşması'nın 5. maddesini işletip işletmeyeceğine Kuzey Atlantik Konseyi'nin vaka bazında karar vereceğini belirtmiştir (NATO, 2014). 2016 Varşova Zirvesi siber uzayı operasyon alanı olarak tanımlamış (NATO, 2016), 2021 Brüksel Zirvesi'nde onaylanan Kapsamlı Siber Savunma Politikası ise önemli ve birikimli kötü niyetli siber faaliyetlerin belirli koşullarda silahlı saldırı sayılabileceğini kabul etmiştir (NATO, 2021). 2022 Stratejik Konsepti bu yaklaşımı yinelemiştir (NATO, 2022). 2024 Washington Zirvesi'nde ise Müttefik Kuvvetler Avrupa Yüksek Karargâhı (SHAPE) bünyesinde NATO Entegre Siber Savunma Merkezi'nin (NICC) kurulmasına karar verilmiştir (NATO, 2024a). Birleşmiş Milletler (BM) çerçevesinde ilerleme farklı bir tempoda gerçekleşmiştir. 2015 Hükümet Uzmanları Grubu (GGE) raporu 11 gönüllü normu uluslararası mutabakata sunmuş (BM Genel Kurulu, 2015), Açık

Uçlu Çalışma Grubu'nun (OEWG) 2021 nihai raporu bu normların uygulanmasını gündemde tutmuştur (BM Genel Kurulu, 2021a). İki çerçeve arasındaki temel ayrım bağlayıcılıkla ilgilidir: NATO üyelerini kolektif savunma yükümlülüğüyle bağlarken BM süreci gönüllülük esasına dayanır. Schmitt'in (2017) editörlüğündeki Tallinn Manual 2.0 her iki çerçevedeki hukuki belirsizliği belgelemiş ve bu belirsizliğin devletlere geniş bir yorum alanı bıraktığını göstermiştir.

Türkiye bu konjonktürde özgün bir konumdadır. 1952'den bu yana NATO üyesi olan ve İttifak'ın güneydoğu kanadında yer alan Türkiye, Rusya'dan S-400 alımı, Çin ile derinleşen ekonomik bağlar ve Körfez ülkeleriyle sürdürülen paralel güvenlik ilişkileri aracılığıyla Batılı müttefiklerinden zaman zaman ayrışan bir dış politika çizgisi izlemektedir. Bu ikilik siber güvenlik alanında da izlenebilir. Siber Güvenlik Başkanlığı 8 Ocak 2025'te 177 sayılı Cumhurbaşkanlığı Kararnamesi ile kurulmuş (177 sayılı CBK, 2025), 7545 sayılı Siber Güvenlik Kanunu 19 Mart 2025'te Resmî Gazete'de yayımlanarak yürürlüğe girmiştir (TBMM, 2025). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) yerli ve milli teknolojileri altı stratejik amaçtan biri olarak tanımlar (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024); 7545 sayılı Kanun da siber güvenliği milli güvenliğin ayrılmaz parçası sayar (TBMM, 2025). Singer ve Friedman'a (2014) göre bir devletin siber güvenlik politikasını kavramak için teknik kapasitenin yanında o politikanın nasıl çerçevelendiğine ve hangi kurumsal tercihlerle biçimlendiğine de bakmak gerekir. Sönmezoğlu'nun (2014) dış politika analizi araçlarıyla okunduğunda bu tercihler, Türkiye'nin çok yönlü dış politika anlayışının siber alandaki yansıması olarak ele alınabilir.

Bu tabloya karşın mevcut akademik literatür iki çerçeve arasındaki farklılaşmayı aynı ölçütlerle ele almamıştır. Erendor (2017), NATO-Türkiye ilişkilerini siber terörizmle mücadele ekseninde incelemiş ve tehdit algılarının normatif boyutunu ortaya koymuş, ancak BM süreçlerini kapsam dışında bırakmıştır. Uluslararası Stratejik Araştırmalar Enstitüsü (IISS, 2023), Türkiye'nin siber kapasitesini kurumsal ve teknik göstergeler üzerinden haritalamış; Türkiye'nin bu kapasiteyi uluslararası norm yapılarıyla nasıl ilişkilendirdiği sorusu ise yanıtsız kalmıştır. Borghard ve Lonergan (2017) siber zorlamanın genel mantığını çözümlerken çoklu ittifak ilişkileri olan devletlerin bu alandaki konumlanmasına değinmemiştir. Türkçe literatürde Güntay (2017) siber savaşı uluslararası sistem ve güvenlik açısından değişen savaş kurgusu içinde, Kurnaz ve Önen (2019) ise Türkiye'nin siber güvenlik stratejilerini Avrupa Birliği'ne uyum süreci bağlamında ele almıştır. Oran'ın (2022) editörlüğündeki Türk dış politikası çalışması tarihsel arka plan için, Sönmezoğlu (2014) ise dış politika analizi için kavramsal araçlar sunar. Bu çalışmaların hiçbiri Türkiye'nin iki ayrı çerçevedeki tutumunu aynı göstergelerle karşılaştırmamaktadır. Daha somut olarak, Türkiye'nin OEWG'deki kendi açıklamalarını, BM Genel Sekreterliğine sunduğu ulusal katkıları ve benimsediği NATO zirve kararlarını tek bir kodlama çerçevesiyle birlikte okuyan bir çalışmaya rastlanmamıştır. Mevcut

çalışmalar ya NATO-Türkiye ilişkisini ya da ulusal kapasiteyi tek başına incelemektedir. Bu makale bu boşluğa odaklanır.

Çalışmanın temel savına göre Türkiye, bağlayıcı NATO çerçevesinde kurumsal katılım ve zirve kararlarının benimsenmesi yoluyla operasyonel uyum gösterirken gönüllü BM sürecinde mevcut norm çerçevesini destekleyen ama katılımı düşük yoğunlukta tutan ve tavsiyelerin gönüllü niteliğini öne çıkaran bir tutum izlemektedir. Egemenlik ve yerlilik vurgusu ise ağırlıklı olarak ulusal belgelerde yer alır. Bu çalışma, söz konusu örüntünün merkezi bir siber diplomasi kararının ürünü olduğunu ileri sürmez. Örüntü, farklı kurumsal bağlamların sunduğu teşviklere tekrarlanan uyarlamalarla açıklanabilecek bir konumlanma olarak ele alınmaktadır. Çalışmaya üç araştırma sorusu yön vermektedir: Türkiye'nin NATO siber mekanizmalarına katılım düzeyi ve normatif tutumu nasıl tanımlanabilir? BM GGE ve OEWG süreçlerindeki doğrudan ve ortak açıklamalar NATO bağlamından hangi boyutlarda ayrışmaktadır? 2025 kurumsal reformları bu örüntüyü dönüştürmekte midir, yoksa pekiştirmekte midir? İkinci bölüm kuramsal çerçeveyi, üçüncü bölüm yöntemi ve tarihsel arka planı sunar. Dördüncü bölümde iki vaka incelenir, beşinci bölüm karşılaştırmalı bulguları, tartışmayı ve politika önerilerini içerir. Altıncı bölüm sonuç ve araştırma gündemine ayrılmıştır.

Kuramsal Çerçeve

Mevcut Kuramların Açıklama Kapasitesi ve Sınırlılıkları

Putnam'ın İki Düzeyli Oyun Kuramı ve Ayrışma Noktası

Uluslararası normlara devlet uyumunu açıklayan kuramsal literatür bu çalışmanın ihtiyacını ancak kısmen karşılamaktadır. Çift katmanlı uyum kavramının neden gerekli olduğunu göstermek için üç yaklaşımın açıklama gücünü ve sınırlarını belirlemek gerekir. Putnam (1988) dış politikayı iki düzey arasındaki etkileşim olarak kavramsallaştırır: devlet liderleri iç politika koalisyonlarını ve uluslararası müzakereleri eş zamanlı yönetmek zorundadır. Bu yaklaşım iç ve dış politika arasındaki bağlantıyı analizin merkezine taşır. Ne var ki model tek bir uluslararası müzakere sürecini varsayar ve bir devletin birden fazla çok taraflı çerçeveye eş zamanlı, farklılaşmış ilişki yürüttüğü durumu kavramsallaştırmaz. Çift katmanlı uyum kavramı Putnam'ın tek uluslararası düzeyini çoğullaştırır ve her platformun kendine özgü bir uyum mantığı üretip üretmediğini sorar.

Normatif Çoğulculuk ve Stratejik Seçici Katılım

Normatif çoğulculuk yaklaşımı (Berman, 2007) farklı normatif rejimlerin bir arada var olabildiğini ve aktörlerin bu rejimlerden seçici biçimde yararlandığını savunur. Yaklaşım birden fazla normatif çerçevenin aynı anda geçerli olduğu durumları çözümlemede güçlüdür, ancak farklı platformlarda gözlenen uyum örüntüsünün hangi yapısal güdülerle ortaya çıktığını açıklamaz. Stratejik seçici katılım yaklaşımı (Morse & Keohane, 2014) ise güçlü devletlerin uluslararası kurumları seçici biçimde destekleyerek ya da alternatif kurumlara yönelerek tercihlerini

gerçekleştirdiğini öne sürer. Güç asimetrisini ve forum değiştirmeyi açıklamada etkili olan bu yaklaşımın orta büyüklükteki devletler için uygulanabilirliği sınırlıdır. Türkiye NATO'dan çekilme ya da OEWG'yi işlevsizleştirme kapasitesine sahip değildir. Orta büyüklükteki devletler kurumları yeniden biçimlendirmekten çok kurumsal bağlama uyum sağlar. Çift katmanlı uyum kavramı bu uyarlamanın farklı platformlarda farklı biçimler alabileceğini ve bu farkın yapısal güdülerle ilişkilendirilebileceğini öngörür.

Yapısal Gelenek: Finnemore-Sikkink ve Acharya

Finnemore ve Sikkink (1998), norm yaşam döngüsü modelinde normların ortaya çıkış, yayılma ve içselleştirme aşamalarından geçtiğini göstermiştir. Model, devletlerin normlara tepkisinin kimlik ve meşruiyet kaygılarını da içerdiğini ortaya koyar ve yalnızca maddi çıkar hesabına dayanan açıklamalardan uzaklaşır. Acharya (2004) bu çerçeveyi norm yerelleştirmesi kavramıyla derinleştirmiştir. Asya bölgeselciligi üzerine yaptığı araştırmada yerel aktörlerin küresel normları edilgen biçimde kabul etmediğini, onları kendi tarihsel pratikleri, kimlik inşaları ve jeopolitik öncelikleriyle uyumlu hâle getirmek için seçip dönüştürdüğünü gösterir. Yerelleştirme basit bir ret değildir: norm biçimsel düzeyde kabul edilir, içerik düzeyinde dönüştürülür. Acharya'nın modeli ise tek bir platform ekseninde kurgulanmıştır ve aynı devletin birden fazla çerçevede eş zamanlı, farklı yerelleştirme pratikleri izleyip izleyemeyeceğini sorunsallaştırmaz.

Uyum Tipolojisi: Börzel, Risse ve Checkel

Börzel ve Risse (2003) Avrupa bütünleşmesi bağlamında üç uyum mekanizması tanımlar. Zorlayıcı uyumda aktör baskı karşısında davranışını değiştirir, fakat tutumu köklü biçimde dönüşmez. Normatif uyumda normlar içselleştirilir ve davranış kimliğin parçası olur. Hesaplamalı uyumda aktör normu ne içselleştirir ne de doğrudan reddeder; maliyet-fayda hesabına dayalı seçici bir tutum sürdürür. Checkel (2005) bu tipolojiyi kurumsal sosyalleşme perspektifiyle tamamlamıştır. Ona göre uzun süreli kurumsal katılım zamanla davranışsal uyumdan tercih değişimine evrilebilir, ancak bu dönüşüm kurumsal bağlamın niteliğine, aktörün kimliğine ve iç siyasi dinamiklere göre farklı yollar izler. Türkiye bağlamında bu ayrım, uzun süreli NATO üyeliğinin İttifak'ın siber savunma normlarını içselleştirdiğine kendiliğinden kanıt sayılamayacağı anlamına gelir. Hesaplamalı uyum ile normatif içselleştirme ayrımı korunduğunda yüksek operasyonel entegrasyon ile egemenlik vurgusunun aynı anda sürmesi çelişkili görünmekten çıkar.

Çift Katmanlı Uyum: Kavramın İşlevselleştirilmesi

Çift katmanlı uyum, yukarıdaki kuramsal birikime dayanan bir analitik araç olarak önerilmektedir. Kavram, bir devletin aynı politika alanında birden fazla uluslararası çerçeveye eş zamanlı ilişki yürütürken bu çerçevelerde farklı uyum biçimleri sergilemesini ve bu farkın güvenlik bağımlılığı, çerçevenin bağlayıcılık düzeyi ve iç siyasi söylemin birlikte etkisiyle biçimlenmesini ifade eder. Kavram üç unsur üzerine kuruludur. Platformlar arası tutarlılık, farklılaşmanın tek seferlik

kalmayıp incelenen dönem boyunca tekrar etmesini anlatır. Mekanizma çoğulluğu, farklılaşmanın tek bir nedene değil birden fazla yapısal etkenin etkileşimine bağlandığını gösterir. Yarı sistematiklik ise örüntünün merkezi bir koordinasyon kararından değil, kurumsal bağlamın sunduğu teşviklere tekrarlanan uyarılmalardan doğduğunu ifade eder. Sistematik bir strateji bilinçli platform ayrıştırması ve merkezi koordinasyon gerektirir; yarı sistematik konumlanmada ise aktör kurumsal bağlamın dayattığı seçici mantığı içselleştirmeden ona uyar. Yarı sistematiklik örüntünün nasıl ortaya çıktığını, çift katmanlı uyum ise nasıl bir örüntü ürettiğini anlatır.

Kavramı mevcut yaklaşımlardan ayıran şey, aynı aktörün farklı platformlardaki davranışını aynı göstergelerle ölçmesidir. Norm uyumu literatürü (Börzel & Risse, 2003; Checkel, 2005) uyumu genellikle tek bir kurum içinde sınıflandırır ve zamanla ya içselleştirmeye ya da kalıcı hesaplama uyuma doğru bir yakınsama bekler. Seçici katılım yaklaşımı (Morse & Keohane, 2014) ise aktörün tercih etmediği kurumdan uzaklaşmasını, rakip normları desteklemesini ya da alternatif bir forum aramasını öngörür. Çift katmanlı uyum bu iki beklentiden farklı gözlenebilir sonuçlar üretir. Buna göre bağlayıcı platformda kurumsal katılım yüksek olmalıdır (üyelikler, zirve kararlarının benimsenmesi, ulusal yapıların İttifak yapılarıyla eşleşmesi). Gönüllü platformda ise katılım düşük yoğunlukta kalmalı, ancak mevcut normlar açıkça reddedilmemeli ve rakip bağlayıcı araçlar desteklenmemelidir. Egemenlik ve yerlilik vurgusunun da çok taraflı müzakere açıklamalarından çok ulusal belgelerde ve ulusal raporlarda yoğunlaşması beklenir. Bu üç beklenti, Tablo 2'de tanımlanan dört kodlama kategorisi (kurumsal katılım, normatif pozisyon, politika çıktıları ve söylemsel çerçeveleme) üzerinden sınanmaktadır. Normatif uyum açıklaması doğru olsaydı iki platformda benzer bir söylem ve benzer bir katılım yoğunluğu; seçici katılım açıklaması doğru olsaydı BM'de rakip normlara destek ya da forum değiştirme girişimleri gözlenmesi beklenirdi.

Yöntem ve Tarihsel Arka Plan

Araştırma Tasarımı ve Metodolojik Gerekeçe

Bu çalışma nitel karşılaştırmalı vaka analizi tasarımını benimsemektedir. Yin (2018), çoklu vaka tasarımının birden fazla vakayı aynı analitik çerçeve içinde karşılaştırarak örüntü tanımlamaya ve kuramsal genellemeye olanak verdiğini belirtir. Gerring (2007) ise vaka analizinin bağlama bağlı süreçlerin incelenmesinde istatistiksel yöntemlerin yetersiz kaldığı durumlarda uygun bir tercih olduğunu vurgular. Burada incelenen ilişki sayısal değil söylemsel ve prosedürelidir. Karşılaştırmanın birimi, tek bir aktörün (Türkiye) iki ayrı kurumsal platformdaki davranışlarıdır. Vaka seçiminde en benzer sistemler tasarımının mantığı izlenmiştir. Aktör, konu (devletlerin siber uzaydaki davranışı) ve zaman aralığı iki vakada sabittir; temel fark kurumsal tasarımda, yani bağlayıcılık düzeyinde ve üyelik yapısındadır. Bu tasarım, gözlenen farkın aktöre ya da konuya değil platformun niteliğine bağlanıp bağlanamayacağını sorgulamaya izin verir. NATO ile OEWS üyelik, karar alma kuralları ve gündem genişliği bakımından da ayrıştığından tasarım en benzer sistemler mantığını katı biçimde

değil, yapılandırılmış ve odaklı karşılaştırma yaklaşımıyla birlikte kullanır (George & Bennett, 2005): her iki vakaya aynı sorular aynı göstergelerle yöneltilir. Zaman aralığı, NATO'nun siber uzayı operasyon alanı olarak tanıdığı 2016 Varşova Zirvesi ile Siber Güvenlik Başkanlığı'nın kurulduğu ve 7545 sayılı Kanun'un yürürlüğe girdiği 2025 yılı arasındır. Bu aralığın dışındaki gelişmeler tarihsel arka plan ya da dönem sonrası değerlendirme olarak açıkça belirtilmektedir.

Belge Seçimi, Veri Kaynakları ve Kodlama Çerçevesi

Belge seçiminde dört ölçüt uygulanmıştır: (i) 2016-2025 döneminde yayımlanmış olmak; (ii) resmî ve kamuya açık olmak, tam metnine erişilebilmek; (iii) Türkiye'nin yazarı olduğu, imzaladığı, katıldığı ya da devlet ve hükümet başkanları düzeyinde kabul ettiği bir metin olmak; (iv) siber güvenliği doğrudan konu almak ya da bu konuya ayrı bir bölüm veya paragraf ayırmak. Basında yer alan beyanlar, gizlilik dereceli belgeler ve ikincil değerlendirmeler derlem dışında tutulmuş, ikincil kaynaklar yalnızca bağlam bilgisi için kullanılmıştır. Derlemdeki belgeler üç gruba ayrılmıştır (Tablo 1). NATO grubu, Türkiye'nin de kabul ettiği zirve bildirilerini ve Stratejik Konsepti kapsar (NATO, 2016, 2021, 2022, 2023, 2024a). BM grubu, Türkiye'nin doğrudan açıklamalarını ve katkılarını ortak açıklamalardan ayırır. Doğrudan metinler Türkiye'nin Genel Sekreterlik raporlarına 2019 ve 2020'de sunduğu yanıtlar (BM Genel Kurulu, 2019, 2020), 19 Şubat 2021 tarihli OEWG gayriresmî toplantısındaki açıklama (Türkiye, 2021), 29 Mart 2022 tarihli OEWG açıklaması (Türkiye, 2022) ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin (CBDDO) 2024'te Genel Sekreterliğe sunduğu ulusal katkıdır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). Ortak metin olarak, Türkiye'nin aday ülke sıfatıyla katıldığı 13 Aralık 2021 tarihli Avrupa Birliği (AB) OEWG açıklaması incelenmiştir (Avrupa Birliği, 2021). 2015 GGE raporu ve 2021 OEWG nihai raporu (BM Genel Kurulu, 2015, 2021a) Türkiye'nin yazarı olmadığı, uzlaşıyla kabul edilen referans metinler olarak kullanılmıştır. Ulusal grup, 2016-2019, 2020-2023 ve 2024-2028 Ulusal Siber Güvenlik Stratejilerini (T.C. Ulaştırma ve Altyapı Bakanlığı, 2016, 2020, 2024), 177 ve 183 sayılı Cumhurbaşkanlığı Kararnamelerini ve 7545 sayılı Kanun'u (177 sayılı CBK, 2025; 183 sayılı CBK, 2025; TBMM, 2025) içerir. IISS (2023) ülke profili, NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'nin (CCDCOE, 2021) Türkiye siber güvenlik teşkilatı raporu ve Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK, 2023) faaliyet raporu bağlam için kullanılan tamamlayıcı ikincil kaynaklardır.

Tablo 1. İncelenen birincil belgeler

Grup	Belge	Tarih	Türkiye'nin konumu	Kaynak
NATO	Varşova Zirvesi Bildirisi	Temmuz 2016	Müttefik olarak ortak kabul	NATO (2016)
NATO	Brüksel Zirvesi Bildirisi (Kapsamlı Siber Savunma Politikası'nın onayı)	Haziran 2021	Müttefik olarak ortak kabul	NATO (2021)
NATO	2022 Stratejik Konsepti	Haziran 2022	Müttefik olarak ortak kabul	NATO (2022)

Grup	Belge	Tarih	Türkiye'nin konumu	Kaynak
NATO	Vilnius Zirvesi Bildirisi	Temmuz 2023	Müttefik olarak ortak kabul	NATO (2023)
NATO	Washington Zirvesi Bildirisi (NICC kararı)	Temmuz 2024	Müttefik olarak ortak kabul	NATO (2024a, 2024b)
BM	Genel Sekreter raporuna Türkiye yanıtı (A/74/120)	2019	Doğrudan katkı	BM Genel Kurulu (2019)
BM	Genel Sekreter raporuna Türkiye yanıtı (A/75/123)	2020	Doğrudan katkı	BM Genel Kurulu (2020)
BM	OEWG gayriresmî toplantısı, sıfır taslağa ilişkin açıklama	19 Şubat 2021	Doğrudan açıklama	Türkiye (2021)
BM	OEWG genel görüşmesinde AB açıklaması	13 Aralık 2021	Aday ülke olarak katılım (ortak açıklama)	Avrupa Birliği (2021)
BM	OEWG ikinci oturum açıklaması	29 Mart 2022	Doğrudan açıklama	Türkiye (2022)
BM	78/237 sayılı Genel Kurul kararı kapsamında ulusal katkı (CBDDO)	21 Nisan 2024	Doğrudan katkı	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2024)
Ulusal	Ulusal Siber Güvenlik Stratejileri (2016-2019, 2020-2023, 2024-2028)	2016, 2020, 2024	Yazar	T.C. Ulaştırma ve Altyapı Bakanlığı (2016, 2020, 2024)
Ulusal	177 ve 183 sayılı CBK; 7545 sayılı Kanun	Ocak-Mart 2025	Yazar	177 sayılı CBK (2025); 183 sayılı CBK (2025); TBMM (2025)

Not: BM grubundaki belge sayısı, bu çalışmanın derlemine gösterir; Türkiye'nin BM süreçlerine toplam katılımını değil. Kamuya açık arşivlere girmemiş açıklamalar derlemde yer almamaktadır.

Analizde içerik analizi ile süreç izleme birlikte kullanılmıştır. İçerik analizinin birimi, belgelerde siber güvenliğe ilişkin her paragraftır. Paragraflar Tablo 2'deki dört kategoriye göre kodlanmıştır. Kategoriler kuramsal çerçeveden tümdengelimli olarak türetilmiş, ilk okumada belirlenen kodlar ikinci okumada tüm belgelere yeniden uygulanarak tutarlılık açısından gözden geçirilmiştir. Söylemsel çerçeveleme kategorisinde üç kavram kümesi izlenmiştir: kolektif savunma, birlikte çalışabilirlik ve İttifak dayanışması; uluslararası hukuk, gönüllü normlar ve kapasite inşası; egemenlik, verinin yurt içinde tutulması ve yerli teknoloji. Her belge için hangi kümenin baskın olduğu ve kümenin belgede hangi işlevle kullanıldığı kaydedilmiştir. Süreç izleme, politika kararlarının kronolojik sırasını (Tablo 1) ve bu kararların ardındaki mekanizmaları belgeler arası karşılaştırmayla izler. Bulgular bölümünde her değerlendirme dayandığı belgeye bağlanmıştır (Tablo 3). Çalışmanın temel sınırlılığı, gizli diplomatik müzakerelerin ve kapalı oturum içeriklerinin analiz dışında kalmasıdır. Bu durum özellikle nedensel mekanizmalara ilişkin çıkarımları sınırlar; bu nedenle beşinci bölümdeki açıklayıcı faktörler kanıtlanmış nedenler olarak değil, gözlenen örüntüyle tutarlı açıklamalar olarak sunulmaktadır.

Tablo 2. Kodlama çerçevesi

Kategori	Göstergeler	Örnek kodlar
Kurumsal katılım	Üyelikler; zirve kararlarının kabulü; ulusal yapıların İttifak yapılarıyla eşleşmesi; BM'de doğrudan açıklama ve katkı sayısı; ortak açıklamalara katılım	CCDCOE sponsor ülke; OEWG açıklaması; Genel Sekreterlik raporuna yanıt
Normatif pozisyon	Mevcut normlara destek; çekince; yeniden yorumlama; gönüllülük vurgusu; yeni bağlayıcı araç talebi	gönüllü niteliğin memnuniyetle karşılanması; BM çerçevesinin uygulanmasına destek

Kategori	Göstergeler	Örnek kodlar
Politika çıktıları	Yasal düzenleme; kurumsal karar; strateji amaçları	7545 sayılı Kanun; 177 ve 183 sayılı CBK; 2024-2028 stratejik amaçları
Söylemsel çerçeveleme	Kavram kümeleri: (a) kolektif savunma ve birlikte çalışabilirlik; (b) uluslararası hukuk, gönüllü normlar ve kapasite inşası; (c) egemenlik, veri yerelliği ve yerli teknoloji	Baskın küme ve kullanıldığı işlev

Türkiye'nin Siber Güvenlik Politikasının Tarihsel Gelişimi

Türkiye'nin siber güvenlik politikasının kurumsal gelişimi dört dönem üzerinden ele alınmaktadır. Dönemleştirme, politikanın hangi konjonktürlerde ve hangi güdülerle biçimlendiğini göstermek ve dördüncü bölümdeki vaka analizine tarihsel bir zemin sağlamak amacını taşır. İlk iki dönem inceleme aralığından önceye düşer ve yalnızca arka plan olarak kullanılmaktadır.

İlk Dönem: Teknik Altyapıdan Politika Aracına (2000-2010)

2000-2010 arasında siber güvenlik, ulusal güvenlik politikasının bağımsız bir bileşeni olarak değil, bilgi toplumuna geçişin teknik bir alt başlığı olarak ele alınmıştır. 2007'de yürürlüğe giren 5651 sayılı Kanun bu dönemin temel yasal adımıdır. Akdeniz ve Altıparmak (2008), kanunun internet yönetişimini güvenlik ekseninden çok içerik kısıtlama ekseninde kurguladığını belgelemiştir. 2010'daki Milli Güvenlik Kurulu kararı ise siber tehditlerin milli güvenlik boyutunu ilk kez açıkça tanımış ve sonraki kurumsallaşmanın zeminini hazırlamıştır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024).

Kurumsallaşma Dönemi (2010-2018)

2010-2018 arası kurumsallaşmanın hız kazandığı dönemdir. 2012 tarihli Bakanlar Kurulu Kararı ile Siber Güvenlik Kurulu oluşturulmuş, 2013-2014 Ulusal Siber Güvenlik Stratejisi ile Ulusal Siber Olaylara Müdahale Merkezi (USOM) BTK bünyesinde faaliyete geçmiştir. Türk Silahlı Kuvvetleri bünyesinde 2012'de kurulan Siber Savunma Merkezi daha sonra Siber Savunma Komutanlığı'na dönüştürülmüştür (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). 2016-2019 stratejisi proaktif savunma ve caydırıcılık yönelimini benimsemiştir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2016). Aynı yıl NATO Varşova Zirvesi siber uzayı operasyon alanı ilan etmiş ve zirve bildirisi Türkiye dahil tüm müttefiklerce kabul edilmiştir (NATO, 2016). Türkiye, Kasım 2015'te CCDCOE'ye sponsor ülke olarak katılmıştır (CCDCOE, 2021). Oran'ın (2022) belgelediği çok yönlülük geleneği bu dönemde siber alanda da sürmüş, Türkiye İttifak kanallarını kullanırken NATO dışı ortaklarla ikili güvenlik ilişkilerini de geliştirmiştir.

Yeniden Yapılanma ve Pekişme (2018-2024)

2018'de cumhurbaşkanlığı hükümet sistemine geçiş siber güvenlik yönetişimini köklü biçimde değiştirmiştir. 703 sayılı Kanun Hükmünde Kararname ile Siber Güvenlik Kurulu kaldırılmış, siber güvenlik projelerini geliştirme görevi CBDDO'ya verilmiştir. 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi kritik verilerin yurt içinde saklanması öngörmüş,

CBDDO 2020'de Bilgi ve İletişim Güvenliği Rehberi'ni yayımlamıştır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). 2024-2028 stratejisi altı stratejik amaçtan beşincisini yerli ve milli teknolojilerin geliştirilmesine ayırmış, uluslararası iş birliğini ise ayrı bir amaç olarak tanımlamıştır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024). Ünal'ın (2022) değerlendirmesine göre bu dönemde dijital güvenlik politikaları altyapı koruması ile teknolojik bağımsızlık ekseninde birlikte kurgulanmıştır. S-400 alımının yarattığı İttifak içi güven bunalımının teknik iş birliği kanallarını dolaylı biçimde etkilemiş olması muhtemeldir; Smeets (2022) siber kuvvet geliştirme üzerine genel düzeyde, formel katılım sürse bile ittifak içi güvenin teknik bilgi paylaşımının derinliğini belirlediğini gösterir. Türkiye özelinde bu etkiyi doğrudan belgeleyen açık bir kaynak bulunmadığından değerlendirme bir olasılık olarak kaydedilmektedir.

2025 Sonrası Yeni Evre

2025 yılı Türkiye'nin siber güvenlik politikasında niteliksel bir dönüşümün yılıdır. 8 Ocak 2025'te 177 sayılı Cumhurbaşkanlığı Kararnamesi ile Cumhurbaşkanlığına bağlı, özel bütçeli Siber Güvenlik Başkanlığı kurulmuştur (177 sayılı CBK, 2025). 12 Mart 2025'te kabul edilen 7545 sayılı Siber Güvenlik Kanunu 19 Mart 2025'te yayımlanarak Başkanlığın görev ve yetkilerini düzenlemiş, siber güvenliği milli güvenliğin ayrılmaz parçası olarak tanımlamıştır (TBMM, 2025). 28 Mart 2025'te yayımlanan 183 sayılı Cumhurbaşkanlığı Kararnamesi ile CBDDO kapatılmış, kamunun dijital dönüşümüne ilişkin görevler Siber Güvenlik Başkanlığı'na eklenmiştir (183 sayılı CBK, 2025). Babaoğlu (2025) bu reformların siber güvenliği bir savunma mekanizmasının ötesinde ulusal kimliğin bileşeni olarak kurguladığını ileri sürer. Tarihsel izlek iki paralel eksen gösterir: NATO çerçevesiyle derinleşen kurumsal entegrasyon ve ulusal belgelerde güçlenen dijital egemenlik vurgusu. Bu iki eksen çift katmanlı uyumun tarihsel zeminidir.

Vaka Analizleri

NATO Siber Güvenlik Çerçevesinde Türkiye

NATO'nun Kurumsal Çerçevesinin Evrimi

NATO'nun siber savunma alanındaki kurumsal temeli, 2007 Estonya saldırılarının ardından 2008'de onaylanan ilk siber savunma politikası ve aynı yıl Tallinn'de kurulan CCDCOE ile atılmıştır. Healey (2013) bu sürecin 20 yılı aşan siber çatışma deneyiminin kurumsal karşılığı olduğunu tarihsel perspektiften belgeler. 2014 Galler Zirvesi siber savunmayı kolektif savunma görevinin parçası saymış ve 5. maddenin bir siber saldırı karşısında işletilip işletilmeyeceğine Kuzey Atlantik Konseyi'nin vaka bazında karar vereceğini belirtmiştir (NATO, 2014). 2016 Varşova Zirvesi siber uzayı operasyon alanı olarak tanımlamış ve müttefikler Siber Savunma Taahhüdü'nü kabul etmiştir (NATO, 2016). 2021 Brüksel Zirvesi'nde onaylanan Kapsamlı Siber Savunma Politikası siyasi, askerî ve teknik boyutları birlikte ele alır. Politikanın tam metni kamuya açık olmadığından bu çalışmada politika, onaylandığı Brüksel Zirvesi Bildirisi üzerinden incelenmiştir. Bildiri, önemli ve

birikimli kötü niyetli siber faaliyetlerin belirli koşullarda silahlı saldırı sayılabileceğini kabul eder (NATO, 2021). 2022 Stratejik Konsepti, tekil ya da birikimli kötü niyetli siber faaliyetlerin silahlı saldırı düzeyine ulaşarak 5. maddenin işletilmesine yol açabileceğini yinelemiştir (NATO, 2022). Rid ve Buchanan'ın (2015) gösterdiği atıf güçlükleri bu ilkenin uygulanmasını zorlaştırır ve müttefiklere fiilî bir yorum alanı bırakır. 2023 Vilnius Zirvesi'nde siber savunmanın caydırıcılık ve savunma duruşuna katkısını artıran yeni bir kavram onaylanmış, Sanal Siber Olay Destek Kapasitesi (VCISC) kabul edilmiştir (NATO, 2023). 10 Temmuz 2024'te Washington Zirvesi'nde ise SHAPE bünyesinde NICC'nin kurulması kararlaştırılmış, merkezin yapısı ve işlevlerinin sonraki aylarda belirleneceği açıklanmıştır (NATO, 2024a, 2024b).

Kurumsal Katılım Göstergeleri

Türkiye'nin NATO siber çerçevesindeki kurumsal katılımı üç gösterge üzerinden değerlendirilebilir. Kurumsal üyelik açısından Türkiye Kasım 2015'ten bu yana CCDCOE'nin sponsor ülkesidir (CCDCOE, 2021). Sponsor ülke statüsü, merkezin araştırma, eğitim ve tatbikat faaliyetlerine katılım ve yönlendirme komitesinde temsil imkânı verir. Zirve kararlarının benimsenmesine bakıldığında, incelenen dönemdeki beş zirve belgesinin (Tablo 1) siber savunmaya ilişkin hükümleri Türkiye dahil tüm müttefiklerce uzlaşıyla kabul edilmiştir. Bu belgelerin hiçbirinde Türkiye'nin siber hükümlere çekince koyduğuna dair kamuya açık bir kayıt bulunmamaktadır. Ulusal yapıların İttifak yapılarıyla eşleşmesi bakımından ise Türk Silahlı Kuvvetleri bünyesindeki Siber Savunma Komutanlığı ve BTK bünyesindeki USOM, NATO muhataplarıyla teknik iş birliğinin ulusal karşılıklarıdır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024; IISS, 2023). Tatbikat katılımı ve teknik bilgi paylaşımının yoğunluğu ise kamuya açık birincil belgelerde düzenli olarak raporlanmadığından bu çalışmada nicel bir gösterge olarak kullanılmamıştır. Erendor'un (2017) belirttiği gibi Türkiye'nin İttifak siber mekanizmalarına katılımı yalnızca dışsal baskıyla açıklanamaz; Türkiye'nin tehdit algısı bu katılımı kendi başına rasyonel kılmaktadır.

Normatif Pozisyon ve Gerilim Alanları

Normatif pozisyon boyutunda Türkiye NATO belgelerine uyumlu bir tutum sergilemektedir. Vilnius Zirvesi Bildirisi'nin siber güvenliğe ilişkin hükümleri Türkiye dahil müttefik devlet ve hükümet başkanlarınca kabul edilmiştir (NATO, 2023). Uluslararası hukukun siber operasyonlara uygulanabilirliği ilkesine karşı resmî bir itiraz kaydı bulunmamaktadır; bu tutum, Keskin'in (1998) çerçevesini çizdiği kuvvet kullanımına ilişkin uluslararası hukuk anlayışıyla tutarlıdır. Gerilim alanları da göz ardı edilmemelidir. S-400 alımı nedeniyle F-35 programından çıkarılma İttifak içinde bir güven sorunu yaratmıştır. Smeets'in (2022) genel düzeyde gösterdiği gibi ittifak içi güven teknik bilgi paylaşımının derinliğini etkiler. Bu kırılmanın siber koordinasyona nasıl yansıdığı kamuya açık belgelerle doğrudan izlenememektedir. Çalışma bu nedenle normatif uyumu belgelenmiş bir olgu, koordinasyon derinliğindeki olası etkileri ise doğrulanmamış bir olasılık olarak ele almaktadır.

2025 Reformlarının NATO Uyumuna Etkisi

2025 reformlarının NATO uyumuna etkisi iki yönde işleyebilir. Siber Güvenlik Başkanlığı'nın kurulmasıyla oluşturulan tek çatı yapısı, dağınık kurumlar arası koordinasyonun yarattığı bilgi kopukluklarını azaltabilir ve İttifak muhatapları için belirgin bir iletişim noktası sunar. Öte yandan kamu kurumlarında ve kritik altyapılarda kullanılacak siber güvenlik ürünlerinin Başkanlıkça yetkilendirilmiş sağlayıcılardan tedarik edilmesini öngören düzenleme (TBMM, 2025) ile yerli teknoloji amacı, NATO birlikte çalışabilirlik standartlarıyla uyum gerektiren alanlarda yeni ayarlamalar gerektirebilir. Drezner'in (2019) silahlaştırılmış karşılıklı bağımlılık çerçevesiyle okunduğunda teknolojik bağımsızlaşma meşru bir ulusal hedeftir, ancak müttefik sistemlerle teknik uyumu sınırlama riski taşır. İnceleme döneminin sonunda bu gerilimin pratikte nasıl çözüleceğini gösteren bir kamu belgesi bulunmamaktadır.

BM Siber Güvenlik Çerçevesinde Türkiye

BM'nin Norm Mimarisi: GGE'den Küresel Mekanizmaya

BM'de siber güvenlik norm geliştirme süreci, Rusya'nın 1998'de Birinci Komite'ye sunduğu karar tasarısıyla başlamıştır. GGE sınırlı sayıda devletin katılımına açık bir uzman grubu olarak çalışmış, 2013 raporu uluslararası hukukun siber uzayda uygulanabilirliğini teyit etmiş, 2015 raporu 11 gönüllü normu uzlaşıyla kabul etmiştir (BM Genel Kurulu, 2015). Korzak (2021) GGE sürecindeki jeopolitik kırımları belgeler: Rusya yeni bağlayıcı araçlar talep ederken Batılı devletler mevcut çerçevenin korunmasını savunmuştur. Bu ayrışma, 2018'de 73/27 sayılı kararla kurulan ve tüm üye devletlere açık olan OEWG'ye de taşınmıştır. Çakmak'ın (2014) BM kurumsal yapısına ilişkin çözümlemesinin işaret ettiği gibi katılımın genişlemesi meşruiyeti artırırken uzlaşi üretmeyi güçleştirir. İlk OEWG'nin 2021 nihai raporu GGE normlarının uygulanmasını merkeze almış (BM Genel Kurulu, 2021a), aynı yıl altıncı GGE de raporunu uzlaşıyla kabul etmiştir (BM Genel Kurulu, 2021b). İkinci OEWG 2021-2025 döneminde çalışmış ve nihai raporunda kalıcı bir Küresel Mekanizma kurulmasını kararlaştırmıştır. İnceleme döneminin dışında kalan bir gelişme olarak bu mekanizmanın örgütlenme oturumu 30-31 Mart 2026'da New York'ta yapılmıştır (Geneva Internet Platform, 2026).

Kurumsal Katılım Düzeyi ve Ölçütler

Türkiye'nin BM siber güvenlik süreçlerine katılımı NATO çerçevesine göre daha seçici ve düşük yoğunluklu bir görünüm sergilemektedir. Bu değerlendirme dört ölçüte dayanır. Uzman gruplarındaki temsil açısından Türkiye 2019-2021 GGE'nin 25 üyesi arasında yer almamıştır (BM Genel Kurulu, 2021b). Derlemde Türkiye'nin OEWG'de kendi adına yaptığı iki doğrudan açıklama bulunmaktadır (Türkiye, 2021, 2022). Yazılı katkılar bakımından Türkiye Genel Sekreterlik raporlarına 2019 ve 2020'de yanıt vermiş (BM Genel Kurulu, 2019, 2020), 2024'te CBDDO aracılığıyla ayrıntılı bir ulusal katkı sunmuştur (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024).

Ortak açıklamalar kategorisinde ise Türkiye 13 Aralık 2021'de AB açıklamasına aday ülke olarak katılmıştır (Avrupa Birliği, 2021). Bu sayılar derlemin kapsamını yansıtır ve Türkiye'nin BM'deki toplam diplomatik faaliyetine eşitlenmemelidir. Yine de NATO'daki sürekli kurumsal üyelik ve her zirvede yenilenen ortak taahhütlerle karşılaştırıldığında BM'deki katılımın aralıklı olduğu söylenebilir. IISS (2023) de Türkiye'nin bu alanda güçlü bir siber diplomasi profili geliştirmediğini saptamaktadır. Bu farkın üç olası açıklaması vardır: Dışişleri Bakanlığı'nın aynı anda birden fazla öncelikli gündemi yönetmesinin yarattığı kapasite kısıtı; NATO'nun sağladığı güvenlik güvencesinin BM'de daha etkin bir konum kazanma teşvikini azaltması; ittifak temelli güvenlik tercihi. Son açıklama, Taşpınar'ın (2008) Türk dış politikasında ittifak temelli güvenlik anlayışı ile bölgesel açılım arayışının birlikte var olduğuna ilişkin çözümlemesiyle uyumludur.

Söylemsel Çerçeveleme: Doğrudan ve Ortak Açıklamalar

Söylemsel çerçeveleme analizinde doğrudan ve ortak açıklamalar ayrı okunmuştur. Türkiye'nin 19 Şubat 2021 tarihli doğrudan açıklaması OEWG sıfır taslağını dengeli bulmuş, uzlaşi ruhunun korunmasını istemiş ve raporda tavsiyelerin gönüllü niteliğine yapılan vurguyu memnuniyetle karşıladığını belirtmiştir. Metindeki tek somut değişiklik önerisi, terör amaçlı kullanım ifadesinin internetle sınırlı tutulmayıp bilgi ve iletişim teknolojilerini kapsayacak biçimde genişletilmesidir (Türkiye, 2021). 29 Mart 2022 tarihli açıklama ise uluslararası hukuka, BM Şartı'na, uluslararası insancıl hukuka ve insan hakları hukukuna saygıyı, GGE'ler eliyle geliştirilen BM sorumlu devlet davranışı çerçevesinin etkin uygulanmasını, Ukrayna'ya yönelik saldırganlıkta siber araçların kullanılmasının reddini, Ulusal Uygulama Anketi önerisine desteği ve küresel temas noktası ağının kurulmasını içerir (Türkiye, 2022). Her iki doğrudan açıklamada da egemenlik, veri yerelliği ya da yerli teknoloji kavramları kullanılmamaktadır. Türkiye'nin aday ülke sıfatıyla katıldığı 13 Aralık 2021 tarihli AB açıklaması da mevcut GGE ve OEWG tavsiyeleri üzerinden ilerlemeyi ve 11 normun uygulanmasını önerir (Avrupa Birliği, 2021). Bu ortak metin Türkiye'nin kendi sözü olarak değil, katıldığı bir tutum olarak kodlanmıştır. Egemenlik ve yerlilik kümesi ise Genel Sekreterliğe sunulan 2024 tarihli ulusal katkıda belirginleşir. Bu metin verinin ülke içinde tutulmasını ve kaynağı ile hedefi yurt içinde olan veri trafiğinin ülke içinde kalmasını stratejik hedefler arasında sayar, yerli siber güvenlik teknolojilerinin geliştirilmesini milli güvenlik meselesi olarak tanımlar. Aynı metin uluslararası standartlarla uyumu ve AB'nin NIS2 direktifinin dikkate alınmasını da hedefler arasında anar (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). Bu belgeler birlikte okunduğunda ayrışmanın NATO ile BM arasındaki basit bir söylem karşıtlığı olmadığı görülür. BM'deki müzakere açıklamaları mevcut normatif çerçeveye uyumludur; farklılaşma, katılımın yoğunluğunda, gönüllülüğe yapılan vurguda ve egemenlik odaklı anlatının müzakere masasından çok ulusal raporlama kanalında dile getirilmesinde ortaya çıkmaktadır. Sönmezoglu'nun (2014) iç ve dış

politika etkileşimine ilişkin çerçevesi bu ayrımı anlamaya yardım eder: 2024-2028 stratejisinde kurumsallaşan yerlilik amacı, ulusal raporlama metninin dilini biçimlendirmektedir.

Gerilim Alanları ve Yapısal Çelişkiler

Türkiye'nin BM çerçevesindeki tutumunda üç gerilim alanı belirlenmiştir. İlk gerilim, gönüllülük tercihi ile daha ileri uygulama beklentileri arasında ortaya çıkar. Türkiye 2021'de tavsiyelerin gönüllü niteliğini öne çıkarırken katıldığı AB açıklaması mevcut normların uygulanmasının güçlendirilmesini talep etmiştir (Türkiye, 2021; Avrupa Birliği, 2021). İki tutum çelişmez, ancak Türkiye'nin taahhüt düzeyini esnek tutma tercihini gösterir. Veri yerelliği ile serbest veri akışı arasındaki karşıtlık ikinci gerilim alanını oluşturur. 2024 ulusal katkısındaki veri yerelliği hedefi (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024), AB'nin açık internet ve serbest veri akışı vurgusundan farklı bir önceliği yansıtır. Egemenlik vurgusunun Rusya ve Çin'in BM'deki pozisyonlarıyla örtüştüğü ileri sürülebilir, ancak Türkiye'nin 2022 açıklamasında Ukrayna'ya yönelik siber saldırganlığı açıkça reddetmesi ve mevcut BM çerçevesini desteklemesi (Türkiye, 2022) bu örtüşmenin sınırlı kaldığına işaret eder. Son gerilim alanı, inceleme dönemi sonrasında ortaya çıkan bir baskıyla ilgilidir. 2026'da çalışmaya başlayan Küresel Mekanizma (Geneva Internet Platform, 2026) devletlerden düzenli ve daha görünür bir katılım bekleyen kalıcı bir forum olduğundan Türkiye'nin aralıklı katılım örüntüsünün sürdürülebilirliğini sorgulatabilir. Bu son değerlendirme 2016-2025 bulgularının bir parçası değil, dönem sonrasına ilişkin bir öngörüdür.

Bulgular, Tartışma ve Politika Önerileri

Dört Boyutun Karşılaştırmalı Değerlendirmesi

Dört boyut iki vakaya aynı biçimde uygulandığında Tablo 3'teki tablo ortaya çıkmaktadır. Kurumsal katılım boyutunda Türkiye NATO'da CCDCOE sponsor ülke statüsü, zirve kararlarının uzlaşısıyla kabulü ve İttifak yapılarıyla eşleşen ulusal birimler aracılığıyla sürekli bir katılım göstermektedir. BM'de ise derlemdeki katılım iki doğrudan açıklama, üç yazılı katkı ve bir ortak açıklamadan oluşur ve GGE üyeliği bulunmamaktadır. Normatif pozisyon boyutunda iki platformda da mevcut çerçeveye açık bir itiraz yoktur; BM'de buna gönüllülük vurgusu eklenir. Politika çıktıları boyutunda 2025 reformları her iki platform için de ortak bir muhatap yapı oluşturur. En belirgin fark söylemsel çerçeveleme boyutundadır, ancak bu fark beklendiği gibi NATO ile BM müzakere açıklamaları arasında değil, çok taraflı açıklamalar ile ulusal belgeler arasında ortaya çıkar. NATO belgelerinde kolektif savunma ve birlikte çalışabilirlik kümesi, Türkiye'nin BM müzakere açıklamalarında uluslararası hukuk, gönüllü normlar ve kapasite inşası kümesi baskındır. Egemenlik, veri yerelliği ve yerli teknoloji kümesi ise 2024-2028 stratejisinde ve Genel Sekreterliğe sunulan 2024 ulusal katkısında yoğunlaşır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024; Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). Bu dağılım incelenen dönem boyunca

tutarlıdır, fakat belge sayısının sınırlı olduğu ve gizli müzakerelerin kapsam dışında kaldığı göz önünde tutulmalıdır.

Tablo 3. Dört boyutta NATO ve BM karşılaştırması

Boyut	NATO	BM (GGE/OEWG)	Dayanak belgeler
Kurumsal katılım	Sürekli: CCDCOE sponsor ülke (2015'ten beri); beş zirve belgesinin kabulü; eşleşen ulusal birimler	Aralıklı: iki doğrudan açıklama, üç yazılı katkı, bir ortak açıklama; 2019-2021 GGE üyeliği yok	CCDCOE (2021); NATO (2016, 2021, 2022, 2023, 2024a); Türkiye (2021, 2022); BM Genel Kurulu (2019, 2020, 2021b)
Normatif pozisyon	Zirve hükümlerine itiraz kaydı yok	Mevcut BM çerçevesine destek; gönüllü niteliğe vurgu; yeni bağlayıcı araç talebi yok	NATO (2023); Türkiye (2021, 2022)
Politika çıktıları	Siber Güvenlik Başkanlığı İttifak için tek muhatap; yetkilendirilmiş tedarik kuralı uyum gerektirebilir	Ulusal katkıda yeni kurumsal yapı ve mevzuat hazırlığı aktarılır	177 sayılı CBK (2025); TBMM (2025); Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2024)
Söylemsel çerçeveleme	Kolektif savunma ve birlikte çalışabilirlik kümesi	Müzakere açıklamalarında uluslararası hukuk, norm ve kapasite kümesi; ulusal katkıda egemenlik, veri yerelliği ve yerli teknoloji kümesi	NATO (2021, 2023); Türkiye (2022); Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2024); T.C. Ulaştırma ve Altyapı Bakanlığı (2024)

Temel Bulgular

Analiz üç bulgu ortaya koymaktadır. Birinci bulgu kurumsal katılım asimetrisidir. Türkiye NATO'da sürekli, BM'de aralıklı ve düşük yoğunluklu bir katılım göstermektedir. Bu fark yalnızca kaynak kısıtıyla açıklanamayabilir; mevcut güvenlik yapısının sunduğu teşviklerin de etkili olması muhtemeldir. İkinci bulgu, söylemsel farklılaşmanın kanal düzeyinde ortaya çıkmasıdır. Türkiye'nin BM'deki müzakere açıklamaları mevcut normatif çerçeveye uyumludur ve egemenlik kavramlarını içermez; egemenlik ve yerlilik vurgusu ulusal strateji belgelerinde ve ulusal raporlama metninde yer alır. Çift katmanlı uyumun ikinci katmanı bu nedenle müzakere söyleminde değil, uygulama ve ulusal raporlama düzeyinde yer alır. Üçüncü bulgu 2025 reformlarının bu örüntüyü dönüştürmekten çok pekiştirdiğidir. Reformlar hem İttifak'la teknik koordinasyonu kolaylaştırabilecek tek bir muhatap yaratmakta hem de yerli tedarik ve veri yerelliği hedeflerine kurumsal bir taşıyıcı sağlamaktadır.

Açıklayıcı Faktörler

Örüntüyle tutarlı üç yapısal etken belirlenmiştir. Bunlar belgelerden doğrudan kanıtlanmış nedenler değil, gözlenen örüntüyü en iyi açıklayan aday mekanizmalardır. Bunların başında güvenlik bağımlılığı gelir. NATO'nun kolektif savunma taahhüdü ve kapasite paylaşımı imkânları Türkiye için operasyonel uyumun güçlü bir gerekçesidir. Nye'in (2010) siber güç çerçevesiyle okunduğunda bu bağımlılık İttifak normlarına direnmenin maliyetini yükseltir. Jeopolitik çoğulculuk ikinci etkidir. Rusya ve Çin ile sürdürülen paralel ilişkiler, BM'de taahhüt düzeyini esnek tutma tercihinin açıklayabilir. Oran'ın (2022) belgelediği çok yönlülük geleneği bu dinamiğin siber alanda da sürdüğü yorumunu destekler. Ancak Türkiye'nin 2022'de mevcut BM çerçevesini açıkça desteklemesi, bu

esnekliğin rakip bir norm koalisyonuna yaklaşma biçiminde değil, taahhüt düzeyini sınırlama biçiminde işlediğini göstermektedir. Son etken iç siyasi söylemdir. Dijital egemenlik vurgusunun savunma sanayii öncelikleriyle birleşmesi bu vurguyu iç politikada meşrulaştırır ve ondan uzaklaşmanın maliyetini artırır. Bu üç etkenin birlikte varlığı, örüntünün kısa vadede değişme olasılığının düşük olduğuna işaret eder. Etkenlerin göreceli ağırlığı ise karar süreçlerine ilişkin birincil veri olmadan belirlenmemektedir.

Kuramsal Geri Bildirim

Bulgular Acharya'nın (2004) norm yerleştirme yaklaşımını kısmen destekler ve genişletir; Börzel ve Risse'nin (2003) hesaplamalı uyum kategorisini de çok platformlu bir bağlama taşır. Türkiye'nin BM normlarına yaklaşımı biçimsel kabul ile ulusal uygulamada yerleştirmenin birlikte görüldüğü bir yerleştirme örüntüsüyle örtüşür: norm metinlerine destek verilir, uygulama ise ulusal öncelikler doğrultusunda veri yerelliği ve yerli teknoloji hedefleriyle biçimlendirilir. NATO'daki davranış ağırlıklı olarak hesaplamalı uyumun izlerini taşır: İttifak'ın sağladığı güvenlik faydaları operasyonel entegrasyonu gerekçelendirir, ancak tam normatif içselleştirmenin gerçekleştiğine dair belgesel kanıt bulunmamaktadır. Bulgular seçici katılım yaklaşımının öngördüğü forum değiştirme ya da rakip normlara destek davranışını da göstermemektedir. Çift katmanlı uyum, bu iki kuramsal kaynağı aynı devletin farklı platformlarda farklı uyum biçimleri sergileyebildiği durumlar için birleştirir. Valeriano et al. (2018), devletlerin siber stratejilerinin ittifak ilişkileri ve tehdit algısından bağımsız düşünülmemeyeceğini gösterir; bu çalışma bu saptamayı platforma özgü uyarlama dinamikleriyle ayrıntılandırmaktadır.

Sürdürülebilirlik ve Yakınsama Baskısı

Çift katmanlı uyumun sürdürülebilirliği iki baskı kaynağıyla sınanacaktır. Bunlardan ilki normatif yakınsama baskısıdır. NICC'nin işlevsel hâle gelmesi ve 2026'da çalışmaya başlayan BM Küresel Mekanizması, devletlerden daha somut ve kamuya açık taahhütler bekleyebilir. Bu iki gelişme inceleme döneminin dışında kalır ve burada yalnızca dönem sonrası bir değerlendirme olarak ele alınmaktadır. Deibert'in (2013) siber uzay yönetişiminin giderek rekabetçi bir görünüm kazandığına ilişkin saptaması bu baskının güçlenebileceğine işaret eder. Teknolojik dönüşüm de ayrı bir baskı kaynağıdır. Yapay zekâ ve otonom sistemlerin siber operasyonlara girmesi iki çerçevede de mevcut normların güncellenmesini gerektirebilir. Bu süreç Türkiye'ye norm tartışmalarında daha etkin rol alma imkânı verirken, İttifak taahhütleri ile yerlilik hedefleri arasındaki gerilimi de derinleştirebilir. Valeriano et al. (2018) teknolojik bağımlılık değiştikçe strateji seçimlerinin maliyetinin de değişeceğini öngörür.

Türkiye örneği karşılaştırmalı araştırmalar için de bir hipotez önerir: hem Batılı hem de Batı dışı ortaklarla güvenlik ilişkileri sürdüren orta büyüklükteki devletler için tek platformlu uyumun maliyeti, platformlar arası farklılaşmanın maliyetinden yüksek olabilir. Hindistan'ın Dörtlü

Güvenlik Diyalogu¹ üyeliği ile Rusya'yla sürdürdüğü savunma ilişkileri ve Brezilya'nın NATO ile ortaklık ilişkileri ile Çin'le derinleşen ekonomik bağları, bu hipotezi sınamak için uygun vakalar sunmaktadır. Türkiye'nin özgünlüğü de göz ardı edilmemelidir: resmî NATO üyeliği, CCDCOE sponsorluğu ve AB aday ülke statüsünün birlikte yarattığı normatif yük, diğer orta büyüklükteki devletlerin deneyiminden farklı bir gerilim ortamı oluşturur.

Politika Önerileri

Bulgular üç politika önerisine zemin hazırlamaktadır. Birinci öneri BM Küresel Mekanizması'ndaki katılımın düzenli hâle getirilmesidir. Mekanizmada görünür bir rol üstlenmek, ulusal çıkarların savunulmasına ve norm tartışmalarına katkıya imkân verir. Bu amaçla Dışişleri Bakanlığı bünyesinde uzmanlaşmış bir siber diplomasi biriminin kurulması ve diğer orta büyüklükteki devletlerle ortak tutum geliştirme mekanizmalarının oluşturulması değerlendirilebilir. İkinci öneri ulusal strateji belgelerinin uluslararası norm tartışmalarıyla daha açık ilişkilendirilmesidir. 2024-2028 stratejisi uluslararası iş birliğini ayrı bir amaç olarak tanımlasa da Türkiye'nin NATO ve BM'deki pozisyonlarıyla bağlantısını ayrıntılı biçimde kurmaz. Gelecek dönem belgelerinde bu bağlantının kurulması diplomatik öngörülebilirliği artırabilir. Son öneri, yerli teknoloji hedeflerinin İttifak birlikte çalışabilirlik gereklilikleriyle dengelenmesidir. Türk siber güvenlik firmalarının NATO birlikte çalışabilirlik sertifikasyon süreçlerine dahil edilmesi ve CCDCOE çalışmalarında Türk araştırmacıların daha fazla yer alması bu dengeyi kurmanın pratik yollarıdır.

Sonuç

Bu çalışma Türkiye'nin NATO ve BM siber güvenlik çerçevelerindeki tutumunu 2016-2025 dönemine ait birincil belgeler üzerinden karşılaştırmış ve çift katmanlı uyum savını dört analiz boyutunda değerlendirmiştir. Bulgular Türkiye'nin bağlayıcı NATO çerçevesinde sürekli bir kurumsal katılım ve operasyonel uyum gösterdiğine, BM'de ise mevcut norm çerçevesini destekleyen ama aralıklı ve gönüllülüğü öne çıkaran bir katılım sergilediğine işaret etmektedir. Egemenlik ve yerlilik vurgusu müzakere açıklamalarında değil, ulusal belgelerde ve ulusal raporlama metninde yoğunlaşmaktadır. Örüntü tamamen bilinçli bir tasarımın ya da yalnızca yapısal koşulların ürünü olarak görünmemektedir. Güvenlik bağımlılığı, jeopolitik çoğulculuk ve iç siyasi söylemle tutarlı, yarı sistematik bir konumlanma olarak yorumlanmaktadır.

Çalışmanın kuramsal katkısı çift katmanlı uyum kavramını norm uyumu literatürüne önermesidir. Kavram Putnam'ın (1988) iki düzeyli oyun yaklaşımını birden fazla uluslararası platformun bulunduğu bir yapıya uyarlar. Acharya'nın (2004) norm yerelleştirmesini tek platformlu analizden çıkarır ve Börzel ve Risse'nin (2003) hesaplamalı uyum kategorisini çok platformlu

¹ ABD, Japonya ve Avustralya ile birlikte oluşturulan gayriresmî stratejik güvenlik grubu.

bağlama taşır. Kavramın gözlenebilir beklentileri (bağlayıcı platformda yüksek katılım, gönüllü platformda ret içermeyen düşük yoğunluklu katılım, egemenlik vurgusunun ulusal belgelerde yoğunlaşması) başka orta büyüklükteki devletlere de uygulanabilir. Kavramın genellenebilirliği bu tür karşılaştırmalı vakalarla sınanmalıdır.

Çalışmanın sınırlılıkları şunlardır: gizli diplomatik müzakereler ve gayriresmî İttifak yazışmaları analizin dışında kalmıştır; BM derlemi kamuya açık açıklamalarla sınırlıdır; 2025 reformlarının uzun vadeli etkilerini değerlendirmek için henüz yeterli süre geçmemiştir. Kodlamanın bağımsız ikinci bir kodlayıcıyla ve nitel veri analizi yazılımıyla tekrarlanması gelecek çalışmalar için önerilir. Araştırma gündemi açısından öncelikli alanlar şunlardır: Küresel Mekanizma'nın ilk döneminde Türkiye'nin konumlanmasının izlenmesi, 2025 reformlarının uluslararası koordinasyona etkisinin karar alıcılarla yapılacak görüşmelerle incelenmesi ve yapay zekâ ile otonom siber sistemlere ilişkin norm tartışmalarında Türkiye tutumunun takibi. Kavramın Hindistan, Brezilya ve Endonezya gibi benzer yapısal koşullara sahip devletlere uygulanması, önerilen kuramsal katkıyı sınamanın en doğrudan yolu olacaktır.

Author Contributions

Çağlar Özer conceived and designed the study, conducted the literature review, collected and analyzed the data, interpreted the findings, and drafted and revised the manuscript. The author read and approved the final version of the manuscript.

Conflict of Interest

The author declares that there are no financial, institutional, professional, or personal conflicts of interest that could have influenced the research, analysis, or publication of this study.

Kaynaklar

177 sayılı CBK. (2025, 8 Ocak). Siber Güvenlik Başkanlığı hakkında Cumhurbaşkanlığı kararnamesi (Kararname No. 177). *Resmî Gazete*, 32776.

183 sayılı CBK. (2025, 28 Mart). Bazı Cumhurbaşkanlığı kararnamelerinde değişiklik yapılmasına dair Cumhurbaşkanlığı kararnamesi (Kararname No. 183). *Resmî Gazete*, 32855.

Acharya, A. (2004). How ideas spread: Whose norms matter? Norm localization and institutional change in Asian regionalism. *International Organization*, 58(2), 239-275. <https://doi.org/10.1017/S0020818304582024>

Akdeniz, Y., & Altıparmak, K. (2008). *Internet: Restricted access. A critical assessment of internet content regulation and censorship in Turkey*. İnsan Hakları Ortak Platformu.

Avrupa Birliği. (2021, 13 Aralık). *EU statement: United Nations Open-Ended Working Group on ICT, general exchange of views*. European External Action Service. https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-united-nations-open-ended-working-group-ict-general-exchange-views_en

- Babaoğlu, C. (2025). Türkiye'nin dijital kalesinde yeni surlar: Siber güvenlik kanunu. *Kriter*, 10(101). <https://kriterdergi.com/yazar/cenay-babaoğlu/turkiyenin-dijital-kalesinde-yeni-surlar-siber-guvenlik-kanunu>
- Berman, P. S. (2007). Global legal pluralism. *Southern California Law Review*, 80(6), 1155-1237. <https://ssrn.com/abstract=985340>
- BM Genel Kurulu. (2015). *Uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler hakkında hükümet uzmanları grubu raporu* (A/70/174). Birleşmiş Milletler. <https://undocs.org/A/70/174>
- BM Genel Kurulu. (2019). *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General* (A/74/120). Birleşmiş Milletler. <https://undocs.org/A/74/120>
- BM Genel Kurulu. (2020). *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General* (A/75/123). Birleşmiş Milletler. <https://undocs.org/A/75/123>
- BM Genel Kurulu. (2021a). *Bilgi ve iletişim teknolojilerinin kullanımında güvenlik üzerine açık uçlu çalışma grubu nihai raporu* (A/75/816). Birleşmiş Milletler. <https://digitallibrary.un.org/record/3908015>
- BM Genel Kurulu. (2021b). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (A/76/135). Birleşmiş Milletler. <https://undocs.org/A/76/135>
- Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, 26(3), 452-481. <https://doi.org/10.1080/09636412.2017.1306396>
- Börzel, T. A., & Risse, T. (2003). Conceptualizing the domestic impact of Europe. K. Featherstone & C. M. Radaelli (Ed.), *The politics of Europeanization* içinde (ss. 57-80). Oxford University Press.
- BTK. (2023). *2022 yılı faaliyet raporu*. Bilgi Teknolojileri ve İletişim Kurumu. <https://www.btk.gov.tr>
- CCDCOE. (2021). *National cyber security organisation: Turkey*. NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoe.org/library/publications/national-cyber-security-organisation-turkey/>
- Checkel, J. T. (2005). International institutions and socialization in Europe: Introduction and framework. *International Organization*, 59(4), 801-826. <https://doi.org/10.1017/S0020818305050289>
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2024, 21 Nisan). *Digital Transformation Office's views on "Developments in the field of information and telecommunications in the context of international security"* [A/RES/78/237 kapsamında ulusal katkı]. UNODA. [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-237-Turkiye-DTO-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-237-Turkiye-DTO-EN.pdf)
- Çakmak, C. (2014). Birleşmiş Milletler Güvenlik Konseyi: Eleştirildiği kadar vazgeçilemeyen bir aktör. N. Doğan, C. Çakmak & K. Aslan (Ed.), *BM sistemi ve BM'de reform tartışmaları* içinde (ss. 35-54). Siyasal Kitabevi.

- Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*. McClelland & Stewart.
- Drezner, D. W. (Ed.). (2019). *The uses and abuses of weaponized interdependence*. Brookings Institution Press.
- Erendor, M. E. (2017). *An analysis of threat perceptions: Combating cyber terrorism: The policies of NATO and Turkey, evaluated using game theory in the context of international law* [Doktora tezi, University of Southampton]. <http://eprints.soton.ac.uk/id/eprint/404985>
- Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, 52(4), 887-917. <https://doi.org/10.1162/002081898550789>
- Geneva Internet Platform. (2026). *Organisational session of the UN Global Mechanism on ICT security*. Digital Watch Observatory. <https://dig.watch/event/organisational-session-of-the-un-global-mechanism-on-cybersecurity>
- George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.
- Gerring, J. (2007). *Case study research: Principles and practices*. Cambridge University Press.
- Güntay, V. (2017). Uluslararası sistem ve güvenlik açısından değişen savaş kurgusu: Siber savaş örneği. *Güvenlik Bilimleri Dergisi*, 6(2), 81-108. <https://doi.org/10.28956/gbd.354150>
- Healey, J. (Ed.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
- IISS. (2023). *Cyber capabilities and national power: A net assessment* (Cilt 2). International Institute for Strategic Studies. <https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/>
- Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
- Keskin, F. (1998). *Uluslararası hukukta kuvvet kullanma: Savaş, karışma ve Birleşmiş Milletler*. Mülkiyeliler Birliği Vakfı Yayınları.
- Korzak, E. (2021). *Russia's cyber policy efforts in the United Nations* (Tallinn Paper No. 11). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf
- Kurnaz, S., & Önen, S. M. (2019). Avrupa Birliği'ne uyum sürecinde Türkiye'nin siber güvenlik stratejileri. *International Journal of Politics and Security*, 1(2), 82-103. <https://izlik.org/JA83LC88SM>
- Morse, J. C., & Keohane, R. O. (2014). Contested multilateralism. *The Review of International Organizations*, 9(4), 385-412. <https://doi.org/10.1007/s11558-014-9188-2>
- NATO. (2014). *Wales summit declaration*. https://www.nato.int/cps/en/natohq/official_texts_112964.htm
- NATO. (2016). *Warsaw summit communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

- NATO. (2021). *Brussels summit communiqué*.
https://www.nato.int/cps/en/natohq/news_185000.htm
- NATO. (2022). *NATO 2022 strategic concept*.
<https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>
- NATO. (2023). *Vilnius summit communiqué*. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique>
- NATO. (2024a). *Washington summit declaration*.
https://www.nato.int/cps/en/natohq/official_texts_227678.htm
- NATO. (2024b, 10 Temmuz). *Allies agree new NATO Integrated Cyber Defence Centre* [Haber].
https://www.nato.int/cps/en/natohq/news_227647.htm
- Nye, J. S. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Oran, B. (Ed.). (2022). *Türk dış politikası: Kurtuluş Savaşı'ndan bugüne olgular, belgeler, yorumlar* (Cilt 2: 1980-2001). İletişim Yayınları.
- Putnam, R. D. (1988). Diplomacy and domestic politics: The logic of two-level games. *International Organization*, 42(3), 427-460. <https://doi.org/10.1017/S0020818300027697>
- 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>
- Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- Smeets, M. (2022). *No shortcuts: Why states struggle to develop a military cyber-force*. Hurst Publishers.
- Sönmezoğlu, F. (2014). *Uluslararası politika ve dış politika analizi*. Der Yayınları.
- T.C. Ulaştırma ve Altyapı Bakanlığı. (2016). *Ulusal siber güvenlik stratejisi (2016-2019)*. <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf>
- T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal siber güvenlik stratejisi ve eylem planı (2020-2023)*. <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-planı-2020-2023.pdf>
- T.C. Ulaştırma ve Altyapı Bakanlığı. (2024). *Ulusal siber güvenlik stratejisi ve eylem planı (2024-2028)*. <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf>
- Taşpınar, Ö. (2008). *Turkey's Middle East policies: Between neo-Ottomanism and Kemalism* (Carnegie Papers No. 10). Carnegie Endowment for International Peace.

TBMM. (2025). 7545 sayılı Siber Güvenlik Kanunu. *Resmî Gazete*, 32846 (19 Mart 2025).

Türkiye. (2021, 19 Şubat). *Statement by Turkey: Informal meeting of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*. UNODA. <https://database.cyberpolicyportal.org/en/entity/mkgi030n23l>

Türkiye. (2022, 29 Mart). *Statement by Turkey: Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies*. UNODA. <https://documents.unoda.org/wp-content/uploads/2022/03/Turkey-Statement-OEWG-29-March-2022.pdf>

Ünal, A. N. (2022). *Siber güvenlik: Küresel trendler ve Türkiye'nin kabiliyetleri* (SETA Yayınları No. 203). SETA. <https://media.setav.org/tr/dosya/2022/09/siber-guvenlik-turkiyenin-kabiliyetleri-ve-kuresel-trendler-raporu-seta-gelisen-askeri-teknolojiler....pdf>

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

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6. bs.). Sage.