



KÜRESEL TEKNOLOJİ STANDARTLARI VE JEOPOLİTİK REKABET: 5G VE YAPAY ZEKÂ ÜZERİNDE KURAL KOYMA MÜCADELESİ

Uğur ARSLAN*

Teorik Makale

ÖZ

Yapay zekâ ve 5G teknolojilerinin damga vurduğu günümüzde teknoloji standartları, salt teknik uyum araçları olmaktan çıkarak küresel yönetim ve güç rekabetinin merkezine yerleşmiş, büyük güçler arasındaki standart belirleme savaşları teknik çekişmelerin ötesinde yapısal güç üretimi ve norm inşası mekanizmaları olarak ortaya çıkmıştır. Standartlar, ekonomik güvenlik, teknolojik bağımlılık ve değer temelli düzen inşasının araçları olarak işlev görmektedir; dolayısıyla küresel düzenin geleceğini belirleyecek uzun vadeli rekabetlerin ana sahnesine dönüşmektedir. Bu bağlamda, günümüz standart savaşlarının merkezinde dört kritik alan öne çıkmaktadır: 5G iletişim protokolleri, yarı iletken üretim süreçleri, yapay zekâ güvenlik ve etik standartları ile veri aktarım düzenlemeleri. Çalışmada, bu alanların her biri hem teknik boyutları hem de jeopolitik yansımalarıyla ele alınmış ve bunlardan ikisi hakkında da vaka çalışması yapılmış, 5G ve yapay zekâ alanlarındaki standart belirleme süreçlerinin uluslararası düzeni ve yönetim mekanizmalarını nasıl yeniden şekillendirdiği incelenmiştir. Bulgular, teknoloji standartlarının üç temel dinamik üzerinden etkili olduğunu göstermektedir: Birincisi, teknik özellikleri jeoekonomik araçlara dönüştürerek güvenlik ve ekonomi sınırını bulanıklaştırması; ikincisi, geleneksel standart kurumlarının tarafsızlığını aşındırarak rekabetçi kurumsal blokların oluşumunu teşvik etmesi; üçüncüsü ise parçalı küresel sistemde orta güçlere normatif girişimcilik alanı açmasıdır. Çalışma, orta güçlerin çok katmanlı diplomasi ve kurumsal kapasite güçlendirmesi yoluyla stratejik özerklik kazanabileceğini vurgulamakta ve teknoloji standartlarını uluslararası ilişkiler literatüründe yeterince incelenmemiş bir yönetim alanı olarak konumlandırmaktadır.

Anahtar Kelimeler: Jeopolitik Rekabet, Rejim Kompleksi, Standartlar Hukuku, Teknoloji Standartları, Teknoloji- Blok Siyaseti

Yasal İzinler: Çalışmada yalnızca kamuya açık bilgiler kullanılması ve insandan veri toplanılmaması sebebiyle, etik kurul izni gerektirmeyen çalışmalar arasında yer almaktadır.

* Dr. (kamu hukuku ve uluslararası ilişkiler), Av. (Ankara Barosu), e- posta: av.arslanugur@gmail.com, ORCID: <https://orcid.org/0000-0002-3987-8465>

Makale Gönderim Tarihi: 7.10.2025

Makale Kabul Tarihi: 30.10.2025

DOI: 10.58635/ufuksbedergi.1798697

APA 7 formatında önerilen atıf: Arslan, U. (2025). Küresel teknoloji standartları ve jeopolitik rekabet: 5G ve yapay zekâ üzerinde kural koyma mücadelesi. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 14(28), 227–264. <https://doi.org/10.58635/ufuksbedergi.1798697>

GLOBAL TECHNOLOGY STANDARDS AND GEOPOLITICAL COMPETITION: THE STRUGGLE TO SET THE RULES ON 5G AND ARTIFICIAL INTELLIGENCE

Theoretical Article

ABSTRACT

In an era defined by the rise of artificial intelligence (AI) and 5G technologies, technology standards have moved beyond being mere instruments of technical compatibility to become central elements of global governance and power competition. The standard-setting battles among major powers have emerged not simply as technical disputes but as mechanisms of structural power production and norm construction. Standards function as tools of economic security, technological dependency, and value-based order-building, thereby constituting the main arena for long-term rivalries that will shape the future of the global order. Within this context, four critical domains stand at the core of contemporary “standards wars”: 5G communication protocols, semiconductor manufacturing processes, AI safety and ethical standards, and cross-border data governance frameworks. Each of these domains is examined in terms of both their technical dimensions and geopolitical implications, with two explored through detailed case studies. The findings demonstrate that technology standards operate through three key dynamics: first, by transforming technical features into geoeconomic instruments and blurring the boundary between security and economy; second, by eroding the neutrality of traditional standardization bodies and fostering the emergence of competitive institutional blocs; and third, by creating opportunities for normative entrepreneurship among middle powers within a fragmented global system. The study argues that middle powers can enhance their strategic autonomy through multi-layered diplomacy and institutional capacity-building, positioning technology standards as an underexplored domain of governance within the international relations literature.

Keywords: Geopolitical Competition, Regime Complex, Standards Law, Technology Standards, Technology-Block Politics

Legal Permissions: The study is among the studies that do not require ethical committee approval, since it only uses publicly available information, and no data is collected from humans.

1. GİRİŞ

Günümüzde büyük güç rekabeti yalnızca askerî kapasitelerin kıyaslanması ya da gümrük tarifeleri üzerinden yürütülen ticari uyuşmazlıklarla sınırlı değildir; bunun ötesinde, teknolojik standartların belirlenmesi giderek küresel düzenin en kritik cephelerinden biri haline gelmektedir (Gallwey, 2025; Saniuk-Heinig, 2025). Bir dönem yalnızca sınırlı bir uzman grubunun dar teknik meselesi olarak görülen teknik standartlar, bugün dijital ekonomilerin işleyişini, kritik altyapıların güvenliğini ve stratejik bağımlılık ilişkilerini onlarca yıl boyunca belirleyecek kuralların çatışmalı zeminini oluşturmakta ve bu yönüyle de kamuoyunun ilgisini üzerine çekmektedir. Beşinci nesil (5G) mobil ağların tanımlanmasından yapay zekâ (YZ) yönetişimine, kuantum şifreleme protokollerinden yarı iletkenlerin üretim süreçlerine uzanan bu alanda, standart belirleme süreçleri teknik mühendislik tercihleri, normatif liderlik ve güç projeksiyonu araçlarıdır.

Özellikle *DeepSeek'in R1* modelinin beklenmedik başarısının ardından yarı iletkenler ve nadir elementler üzerinde büyüyen ABD- Çin rekabeti, üçüncü Nesil Ortaklık Projesi (3rd Generation Partnership Project- 3GPP)¹ ve Uluslararası Telekomünikasyon Birliği (ITU) gibi forumlarda yoğunlaşarak, küresel tedarik zincirlerini parçalamakla kalmamakta aynı zamanda uluslararası normların meşruiyet mücadelesini de derinleştirmektedir. Bu tablo, uluslararası politikada ana değişken olarak teknolojinin ekonomik bir rekabet alanı ve jeopolitik düzenin geleceğini belirleyen bir “stratejik savaş alanı” haline geldiğini göstermektedir (Lee, 2021). Bu bağlamda, günümüz standart savaşlarının merkezinde dört kritik alan öne çıkmaktadır: 5G iletişim protokolleri, yarı iletken üretim süreçleri, yapay zekâ güvenlik ve etik standartları ile veri aktarım düzenlemeleri. Aşağıdaki bölümlerde, bu alanların her biri hem teknik boyutları hem de jeopolitik yansımalarıyla ele alınacak ve bunlardan ikisi hakkında da vaka çalışması yapılacaktır.

Teknoloji standartlarının siyaseti, gündelik hayatın altyapısına gömülü normatif tercihler üretmekle kalmaz aynı zamanda küresel ölçekte hangi teknik özelliklerin birlikte işlerliği sağlayacağını, lisans gelirlerinin kimlere aktarılacağını ve hangi aktörlerin hangi piyasalarda egemenlik kuracağını belirlemesi bakımından kurucu bir rol üstlenmektedir. Lawrence Lessig'in “kod hukuktur” önermesi, dijital çağda teknik altyapıların toplumsal düzeni şekillendirme kapasitesine işaret ederken, bu yaklaşım aynı zamanda Michel Foucault'nun *iktidar* kuramıyla da kesişmektedir. Nitekim, Foucault'nun “iktidarın mikro-fiziği” ve “iktidar teknolojileri” kavramları, iktidarın hukuksal ya da devlet merkezli mekanizmalar dışında bireylerin gündelik pratiklerini düzenleyen teknik, kurumsal ve söylemsel araçlar vasıtasıyla işlediğini vurgulamaktadır (Foucault, 1995).

Lessig'in belirttiği üzere, toplumsal davranışları şekillendiren dört temel unsur vardır: hukuk, piyasa, sosyal normlar ve mimari (dijital bağlamda kod). Dolayısıyla kod, çevrimiçi dünyada “hukuk” gibi işleyen bir mimari çerçevedir (Lessig, 1999). Bu nedenle “kod hukuktur” ifadesi, teknoloji standartlarının uluslararası hukuk ile güç politikası arasındaki gerilimin somut bir testi olduğunu göstermektedir. Bu bakış açısı, uluslararası hukuk ve norm meşruiyeti literatürünün işaret ettiği standart belirleme sorunlarıyla doğrudan ilişkilidir. Zira ITU veya 3GPP gibi forumlarda belirlenen teknik standartlar, mühendislik uyumluluğu sağlamakla birlikte hangi aktörlerin meşru norm üreticisi olduğunu, hangi değerlerin küresel ölçekte kabul göreceğini ve

¹ 3rd Generation Partnership Project (3GPP), 1998'de Avrupa, ABD, Japonya, Güney Kore ve Çin'in bölgesel standart kuruluşlarının ortak girişimiyle kurulan; 3G'den 6G'ye uzanan mobil iletişim standartlarını belirleyen teknik iş birliği platformudur. Günümüzde, küresel telekom rekabetinde başlıca şirketlerin ve devletlerin normatif etki alanlarını genişletmeye çalıştığı stratejik bir forum niteliğindedir (3GPP, 2025a)

hangi davranışların mümkün veya imkânsız olacağını belirlemektedir (Frank, 1990; Koskenniemi, 2006).

Bu gerçeklik günümüzde adeta bir “standartlar hukuku” biçimini almıştır. Zira bu standartları yazan aktörler kalıcı bir yapısal güç elde etmektedir. Bunu fark eden ABD ve Çin gibi aktörler uluslararası standardizasyon girişimlerini yönlendirmek veya engellemek için agresif adımlar atarken (Tobin, 2018), ABD, yapay zekâyı küresel güç dengesini değiştirebilecek dönüştürücü bir teknoloji olarak çerçevelemekte, yapay zekâ geliştirme ve yönetimini, Amerikan çıkarlarını korumak için yerel inovasyonu, stratejik ortaklıkları ve dış politikayı entegre eden bir ulusal güvenlik zorunluluğu olarak konumlandırmaktadır. Bu, stratejinin temel unsurlarından biri, ABD liderliğinde bir ittifak kurmak, ABD ile uyumlu güvenlik standartlarını, yazılım ve donanımları teşvik etmek ve müttefikleri ve ortakları Amerikan teknoloji yığınınına bağlayan bir birlikte çalışabilirlik ağı oluşturmaktır (Gallwey, 2025).

Son yirmi yılda Çin Halk Cumhuriyeti, kasıtlı devlet destekli stratejilerle küresel teknoloji arenasındaki konumunu hızla güçlendirmiş; bu yükseliş, YZ, 5G, kuantum bilişim ve yarı iletkenler gibi öncü alanlara yapılan on milyarlarca ABD doları düzeyindeki yatırımlarla ivme kazanmıştır (Abdikarov, 2023). Bu yatırımlar, yerli inovasyonu teşvik etmek ve dışa bağımlılığı azaltmak amacıyla tasarlanmış olup, 2015’te başlatılan “*Made in China 2025*” ve *Kuşak ve Yol Girişimi*’nin “*Dijital İpek Yolu*” bileşeni bu çabaların somut örneklerini oluşturmaktadır. Bu programlar sayesinde ticari harcamalar devlet kontrolü ve mali teşviklerle bütünleştirilerek teknolojik özerkliği ve uluslararası nüfuzu pekiştirmektedir. Bu girişimlere, 2017’de yayımlanan “*Yeni Nesil Yapay Zekâ Gelişim Planı*” gibi sektörel yol haritaları eşlik etmekte olup, plan 2020’ye kadar yakalama, 2025’e kadar atılımlar ve 2030’a kadar küresel öncülük evrelerini tanımlayarak Çin Komünist Partisinin bu alanlarda özerklik ve liderlik hedefini vurgulamaktadır (Saniuk-Heinig, 2025).

AB ise tarihsel olarak hem tek pazara hem de küresel ekonomiye fayda sağlayan birlikte çalışabilirlik gibi değerleri korumak için rekabet ve işbirliği arasında denge kuracak üçüncü bir yol arayışında olup “Brüksel etkisi” olarak adlandırılan düzenleyici kapasitesini kullanarak kendi normlarını ihdas etmeye çalışmaktadır (Zuniga vd., 2024). AB’nin dijital stratejisi, uzun yıllardır düzenleyici çerçevelere ve veri minimizasyonu, tüketici koruması ile hesap verebilirlik gibi hak temelli ilkelere dayalı temele oturtulmuştur. *AB Genel Veri Koruma Yönetmeliği* (GDPR), ve *Veri Koruma Direktifi* gizlilik standartları bakımından küresel bir referans noktası teşkil etmiş ancak, son dönemde Avrupalı politika yapıcılar, dijital altyapıda stratejik özerkliği ön plana çıkarmıştır. AB’nin *Dijital Hizmetler Yasası (DSA)*, *Dijital Operasyonel Dayanıklılık Yasası (DORA)* ve *Siber Dayanıklılık Yasası (CRA)* gibi girişimler, dijital sistemlerin yabancı etki veya baskı unsurlarına karşı maruz kalabileceği yönündeki artan farkındalığı yansıtmaktadır. 2025’te, AB’nin DMA² kapsamında Apple’a 500 milyon euro ceza kesmesi (Milmo, 2025), AB’nin Google’a verdiği ceza (Özkan, 2024) bu etkinin somut örneklerini oluşturmakta, küresel şirketler, USB-C zorunluluğu gibi AB standartlarını dünya çapında benimsemek zorunda kalmaktadır (European Parliament, 2022). Benzer biçimde, Bilgisayarlar, Gizlilik ve Veri Koruması (Computers, Privacy and Data Protection -CPDP) platformu,

² Digital Markets Act (DMA), AB’nin dijital ekonomide rekabeti artırmak, adil pazar koşullarını sağlamak ve büyük teknoloji şirketlerinin (“geçit bekçileri” olarak adlandırılan gatekeeper’lar) hakimiyetini sınırlamak amacıyla çıkardığı kapsamlı bir düzenlemedir. Bu yasa, dijital sektördeki rekabet edilebilirliği ve adilliği hedefleyerek, Google, Apple, Meta (Facebook), Amazon, Microsoft ve ByteDance (TikTok) gibi dev şirketlerin platformlarını düzenler. DMA, geleneksel rekabet hukuku kurallarını (örneğin, AB Rekabet Hukuku) tamamlar ancak değiştirmez; önleyici (ex-ante) bir yaklaşım benimser ve büyük platformların pazar gücünü proaktif olarak sınırlamayı amaçlar. Yasanın temel felsefesi, “Brüksel Etkisi” ile AB normlarını küresel ölçeğe ihraç etmek ve dijital pazarların parçalanmasını önlemektir (European Commission, 2022).

Avrupa'nın teknoloji standartları rejim kompleksinde önemli bir düğüm noktasıdır. Çeşitli kurumların katılımıyla küresel bir ağa dönüşen CPDP, gizlilik, veri koruması ve yapay zekâ yönetişimi konularında normatif etkileşim ve politika uyumu üreten bir platform işlevi görmektedir. 19–22 Mayıs 2026'da Brüksel'de düzenlenecek CPDP 2026 konferansı, dijital standartların etik temelli biçimlenişine odaklanarak AB'nin teknoloji yönetişimi alanındaki normatif liderliğini pekiştiren stratejik bir girişim niteliği taşımaktadır. Böylece AB'nin etik temelli dijital yönetim modelini güçlendirerek küresel standart belirleme kapasitesini desteklemektedir (CPDP, 2025).

“Teknoloji-blok siyaseti” olarak adlandırılabilir bu yeni kural koyma mücadelesi ikili rekabetin ötesine taşmaktadır. Japonya, Güney Kore, Hindistan ve AB gibi orta güçler ile Türkiye gibi yükselen aktörler; Uluslararası Telekomünikasyon Birliği (ITU), Uluslararası Standardizasyon Örgütü (ISO), Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), 3GPP, Dünya Fikri Mülkiyet Örgütü (WIPO), Uluslararası Elektroteknik Komisyonu (IEC), İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN), Dünya Ticaret Örgütü'nün (WTO) Ticarete Teknik Engeller Komitesi (TBT), Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) ve Dünya Ağ Konsorsiyumu (W3C) gibi çok katmanlı bir kurumsal zeminde yol almak zorundadır. Bu devletler ve yapılar ekonomik teşvikler, güvenlik kaygıları ve ittifak yükümlülükleri arasında denge kurarken stratejik özerkliklerini de korumaya çalışmaktadır.

Söz gelimi, Güney Kore'nin, Korean Agency for Technology and Standards (KATS) koordinasyonunda ve ISO, IEC ile ITU'nun ortak ev sahipliğinde 2025 yılı Aralık ayında Seul'de düzenleyeceği *Uluslararası Yapay Zekâ Standartları Zirvesi*, orta güçlerin küresel teknoloji yönetişimindeki artan görünürlüğünü yansıtmaktadır (ISO, 2025). Bu zirve, ASEAN ve Dijital Ekonomi Çerçeve Anlaşması (DEFA)³ gibi bölgesel mekanizmalar aracılığıyla yürütülen veri harmonizasyonu ve dijital entegrasyon çabalarının, küresel standart ekosistemine nasıl entegre olabileceğini göstermektedir. Keza, Hindistan, Almanya, Hollanda, Japonya ve Türkiye gibi orta güçlerin yanı sıra, Orta Doğu'da BAE, Latin Amerika'da Brezilya ve Afrika'da Güney Afrika gibi aktörler de 5G ve yapay zekâ yönetişiminde stratejik özerklik arayışlarını sürdürmekte; Quad, ASEAN, UNESCO, MİKTA ve BRICS+ gibi platformlarda ABD- Çin kutuplaşmasına alternatif normatif zeminler inşa etmeye yönelmektedir. Bu durum, standart belirleme süreçlerinin yalnızca büyük güçlerin rekabet alanı olmaktan çıkarak, orta güçlerin normatif kapasite ve rejim girişimciliği yoluyla etki üretebildiği çok katmanlı bir yönetim yapısına evrildiğini göstermektedir. Nitekim ISO'nun *2025 Yapay Zekâ Veritabanı Girişimi*, bu ülkelerin kurumsal katılımını artırarak rejim kompleksinin çeşitlenmesine ve uluslararası standartlaşmanın daha kapsayıcı bir nitelik kazanmasına katkıda bulunmaktadır (ISO, 2025).

Bu çalışma, teknoloji standartları üzerindeki mücadelenin küresel yönetişimi üç temel biçimde dönüştürdüğünü savunmaktadır. Birincisi, teknik özellikleri jeoekonomik devlet aracına dönüştürerek ekonomi ile güvenlik politikası arasındaki sınırı bulanıklaştırmaktadır; örneğin, ABD'nin *CHIPS Act* sübvansiyonları ve *Yarışı Kazanmak* adını verdiği stratejisi (Winning the Race) ile Çin'in *Küresel Yapay Zekâ Yönetişim Eylem Planı* (*Global Artificial Intelligence*

³ASEAN Dijital Ekonomi Çerçeve Anlaşması (DEFA), ASEAN'ın 10 üyesinin dijital entegrasyonunu güçlendirmek için müzakere ettiği ilk bölge çapında dijital ekonomi anlaşmasıdır; Aralık 2023'te başlayan müzakereler, Ekim 2025 itibarıyla önemli ilerleme kaydetmiş olup, 2025 sonunda esaslı bir kısım imzalanması ve 2026'da tam imzalanması beklenmektedir. Anlaşma, dijital ticaret, e-ticaret, ödemeler, dijital kimlik, siber güvenlik, veri akışları, yeni teknolojiler (AI, blockchain) ve yetenek hareketliliğini kapsar; bu sayede dijital ekonomiyi 2030'a kadar 2 trilyon dolara çıkararak GSYİH'nin %26-28'ini dijitalleştirmeyi, 3,5 milyon iş yaratmayı ve KOBİ'leri güçlendirmeyi hedefler. Veri dolaşımında esneklik sağlanırken, ulusal kapasite geliştirme (eğitim, altyapı) ile kapsayıcı büyüme teşvik edilecektir (PS Centre, 2025).

Governance Action Plan) ve *China Standards 2035* gibi hamleleri ⁴ bu alanı jeopolitik bir araca çevirmektedir (Gallwey, 2025). İkincisi, mezkûr rekabet ortamı, geleneksel standart belirleme organlarının tarafsızlığını zorlamakta ve rakip bölgesel ya da ideolojik blokların oluşumunu teşvik etmektedir. 53 ülke katılımı ile Clean Network’ün⁵ ITU/ISO’daki Çin etkisini sınırlaması bu duruma örnek olarak gösterilebilir. Üçüncüsü, giderek parçalanmış bir uluslararası düzende “norm girişimcisi” olarak hareket etmeyi hedefleyen orta güçler için yeni fırsatlar ve kısıtlar ortaya çıkmaktadır. Söz gelimi, AB’nin *AI Act*’i ile Güney Kore’nin kapasitesi, niş norm ihracını mümkün kılarken uyum maliyetlerini de artırmaktadır.

5G ve yapay zekâ yönetişimi örneklerini inceleyen bu çalışma, standardizasyonun XXI. yüzyıl uluslararası ilişkilerinde kritik, ancak yeterince analiz edilmemiş bir boyut haline geldiğini ortaya koymaktadır. 2025 itibarıyla yapay zekânın jeoteknolojik rekabetin merkezine yerleşmesi, teknik standartları uyum mekanizmaları olmaktan çıkararak, güç projeksiyonu ve stratejik etki üretiminin “görünmez savaş alanı” haline getirmiştir. Bu bağlamda, standart belirleme süreçleri teknik uzlaşıdan öte, normatif liderlik ve jeopolitik rekabetin kurumsal tezahürü olarak değerlendirilmektedir.

2. TARİHSEL ARKA PLAN

2.1. Genel Olarak

Teknoloji standartlarının jeopolitik bir rekabet alanına dönüşmesi, tarihsel süreklilik gösteren bir olgudur. Bu süreç, Sanayi Devrimi’nden itibaren uluslararası ticaretin genişlemesi ve bilimsel bilginin kurumsallaşmasıyla paralel biçimde evrilmiştir XVIII. yüzyıl sonu ile XIX. yüzyıl başında şekillenen Sanayi Devrimi, İngiltere’nin emperyal birimleri ile kıta Avrupa’sının geleneksel ölçü birimleri gibi farklı ulusal ölçü sistemlerinin uyumlaştırılmasını zorunlu kılmış, böylece ekonomik verimliliğin artırılması ve diplomatik etkileşimin kolaylaştırılması yönünde standartlaşmanın temelleri atılmıştır (Mokyr, 2002).

XIX. yüzyılın ortasında kabul edilen metrik sistem, standartlaştırmanın teknik, ekonomik ve diplomatik bir mesele haline geldiğini göstermektedir. 1798’de Paris’te toplanan uluslararası komisyon, metre ve kilogramın değerlerini belirlerken bilimsel mutabakatı bir diplomasi aracı olarak kullanmış, Napolyon’un imparatorluk ölçüleri politikası ise bu süreci kıtasal ölçekte hızlandırmıştır. Fransız Devrimi sonrasında 1795’te Fransa’da resmileşen metrik sistem, 1875 tarihli *Metre Sözleşmesi* ile kurumsal bir niteliğe kavuşmuş ve 20 devletin katılımıyla kurulan Uluslararası Ağırlıklar ve Ölçüler Bürosu (BIPM) tarafından yönetilmeye başlanmıştır. Metrik sistemin yaygınlaşması Aydınlanma Çağı’nın rasyonalite ve evrensellik ideallerinin diplomatik ve ekonomik bir uzantısı olarak görülebilir. Portekiz (1814) ve Hollanda (1816) gibi ülkelerde

⁴ *China Standards 2035*, Çin Halk Cumhuriyeti’nin (Çin) 2018 yılında başlatılan ve 2035 yılına kadar uzanan stratejik bir standartlaşma planıdır. Bu plan, Çin hükümeti ve önde gelen teknoloji şirketleri (örneğin, Huawei, Alibaba) tarafından geliştirilen bir yol haritasıdır ve özellikle 5G, Nesnelerin İnterneti (IoT), YZ, bulut bilişim, kuantum teknolojileri ve ileri iletişim teknolojileri gibi yükselen teknolojilerde küresel standartları belirleme ve etkileme hedefini taşır (Wu, 2022); *Made in China 2025* sanayi stratejisinin bir devamı niteliğindedir ve Çin’in küresel teknoloji liderliğini pekiştirmeyi amaçlar. Tüm rapor henüz kamuoyuna tam olarak açıklanmamış olsa da 2021’de *Ulusal Standardizasyon Gelişim Çerçevesi* (NSD) ve 2022’de *Ulusal Standardizasyon Gelişim Eylem Planı* (SAMR tarafından yayınlanan) gibi belgelerle somutlaştırılmıştır (Wei, 2022).

⁵ *Clean Network*, ABD Dışişleri Bakanlığı tarafından 2020 yılında başlatılan bir girişimdir ve küresel telekomünikasyon ağlarında güvenliği artırmayı amaçlayan bir dizi politika ve stratejiyi ifade eder. Temel hedefi, özellikle 5G ve diğer kritik iletişim altyapılarında, “güvenilir olmayan” teknoloji sağlayıcılarının (örneğin, Çin merkezli Huawei ve ZTE gibi şirketlerin) etkisini sınırlamak ve güvenli, şeffaf bir dijital ekosistem oluşturmaktır. *China Standards 2035* gibi Çin’in teknoloji alanındaki artan etkisine karşı bir jeopolitik hamle olarak değerlendirilebilecek bu girişim ABD liderliğinde müttefik ülkeleri bir araya getirerek standartlar, altyapı ve veri güvenliği üzerinde ortak bir çerçeve oluşturmayı hedeflemektedir (Saniuk-Heinig, 2025).

metrik sistemin benimsenmesi, bu standardın siyasi ve ekonomik alanlarda uzlaşmayı kolaylaştırıcı işlevini ortaya koymuştur (Hallerberg, 1973).

Ekonomik açıdan bakıldığında, metrik sistemin yaygınlaşması ticaret engellerini azaltmış ve özellikle XIX. yüzyıl Almanya ve İtalya birleşmelerinde siyasal bütünleşmenin bir başka aracı olarak da işlev görmüştür. Bu dönüşüm, küresel ticaret hacminde %20–30 oranında bir artışa katkı sağlarken, standartların yalnızca ekonomik değil, jeopolitik bir güç unsuru haline geldiğini göstermiştir (Mokyr, 2002). İngiltere’nin kendi emperyal ölçü sistemini sürdürme konusundaki direnci ve bu direncin ABD’ye tevarüs etmesi Avrupa’nın teknik entegrasyonunu yavaşlatırken, metrik sistemin yayılması sömürgecilik sonrası ulus-devletlerin modernleşme süreçlerini hızlandırmıştır (Hallerberg, 1973).

Soğuk Savaş sürecinde diğer alanlarda olduğu gibi teknolojik alanda da ortaya çıkan rekabet ortamı, standartları teknik uyum araçları olmaktan çıkararak, ulusal güvenlik stratejisinin ve ideolojik mücadelenin merkezine yerleştirmiş, standart belirleme süreçleri adeta ideolojik bloklaşmanın teknik bir uzantısına dönüşmüştür. Söz gelimi, ABD’nin 1949’da kurduğu Koordineli İhracat Kontrol Komitesi (COCOM) aracılığıyla uyguladığı teknoloji ambargoları, Sovyet askeri standartlarını küresel sistemden izole etmiş, buna karşın Sovyetler kendi kapalı teknik normlarını geliştirmeye yönelmiştir. Bilgisayar ve elektronik alanındaki rekabet, ABD’nin açık inovasyona dayalı modelinin Sovyet girişimlerine karşı üstünlük kazanmasına yol açmış, bu üstünlük nükleer ve uzay yarışında da belirleyici olmuştur (Edgerton, 2006; Graham, 1993).

Soğuk Savaş’ın sona ermesinin ardından 1990’lar ve 2000’lerde hız kazanan küreselleşme dalgası, uluslararası ticaretin ve teknolojik etkileşimin kurumsal çerçevesini derinleştirerek daha bütünleşik bir standart düzeni oluşturma yönündeki eğilimleri güçlendirmiştir. Bu dönemde WTO’nun 1994 tarihli *Ticarette Bağlantılı Fikri Mülkiyet Hakları Anlaşması* (TRIPS), fikri mülkiyet haklarına ilişkin asgari standartları belirleyerek telif ve patent korumasını küresel ticaret sisteminin temel unsurlarından biri haline getirmiştir (WTO,). TRIPS’in yürürlüğe girmesiyle, dünya ticaretinin yaklaşık %98’ini temsil eden 166 üye ülke ortak bir normatif çerçeveye dahil olmuş, standart rekabetini ticari liberalizasyon zeminine taşımıştır. Aynı dönemde ISO ve ITU gibi kurumlar, küresel entegrasyon süreciyle birlikte etkilerini genişletmiştir. Bu gelişmeler, standartların teknik uyum araçları olduğu kadar, aynı zamanda ticaretin düzenlenmesi ve piyasa erişiminin belirlenmesi açısından stratejik unsurlar haline geldiğini göstermektedir. Örneğin ISO’nun 1990’larda geliştirdiği kalite yönetim sistemleri (ISO 9000 serisi), uluslararası tedarik zincirlerinde üretim süreçlerinin uyumlaştırılmasını sağlamış, ITU’nun Dünya Radyokomünikasyon Konferansları (WRC) ise frekans tahsisini küresel ölçekte harmonize etmiştir (Maskus, 2000).

Çok uluslu şirketlerin yükselişi, standart belirleme süreçlerinde devletlerin doğrudan rolünü kısmen azaltsa da 5G, yarı iletken üretimi ve ileri bilişim teknolojileri gibi stratejik sektörlerde kamu desteği belirleyici olmaya devam etmiştir. Özellikle 2000’lerde bilgi ve iletişim teknolojileri (ICT) alanında kabul edilen IEEE ve Wi-Fi gibi standartlar, küreselleşmeyi desteklemiş ancak AB’nin veri koruma düzenlemelerinde olduğu gibi ulusal çıkar ve normatif yaklaşımlar arasındaki farklılıklar, yeni türden standart çatışmalarını gündeme getirmiştir (Maskus, 2000). Bu dönemin genel özelliği, standartların teknik uyumdan ziyade ekonomik rekabet ve normatif liderlik araçlarına dönüşmesidir.

Günümüz çok kutuplu yapısı, standartları “görünmez bir savaş alanı” haline getirirken; orta güçlere, büyük güç rekabeti arasında niş liderlik ve bölgesel norm üretimi gibi yeni fırsatlar sunmaktadır. Bu tarihsel evrim, standart savaşlarının teknik mühendislik tartışmalarından çok,

stratejik özerklik, ekonomik güvenlik ve normatif nüfuz mücadelelerinin kesişiminde şekillendiğini göstermektedir.

2.2. ABD’de Standartlaşma

Amerikan Ulusal Standartlar Enstitüsü (ANSI), 1918’de Amerikan Mühendislik Standartları Komitesi olarak kurulmuş olsa da bağlayıcı düzenlemelerden yoksun olması standart geliştirme konusunda gerekli ilerlemeyi gösterememesine neden olmuştur. Buna karşın, özel sektör liderliğindeki, çok paydaşlı ve gönüllü fikir birliği temelli *Gönüllü Mutabakat Standartları* (Voluntary Consensus Standards- VCS) modeli kurumsallaşmaya başlamıştır. VCS, piyasa odaklı esneklik ile katı bürokrasi arasında ara bir yol sunmuş; özel şirketler, teknik uzmanlar ve sivil toplum kuruluşları (çoğunlukla ABD-Avrupa merkezli) tarafından yönetilen bu ittifak, laissez-faire felsefesini⁶, fikir birliğini ve gönüllü katılımı somutlaştırarak ABD normlarının, değerlerinin ve çıkarlarının teknolojik standartlar yoluyla meşrulaştırılmasına ve küresel yayılmasına zemin hazırlamıştır (Zuniga vd., 2024).

Standartların stratejik bir araç olarak taşıdığı değer özellikle Soğuk Savaş döneminde belirginleşmiştir. Bu dönemde ABD ve Sovyetler Birliği, askeri ve uzay teknolojileri başta olmak üzere pek çok teknik alanı ulusal güvenliğin ayrılmaz bir parçası olarak görmüş ve kendi teknolojik standartlarını küresel ölçekte yaygınlaştırma çabasına girmiştir. Bu rekabet, teknolojik bölünmenin ilk dalgasını da tetiklemiştir (Edgerton, 2006). ABD, ANSI ve IEEE gibi kurumları destekleyerek Batı Bloku içerisinde “açık standartlar” anlayışını teşvik etmiştir.⁷ Özellikle Ulusal Bilim Vakfının (NSF) Soğuk Savaş yıllarındaki merkezi rolü, bilgisayar ve uzay teknolojilerinde standartlaşmayı hızlandırmıştır (Edgerton, 2006). Buna karşın, Sovyetler Birliği, kapalı ve planlı sistemlere yönelmiş, ideolojik kısıtlamalar ve Batı teknolojilerinin taklidine dayalı üretim modeli nedeniyle ülke standart üretme ve yayma bakımından rakiplerinden geride kalmıştır (Graham, 1993).

1960-1970’lerde tüketici güvenliği kaygılarının yanı sıra VCS içindeki anti-tröst ihlalleri (büyük şirketlerin rakipleri dışlama taktikleri) nedeniyle hükümetler, standart belirlemede etkinleşmiştir. Federal kurumlar sağlık, tüketici ve çevre standartları başlıklarında etkin hale gelirken, piyasa-devlet dengesini yeniden tanımlamıştır. Reagan’ın 1980’de başkan seçilmesiyle canlanan politik-ekonomik manzarada *OMB A-119* başlıklı düzenleme ABD standart stratejisinin temel taşı haline gelmiştir. Bu belge kırk yıldan fazla süreyle uluslararası ISO/IEC gibi SDO’ların temelini oluşturmuştur. Avrupa merkezli SDO’ların bürokratik yavaşlığı, neo-liberal ilkelerin uluslararasılaşmasının bir örneği olarak ABD konsorsiyumlarını (örneğin, WiFi standartları) teşvik ederek, VCS’nin inovasyon odaklı evrimini hızlandırmıştır (Zuniga vd., 2024).

XXI. yüzyılın ikinci on yılında başka bir söyleyişle küresel teknoloji rekabetinin yoğunlaştığı dönemde, ABD’nin standardizasyon politikaları stratejik bir boyut kazanmıştır. Bu doğrultuda, Washington yönetimi ve Kongre, teknolojik yeniliklerde norm belirleme kapasitesini güçlendirmeye yönelik çeşitli yasal ve kurumsal girişimlere yönelmiştir. Nitekim, ABD

⁶ *Laissez-faire*, ekonomik faaliyete devlet müdahalesinin en aza indirilmesini savunan klasik liberal bir görüştür. Bu yaklaşıma göre piyasa, bireylerin serbest etkileşimi yoluyla kendi dengesini doğal biçimde bulur; devletin rolü mülkiyetin ve sözleşme özgürlüğünün korunmasıyla sınırlı olmalıdır.

⁷ Cargill’e göre, SO, IEC, ITU ve WTO gibi kurumlarca şekillenen standartlar sistemi, II. Dünya Savaşı sonrası dönemin sermaye yoğun sanayi toplumuna uygun biçimde inşa edilmiştir. Bu yapı, temel amacı büyük güçlerin ve sanayileşmiş ülkelerin ortak çıkarlarını dengelemek olan bir düzen yaratmış, ancak teknik kapasitesi zayıf veya gelişmekte olan ülkeler için dezavantajlı sonuçlar doğurmuştur. Bu sistem, güçlü teknik altyapıya ve fikri mülkiyet birikimine sahip aktörleri desteklerken, sanayileşme sürecini yeni başlatan ülkeleri dışlamıştır (Cargill, 2022).

Kongresinde sunulan birçok yasa tasarısı, küresel teknoloji standartlarında Amerikan liderliğini güçlendirmeyi hedeflemiştir. Bu kapsamda, 2021 *Teknoloji Standartları Görev Gücü Yasası* hükümete, ortaya çıkan yeni teknolojilere ilişkin standartların belirlenmesinde aktif rol oynayacak bir görev gücü kurulması yönünde yetki vermiş (Congress, 2021), çeşitli Amerikan düşünce kuruluşları da ülkenin küresel standart belirleme alanındaki öncü konumunu yeniden tesis etmesi ve bu alanda stratejik bir vizyon geliştirmesi gerektiğini savunmuştur. Nitekim, 2020 yılında Donald Trump yönetimindeki Birleşik Devletler hükümetinin, “*ABD’nin Çin Halk Cumhuriyeti’ne Stratejik Yaklaşımı*” başlıklı belgede “standards” teriminin birçok kez kullandığı görülmektedir (Lee, 2021).

ABD Ulusal Standartlar ve Teknoloji Enstitüsü, 2019 yılında “*AI’da ABD Liderliği: Teknik Standartların ve İlgili Araçların Geliştirilmesinde Federal Katılım Planı*”nı yayınlamış (US Department of Commerce, 2019), 2020 yılında göreve gelen Başkan Joe Biden konuyla ilgili makalesinde uluslararası ekonomide kural koymanın önemini vurgulamıştır. Eski başkan, salt “standart” terimini kullanmasa da Çin kaynaklı zorluklarla ilgili olarak selefi ile aynı mesajı göndermiştir:

“70 yıl boyunca, Demokrat ve Cumhuriyetçi başkanlar yönetimindeki Amerika Birleşik Devletleri, kuralların yazılmasında, anlaşmaların yapılmasında ve uluslar arasındaki ilişkilere rehberlik eden ve kolektif güvenlik ve refahı ilerleten kurumların canlandırılmasında öncü bir rol oynadı.... Temiz enerji, kuantum hesaplama, yapay zekâ söz konusu olduğunda Çin’in veya başka birinin gerisinde kalmamız için hiçbir neden yok.” (Biden, 2020)

Biden yönetimi, Şubat 2021’de yayımlanan “*Amerika’nın Tedarik Zinciri Hakkında Başkanlık Kararnamesi*” ile stratejik öneme sahip ürünlerin tedarik zincirlerine ilişkin inceleme süreci başlatmıştır. Bu sürecin sonucunda hazırlanan “*Dayanıklı Tedarik Zincirleri Oluşturmak, Amerikan Üretimini Canlandırmak ve Kapsayıcı Büyümeyi Teşvik Etmek*” başlıklı raporda, standartlar fiyat rekabetinin ötesinde ürün ve hizmetlerin farklılaştırılmasına olanak sağlayan ve “yukarıya doğru bir rekabet”i teşvik eden güçlü araçlar olarak vurgulanmıştır. Raporda ayrıca, hükümetin standart belirleme süreçlerinde ve yüksek nitelikli işletme uygulamalarını teşvik etmede daha etkin bir rol üstlenmesi gerektiği belirtilmektedir. Bu bağlamda, güçlü ulusal standartların oluşturulması veya küresel standartların benimsenmesi yönünde yapılacak girişimlerin, özel sektörün dayanıklı ve sürdürülebilir üretim pratikleri geliştirme kapasitesini destekleyeceği ifade edilmiştir (The White House, 2021).

2.3. Avrupa Ekonomik Entegrasyonu ve Standardizasyon Reformu

XIX. yüzyılda demiryolları, elektrik ve telgraf gibi erken ağ teknolojilerinin etkisiyle, Avrupa’da ilk uluslararası standartlar filizlenmeye başlamıştır. 1901’de dünyanın ilk ulusal standartlar organı olan İngiliz Standartlar Enstitüsü (BSI) kurulmuş (BSI, 2025), I. Dünya Savaşı’nın eşliğinde diğer Avrupa devletleri de bu örneği izleyerek, kıta genelinde kendi standardizasyon yapılarını kurmuşlardır. Bu yarı kamusal kuruluşlar, ulusal standartların geliştirilmesi ve yayımlanmasını koordine ederek, hiyerarşik ulusal standart ağlarının oluşmasını sağlamıştır. II. Dünya Savaşı sonrası iyimserlik dalgasında 1947’de Uluslararası Standardizasyon Örgütü (ISO) kurulmuş, ISO, 1947-1964 arası ilk evresinde ağırlıklı olarak Batı Avrupa odaklı bir girişim olmasına rağmen, hızla en kapsamlı uluslararası standart geliştirme örgütü (SDO) haline gelmiştir (ISO, 2017).

Savaş sonrası dönemde artan uluslararası rekabet ve Soğuk Savaş dinamikleri, Avrupa’da yalnızca ekonomik entegrasyonu değil, teknik standartlaşma çabalarını da hızlandırmıştır. 10 Haziran 1960’ta AET ve EFTA ülkelerindeki ISO ve IEC temsilcileri, CEN ve CENEL (daha

sonra CENELEC) olmak üzere iki Avrupa standardizasyon örgütünün kurulması konusunda anlaşmış, 1973'te CENELEC (CENELCOM ve CENEL'in birleşmesiyle) hayata geçmiştir. 1980'lerin ortalarında "Tek Avrupa Pazarı" vizyonu, ağ sektörlerinde liberalleşmeyi hızlandırmış ve AET'nin 1985'te ilan ettiği *Yeni Yaklaşım* ile standartlaşma süreci kurumsal bir dönüşüm geçirmiştir. Bu model, teknik standartların hazırlanmasını Avrupa standart kuruluşlarına devrederek kamu-özel ortaklığına dayalı bir yapı kurmuş; AET ise sağlık, güvenlik, çevre ve tüketici koruması gibi temel alanlarda asgari gereklilikleri belirleyen direktiflerle düzenleyici çerçeveyi korumuştur. 1989'dan itibaren *Küresel Yaklaşım Politikası*'yla bütünleştirilen bu sistem, test, muayene ve sertifikasyon süreçlerinin uyumlaştırılması yoluyla ürünlerin AET genelinde karşılıklı tanınmasını sağlamış; böylece Avrupa Tek Pazarının ve Ekonomik ve Parasal Birliğin kurumsal temelini güçlendirmiştir. 13 Kasım 1984'te *Avrupa Komisyonu ile CEN ve CENELEC arasında İşbirliğine İlişkin Genel Yönergeler* kabul edilmiş, bu belgeler standartların kamu politikası ve mevzuatta oynayabileceği rolü ilk kez resmi olarak tanımıştır. Haziran 1991'de *ISO ile CEN arasında Teknik İşbirliğine Dair Viyana Anlaşması* yayımlanmış ve iki örgüt arasındaki işbirliği ilkeleri belirlenmiştir. 1 Ocak 1993'te Avrupa Tek Pazarı kurulmuş ve CEN ile CENELEC, pazarın bütünlüğünü sağlamak, ürünlerin yüksek kalite ve güvenlik standartlarını karşılamasını temin etmek için merkezi bir rol üstlenmiştir. *Uyumlaştırılmış standartlar*, Avrupa mevzuatının uygulanabilirliğini sağlarken, 28 Mart 2003'te CEN, CENELEC ve ETSI ile Avrupa Komisyonu ve Avrupa Serbest Ticaret Birliği arasında *Temel İşbirliği Anlaşması* imzalanmış; 9 Temmuz 2008'de *Avrupa Tek Pazarı için Yeni Mevzuat Çerçevesi* (NLF) kabul edilmiştir. 25 Ekim 2012'de 1025 sayılı *Avrupa Standardizasyon Yönetmeliği*, 14 Ekim 2016'da Frankfurt Anlaşması ile revize edilen *IEC-CENELEC Anlaşması* ve 1 Şubat 2021'de *CEN ve CENELEC Stratejisi 2030* ile Avrupa standardizasyonu, dijital ve yeşil dönüşümlere katalizör görevi görecektir şekilde güçlendirilmiştir. Bununla birlikte, konsorsiyum standartlarının AB hukukuna meydan okuması, Avrupa standardizasyon kuruluşlarını bölgesel odaklı yapısı ve KOBİ'ler ile tüketicilerin düşük temsili gibi sorunlar, sistemin etkinliğini sınırlamıştır. Bu zorluklar, Çin'in küresel standartlaşmadaki yükselişiyle birleşerek 2022 tarihli *AB Standardizasyon Stratejisi*'nin hazırlanmasına zemin hazırlamış; belge, Avrupa'nın rekabet gücünü artırmak amacıyla standartlaşmanın jeostratejik önemini yeniden tanımlamıştır. Strateji, yeni jeopolitik değerlendirmeleri ve standartların ikili geçişlerdeki rolünü yansıtmıştır. Son olarak, 20 Ocak 2023'te Avrupa Standardizasyonu Yüksek Düzeyli Forumu'nun ilk toplantısı gerçekleştirilmiş, forum Avrupa standardizasyon uzmanlıklarını bir araya getirerek bu alanın daha geniş kitlelere ulaşmasını hedeflemiştir (European Commission, 2022b; CENELEC, 2023; Zuniga vd., 2024)

2.4. Çin Standardizasyon Sisteminin Tarihsel Evrimi

Birleşik Devletler ve AB'nin aşağıdan yukarıya standartlaşma modellerine karşın, Çin'in sistemi tarihsel olarak yukarıdan aşağıya bir yapıya dayanmış; bu dinamik, hükümetlerin ekonomik kalkınmayı araçsallaştırdığı gelişmekte olan ülkelerin tipik bir özelliği olarak belirginleşmiştir. Sanayi politikası odaklı bu ters mantık, çağdaş Çin stratejisinin temelini oluşturmuştur. 1978 öncesi dönemde, planlı ekonomi bağlamında standardizasyon tamamen hükümet koordinasyonunda yürütülmüş; Deng Xiaoping'in yükselişi ve ekonomik yeniden açılımla birlikte, ülke uluslararası standardizasyona (örneğin, ISO) ilgi göstermeye başlamıştır (Wang, 2011).

1988 Standardizasyon Yasası, sistemi; ulusal, endüstriyel, yerel ve kurumsal düzeylerde yapılandırmış, işletme standartları hariç tüm seviyeler, hükümet teknik komiteleri tarafından geliştirilmiştir. Gelişmiş ekonomilerden esinlenen Çin, bu yasada *gönüllü standartlar* kavramını tanıtmıştır (Wang, 2011). 1980'ler ve 1990'lar boyunca, Çin "taklitçi" bir politika izleyerek uluslararası standartları benimsemiş ve öncelikle bir "standart alıcısı" konumunda

kalmıştır. Bu reform evresi, 2001 Dünya Ticaret Örgütü (DTÖ) katılımıyla sona ermiş; katılım, Çin ürünlerinin pazar erişimini artırma motivasyonu taşısa da teknik düzenlemeler, standartlar ve fikri mülkiyet gibi yeni engellerle karşılaşmıştır. Bu deneyim, yerli inovasyonu teşvik eden “yakalama standartları” stratejisini doğurmuş; Çin teknolojilerine ve yerli fikri mülkiyete dayalı standart geliştirme zorunluluğunu vurgulamıştır. Politika değişikliği, Bilim ve Teknoloji Bakanlığı, Çin Standardizasyon İdaresi (SAC) ve sektörel bakanlıklarca yönetilen döngüsel inceleme süreçlerini başlatmıştır. SAC’ın 2006 *On Birinci Beş Yıllık Kalkınma Planı* 1988’den beri ilk büyük politika güncellemesi olarak, standardizasyonu kilit sektörlerde yerli inovasyonun temeli olarak tanımlamış, “yaparak öğrenme”yi teşvik etmek üzere sektörel stratejiler, yabancı ittifaklar ve özel sektör katılımını artırmış, uluslararası SDO’larda aktif rolü özendirmiştir. Ne var ki, piyasa eğilimlerine rağmen, işletmeler Çin Komünist Partisi önceliklerine tabi kalmıştır (Wang, 2011; Ernst, 2011)

2000’li yıllarda Çin, kablosuz ağ (Wi-Fi) ve üçüncü nesil mobil iletişim (3G) için kendi ulusal standartlarını (WAPI ve TD-SCDMA) küresel ölçekte kabul ettirmeye çalışmış; bu girişimler başarısız ve maliyetli sonuçlansa da, ülkeye uluslararası standart belirleme örgütlerinde (SDO’lar) önemli bir kurumsal deneyim kazandırmıştır. Günümüzde Çin, tamamen yukarıdan aşağıya yaklaşımdan pragmatik bir hibrit modele evrilmekte; bu geçiş, küresel tanınma mücadelesinin her endüstriyel stratejinin alt metni olarak kalmasıyla pekişmektedir. Bu eğilim, Aralık 2021’de yayımlanan ulusal standartlar sisteminin yüksek kaliteli gelişimini teşvik etmeye yönelik *14. Beş Yıllık Plan*’da da açıkça ortaya konmuştur (Zuniga vd., 2024).

2010’lu yıllardan itibaren ABD–Çin rekabeti, teknoloji standartları yarışında yeni bir evreye geçilmesine yol açmış, ABD, Çin ve AB gibi büyük küresel ekonomilerin tümü, uluslararası standartların belirlenmesine stratejik önem atfetmişlerdir. Huawei’nin 5G altyapısında küresel ölçekte öne çıkması, yarı iletken tedarik zincirlerinde Tayvan’ın stratejik konumu ve yapay zekâ algoritmalarının veri düzenlemelerine bağımlı doğası, standart belirleme süreçlerini yeniden jeopolitik gündemin merkezine taşımıştır (Lee, 2020). Çin, stratejik sanayi planını yayınladığı 2015 yılından itibaren çabalarını hızlandırmış ve bu durum, Çinli şirketleri ve kurumları uluslararası standart belirleme sürecine katılımlarını artırmaya teşvik etmiştir. Çinli aktörler, aktif katkılar, teklif taslaklarının hazırlanması ve SDO’lar içindeki liderlik rolleri açısından standart belirleme kuruluşları ile olan ilişkilerini büyük ölçüde artırmıştır. Bu durum, artık, Çin’in bir takipçi olmaktan ziyade, uluslararası standart belirleyici olma hırısını ve arzusunu yansıtmaktadır (Milne ve Wang, 2022).

Çin, küresel yapay zekâ yönetişimine ilişkin stratejik vizyonunu, 26 Temmuz 2025’te yayımladığı “*Küresel Yapay Zekâ Yönetişimi Eylem Planı*” ile kurumsal bir çerçeveye oturtmuştur. Bu belge, Ekim 2023’te Devlet Başkanı Şi Jinping tarafından ilan edilen “*Küresel Yapay Zekâ Yönetişimi Girişimi*”nin somutlaştırılmış bir uygulama planı niteliğindedir. 2025 Dünya Yapay Zekâ Konferansı’nda (WAIC) Başbakan Li Qiang tarafından duyurulan Eylem Planı, küresel AI yönetişiminin koordinasyonu için 13 maddelik bir yol haritası önermekte ve Çin’in artan teknolojik rekabet ortamında küresel standartların belirlenmesinde etkin bir aktör olma hedefini açık biçimde ortaya koymaktadır. Plan, özellikle altyapı geliştirme, sektörel uygulama, veri kalitesi ve güvenliği, açık ve kapsayıcı bir ekosistem oluşturma, sürdürülebilirlik ve uluslararası işbirliği başlıklarında odaklanmaktadır. Standartlaşma boyutunda ise Çin, ITU, ISO ve IEC gibi kuruluşlar üzerinden uluslararası normlar arasında uyum ve kapsayıcılığın artırılmasını hedeflemektedir. Bu kapsamda, algoritmik önyargıların ortadan kaldırılması, güvenlik ve etik alanlarında teknik standartların hızla güncellenmesi, birlikte işlerliğin güçlendirilmesi ve gelişmekte olan ülkelerin kapasite inşasının desteklenmesi öncelikli hedefler arasındadır. Eylem Planı ayrıca, özellikle Küresel Güney ülkelerinde dijital altyapı kapsayıcılığı ve teknoloji transferi konularına önem vermekte; temiz enerji, akıllı bilişim

altyapısı, veri merkezleri ve su–enerji verimliliği standartları gibi alanlarda uluslararası işbirliğini teşvik etmektedir. Aynı gün Çin hükümeti, merkezi Şanghay’da bulunması planlanan küresel bir Yapay Zekâ İşbirliği Örgütü (Global AI Cooperation Organization) kurulması önerisini de gündeme getirmiştir. Bu örgütün, BM kurumlarının çalışmalarını tamamlayıcı biçimde, küresel AI gelişimini ve regülasyonunu koordine etme, bilgi paylaşımını artırma ve teknolojik tekelleşmeyi önleme amacı taşıdığı belirtilmiştir (ANSI, 2025).

Çin’in bu küresel yönetim hamlesi, 2017’den itibaren yürürlüğe koyduğu *Veri Güvenliği Yasası (Data Security Law)*, *Siber Güvenlik Yasası (Cybersecurity Law)*, *Kişisel Bilgilerin Korunması Yasası (Personal Information Protection Law)* ve *Derin Sentez Teknolojileri ile Üreten Yapay Zekâ Hizmetlerine İlişkin Tedbirler (Interim Measures for Generative AI Services, 2023)* gibi kapsamlı ulusal düzenlemelerin devamı niteliğindedir. Bu mevzuat, güvenlik, etik denetim ve “sosyalist temel değerlere” uygunluk ilkeleri etrafında şekillenmiş; *Yeni Nesil Yapay Zekâ için Etik Normlar (2021)* ve *Yapay Zekâ Endüstrisi için Ulusal Standardizasyon Rehberi (2024)* gibi belgelerle desteklenmiştir. Bu normatif çerçevenin uygulanmasında başta Pazar Düzenleme Devlet İdaresi (SAMR), Çin Siber Uzay İdaresi (CAC) ve Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT) olmak üzere çok sayıda kurumsal aktör rol oynamaktadır. Standart geliştirme alanında ise Çin Elektronik Standardizasyon Enstitüsü (CESI), Ulusal Yapay Zekâ Teknik Komitesi ve Siber Güvenlik Teknik Komitesi aracılığıyla, ISO/IEC Ortak Teknik Komiteleri ile doğrudan etkileşim içinde çalışmaktadır (ANSI, 2025).

3. KURAMSAL ÇERÇEVE

3.1. Genel Olarak

Teknoloji standartlarının siyasallaşması, uluslararası ilişkiler literatürünün birden fazla alt alanıyla kesişen çok katmanlı bir olgudur. Standartların teknik uyumluluğu sağlayan mühendislik çözümleri olduğu kadar; ekonomik maliyetleri belirleyen, pazar erişimini kısıtlayan ve normatif öncelikleri ihraç eden birer güç aracı olduğu yukarıda belirtilmiştir. 2025 itibarıyla, standart belirleme süreçlerinde ABD-Çin rekabeti, *AI Act* GPAI kurallarının⁸ Ağustos 2025’te yürürlüğe girmesi gibi gelişmeler rejim kompleksini derinleştirerek jeoekonomik devletçiliğin somut birer örneğini oluşturmaktadır. Bu çalışma, söz konusu rekabeti açıklamak için dört tamamlayıcı kavramsal mercekten yararlanmaktadır: rejim kompleksi, güç tipolojileri, jeoekonomik devletçilik ve normatif meşruiyet.

3.2. Rejim Kompleksi Yaklaşımı

Rejim kompleksi yaklaşımı (Keohane ve Victor, 2011), standart belirleme süreçlerini tekil ve hiyerarşik bir kurum yerine, ITU, 3GPP, ISO, OECD, AB, G7, IEEE⁹ ve özel konsorsiyumlar

⁸ *AB Yapay Zekâ Yasası (EU AI Act)*, AB’nin YZ sistemlerini risk temelli bir yaklaşımla düzenleyen kapsamlı bir yasal çerçevedir. Bu yasa, 1 Ağustos 2024’te yürürlüğe girmiş olup, genel amaçlı yapay zekâ (General-Purpose Artificial Intelligence - GPAI) modelleri için özel kurallar içermektedir. GPAI kuralları, AI Act’in 50-55. maddelerine dayanır ve özellikle büyük dil modelleri (LLM’ler) gibi geniş kapsamlı, çoklu görevleri yerine getirebilen modelleri (örneğin, GPT serisi, Llama modelleri) hedefler. Bu kurallar, 2 Ağustos 2025 itibarıyla tam olarak yürürlüğe girmiş olup, şeffaflık, güvenlik, telif hakları ve sistemik risk yönetimi gibi alanları kapsar. Kurallar, YZ modellerinin AB pazarına sunulması veya hizmete konulması durumunda zorunludur ve sağlayıcılar (providers) için bağlayıcıdır. GPAI kuralları, AB’nin “güvenilir YZ” vizyonunu yansıtır ve modellerin eğitim verilerinden risk değerlendirmesine kadar tam bir yaşam döngüsü yönetimi gerektirir (EU, 2024).

⁹ *IEEE (Elektrik ve Elektronik Mühendisleri Enstitüsü)*, 1963’te ABD’de kurulan, elektrik, elektronik, bilgisayar bilimi ve telekomünikasyon alanlarında küresel standartlar geliştiren bir organizasyondur. Wi-Fi (IEEE 802.11), Ethernet (IEEE 802.3) ve YZ etiği (P7000 serisi) gibi standartlarla tanınır. 2025’te 400.000+ üyesiyle, 5G, 6G ve siber güvenlikte liderdir. ABD-Çin rekabeti kurumun tarafsızlığını zorlarsa da, IEEE Clean Network ve AB 5G Toolbox ile uyumlu çalışır (IEEE, 2025).

gibi çoklu ve kısmen örtüşen kurumsal alanların etkileşimi olarak kavramaktadır. Bu perspektif, (küresel iklim değişikliği rejim kompleksindeki gibi) 5G'den YZ'ye kadar farklı standart forumlarının birbirini nasıl tamamladığını veya rekabet ettiğini analiz etmeye imkân tanımaktadır. Örneğin, ABD ATIS¹⁰ üzerinden 3GPP'ye daha fazla ağırlık verirken, Çin ise CCSA¹¹ aracılığıyla ITU içinde daha etkin hale gelmeye çalışması rejim kompleksine uygun bir örnek oluşturmaktadır. Gerçekten de Çin, çok taraflı kurumlara yalnızca katılmakla kalmayıp, bunları Çin tercihlerini yerleştirmek için araçlara dönüştürmeyi hedeflemekte, ITU gibi standart belirleme kuruluşlarına da büyük yatırımlar vasıtasıyla angajmana girerek ve kural yazımında öncü avantaj elde etmeye çalışmaktadır (Baumann ve Haug, 2023). Keza, Çin'in *Kuşak ve Yol Girişimi* (BRI)'nde de Pekin'in küresel çıkarlarını ve vizyonunu ilerletmek için uluslararası normları, standartları ve ağları yeniden şekillendirmek ve aynı zamanda Çin'in yerel ekonomik gereksinimlerine hizmet etmek için tasarlandığı ifade edilmektedir. Nitekim BRI aracılığıyla Çin'in çeşitli ülke veya bölgelerle 52 adet standart işbirliği anlaşması imzaladığına dikkat çekilmiştir (Lee, 2021)

Uluslararası ilişkiler literatüründe “rejim” kavramı, belirli bir konu alanını düzenleyen normlar, kurallar ve karar alma prosedürlerinin bütününe ifade eder (Keohane, 1984). Ancak teknoloji standardizasyonu, tek bir kurumsal düzen yerine, kısmen örtüşen ve birbirini bazen tamamlayan bazen de dışlayan çoklu kurallardan oluşan bir rejim kompleksi olarak işlemektedir. ITU, ISO, IEEE gibi örgütler; ETSI gibi bölgesel konsorsiyumlar ve W3C gibi özel sektör platformlarıyla birlikte parçalı bir yönetim alanı yaratmaktadır. Bu parçalanmış yapı, büyük güçlerin farklı forumları stratejik biçimde seçerek (forum shifting/ forum shopping) etki alanlarını genişletmelerine olanak tanırken, orta güçlere de niş alanlarda girişim fırsatları sunmaktadır. Nitekim, güncel bazı gelişmeler, uluslararası yönetim ağlarının ne kadar esnek ve rekabetçi hale geldiğini göstermektedir. Söz gelimi, Avrupa Komisyonu Avrupa standardizasyon kuruluşlarıyla birlikte çalışmakta, AB'nin *Yapay Zekâ Yasası (AI Act)* ile OECD'nin 2024'te güncellediği *Yapay Zekâ İlkeleri*, Çin'in *China Standards 2035* stratejisinde sunduğu alternatif standart yol haritasını büyük ölçüde dışlamaktadır. Benzer biçimde, Birleşik Arap Emirlikleri ve İsrail gibi Ortadoğu ülkeleri, Brezilya, Meksika ve Şili gibi Latin Amerika aktörleri ile Güney Afrika ve Kenya gibi Afrika ülkeleri, kendi bölgesel düzenlemelerini geliştirirken ABD veya Çin kutuplarından birine yakınlaşmakta veya çeşitli çok taraflı forumlarda angajman göstererek standart belirleme süreçlerinde stratejik konum elde etmeye çalışmaktadır (Cooper vd., 2025; OECD 2025a; OECD 2025b; UNESCO, 2024a; ENA, 2025).

Küresel yapay zekâ rejim kompleksinde normatif özerklik peşinde koşan bir aktör olarak Afrika Birliğinin 2024 tarihli *Kıtasal Yapay Zekâ Stratejisi* (African Union, 2024) ve 2025 yılında kabul edilen “*Yapay Zekânın Geliştirilmesi ve Düzenlenmesine İlişkin Yüksek Düzeyli Politika Diyaloğu Bildirisi*” (African Union Commission, 2025) Küresel Güney'in rejim kompleksindeki konumunu göstermesi bakımından önemlidir. Afrika Birliğinin yaklaşımı, Batı merkezli regülasyon modellerine kıyasla daha kapsayıcı, etik temelli ve kalkınma odaklı bir yapay zekâ yönetişimi vizyonu önermektedir. Stratejide, veri mahremiyeti, algoritmik adalet,

¹⁰ ATIS (Alliance for Telecommunications Industry Solutions), 1983'te ABD'de kurulan, kâr amacı gütmeyen bir standartlaşma organizasyonudur. Bilgi ve iletişim teknolojileri (ICT) sektöründe teknik ve operasyonel standartlar geliştirir; ABD merkezli olup, Washington D.C.'de faaliyet gösterir. ANSI (American National Standards Institute) tarafından akredite edilmiş olup, 200'den fazla üye şirket (örneğin, AT&T, Verizon, T-Mobile) ile telekomünikasyon, 5G, 6G, siber güvenlik ve bulut hizmetleri gibi alanlarda standartlar belirler. (ATIS, 2025)

¹¹ CCSA (China Communications Standards Association), Çin'in telekomünikasyon ve bilgi teknolojileri standartlarını geliştiren ulusal organizasyonudur. 2002 yılında kurulan CCSA, Çin Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT) denetiminde çalışır ve 5G, 6G, YZ, Nesnelerin İnterneti (IoT) ve bulut bilişim gibi alanlarda standartlar oluşturur. Çin'in teknoloji ekosisteminde kilit bir rol oynar ve uluslararası standart kuruluşlarında (ITU, 3GPP, ISO) Çin'in etkisini artırmak için faaliyet gösterir (CCSA, 2025)

hesap verebilirlik ve sürdürülebilirlik gibi ilkeler, sadece etik standartlar olarak değil; Afrika'nın dijital egemenliğini güçlendirecek rejim inşası araçları olarak tanımlanmıştır. Bu durum, Küresel Güney'in giderek artan biçimde “rejim alt-sistemleri” yaratarak küresel teknoloji yönetiminde ağırlık kazandığını göstermektedir. Latin Amerika'da “*Latin Amerika ve Karayipler'de Etik Yapay Zekanın Geliştirilmesi*” (Declaración de Santiago) girişimi (Cumbre Ministerial y de Altas Autoridades de América Latina y el Caribe, 2023), Güneydoğu Asya'da ASEAN'ın “*AI Governance Framework*”ü ve Afrika Birliğinin mezkûr stratejisi, kolektif biçimde Küresel Güney'in alternatif normatif düzen yaratma kapasitesini temsil etmektedir.

Bu durum, ülkelerin farklı uluslararası kuruluşlar arasında stratejik geçişler yaparak jeopolitik etki alanlarını genişletmelerine yol açmakta ve standart belirleme süreçlerini küresel rekabetin bir aracı haline getirmektedir. Rejim kompleksi yaklaşımı bağlamında bu gelişmeler, yapay zekâ yönetişiminin geleceğini tek bir hegemonik eksen yerine çok merkezli normatif rekabet dinamiği içinde şekilleneceğini göstermektedir. Belirli bir alanda tek ve bütünselik bir kurum yerine, kısmen örtüşen, bazen rekabet eden, bazen de birbirini tamamlayan çoklu kurallar ve aktörler bir arada varlık göstermekte, bu parçalanmış yapı, orta ve küçük güçlere niş alanlarda inisiyatif alma fırsatları sunarken, aynı zamanda çoklu standart ortamının yarattığı uyum maliyetlerini artırmakta ve küresel tedarik zincirlerinde belirsizlik üretmektedir. Örneğin, ASEAN'ın 2025'te başlattığı *Dijital Ekonomi Çerçeve Anlaşması (DEFA)*, bölge ülkeleri arasında siber güvenlik, veri aktarımı ve dijital standartların uyumlaştırılmasını amaçlamaktadır. Bu süreç, AB ile geliştirilen stratejik ortaklık (EU–ASEAN Blue Book) sayesinde hem doğrudan yabancı yatırımların artmasına hem de bölgenin norm üretme kapasitesinin güçlenmesine katkı sağlamaktadır (EEAS, 2024). Benzer biçimde, 25–26 Kasım 2025'te Kuala Lumpur'da düzenlenecek olan ASEAN Teknoloji Zirvesi, bölgesel düzeyde sınır ötesi dijital işbirliğini teşvik etmeyi hedeflerken, aynı zamanda AB, ABD ve Çin'in dijital yönetim yaklaşımlarının kesiştiği bir etkileşim alanı olarak öne çıkmaktadır (Malaysia SME, 2025). Buna paralel olarak, UNESCO'nun 2023 yılında yayımlamış olduğu *Yapay Zeka Etiğine İlişkin Öneri'leri (Recommendation on the Ethics of Artificial Intelligence)* 2024 itibarıyla UNESCO'nun 194 üye ülkesinin tamamında geçerlidir (UNESCO, 2024b) ve ASEAN üyesi devletlerde yapay zekâ etiği ve veri koruma standartlarının uyumlaştırılmasında referans belge niteliği taşımaktadır. OECD'nin *Digital Economy Outlook 2024* raporunda ise veri taşınabilirliği, sınır ötesi veri akışları ve dijital güvenlik politikalarının çok katmanlı yönetimle desteklenmesi gerektiği vurgulanmış; böylece OECD, teknik standardizasyonun yanında “normatif koordinasyon” alanında da merkezi bir rol üstlenmiştir (OECD, 2024c).

Bununla birlikte, forumların çoğulluğu yalnızca fırsat değil, aynı zamanda risk de yaratmaktadır. ASEAN'ın Ocak 2025'te genişlettiği *YZ Yönetişim Belgesi (AI Governance Document)* ve *Siber Uzay Normları Kontrol Listesi (Checklist on Cyberspace Norms)*, normatif açıdan yenilikçi girişimler olsa da bu çabalar, altyapı yetersizlikleri ve Çin'in Malezya'daki veri merkezlerine müdahaleleri gibi dış baskılar (Huang ve Lin, 2025) gibi nedenlerle kırılgan hale gelmektedir. Özellikle Küresel Güney'de, ASEAN ve Afrika Birliği gibi örgütlerin sınırlı regülasyon kapasitesi, yabancı yatırım dinamikleriyle birleştiğinde, yeni normların ortaya çıkmasını teşvik ederken aynı zamanda dış aktörlerin etki alanını da paralel biçimde genişletmektedir. Dolayısıyla, kurumsal parçalanma teknik yönetim boşluklarını ve “normatif rekabet” alanlarını çoğaltmakta, bu da küçük ve orta güçler için hem özerklik fırsatlarını hem de bağımlılık risklerini aynı anda derinleştirmektedir. Keza, ABD'nin, gelişmekte olan endüstriler için inovasyon ve standartların belirlenmesinde liderlik etmeye ve ayrımcı endüstriyel standartların küresel standartlar haline gelmemesini sağlamak için müttefikler ve ortaklarla birlikte çalışmaya devam etme arzusu da bu kabildendir.

3.3. Güç Tipolojileri Literatürü

Güç tipolojileri literatürü (Farrell ve Newman, 2019; Nye, 2011) standart belirleme süreçlerinin sert askerî kapasiteyle birlikte normatif ve yumuşak güçle de bağlantılı olduğunu göstermektedir. Nye'nin *The Future of Power* eserinde tanımladığı üzere, teknik standartların doğrudan zorlama olmaksızın davranışları yönlendiren bir “yumuşak güç” ve “sert güç”le yumuşak gücün birlikte domine ettiği “akıllı güç” ürettiği anlaşılmaktadır. Nitekim, Huawei'nin 2025 itibarıyla küresel 5G patentlerinin kayda değer bir kısmını elinde bulundurması¹² (Sandys, 2023) ve bu konumunu lisans politikaları¹³ aracılığıyla stratejik bir bağımlılık mekanizmasına dönüştürmesi, teknoloji standartlarının teknik ve aynı zamanda jeoekonomik ve normatif bir güç aracı hâline geldiğini göstermektedir. Benzer biçimde, ABD'nin Clean Network girişiminde uyguladığı “güvenilir satıcı” kriterleri de teknik güvenlik söylemi altında benzer bir dışlayıcı etki yaratarak, küresel teknoloji ekosisteminde normatif kutuplaşmayı derinleştirmektedir.

Farrell ve Newman'ın “*Weaponized Interdependence*” başlıklı makalesi, gücü küresel ekonomik ağlardaki asimetriklerle açıklamıştır. Farrell ve Newman'a göre küreselleşmiş ekonomi ve dijitalleşme, devletleri ve kurumları karşılıklı bağımlılık (interdependence) ilişkileriyle birbirine bağlamıştır. Ancak bu bağımlılık simetrik değildir. Bazı devletler (özellikle ABD), küresel finansal sistem, internet altyapısı, ödeme ağları (SWIFT), teknoloji standartları ve veri akışları gibi merkezî ağ düğümlerini (network hubs) kontrol ettikleri için, bu karşılıklı bağımlılığı bir güç aracına dönüştürebilmektedir. Örneğin ABD'nin *Entity List* kısıtlamaları¹⁴, Çin'in (Huawei'nin Kirin 9000s çipi ihracı gibi)¹⁵ kritik tedarik zincirlerini hedefleyerek kendisine yapısal kaldıraç sağlamakta, standartları belirleyen aktör olarak ABD, hem ekonomik avantaj (lisans gelirleri, pazar hâkimiyeti) hem de düzenleme üstünlüğü biçiminde normatif etki elde etmeyi amaçlamaktadır. Keza, 2025'te AB'nin *5G Toolbox* yaklaşımı¹⁶ da gücü normatif yumuşaklıkla birleştirerek stratejik özerkliğini artıran

¹² Huawei'nin “3007 SEP ailesi”, şirketin 5G standartları kapsamında Standart Esaslı Patent (Standard Essential Patent – SEP) olarak bildirilen 3.007 patent grubunu ifade etmektedir. Bu patentler, 5G teknolojilerinin uygulanabilmesi için teknik olarak zorunlu nitelikte olup, Huawei'ye küresel lisanslama süreçlerinde stratejik bir müzakere gücü kazandırmaktadır. Böylece şirket teknolojik standardizasyonun şekillenmesinde ve jeoekonomik rekabette fikrî mülkiyet üzerinden etki kurmada belirleyici bir aktör haline gelmiştir (Grey, 2023)

¹³ FRAND (Fair, Reasonable and Non-Discriminatory) lisanslaması, standart zorunlu patentlerin (SEP) adil, makul ve ayrımcı olmayan koşullarda lisanslanmasını öngören ilkedir. Bu mekanizma, 3GPP ve ETSI gibi uluslararası standart kuruluşlarının üyelerine, patentlerini tekelsel biçimde kullanmamayı ve standart uyumunu korumayı taahhüt ettirir. FRAND, teknolojiye erişimi kolaylaştırırken, fikrî mülkiyet hakları ile rekabet hukukunun dengelenmesini amaçlar (Contreras, 2015).

¹⁴ *Entity List* (Varlık Listesi), ABD'nin ulusal güvenliği veya dış politika çıkarlarına aykırı faaliyetlerde bulunduğu düşünülen yabancı kişi, şirket, kurum veya organizasyonların yer aldığı listedir. Bu listeye giren taraflara, ABD menşeli ürünlerin, yazılımların, teknolojilerin lisanssız olarak ihracatı, yeniden ihracatı veya transferi yasaklanır (Bureau of Industry and Security, 2025).

¹⁵ Huawei'nin Kirin 9000s çipinin ihracı, ABD'nin ihracat kısıtlamalarına rağmen Çin'in ileri yarı iletken üretiminde kendi kendine yeterliliğe yaklaştığını göstermektedir. SMIC'in 7 nm teknolojisiyle ürettiği bu işlemci, Çin'in teknolojik özerklik ve standart belirleme kapasitesinde önemli bir eşiğe işaret ederken, aynı zamanda küresel tedarik zincirlerinde jeoekonomik rekabetin yeni bir boyut kazanmasına yol açmıştır (Kirton ve Cherney 2023).

¹⁶ AB'nin 5G Toolbox yaklaşımı, 2020'de kabul edilen ve üye devletlerin 5G altyapılarında güvenliği güçlendirmesi için hazırlanan ortak bir risk azaltma çerçevesidir. Bu yaklaşım, yüksek riskli tedarikçilerin kritik bileşenlerden dışlanması, tek bir firmaya bağımlılığın önlenmesi, güvenlik sertifikasyonları ve yazılım güncellemelerinin güvenli yönetimi gibi stratejik ve teknik önlemleri içerir. Ayrıca bilgi paylaşımı ve standartların uyumlaştırılması gibi destekleyici mekanizmalar da öngörülmüştür. Ayrıca bilgi paylaşımı ve standartların yaygınlaşmasını engellemeden, AB genelinde ortak bir güvenlik çitası belirleyerek siber güvenlik ve ulusal güvenliği sağlamaktır (European Commission, 2020).

önemli bir örnek olarak öne çıkmaktadır. Bu gelişmeler, standart belirlemenin çoğu zaman görünmez ama uzun ömürlü bir güç kaynağı olduğunu göstermektedir.

3.4. Jeoekonomik Devletçilik Kavramı

Jeoekonomik devletçilik (Blackwill ve Harris, 2016) kavramı, devletlerin ekonomik araçları stratejik hedefler için kullanma eğilimini öne çıkarmış, standartlar teknik uyumu sağlamakla birlikte, devletlerin jeostratejik konumlarını pekiştiren dış politika araçlarına dönüşmüştür. Blackwill ve Harris'in *War by Other Means* eserinde, jeoekonomi; "silahlı olmayan araçlarla jeopolitik hedefleri ilerletme" olarak tanımlanmıştır. Bu kapsamda ticaret, yatırım ve enerji politikalarıyla rakipleri cezalandırma ya da müttefikleri kazanma stratejik bir yöntem haline gelmiştir.

Çipler, 5G ve yapay zekâ gibi stratejik teknolojiler üzerindeki düzenlemeler ve karşı hamleler, devletlerin ulusal güvenlik gerekçeleriyle piyasa mekanizmalarına müdahalesini meşrulaştırdığı yeni bir jeoekonomik paradigma yaratmıştır. Bu süreçte, standart belirleme artık yenilik ve verimlilikle ilgili olduğu kadar stratejik özerklik, tedarik zinciri kontrolü ve normatif güç inşasıyla da tanımlanmaktadır. Söz gelimi, ABD'nin AI Diffusion Framework'ü¹⁷ ve 2025'te uygulamaya koyduğu Nvidia çip ihracat yasağı (Teng, 2024) jeoekonomik devletçiliğin yükselişiyle de ilişkilendirilebilir. AB'nin *Doğrudan Yabancı Yatırım Tarama* mekanizmaları, *5G Toolbox* yaklaşımı ve *CHIPS Act* kapsamındaki çeşitli sübvansiyonları gibi tedarik zinciri politikaları ve *Clean Network* girişimi, Çin'in *Made in China 2025* hedefleri ve uygulamalar birlikte değerlendirildiğinde, standart belirleme süreçlerinin giderek jeopolitik rekabetin temel alanı haline geldiğini göstermektedir. Çin'in 5G ekosisteminde kendi standartlarını (örneğin WAPI, TD-SCDMA, NB-IoT) yaygınlaştırma çabaları bu eğilimi daha da derinleştirmektedir.

Bu rekabet ortamında, Hollanda'nın 2025'te Çinli Nexperia'nın Almanya'daki yarı iletken tesisine el koyması (Hajdari, 2025) Avrupa'da stratejik yatırımların güvenlik temelli denetimini hızlandırdığına işaret etmektedir. Bu gelişme, Almanya'nın otomotiv endüstrisinde yaşanan çip darboğazını daha görünür kılmış (Beardsley, 2025), aynı dönemde, Çin'in 2024 yılında Nvidia'ya karşı başlattığı tekel soruşturması (Kharpal, 2025), küresel çip piyasasında karşılıklı misilleme döngüsünün bir yansıması olarak ortaya çıkmış ve teknoloji standardizasyonunun politik ve stratejik bir alana dönüştüğünü göstermiştir.

3.5. Normatif Meşruiyet Literatürü

Teknolojik düzenlemeler, kimlerin meşru norm üreticisi olduğu sorusunu gündeme getirirken forum kompleksindeki boşlukları da derinleştirmektedir. Uluslararası hukuk ve norm meşruiyeti literatürü (Franck, 1990; Koskeniemi, 2005), teknoloji standartlarının teknik uyumun ötesinde meşru norm üretimi meselesi olduğunu vurgulamaktadır. Franck'ın *The Power of Legitimacy Among Nations* başlıklı eserinde tanımladığı meşruiyet, kuralların "çekim gücü" (pull to compliance) ile ölçülmektedir. *Belirlilik* (determinacy), *sembolik doğrulama* (symbolic validation), *tutarlılık* (coherence) ve *uyum* (adherence) kriterleri bu çekim gücünün kıstaslarıdır. Bu ölçütler baz alındığında AB'nin *Genel Veri Koruma Tüzüğü* (GDPR)'nin bireysel hak odaklı modeli, veri korumasını evrensel bir insan hakkı normu olarak kodlayarak AB'nin norm ihracatını meşrulaştırırken aynı zamanda Franck'ın "belirlilik" ve "sembolik doğrulama" ölçütlerini güçlendiren bir normatif tutarlılık da yaratmaktadır. Buna karşın, Çin'in

¹⁷ "AI Diffusion Framework" (resmî adıyla *Framework for Artificial Intelligence Diffusion* veya *AI Diffusion Rule*) ABD tarafından geliştirilen bir düzenleyici / stratejik çerçevedir. Bu çerçeve, yapay zekâ teknolojilerinin yayılımını ("diffusion") kontrol altına almayı, ABD'nin AI liderliğini korumayı ve stratejik riskleri (özellikle teknoloji transferini ve advers aktörlerin eline geçmesi) azaltmayı amaçlar (Heim, 2025).

Kişisel Bilgilerin Korunması Yasası (PIPL)¹⁸, veri yönetişimini bireysel mahremiyetten ziyade ulusal güvenlik ve kolektif refah ilkeleri üzerinden tanımlayarak, devlet denetimine dayalı alternatif bir meşruiyet iddiası geliştirmektedir. Böylece iki rejim, uluslararası alanda teknik standartlarda olduğu gibi “meşruiyetin kaynağı” konusunda da rekabet eden iki farklı normatif anlatıyı temsil etmektedir (Kitchen, 2020).

Koskenniemi’nin *From Apology to Utopia* (2005) çalışması ise, uluslararası hukuk argümanlarının “güç temelli” ile “ütopyacı” (evrenselci ve normatif) kutuplar arasında salındığını ileri sürmüştür. Bu yaklaşım, teknoloji standartlarının da benzer bir ikili gerilim içinde şekillendiğini düşündürür. Bir yanda teknik standartların küresel ticari düzenin rasyonel araçları olarak meşrulaştırılması, diğer yanda bu standartların evrensel değerler ve kamusal çıkar adına savunulması (ütopyacı söylem) vardır. Dolayısıyla, normatif meşruiyetin kaynağına ilişkin tartışma, teknik uyumun ötesinde güç ve değer arasındaki bu yapısal diyalektiği de yansıtmaktadır. Bu ikilem teknoloji standartlarına da yansımıştır. ITU ve 3GPP gibi teknik forumlar işbirliği vaadiyle meşruiyet kazanırken, forum seçimleri bu ideali gölgeleyen stratejik bir güç mücadelesi haline gelmiştir.

Ayrıca, realist perspektiften (Mearsheimer, 2001) standartlar, büyük güçlerin çıkarlarını yansıtan araçlar olarak yorumlanabilir. Liberal kurumsalcılık yaklaşımıyla (Keohane, 1984; Keohane ve Nye, 2012) ise bu forumlar, işbirliğini teşvik eden, şeffaflığı artıran ve maliyetleri düşüren unsurlar olarak değerlendirilebilirken, konstrüktivist teoriye (Wendt, 1999; Finnemore ve Sikkink, 1998) göre ise standartlar, kimlik ve değerlerin yeniden üretildiği normatif bir mücadele alanı olarak görülebilir.

Yukarıda özetlenen kuramsal yaklaşımlar, çalışmanın politika analizine kavramsal bir çerçeve sunmaktadır. Rejim kompleksi, güç tipolojileri, jeoekonomik devletçilik ve normatif meşruiyet kavramları; standart belirleme süreçlerini teknik uyumun ötesinde, güç, çıkar ve değer rekabetinin iç içe geçtiği çok katmanlı yönetim ağları olarak kavramayı mümkün kılmaktadır. Bu kavramsal mercekler, bir sonraki bölümde ayrıntılı biçimde ele alınacak olan küresel teknoloji yönetişiminde rejim karmaşası, forum alışverişi ve normatif rekabet dinamiklerini açıklamak için analitik bir temel oluşturmaktadır.

4. KÜRESEL TEKNOLOJİ YÖNETİŞİMİNDE REJİM KARMAŞASI VE NORMATİF REKABET: PARÇALANMA, FORUM SEÇİMİ VE NORM İHRACI

Kuramsal çerçevenin ortaya koyduğu çok katmanlı yapı, teknoloji yönetişiminde birbirine rakip veya örtüşen forumların (OECD, ITU, 3GPP, ISO vb.) neden aynı anda etkili olabildiğini anlamak açısından açıklayıcıdır. Bu kurumlar, yalnızca teknik standartların belirlenmesinde değil aynı zamanda dijital ekonomi, veri akışı, yapay zekâ ve siber güvenlik gibi alanlarda norm üretiminin de merkezinde yer almaktadır. Dolayısıyla, küresel düzeyde ortaya çıkan “rejim karmaşası”, güç rekabetinin teknik terminolojiye, diplomatik dilin ise standartlara yansıdığı bir alan olarak belirmektedir. Bu çerçevede analiz hem normatif meşruiyet tartışmalarını hem de çıkar temelli düzenleme stratejilerini birlikte değerlendirerek, devletler ve özel aktörler arasındaki etkileşim ağlarını çözümlemeyi amaçlamaktadır.

Yukarıda teknoloji standartlarının giderek artan stratejik öneminin, küresel yönetim mimarisinde yeni gerilimler yarattığı ifade edilmiştir. Klasik anlamda uluslararası kurumlar uzun süre boyunca teknik konularda görece tarafsız bir zemin sunmuşlardır. Örneğin, ITU’nun

¹⁸ Çin’in PIPL düzenlemesi, *Personal Information Protection Law* (Kişisel Bilgilerin Korunması Kanunu) olarak bilinir ve Çin’de 1 Kasım 2021’de yürürlüğe girmiştir. Bu düzenleme, GDPR’ye benzer şekilde kişisel verilerin korunmasını amaçlar, ancak Çin’in siyasi ve ekonomik bağlamına özgü bazı farklılıklar içerir (PIPL, 2022).

radio ve ağ standartlarını koordine etmesi, 3GPP'nin mobil teknolojiler için spesifikasyonlar geliřtirmesi ve ISO'nun ticari engelleri azaltan uluslararası standartları teřvik etmesi, küresel uyumluluęu desteklemiřtir. Ancak son on yılda, büyük güç rekabetinin derinleřmesi ve teknolojik egemenlik stratejilerinin ön plana çıkmasıyla bu forumların iřlevi ve meřruiyeti ciddi biçimde sorgulanır hâle gelmiřtir. Bu tablo, teknoloji standartlarının gelecekte teknik mühendislik ve küresel yönetim mimarisinin meřruiyeti, sürdürülebilirlięi ve güç dengeleri ağısından da belirleyici olacağını göstermektedir.

Standart savařlarının kurumsal düzeyde yarattıęı parçalanma, çok kutuplu dünya düzeninin karakteristik bir özellięi olarak giderek daha görünür hale gelmektedir. Örneęin, ABD ve Çin'in standart belirleme forumlarında yürüttükleri diplomatik manevralar ve teknoloji odaklı iřbirlikleri, süreci teknik olmaktan çıkarıp uluslararası jeopolitik rekabet alanına dönüřtürmektedir. Standartların teknik, ekonomik ve normatif boyutları arasındaki keřiřim, uluslararası iliřkilerde yeni bir rekabet ve iřbirlięi sahası yaratmaktadır. Öte taraftan, standart belirleme süreçlerinin farklı örgüt ve platformlara daęılmış olması, devletler ve özel sektör aktörlerine stratejik forum seçimi imkânı sağlamaktadır. Örneęin, ABD ve müttefikleri 5G standartlarını ağırlıklı olarak 3GPP üzerinden şekillendirirken, Çin ITU ve ISO'daki teknik komitelerde daha proaktif bir rol üstlenmektedir. Bu çoklu forum yapısı, standartların küresel ölçekte tek bir mutabakatla kabul edilmesini zorlařtırmakta ve bölgesel veya ikili düzenlemelerin ön plana çıkmasına yol açmaktadır.

Kurumsal parçalanma ve koordinasyon eksiklięi, günümüz uluslararası düzeninde rejim karmařasının en görünür tezahürlerinden biridir. Yapay zekâ güvenlięi, veri aktarımı ve yarı iletken üretimi gibi stratejik alanlarda yařanan yönetim ağıkları, teknik standardizasyon sorunları dıřında farklı kurumsal mantıkların ve düzenleyici önceliklerin çeliřmesinin sonucudur. Örneęin, OECD'nin *Yapay Zekâ İlkeleri* ve AB'nin *AI Act* kapsamında geliřtirilen genel amaçlı yapay zekâ (GPAI) düzenlemeleri, řeffaflık, hesap verebilirlik ve telif uyumu konularında yüksek řeffaflık ve açıklanabilirlik standartları getirirken; Çin'in Nisan 2025'te yürürlüęe koyduęu üretken yapay zekâ (Generative AI – GenAI) geçici güvenlik standartları, içerik güvenlięi, veri egemenlięi ve politik istikrar gibi ulusal güvenlik temelli ilkeleri önelemektedir. Bu farklı yönetim mantıkları, küresel ölçekte faaliyet gösteren platformlar ağısından ciddi bir düzenleyici gerilim yaratmaktadır. Nitekim OpenAI, Google DeepMind ve Anthropic gibi Batılı teknoloji řirketleri, AB mevzuatı kapsamında kimi yükümlölüklerine tabi olurken; Baidu ve SenseTime gibi Çinli řirketler ise ulusal içerik filtreleme ve veri denetimi gibi farklı protokollere uymak zorundadır. Dolayısıyla aynı tür üretken yapay zekâ teknolojileri, farklı hukukî rejimlerde farklı biçimlerde tanımlanmakta ve denetlenmektedir. Bu durum, uluslararası düzeyde teknolojik birlikte iřlerlięin önünde önemli bir engel oluřtırmakta; küresel AI yönetimini jeopolitik bloklařma yönünde şekillendirmektedir. Benzer biçimde, GDPR'nin Schrems II kararından¹⁹ sonra zorunlu hale gelen Transfer Impact Assessment (TIA) süreçleri ile ABD Adalet Bakanlığı'nın (DOJ) veri eriřimine iliřkin düzenlemeleri²⁰ arasındaki farklar,

¹⁹ *Schrems II* kararının (C-311/18, 2020) ardından, Avrupa Birlięi dıřına kiřişel veri aktarımı yapan kuruluşlar için Transfer Impact Assessment (TIA) süreçleri GDPR kapsamında zorunlu hale gelmiř, TIA, dıř veri aktarımında yalnızca biçimsel deęil, maddi koruma düzeyini de deęerlendiren bir uyum mekanizması haline gelmiřtir Avrupa Adalet Divanı, *EU-US Privacy Shield* mekanizmasını geçersiz kılarak, üçüncü ölkelere yapılan veri aktarımlarında "eřdeęer koruma" ilkesinin saęlanması şart kořmuřtur. Bu doęrultuda, Madde 46'daki Standart Sözleřme Maddeleri (SCCs) tek başına yeterli görölmemekte; veri sorumlularının, alıcı ölkenin gözetim rejimini, veri eriřim risklerini ve alınan teknik/organizasyonel önlemleri analiz ettięi TIA belgelerini hazırlaması gerekmektedir (European Data Protection Board [EDPB], 2021).

²⁰ ABD Adalet Bakanlığı (DOJ) düzenlemeleri, teknolojik standart rekabetinin hukuki boyutunu şekillendiren başlıca politika araçlarından biridir. DOJ düzenlemeleri teknik standartların ötesine geçerek ABD'nin hukuk temelli norm ihracı stratejisini desteklemektedir. DOJ, özellikle antitröst ve ulusal güvenlik temelli incelemeler yoluyla teknoloji řirketlerinin piyasa davranıřlarını düzenlemekte; böylece ekonomik güvenlięi normatif düzeyde

veri aktarımı alanında benzer bir parçalanmayı yansıtmaktadır. Bu farklılıklar, özellikle bulut bilişim ve AI model eğitimi gibi alanlarda faaliyet gösteren çok uluslu şirketler için artan hukuki belirsizlik, uyum maliyetleri ve yönetim tutarsızlıkları yaratmaktadır. Bu parçalanmış yapı, büyük güçlerin kendi normatif modellerini küresel ölçekte yaymasına stratejik bir fırsat sunmaktadır. Bu modeller, finansman mekanizmaları, teknik eğitim programları ve ihracat politikaları aracılığıyla üçüncü ülkelere ihraç edilmekte ve böylece teknoloji standartları, salt teknik uyum meselesinden çıkıp jeopolitik strateji ve normatif liderlik mücadelesinin aracı haline gelmektedir.

5. GÜNCEL STANDART ALANLARI VE REKABET DİNAMİKLERİ

5.1. Genel Olarak

Standart; çoğaltma veya ara bağlantı (interoperability) imkânı tanıyan belirli teknik parametreleri tanımlayan teknik belgedir. Bu belge, farklı aktörlerin söz konusu ürünün, hizmetin veya teknolojinin kullanımına katılabilmesini ve bundan pay alabilmesini mümkün kılar (Cargill, 2022). Başka bir söyleyişle, teknik standartlar, çeşitli mal ve hizmetlerin “kalitesini”, “güvenliğini” ve “uyumluluğunu” artırmak amacıyla oluşturulan teknik tanımlar ve süreçlerdir. Bu standartlar, gelecekteki ürünlerin ve teknolojik gelişimlerin yönünü belirleyen temel çerçeveler olarak işlev görür. Zira, bunlar; “kilitlenme etkileri (lock-in effects)” ve “yola bağımlılık (path dependency)” yaratarak belirli teknolojilerin veya yöntemlerin diğerlerine kıyasla avantajlı hale gelmesine neden olurlar. Dolayısıyla, standartların belirlenmesi toplumsal refah ve verimlilik açısından önemli faydalar sağlamakla birlikte hangi teknolojilerin geleceğin pazarlarında baskın hale geleceği ve bu standartlara erken uyum sağlayan aktörlerin ekonomik ve stratejik üstünlük elde edip etmeyeceği konusunda da belirleyici etkiler doğurur (Seaman, 2020).

Teknoloji standartları, küresel ekonominin görünmez mimarisi niteliğinde olup, uluslararası düzenin işleyişini şekillendiren normatif kurallar bütünü olarak işlev görmektedir. Donanım ve yazılım arasında birlikte çalışabilirliği mümkün kılmak, veri güvenliği ve gizliliğini sağlamak, pazar girişini ve rekabeti düzenlemek gibi işlevleriyle standartlar, yalnızca teknik tercihler değil aynı zamanda ekonomik çıkarların, jeopolitik stratejilerin ve normatif güç projeksiyonunun da merkezinde yer almaktadır. Bu nedenle standart belirleme süreçleri, devletlerin stratejik özerklik arayışlarının, şirketlerin küresel rekabet stratejilerinin ve büyük güçler arasındaki hegemonya mücadelesinin kesişim noktasını oluşturmaktadır.

Standartlar, teknik uyumun ötesinde ekonomik güvenlik, teknolojik bağımlılık ve değer temelli düzen inşasının araçları olarak işlev görmekte; dolayısıyla küresel düzenin geleceğini belirleyecek uzun vadeli rekabetlerin ana sahnesine dönüşmektedir. Günümüzde bu rekabetin merkezinde dört kritik alan öne çıkmaktadır: 5. nesil mobil iletişim protokolleri (5G), yarı iletken üretim zincirleri, yapay zekâ güvenlik ve etik standartları ile uluslararası veri aktarım düzenlemeleri.

5.2. 5G İletişim Standartları

5G teknolojisi, daha yüksek bant genişliği ve hızlı veri iletimi ihtiyacına yanıt vermekle kalmamakta, aynı zamanda yenilikçi ve yıkıcı potansiyelleriyle dijital ekosistemi yeniden şekillendirmektedir. 5G, bireyler, işletmeler ve devletler açısından hem yeni fırsatlar hem de artan siber ve ekonomik bağımlılıklar gibi riskleri beraberinde getiren bir dijital dönüşüm dalgası yaratmaktadır. Bağlantılı cihaz sayısındaki büyük artış ve veri akışının hızlanması,

kurumsallaştırmaktadır. Bu çerçevede, Huawei ve TikTok gibi firmalara yönelik CFIUS ve FCPA uygulamaları, rekabet hukukuna ve jeoekonomik devletçiliğe dayalı bir dış politika aracına dönüşmüştür (WilmerHale, 2025).

otonom araçlar, bulut bilişim, makine öğrenimi ve nesnelerin interneti (IoT)²¹ gibi gelişmekte olan teknolojilerin yaygınlaşmasını mümkün kılmaktadır. Aynı zamanda bu gelişmeler, dijital platformların, sosyal ağların ve geleneksel iş modellerinin dönüşümüne yol açarak yeni ağ mimarilerini teşvik etmektedir (Nestoras ve Cappelletti, 2022).

Yapılan araştırmalar, 5G teknolojisinin 2035 yılına kadar 13 trilyon dolardan fazla yeni ekonomik değer yaratabileceğini ve yalnızca 5G küresel değer zincirinde 22 milyondan fazla istihdam sağlayabileceğini öngörmektedir. 5G'nin potansiyel uygulamaları, yalnızca daha hızlı mobil cihazlarla sınırlı kalmayıp, çok daha geniş bir yelpazeye yayılmaktadır. Bu sistem; mobil geniş bant, ultra güvenilir düşük gecikmeli iletişim, devasa makine tipi iletişim, enerji verimliliği ve güvenlik başlıklarında iyileştirmeler vadetmektedir. Bu alanlarda eşzamanlı olarak gerçekleştirilen iyileştirmeler, verileri üretme, işleme, iletme, depolama ve güvence altına alma kapasitesine sahip, gerçekten bağlantılı bir dünyanın gereksinimlerini karşılayan ağların oluşmasını mümkün kılmakta ve bu ağlar aracılığıyla söz konusu dünyanın yarattığı faydalardan etkin bir şekilde yararlanılmasını sağlamaktadır (Kitchen, 2020).

5. nesil mobil iletişim altyapısı, yalnızca gigabit seviyesinde veri iletimi ve milisaniye düzeyinde düşük gecikme kapasitesi sağlamakla kalmayıp, otonom araçlar, endüstriyel otomasyon, nesnelerin interneti ve kritik altyapı kontrol sistemleri gibi geleceğin teknolojileri için merkezi bir omurga niteliği taşımaktadır.²² Bu özellikler sayesinde 5G; yüksek hızlı mobil geniş bant (eMBB), ultra güvenilir ve düşük gecikmeli iletişim (URLLC) ile yoğun makine tipi iletişim (mMTC) olmak üzere üç temel kullanım senaryosunu destekleyen bir iletişim platformuna dönüşmektedir. Örneğin, URLLC sayesinde endüstriyel robotlar gerçek zamanlı senkronizasyonla çalışabilirken, mMTC ile milyarlarca IoT cihazı aynı anda bağlanabilir. Bu nedenle, 5G standartlarının belirlenmesi süreci, uluslararası hukuk ve yönetim alanında güç rekabetinin en görünür sahnesine dönüşmüş; teknik standartlar, devletlerin normatif etki ve jeopolitik kaldıraç inşa etmesinin stratejik araçları hâline gelmiştir.

5G teknolojisinde ABD, Çin ve müttefikleri arasındaki rekabet, iki kutuplu güç mücadelesi bağlamında, ABD- Çin ilişkilerinin doğasına dair daha geniş bir tartışmayı yeniden gündeme getirmektedir. ABD- Çin rekabeti, XX. yüzyıldaki ABD- Sovyet çatışmasına benzer biçimde yeni bir “Soğuk Savaş” olarak çerçevelenmektedir. Rekabetin kökenlerine ilişkin farklı açıklamalar bulunmaktadır. Bunlar arasında; Çin'in Amerikan çıkarlarına meydan okuyan ekonomik gücünün olağanüstü yükselişi, komünist rejimin bu yükselişten aldığı özgüven ve liberal uluslararası düzenin revizyonu yönündeki iddialı tutumu öne çıkmaktadır. Farklı

²¹ IoT, fiziksel nesnelerin sensörler, yazılımlar ve teknolojilerle internete entegre edilerek veri alışverişi yapmasını sağlayan bir ağ paradigması olarak tanımlanmıştır. Bu sistem, akıllı ev cihazları, endüstriyel makineler ve tıbbi ekipmanlar gibi unsurların özerk etkileşimini mümkün kılmış; veri toplama, analiz ve otomasyonu dönüştürmüştür. IoT'nin mekanizması, gömülü sensörlerin veri algılaması, bulut tabanlı iletim ve yapay zekâ tabanlı işlemeye dayanmıştır.

²² 3GPP ve ITU tarafından belirlenen frekans tahsisi, sub-6 GHz ve mmWave bantları gibi teknik parametreler, OFDM tabanlı New Radio arayüzü gibi modülasyon teknikleri, ağ dilimleme (network slicing) ve 5G AKA kimlik doğrulama gibi güvenlik protokolleri ağ performansını ve küresel pazar paylarını ve ulusal güvenlik stratejilerini doğrudan şekillendirmektedir. 3GPP Release 18 paketi, kamuoyunda “5G-Advanced” veya “5.5G” olarak adlandırılan yeni nesil mobil iletişim standartlarını tanımlamakta olup, Aralık 2023 itibarıyla Radyo Erişim Ağı (RAN) spesifikasyonlarını dondurarak ve standartlaştırma sürecinin 2025'in ikinci yarısında tamamlanması öngörülmektedir. Bu sürüm, mevcut 5G altyapısına kıyasla yapay zekâ tabanlı ağ optimizasyonu, otonom yönetim kapasitesi ve karasal olmayan ağlar (Non-Terrestrial Networks, NTN) aracılığıyla uydu bağlantısının entegrasyonu gibi yenilikçi özellikler içermektedir. Radyokomünikasyon sektörü altında faaliyet gösteren WP5D Çalışma Grubu, söz konusu gelişmeleri IMT-2020 çerçevesinin bir uzantısı olarak resmen onaylamış ve aynı zamanda “IMT-2030” başlığı altında 6G vizyonuna yönelik ön hazırlıklara başlamıştır (3GPP, 2025). Bu çerçevede Release 18, 5G'nin olgunlaşma evresini temsil etmekle kalmayıp, küresel mobil iletişimin 6G dönemine geçişinde teknik ve kavramsal bir köprü işlevi görmektedir.

unsurların etkili olduğu bu süreçte, ABD ile Çin arasındaki belirgin ideolojik farklılıklar ve bunların daha geniş jeopolitik dinamiklerle kesişimi, söz konusu çatışmanın temel itici güçlerinden biri olarak değerlendirilmektedir (Nestoras ve Cappelletti, 2022).

5G üzerindeki jeopolitik rekabet, yeni ekonomik düzenin temellerini kimin şekillendireceğini ve modern yönetişimin teknik altyapısını kimin inşa edeceğini belirleyecek seviyededir. Zira, 5G ekipmanı ve altyapısında tek bir tedarikçinin hâkimiyet kurması, ulusal ve uluslararası güvenlik açısından ciddi riskler barındırmaktadır. Bu bağlamda, Çin'in 5G pazarında baskın sağlayıcı konumuna gelmesi özellikle kritik görülmektedir. Böyle bir durumda Çin, 5G ağları üzerinden bilgi akışını kontrol etme kapasitesine ulaşarak veri güvenliği ve altyapı yönetimi üzerinde stratejik bir üstünlük elde edebilir. Çin'in 5G hâkimiyeti, ciddi veri güvenliği endişelerini gündeme getirince Birleşik Devletler hükümeti, uluslararası standardizasyondaki hegemonik üstünlüğünü muhafaza etmek amacıyla özel sektörle daha entegre işbirliği planları geliştirmiş; bu girişim, *Ulusal Standartlar Stratejisinin* (National Standards Strategy) 2023'te yayımlanmasına yol açmıştır. Bu belge, kritik ve yeni ortaya çıkan teknolojilerde ABD liderliğini pekiştirmeyi hedefleyerek, özel sektörün standart geliştirme süreçlerindeki önceliğini vurgulamış, hükümetin rolünü ise kamu-özel ortaklıkları yoluyla destekleyici bir konuma indirgemıştır (Zuniga vd., 2024).

AB, 5G teknolojisinin potansiyel risklerinin farkında olup Huawei'nin kıta çapında yasaklanması gibi koordineli önlemleri tartışmaktadır. AB, dijital tek pazar ve veri koruma (GDPR), siber güvenlik (NIS) ile elektronik iletişim (EECC) alanlarında yasama paketleri kabul etmiş ve 5G ağlarının sınırlı coğrafyalarda uygulanmasını başlatmıştır. Üye devletler, Çinli 5G ekipman üreticilerine karşı farklı yaklaşımlar benimsemiş, bazı ülkeler açıkça yasaklarken, diğerlerinin hâlen mevzuat çalışması içinde oldukları görülmektedir. AB, ulusal başkentlere hareket serbestisi tanıyan yönergeler sunmuş olup, gelecekte Çin kaynaklı risklere karşı koordineli bir yanıt da dahil olmak üzere, kıta çapında 5G uygulamalarını desteklemesi olasıdır (Nestoras ve Cappelletti, 2022).

Huawei'nin 5G alanındaki patent üstünlüğü ile ABD'nin güvenlik gerekçeleriyle uyguladığı ihracat kısıtlamaları, teknoloji standartlarının belirlenmesinin hem teknik hem de jeopolitik boyutlar taşıdığını açık biçimde göstermektedir. Huawei'nin kendi lisanslama yöntemi üzerinden oluşturduğu ekonomik bağımlılık ilişkileri, Batılı rakipleri Nokia ve Ericsson'un rekabet gücünü zayıflatmakta ve küresel pazar dengelerini etkilemektedir. Bu koşullar altında 5G standartları, teknik uyumun sağlanması ile birlikte uluslararası güç mücadelesinde stratejik araç haline gelmiştir. Çin'in *China Standards 2035* vizyonu kapsamında yürüttüğü standart-forum diplomasisi, ABD'nin WRC-23 sürecindeki spektrum harmonizasyonu tartışmalarına yön verirken²³ orta ölçekli ülkeler, bu dinamik rekabet ortamında seçici entegrasyon ve iş birliği fırsatları elde edebilmektedir.

5.3. Yarı İletken Üretim Standartları

XXI. yüzyılın güç rekabeti artık savaş alanlarında değil, yarı iletkenlerin mikroskobik devrelerinde yaşanmaktadır. Devletlerin uluslararası sistemdeki konumu, askeri kapasite kadar teknolojik üstünlükle de belirlenmektedir (Khan, 2025). ABD ve Birleşik Krallık'ın son savunma stratejilerinde vurgulandığı üzere, yapay zekâ ve yarı iletkenler ekonomik büyüme,

²³ WRC-23 (*World Radiocommunication Conference 2023*), ITU tarafından düzenlenen ve mobil iletişimde hangi frekans bantlarının hangi teknolojiler (örneğin 5G, 6G, uydur iletişimi) için kullanılacağını belirleyen küresel düzeydeki en önemli toplantıdır. Spektrum harmonizasyonu ise, dünyanın farklı bölgelerinde aynı frekans bantlarının benzer amaçlarla kullanılması, böylece cihazların ve ağların küresel uyumluluğunun sağlanması anlamına gelir (ITU, 2023).

askeri modernizasyon ve stratejik özerklik için temel teknolojiler haline gelmiştir (HM Government, 2025; The White House, 2022). Bu yüksek katma değerli alanlar, karmaşık patent ağları ve Ar-Ge yatırımlarıyla küresel güç dengesinin kalbinde yer almaktadır (Staglianò, 2024; Leicht, 2025). Nitekim, 2023 itibarıyla 70’den fazla ülke ulusal yapay zekâ stratejisi yürürlüğe koymuştur (Körömi, 2025).

Soğuk Savaş’ın nükleer caydırıcılığa dayalı ikili rekabetinden farklı olarak, günümüzdeki güç mücadelesi ekonomik, kurumsal ve normatif boyutlar taşımaktadır. Teknolojik üstünlüğün göstergesi olarak kabul edilen yarı iletkenler ve YZ hakimiyeti, küresel standart koyma kapasitesinin de göstergesi haline gelmiştir. Zira, savaş uçaklarından otomobillere, cep telefonlarından enerji şebekelerine kadar tüm kritik altyapı bu mikroçiplere bağımlıdır. Uzmanlara göre, günümüzde yarı iletken endüstrisi küresel ekonominin görünmez omurgasıdır. Bu, 2020’de dünya GSYİH’sının yalnızca %0,5’ini oluştursa da otomotiv, savunma ve iletişim gibi trilyon dolarlık sektörlerin temelini teşkil etmektedir (Amato-Montanaro, 2024). Bu nedenle üretim zincirindeki aksama ekonomik güvenliğin yanı sıra ulusal savunmayı da doğrudan etkiler. Dolayısıyla, Miller’in (2022) ifadesiyle yarı iletkenler “modern ekonominin petrolü” haline gelmiştir. Bu durum, küresel düzenin giderek teknoloji jeopolitiği üzerinden şekillendiğini göstermektedir.

2010’ların sonlarından itibaren Çin’in yükselişi, fikri mülkiyet, siber güvenlik ve inovasyon alanlarındaki gerilimlerle “çip savaşı”nı başlatmıştır. ABD’nin gelişmiş çiplere erişimi sınırlayan yaptırımları yalnızca Pekin’i değil, Tayvan (TSMC), Hollanda (ASML) ve Güney Kore gibi ara güçleri de jeopolitik baskı altına almıştır (Mak, 2022). Yukarıda da ifade edildiği üzere, günümüzde çip üretimi, nanometre düzeyinde son derece hassas bir teknoloji gerektiren karmaşık bir süreçtir (TSMC, 2025a). Bu alanda kullanılan makineler, yazılımlar ve malzemeler, küresel tedarik zincirinin en kritik unsurları arasında yer almaktadır. Çip üretiminde 2 nm düğümünde²⁴ 10^{-9} metre ölçeği gibi litografi hassasiyeti, malzeme saflığı, 3D NAND ve GAAFET transistörler²⁵ ve EDA araçları²⁶ küresel tedarik zincirinin en kritik bileşenleridir (Semiconductor Engineering, 2025; Synopsys, 2025). Bu alanda ASML’nin ekstrem ultraviyole (EUV) litografi makineleri ve TSMC’nin 3 nm üretim süreçleri fiilen pazar standardı haline gelmiştir (TSMC, 2025b). Yeni nesil High-NA EUV sistemleri²⁷ sub-2 nm

²⁴ “Düğüm” (node), yarı iletken üretiminde transistör yoğunluğu, güç verimliliği ve performans seviyesini belirleyen üretim süreci teknolojisini ifade eden ölçüt olup “2 nm” gibi ifadeler bu nesil ölçek küçülmesini gösterir.

²⁵ 3D NAND ve GAAFET, yarı iletken teknolojilerinde ileri üretim aşamalarını temsil eder. 3D NAND, veri depolama çiplerinde hücrelerin dikey olarak istiflenmesiyle daha yüksek yoğunluk, düşük maliyet ve artan performans sağlar; böylece klasik 2D mimariden üç boyutlu yapıya geçişi ifade eder. GAAFET (Gate-All-Around FET) ise, iletken kanalı tüm çevresinden saran kapı yapısıyla enerji verimliliğini artıran ve sızıntı akımlarını azaltan yeni nesil bir transistör mimarisidir. Bu iki teknoloji, daha küçük, hızlı ve verimli çiplerin üretilmesini mümkün kılar (Lee vd., 2012)

²⁶ EDA (Electronic Design Automation) araçları, mikroçiplerin tasarım, simülasyon ve doğrulama süreçlerini otomatikleştiren yazılımlardır. Cadence ve Synopsys gibi ABD merkezli şirketler tarafından geliştirilen bu araçlar, entegre devrelerin nanometre ölçeğinde hassas biçimde tasarlanmasını sağlar. Yarı iletken üretiminin temelini oluşturan EDA yazılımları, teknolojik inovasyonun yanı sıra küresel çip rekabetinde de stratejik bir öneme sahiptir (Synopsys, 2025).

²⁷ High-NA EUV sistemleri (High Numerical Aperture Extreme Ultraviolet Lithography Systems), yarı iletken üretiminde kullanılan en ileri düzey litografi teknolojisidir. Bu sistemler, mevcut EUV (Aşırı Morötesi) litografi makinelerinin geliştirilmiş versiyonudur ve numerical aperture (NA) değerini 0.33’ten 0.55’e çıkararak, daha küçük transistör boyutlarının ve daha yüksek yoğunlukta çip üretiminin mümkün olmasını sağlar. Yani, bir nevi “daha keskin mercekle” etkisiyle, üreticiler aynı alana daha fazla bilgi sığdırabilir. High-NA EUV teknolojisi, 2 nanometre (nm) ve altı üretim süreçlerine geçişte kilit rol oynamaktadır. Bu sayede çipler daha güçlü, enerji verimli ve hızlı hale gelir. Ancak bu sistemlerin maliyeti oldukça yüksektir ve şu anda yalnızca ASML (Hollanda) tarafından üretilmektedir. Özetle, High-NA EUV, yarı iletken sektöründe Moore Yasası’nın sürdürülebilirliğini sağlayan kritik bir teknolojik sıçrama olarak görülmektedir (ASML, 2024).

düğümlelerini (2 nanometrenin altındaki üretim) mümkün kılacaktır (CNBC, 2025). Her biri yaklaşık 350 milyon avro değerindeki bu makineler, yapay zekâ ve kuantum bilgisayarlar gibi ileri teknolojilerin ihtiyaç duyduğu üst düzey işlem gücünün sağlanmasında kilit rol oynayacak; bu da TSMC'nin 2026 için planladığı A16 üretim süreci²⁸ gibi yeni nesil yeniliklerin önünü açacaktır (Bloomberg, 2024; Yahoo Finance, 2024).

Bu bağlamda ABD'nin ihracat kontrolleri ve CHIPS Act politikası teknik standartların ticari ve stratejik bir değer taşıdığını göstermektedir (Reuters, 2025; Tech in Asia, 2025). Intel'in üretime geçmesi planlanan High-NA EUV siparişleri, TSMC'nin 2 nm üretim hedefi; Çin'in Huawei/SMIC ortaklığında yürüttüğü LDP litografi denemeleri AB'nin *European Chips Act* ile belirlediği 2030'a kadar %20 pazar payı hedefi bu alandaki rekabetin hiç olmadığı kadar arttığını göstermektedir (TrendForce, 2025; Digitimes, 2025; Evertiq, 2025). Dolayısıyla, yarı iletken standartları, teknik uzmanlık ile uluslararası güç projeksiyonunun kesiştiği kritik bir kavşaktır (Hollands, 2025). ASML'nin EUV litografideki fiili tekel konumu (Seeking Alpha, 2025), Hollanda'nın 2025'te ABD ile uyumlu şekilde ihracat lisanslarını sıkılaştırmasıyla tedarik zincirlerinin çeşitlendirilmesini zorunlu kılmaktadır (Bloomberg, 2025). Samsung'un 2 nm yarışında High-NA EUV sistemlerine yönelmesi (TweakTown, 2025), bu sürecin jeoekonomik devletçiliğin en somut örneklerinden biri haline geldiğini ortaya koymaktadır (Ruck, 2024).

5.4. Yapay Zekâ Güvenlik Protokolleri

YZ, blok zincir, kuantum bilişim ve biyoteknoloji gibi yükselen teknolojiler, mevcut standart belirleme mekanizmalarını zorlayan dinamik bir alan sunmaktadır. Bu teknolojilerin hızlı evrimi, bağlayıcı küresel kuralların henüz oluşmaması nedeniyle “yumuşak hukuk” araçlarını öne çıkarmakta, standartlar, teknik rehber olmanın ötesinde ideolojik ve regülasyonel rekabetin de bir aracı hâline gelmektedir.

YZ sistemlerinde algoritmik şeffaflık, veri gizliliği, hesap verebilirlik ve etik kullanım ilkeleri, henüz küresel mutabakata ulaşmamış standartlardır. Bu farklılıklar, YZ standartlarının parçalı bir rejim kompleksi şeklinde geliştiğine/gelişeceğine işaret etmektedir. Söz gelimi, OECD'nin *Yapay Zekâ İlkeleri*, insan merkezlilik, şeffaflık ve risk yönetimi gibi ilkeler çerçevesi sunarken (OECD, 2024b) benzer biçimde, OECD'nin *Yapay Zekâ Olay Bildirim Çerçevesi* (AI incident reporting framework)²⁹ küresel koordinasyonu teşvik ederken (OECD, 2025a), Ağustos 2025'te yürürlük kazanan AB *Yapay Zekâ Yasası*, GPAI (General Purpose AI) kurallarını yürürlüğe koymuş olup, sistemik riskli modeller için risk değerlendirme ve şeffaflık zorunluluğu getirmiştir (Nemko Digital, 2025). Çin'in (*New Generation AI Development Plan ve China Standards 2035 gibi*) veri merkezli yaklaşımı ulusal standartlarla alternatif bir yol haritası sunmaktadır (Zhang, 2025; ORCA Asia, 2025). Bu yapıda devlet denetimli veri egemenliği, AB'nin risk temelli modelinden ayrılmakta (International Association of Privacy Professionals,

²⁸ TSMC'nin A16 çipi, GAAFET transistörleri ve arkadan güç iletimi (Backside Power Delivery / Super Power Rail) gibi yenilikçi tasarımlarıyla, daha fazla transistör yoğunluğu, daha yüksek işlem hızı ve daha düşük güç tüketimi sunmaktadır. Bu sayede hem akıllı telefonlar hem de yapay zekâ ve veri merkezleri gibi yüksek performans gerektiren alanlar için kritik avantajlar sağlamaktadır. 2026'nın ikinci yarısında kütle üretimine geçmesi planlanan A16, çip üretiminde yeni bir standart oluşturarak, daha güçlü ve verimli elektronik cihazların önünü açacaktır (TSMC, 2025c).

²⁹ OECD'nin AI Incident Reporting Framework, yapay zekâ sistemlerinde ortaya çıkan güvenlik, etik veya operasyonel olayların standart biçimde raporlanmasını sağlayan bir mekanizma olup hem YZ sistemlerinin güvenliğini ve şeffaflığını artırmakta hem de uluslararası normların geliştirilmesine katkı sağlamaktadır. Bu çerçevede, kurumların olayları merkezi bir veri tabanına veya ulusal otoritelere bildirmesini, benzer hataların tekrarlanmamasını ve küresel ölçekte erken uyarı ve koordinasyon mekanizmalarının işletilmesini amaçlar. (OECD, 2024a).

2025), Çin'in kendi veri koruma yaklaşımını uluslararası alanda yaygınlaştırmaya çalıştığı gözlemlenmektedir (DLA Piper, 2025)

5.5. Veri Aktarım Düzenlemeleri

Kişisel verilerin sınır ötesi aktarımı hem ekonomik değer hem de siber güvenlik riski taşıdığından AB, GDPR düzenlemeleri ile bireylerin kişisel verileri üzerindeki kontrolünü ve haklarını öncelikli olarak karakterize etmiştir. Benzer biçimde, Schrems II kararıyla³⁰ belirlenen çerçeve doğrultusunda, 2025 itibarıyla gerçekleştirilecek Transfer Etki Değerlendirmeleri (TIA), özellikle Çin'e veri aktarımını sıkı denetim altına almayı hedeflemektedir.

AB'nin korumacı veri koruma yaklaşımlarına kıyasla, ABD'nin nispeten piyasa odaklı düzenlemeleri ile Çin'in siber egemenlik stratejisi, veri standartlarının jeopolitik boyutunu derinleştirmiştir. Teknik güvenlik standartları, şifreleme uygulamaları ve veri yerelleştirme (localization) zorunlulukları³¹, devletlerin teknoloji egemenliği, ulusal güvenlik ve dijital rekabet hedefleriyle doğrudan bağlantılı düzenleyici araçlar haline gelmiştir. Çin'in 2024–2025 dönemi boyunca yayımladığı düzenlemeler, özellikle *Sınır Ötesi Veri Akışının Teşvik Edilmesi ve Düzenlenmesine İlişkin Hükümler (Promoting and Regulating Cross-boundary Data Flows)* gibi normlar, uluslararası veri akışını teşvik etme vaadi taşıırken, aynı zamanda veri ihracatı için güvenlik değerlendirmelerini zorunlu tutarak devlet gözetimini güçlendirmektedir. Bu yaklaşım, veri işleme süreçlerini bireysel rıza, minimizasyon ve şeffaflık ilkeleri üzerine kuran GDPR modelinden belirgin bir kopuş göstermektedir.

ABD'nin dijital güvenlik politikaları, teknolojik rekabetin jeopolitik bir boyut kazanmasıyla giderek daha korumacı ve standart temelli bir nitelik kazanmıştır. Bu dönüşümün merkezinde, veri akışlarının ve bilgi-iletişim teknolojileri altyapısının ulusal güvenlik kapsamında yeniden tanımlanması yer almaktadır. Mayıs 2019'da Başkan Trump, *Yönetici Emri 13873* ile ulusal acil durum ilan ederek, yabancı aktörlerin ABD'nin bilgi ve iletişim teknolojileri tedarik zincirlerinden yararlanabileceği riskine dikkat çekmiş ve bu alanda federal düzeyde güvenlik standartlarının belirlenmesinin önünü açmıştır (The White House, 2019). Bu çerçeve, Biden yönetimi döneminde genişletilmiştir. 28 Şubat 2024 tarihli *Yönetici Emri 14117*, “endişe duyulan” devletlerin Amerikalıların toplu hassas kişisel verilerine erişimini sınırlamayı hedeflemiş ve veri yönetişimi süreçlerinde yeni güvenlik kriterleri tanımlamıştır (Federal Register, 2024). Adalet Bakanlığı tarafından geliştirilen nihai kural, 8 Nisan 2025 itibarıyla yürürlüğe girmiş ve uluslararası veri işlemlerine ilişkin teknik ve hukuki uyum standartlarını detaylandırmıştır (Federal Register, 2025). Gizlilik, erişim kontrolü ve gözetim denetimi eksenindeki bu düzenlemeler, ulusal güvenliğe yönelik önlemler ve ABD'nin küresel veri yönetişiminde kendi normatif modelini inşa etme girişimi olarak da değerlendirilmektedir. Bu yaklaşım, 2024 tarihli *Protecting Americans from Foreign Adversary Controlled Applications (PAFACA)* Yasası ile pekişmiş; yasa, ulusal güvenlik riski taşıyan yabancı uygulamaların (özellikle TikTok örneğinde olduğu gibi) veri erişim alanını sınırlayarak Washington'un dijital egemenlik stratejisinin bir parçası haline gelmiştir (The White House, 2025).

³⁰ Schrems II kararı, 2020'de AB Adalet Divanının verdiği ve AB vatandaşlarının kişisel verilerinin AB dışına aktarımını sıkı şekilde düzenleyen bir karardır. Karar, ABD'ye veri transferlerini öngören Privacy Shield mekanizmasını geçersiz kılmış, şirketlerin Standard Contractual Clauses (SCC) kullanırken ek olarak veri güvenliği değerlendirmesi (Transfer Impact Assessment, TIA) yapmalarını zorunlu kılmıştır. Bu şekilde, AB'deki bireylerin veri gizliliği hakları, uluslararası ticari ilişkiler ve veri transferlerinden önce korunmuş olmaktadır (European Parliament. 2020).

³¹ ISO 27001 uyumlu şifreleme uygulamaları ve veri lokalizasyonu yükümlülükleri, veri aktarımını güvenli hale getirmek, kişisel verileri korumak ve ülkesel yasalara uygunluğu sağlamak amacıyla benimsenen temel standartlar ve düzenlemelerdir (ISO, 2022).

ABD'nin Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) çerçevesinde belirlediği siber güvenlik gereklilikleri, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından öngörülen standartlara dayanmaktadır. Bu çerçeve, Ekim 2025'e kadar tamamlanması öngörülen due diligence yükümlülükleriyle, tedarikçi ve iş ortaklarının güvenlik risklerinin önceden değerlendirilmesini ve gerekli önlemlerin alınmasını zorunlu kılmaktadır (NIST, 2024). Söz konusu düzenlemeler, teknik uyum gerekliliği ile birlikte tedarik zincirlerinin güvenlik temelli yeniden ölçeklendirilmesi anlamına gelmektedir. Bu durum, özellikle uluslararası teknoloji şirketlerinin Amerikan pazarına erişiminde yeni bir uyum rejimi yaratmakta ve küresel düzeyde veri yönetişimi standartları üzerinde dolaylı bir baskı oluşturmaktadır. CISA-NIST eksenli bu güvenlik mimarisi, tedarikçi ilişkilerini sıkı biçimde denetleyerek hem ekonomik egemenliği güçlendirmekte hem de küresel normatif rekabeti derinleştirmektedir.

6. KARŞILAŞTIRMALI VAKA ANALİZİ: 5G VE YAPAY ZEKÂ STANDARTLARINDA ORTAK DİNAMİKLER

6.1. Genel Olarak

5G ve yapay zekâ standartları, teknolojinin jeopolitik rekabetin merkezinde nasıl konumlandığını gösteren iki çarpıcı örnektir. Bu bölüm, her iki vakanın ortak dinamiklerini üç temel dönüşüm eksenini üzerinden incelemektedir: teknik standartların jeoekonomik devletçiliğin araçlarına dönüşmesi, geleneksel standart belirleme kurumlarının tarafsızlığının aşınarak bloklaşmayı hızlandırması ve parçalanmış küresel düzende orta ölçekli devletlere norm girişimciliği alanı açılması. Bu analizde Yin'in (2018) çoklu vaka yöntemine dayalı süreç izleme yaklaşımı benimsenmiştir. Böylece 3GPP ve ITU gibi platformlar arasındaki kurumsal etkileşimler, nedensel mekanizmaları ve karar alma süreçlerini izleyerek çözümlenmektedir. Bu yöntem, vakalar arası benzerlik ve farklılıkları ortaya koyarak normatif ve kurumsal dönüşümlerin nasıl geliştiğini bütüncül biçimde açıklamaya imkân tanımaktadır. Bulgular, standart belirlemenin teknik bir uzlaş olmanın ötesinde yapısal güç üretimi ve normatif düzen inşası açısından stratejik bir alan haline geldiğini ortaya koymaktadır.

6.2. Teknik Özelliklerin Jeoekonomik Araçlara Dönüşümü: Huawei Vakası

2010'lu yıllardan itibaren standart savaşları, Soğuk Savaş'ın ideolojik bloklaşmasından farklı olarak jeoekonomik çok kutupluluk koşullarında yeniden biçimlenmiştir. Bu dönemde teknolojik standartlar, teknik koordinasyon araçları olmakla birlikte aynı zamanda ekonomik güvenlik, stratejik özerklik ve normatif nüfuz mücadelelerinin kesişim alanları hâline gelmiştir. Özellikle 5G, YZ ve yarı iletken üretimi gibi alanlarda yaşanan gelişmeler, devletlerin teknoloji politikalarını doğrudan jeopolitik rekabetin parçasına dönüştürmüştür. Bu bağlamda standart belirleme süreçleri, rejim kompleksleri içinde çok katmanlı bir güç mücadelesine evrilmiş; teknik uzmanlık, ekonomik çıkar ve siyasi meşruiyet arasındaki denge, yeni bir stratejik rekabet biçimini doğurmuştur. Bu dönüşümün en görünür örneklerinden biri, Huawei Technologies Co., Ltd.'nin 5G ve YZ standartlarındaki yükselişidir. Bu alandaki ABD-Çin rekabeti, 5G ve Huawei konusundaki anlaşmazlıkta açıkça ortaya çıkmıştır. Anlaşmazlığın merkezini 5. nesil mobil ağ teknolojisinin temelini oluşturan standartlar oluşturmıştır. Çinli şirketlerin sahip olduğu standart temel patentlerin (standard essential patents- SEP) ezici sayısı Çin'in 5G standardizasyonunda hâkim konumda olduğunu ve özellikle bilgi ve iletişim teknolojisinde uluslararası standardizasyon rejiminde ABD'yi geride bıraktığını göstermiştir (Lee, 2021).

Küresel teknoloji standartları alanında fikri mülkiyet sahipliği, jeoekonomik rekabetin en görünür göstergelerinden biri hâline gelmiştir. Özellikle 5G standardına ilişkin temel patentler (SEP'ler) devletlerin ve teknoloji şirketlerinin normatif ve teknik etki kapasitesini doğrudan yansıtmaktadır. Huawei, bu alandaki yoğun Ar-Ge yatırımları sayesinde hâlen dünyanın en

büyük patent sahiplerinden biri olarak öne çıkmaktadır.³² 2025 itibarıyla Huawei, 5G patent rekabetinde Samsung, LG, Qualcomm ve Ericsson’u geride bırakarak liderliğini korumakta; bu durum, Çin’in *China Standards 2035* stratejisiyle de örtüşmektedir. Huawei’nin teknik liderliği, patent hâkimiyeti yoluyla normatif etki kurma kapasitesini artırmakta, böylece teknoloji standartlarının jeopolitik güç projeksiyonuna dönüşmesini somutlaştırmaktadır.

Huawei’nin yükselişi, ABD’nin 2020’de başlattığı Clean Network girişimiyle doğrudan bir jeopolitik çatışma hattına dönüşmüştür. Bu girişim, Huawei ve ZTE gibi “güvenilir olmayan” tedarikçileri dışlamayı hedeflemiş; 2025 itibarıyla 53 ülke programa katılmış, özellikle Latin Amerika’da (örneğin Brezilya ve Ekvador) etkisini artırmıştır (U.S. Department of State, 2025). Buna karşın Avrupa’da etki sınırlı kalmış, AB, *5G Bağlantı Araç Seti* (2021) ile *Güvenlik Araç Seti* (2020) kapsamında Huawei’i yüksek riskli tedarikçi olarak nitelendirmiş ve kritik altyapılarda kısıtlanmasını önermiştir (European Parliament, 2025; Nestoras ve Cappelletti, 2022). Bu tartışmalar, aynı zamanda AB’nin *Akıllı Ağlar ve Hizmetler Ortak Girişimi* (SNS JU) aracılığıyla 6G dönemine yönelik birleşik bir standart çerçevesi oluşturma çabasını da hızlandırmıştır (European Commission, 2025). Bu politikalar, Batı’nın teknoloji tedarik zincirlerini güvenlikleştirme eğilimini güçlendirirken, aynı zamanda küresel rejim kompleksindeki normatif parçalanmayı derinleştirmiştir.

Bu yönüyle Huawei vakası, teknoloji standartlarının görünmez güç biçimlerine dönüşümünü ve orta güçlerin bu yapısal dönüşüm içindeki manevra alanını analitik biçimde ortaya koymaktadır. Bu süreç, orta güçlere de özgün fırsatlar sunmakta, orta güçlerin teknoloji standartları alanında jeoekonomik özerklik arayışlarını çok taraflı diplomasiyle birleştirmektedir. Söz gelimi, Güney Kore, *European Chips Act* kapsamındaki iş birlikleri ve *AI Seoul Summit 2025* gibi platformlar üzerinden dengeleyici bir norm aktörü rolü üstlenirken; Türkiye, MİKTA çerçevesindeki teknik uyum projeleriyle seçici entegrasyon stratejisini güçlendirmektedir. Ancak bu durum, küresel yönetişimi daha parçalı hâle getirerek rejim kompleksinin derinleşmesine yol açmaktadır.

6.3. Standart Organlarının Tarafsızlığının Aşınması ve Bloklama

Diğer taraftan, 5G ve yapay zekâ vakalarında da görüldüğü üzere, rejim kompleksinde yaşanan *forum kaydırma* (forum seçimleri) dinamikleri, ilgili yapıların tarafsızlığını aşındırmaktadır. Söz gelimi, 5G alanında ABD’nin ATIS (Telekomünikasyon Endüstrisi Çözümleri İttifakı) üzerinden 3GPP’ye ağırlık vermesi, Çin’in Çin İletişim Standartları Birliği (CCSA) aracılığıyla ITU-R Radyokomünikasyon Sektörü 5D Çalışma Grubu’nda üstlendiği proaktif rol ile çatışarak bloklamayı tetiklemektedir. Keza Clean Network girişimine 50’den fazla ülkenin katılımı, bu teknik forumların giderek ideolojik ve normatif arenalara dönüştüğünü göstermektedir (U.S. Department of State, 2025).

YZ’de ise OECD’nin 2024 ilkeleri ve AB AI Act’in GPAI kuralları, Çin’in ulusal standartlarını dışlayarak benzer bir parçalanmaya neden olmaktadır. ISO’nun 2025 *YZ Veritabanı Girişimi*’nin ise bu rekabeti daha da kronikleştirmekte olduğu söylenebilir (OECD, 2024a). Bu çalışmada da ortaya konulduğu üzere, 5G standartlarının frekans ve donanım odaklı forumlarında oluşan rekabetin, yapay zekânın etik temelli ve yumuşak hukuk ağırlıklı yönetim çerçevesine kıyasla daha belirgin bir jeopolitik kutuplaşma yarattığını göstermektedir. Bununla

³² 2024–2025 döneminde yayımlanan sektör raporları, toplam bildirilen (declared) 5G SEP ailelerinin sayısının yaklaşık 56.000 ila 85.000 arasında değiştiğini, Huawei’nin ise bu havuzda yaklaşık %12–%19 aralığında bir payla en üst sıralarda yer aldığını göstermektedir (Parola Analytics, 2025). Ayrıca Avrupa Patent Ofisinin 2024 Patent Endeksi verilerine göre Huawei, aynı yıl Avrupa’daki en aktif başvuru sahiplerinden biri olmayı sürdürmüş ve küresel ölçekte 150.000’in üzerinde etkin patente ulaşmıştır (European Patent Office, 2025; Huawei, 2025).

birlikte, her iki alan da uluslararası rejim kompleksini daha da derinleştirerek, geleneksel olarak tarafsız kabul edilen kurumların giderek güç siyasetinin dinamiklerine tabi hale gelmesine yol açmaktadır.

6.4. Orta Güçlere Norm Girişimciliği Fırsatları

Vaka analizleri, parçalanmış uluslararası düzende orta güçlerin giderek artan biçimde niş alanlarda etkinlik kazandığını ortaya koymaktadır. Söz gelimi, Hollanda'nın yarı iletken odaklı *Semicon Board NL* girişimi ve Avrupa-Tayvan ortak standart geliştirme çabaları, teknoloji güvenliği ile tedarik zinciri direncinde orta güç diplomasisinin artan önemini göstermektedir (Rijksoverheid, 2025; Government of Netherlands, 2025). Tayvan, özellikle Almanya ve Hollanda ile yürüttüğü düzenleyici uyum süreçleri aracılığıyla tedarik zinciri güvenliği ve yapay zekâ uygulamalarının sertifikasyonu gibi alanlarda yeni normatif çerçeveler üretmektedir. Almanya ise *High-Tech Strategy 2025* kapsamında yapay zekâ ve 5G ekosistemine verdiği öncelikle AB içinde standart belirleme kapasitesini orta güç koordinasyonu üzerinden güçlendirmektedir (The Federal Government, 2025).

Bu süreçte, Latin Amerika ve Afrika ülkeleri de artan biçimde standart yönetişimine dâhil olmaktadır. Brezilya, 2024'te yayımladığı *Artificial Intelligence Strategy* ile OECD ilkeleriyle uyumlu ancak veri egemenliği vurgusu yüksek bir çerçeve benimsemiş; Meksika ise Inter-American Development Bank (IDB) desteğiyle bölgesel 5G güvenlik standartlarını geliştirme sürecine katılmıştır (OECD, 2025c). Nijerya ve Güney Afrika Cumhuriyeti; Afrika Birliğinin *Kıta Yapay Zekâ Stratejisi* ve BM Genel Kurulunun *Sürdürülebilir Kalkınma İçin Güvenli, Emniyetli ve Güvenilir Yapay kararı ile Sistemlerinin Fırsatlarından Yararlanılması* başlıklı kararı (UN, 2024) ile uyumlu olarak veri altyapısı, etik denetim ve standart sertifikasyonu alanlarında bölgesel öncülük üstlenmektedir (Muhammed, 2024; Thomson Reuters Foundation, 2025). Orta Doğu bağlamında ise İsrail, siber güvenlik ve yapay zekâ alanındaki yüksek Ar-Ge kapasitesi sayesinde OECD ve ISO platformlarında aktif standart katılımcısı haline gelmiştir (OECD, 2025b). Suudi Arabistan ve Birleşik Arap Emirlikleri, sırasıyla *National AI Ethics Framework* (2024) ve *UAE National AI Strategy 2031* belgeleriyle yapay zekâ yönetişiminde kurumsal standart uyumu hedeflemekte, Çin ve Batı teknolojileri arasında "pragmatik uyum" stratejisi izlemektedir (Gulf Magazine, 2025; Falk, 2025).

Bu durum, orta güçlerin teknoloji rekabetinde büyük güçler arasındaki yapısal boşlukları, regülasyon ve altyapı diplomasisi yoluyla stratejik avantaja dönüştürme kapasitesine işaret etmektedir. Örneğin, Birleşik Arap Emirlikleri'nin teknoloji vizyonunda merkezi konumda bulunan G42, yapay zekâ ve bulut bilişim altyapılarına odaklanan stratejik bir teknoloji şirketi olarak, orta güçlerin standart belirleme alanında izlediği niş diplomasiye dikkat çekici bir örnek sunmaktadır. Şirket, Microsoft ile 2024 yılında gerçekleştirdiği kapsamlı ortaklık anlaşmasıyla ulusal kapasite inşası ile birlikte küresel yapay zekâ yönetişimi ekosistemine entegrasyonu da hedeflemiştir (G42, 2025; Reuters, 2024). G42'nin faaliyetleri, BAE'nin "Etik Yapay Zekâ" çerçevesiyle birlikte değerlendirildiğinde, Körfez bölgesinde normatif ve teknik standartların birlikte şekillendiği yeni bir politika alanını temsil etmektedir.

Orta güç ülkeler, küresel teknoloji standart savaşlarında niş politika fırsatlarını değerlendirerek stratejik özerkliklerini güçlendirmekte, parçalı uluslararası düzende hem rekabetçi hem de normatif bir pozisyon elde etme olanağı bulmaktadır. G42 gibi öncü yapay zekâ girişimleri, stratejik yatırımlar ve uluslararası iş birlikleriyle rekabette avantaj elde ederken; Meksika, Nijerya, Şili, Güney Afrika, Suudi Arabistan, İsrail ve Brezilya gibi ülkeler, fintech, biyomedikal, siber güvenlik ve tarım teknolojileri alanlarında yerel şirketler aracılığıyla hem ekonomik değer yaratmakta hem de bölgesel normatif etki geliştirmektedir. Bu girişimler, devlet destekleri ve küresel ortaklıklarla büyümesine rağmen, etik kullanım ve veri gizliliği gibi

zorlukları da beraberinde taşımaktadır. Karşılaştırmalı olarak değerlendirildiğinde, 5G alanındaki altyapı temelli girişimler daha somut ekonomik getiriler sağlarken, yapay zekâ alanındaki etik ve yönetim odaklı düzenlemeler normatif etkinliği güçlendirmektedir. Her iki süreç de orta güçlerin norm girişimciliğini pekiştirerek, parçalanmış küresel düzenin kısıtlarını stratejik fırsatlara dönüştürdüğünü göstermektedir.

7. SONUÇ

Teknoloji standartları, XXI. yüzyılın uluslararası ilişkilerinde adeta “görünmez bir savaş alanı” haline gelmiştir. Bu alanda normatif ve teknik liderlik kazanmak kısa vadeli ekonomik avantajlarla birlikte uzun vadeli yapısal güç kazanımı açısından da önemlidir. Bu çalışma, teknoloji standartlarının jeopolitik rekabet içindeki kural koyma mücadelesini merkeze alarak, 5G ve yapay zekâ vakalarını rejim kompleksi, güç tipolojileri, jeoekonomik devletçilik ve norm meşruiyeti boyutlarıyla incelemiştir. Zira, bu standartlar, jeoekonomik araçlara dönüşerek patent hâkimiyeti üzerinden ekonomik gücü yeniden tanımlamakta; tarafsızlık ilkesini aşındırarak bloklaşmayı teşvik etmekte ve orta güçlere norm girişimciliği yoluyla stratejik fırsatlar sunarak küresel yönetişimin doğasını dönüştürmektedir. 5G ve yapay zekâ vakaları, bu dönüşümlerin rejim kompleksinin dinamik yapısında somutlaştığını ve standart savaşlarının yeni biçimlerde yapısal güç ürettiğini göstermektedir. Bulgular, teknik standardizasyonun teknolojik, siyasi ve normatif bir süreç haline geldiğini ortaya koymaktadır. Politika düzeyinde ise orta güçlerin çok katmanlı diplomasi, ulusal kapasite inşası, normatif esneklik stratejileri (çifte uyum yaklaşımı) ve bölgesel işbirliği mekanizmaları yoluyla özerkliklerini artıracabilecekleri sonucuna ulaşılmaktadır. Standartlar teknik uyumu aşarak jeoekonomik araçlara evrilmekte bu da bölgesel bloklaşmayı hızlandırmakta, orta güçler içinse niş fırsatlar doğmaktadır. Bu dinamikler, standart belirlemenin teknik olduğu kadar güç üreten bir süreç olduğunu da vurgulamaktadır. Lessig’in “kod hukuktur” önermesiyle uyumlu biçimde, dijital altyapılar normatif düzeni şekillendirmektedir.

Teknoloji ortamını şekillendirmek isteyen orta ve küçük ölçekli devletler için çok katmanlı bir diplomasi yaklaşımının benimsenmesi, tek bir uluslararası örgüt veya blokla sınırlı kalmadan, çeşitli standart belirleme forumlarında eş zamanlı temsil stratejilerini hayata geçirmeyi gerektirmektedir. Bu strateji, teknik yeniliklerin yakından izlenmesini sağlayarak, ulusal çıkarlara uygun niş katkılar sunma imkânını da beraberinde getirmektedir/ getirecektir. Öte yandan, teknolojik standart belirleme süreçlerine etkin bir katılımın sağlanması, salt diplomatik varlık ile sınırlı kalmayıp, sağlam kurumsal ve teknik kapasitelerin geliştirilmesini zorunlu kılmaktadır. Bu doğrultuda, patent üretimini teşvik etmek, test laboratuvarlarının kurulmasını desteklemek ve regülasyon uyum mekanizmalarını güçlendirmek amacıyla kamu ile özel sektör arasındaki ortaklıkların sistematik biçimde özendirilmesi hayati bir önemi haizdir. Buna karşın, küresel arenada farklı normatif blokların yükselişi, ülkeleri önemli uyum maliyetleriyle karşı karşıya bırakmaktadır. Bu kaçınılmaz durum karşısında, ticari çıkarlar ile güvenlik önceliklerini dengede tutan dinamik bir “ikili uyum” (dual alignment) stratejisinin benimsenmesi elzemdir. Böylece, normatif esneklik ve uyum süreçleri daha sürdürülebilir bir temele oturtulabilir ve ASEAN, AB veya Afrika Birliği gibi bölgesel örgütler aracılığıyla ortak standart geliştirme girişimlerini güçlendirmek, orta güçlere çoklu standart ortamında bölgesel pazarlık gücünü pekiştirme ve teknolojik özerklik için stratejik manevra alanları yaratma imkânı sunabilir.

KAYNAKÇA

- 3GPP. (2023). *TR 37.817: Study on ai/ml for NR air interface. 3rd generation partnership project.* <https://www.3gpp.org/technologies/ai-ml-nr>
- 3GPP. (2024). *Release 18. 3rd generation partnership project.* <https://www.3gpp.org/specifications-technologies/releases/release-18>
- 3GPP. (2025a). *About 3GPP.* <https://www.3gpp.org/about-3gpp>
- 3GPP. (2025b). *RAN1: 5G-advanced and rel-18 completion.* <https://www.3gpp.org/technologies/ran1-rel18>
- Abdikarov, R. (2023). Technological rise of China. *Eurasian Research Journal (ERJ)*, 5(3), 71–84.
- African Union. (2024). *Continental Artificial Intelligence Strategy.* [Strategy Document]. <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>
- Amato-Montanaro, M. (2024). The chip war: assessing US policy against China moving forward. *Columbia Political Review.* <https://www.cpreview.org/articles/2024/11/the-chip-war-assessing-us-policy-against-china-moving-forward>
- ANSI. (2025). *China Announces Action Plan for Global AI Governance.* [Press release] <https://www.ansi.org/standards-news/all-news/8-1-25-china-announces-action-plan-for-global-ai-governance>
- ASML. (2024). *High-na euv lithography: enabling the next generation of microchips.* <https://www.asml.com/en/technology/lithography-principles/euv-lithography/high-na-euv>
- ATIS. (2025). *Overview.* <https://atis.org/overview/>
- Baumann, M. O. & Haug, S. (2023.). How China is reshaping UN development work. *The Loop.* <https://theloop.ecpr.eu/how-china-is-reshaping-united-nations-development-work/>
- Beardsley, S. (2025): *Nexperia krizi: Avrupa'da otomobil üretimi tehlikede.* DW. <https://www.dw.com/tr/nexperia-krizi-avrupada-otomobil-%C3%BCretimi-tehlikede/a-74487133>
- Biden, J. (2020). Why America must lead again: Rescuing u.s. foreign policy after Trump. *Foreign Affairs.* <https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again>
- Blackwill, R. D., & Harris, J. M. (2016). *War by other means: geoeconomics and statecraft.* Cambridge, MA: Harvard University Press.
- Bloomberg. (2024). *ASML to ship its \$380 million chip machine to TSMC this year.* <https://www.bloomberg.com/news/articles/2024-06-05/asml-to-ship-its-380-million-machine-to-tsmc-samsung-this-year>
- Bloomberg. (2025). *Dutch align with US export controls on some ASML chip tools.* <https://www.bloomberg.com/news/articles/2025-01-15/dutch-align-with-us-export-controls-on-some-asml-chip-tools>

- BSI. (2025). *A History of Looking Forward*. <https://www.bsigroup.com/en-IE/about-bsi/our-history/>
- Cargill, C. (2022). Behind the geopolitical conflicts around global technology standards. *Oxford Global Society*. <https://oxgs.org/2022/10/20/behind-the-geopolitical-conflicts-around-global-technology-standards/>
- CENELEC. (2023). *CEN and CENELEC celebrates Europe Day: a look back at the shared history of the European Union and European Standardization*. <https://www.cenelec.eu/news-events/news/2023/brief-news/2023-05-09-europe-day/>
- China Communications Standards Association. (2025). *Standards*. [Standards]. <https://www.ccsa.org.cn/english/>
- CNBC. (2025). *Exclusive look at High NA, ASML's new \$400 million chipmaking colossus*. <https://www.cnbc.com/2025/05/22/exclusive-look-at-high-na-asmls-new-400-million-chipmaking-colossus.html>
- Congress. (2021). *Technology Standards Task Force Act of 2021*. [Official document]. <https://www.congress.gov/bill/117th-congress/senate-bill/1498>
- Contreras, J. L. (2015). A brief history of FRAND: Analyzing current debates in standard setting and antitrust through a historical lens. *Antitrust Law Journal*, 80 (1), 39–120.
- Cooper, D. & Haley B. & Govender, D. & Mokdad, A. & Mkhize, M. (2025). *Kenya's AI strategy 2025–2030: signals for global companies operating in Africa*. Policy paper. <https://www.covafrica.com/2025/04/kenyas-ai-strategy-2025-2030-signals-for-global-companies-operating-in-africa/>
- CPDB. (2025). *About CPDP*. <https://www.cpdconferences.org/about-cpdp>
- Cumbre Ministerial y de Altas Autoridades de América Latina y el Caribe. (2023). *Declaración de Santiago: Para promover una inteligencia artificial ética en América Latina y el Caribe*. https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf
- Digitimes. (2025). *SMIC initiates testing of domestically produced lithography equipment*. <https://www.digitimes.com/news/a20250917PD236/smic-duv-equipment-testing-asml.html>
- DLA Piper. (2025). *Data protection laws in China*. <https://www.dlapiperdataprotection.com/index.html?c=CN>
- EEAS. (2024). *EU-ASEAN Blue Book 2024-2025*. [Policy report]. https://www.eeas.europa.eu/delegations/association-southeast-asian-nations-asean/eu-asean-blue-book-2024-2025_en
- Edgerton, D. (2006). *The shock of the old: Technology and global history since 1900*. Oxford University Press.
- ENA. (2025). *UAE strategy integrates cybersecurity with AI: Mohamed Al Kuwaiti*. <https://www.wam.ae/en/article/bm78miz-uae-strategy-integrates-cybersecurity-with-ai>

- Ernst, D. (2011). Indigenous innovation and globalization: The challenge for China's standardization strategy. Policy-oriented research report. *Centre for International Governance Innovation and East-West Center*. <https://www.eastwestcenter.org/sites/default/files/private/ernstindigenousinnovation.pdf>
- European Commission. (2020). *The EU toolbox for 5G security: Factsheet / infographic*. [Policy framework]. <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security>
- European Commission. (2022a). *The digital markets Act: Ensuring fair and open digital markets*. [Official document]. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
- European Commission. (2022b). *New approach to enable global leadership of EU standards promoting values and a resilient, green and digital single market*. [Policy communication]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661
- European Commission. (2025). *The smart networks and services joint undertaking*. [Strategy document]. <https://digital-strategy.ec.europa.eu/en/policies/smart-networks-and-services-joint-undertaking>
- European Data Protection Board. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0)*. [Policy framework]. <https://edpb.europa.eu>
- European Parliament. (2025). *Answer given by executive vice-president Virkkunen on behalf of the European Commission*. Strategy document. [Parliamentary answer]. https://www.europarl.europa.eu/doceo/document/E-10-2025-003060-ASW_EN.html
- European Union. (2024). *The AI Act Explorer*. <https://artificialintelligenceact.eu/ai-act-explorer/>
- European Patent Office. (2025). *Patent index 2024: European innovation remains robust*. EPO [Press Release]. <https://www.epo.org/en/news-events/press-centre/press-release/2025/1352247>
- Evertiq. (2025). *EU member states push for stronger Chips Act 2.0*. <https://evertiq.com/design/2025-09-30-eu-member-states-push-for-stronger-chips-act-20>
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351
- Federal Register. (2024). *Preventing access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern*. [Government report]. <https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related>
- Federal Register. (2025). *Preventing access to U.S. sensitive personal data and government-related data by countries of concern or covered persons*. [official document].

<https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern>

- Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, 52(4), 887–917. <https://doi.org/10.1162/002081898550789>
- Franck, T. M. (1990). *The power of legitimacy among nations*. Oxford University Press.
- G42. (2025). *G42 and Microsoft launch responsible AI future foundation*. <https://www.g42.ai/resources/news/g42-and-microsoft-launch-responsible-ai-foundation>
- Gallwey, G. (2025). The global AI rules race: China’s strategic response to US tech dominance. [Policy analysis report]. *Geopolitical Monitor*. <https://www.geopoliticalmonitor.com/the-global-ai-rules-race-chinas-strategic-response-to-us-tech-dominance/>
- Government of Netherlands. (2025). *Klever: export controls on advanced semiconductor manufacturing equipment to be tightened*. [Government report]. <https://www.government.nl/latest/news/2025/01/15/klever-export-controls-on-advanced-semiconductor-manufacturing-equipment-to-be-tightened?utm>
- Graham, L. R. (1993). *Science in Russia and the Soviet Union: A short history*. Cambridge University Press.
- GreyB. (2023). *Who owns core 5G patents?* <https://www.greyb.com/blog/5g-patents/>
- Gulf Magazine. (2025) *Saudi Arabia AI ethics framework: Leading the way in ethical AI*. <https://gulfmagazine.co/saudi-arabia-ai-ethics-framework-leading/>
- Hajdari, U. (2025). *Hollanda, Çinli Nexperia’nın kontrolünü devraldı: Ekonomik güvenlik riski*. <https://tr.euronews.com/business/2025/10/13/hollanda-cinli-nexperianin-kontrolunu-devraldi-ekonomik-guvenlik-riski>
- Hallerberg, A. E. (1973). The metric system: Past, present—future? *The Arithmetic Teacher*, 20(4), 247–255. <http://www.jstor.org/stable/41188244>
- Heim, L. (2025). Understanding the artificial intelligence diffusion framework: Can export controls create a U.S. led global artificial intelligence ecosystem? [Policy paper]. *RAND Corporation*. <https://www.rand.org/pubs/perspectives/PEA3776-1.html>
- HM Government. (2025). *The strategic defence review 2025: Making Britain safer—secure at home, strong abroad*. [Strategy document]. <https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad>
- Hollands, T. (2025). Can ASML secure Europe’s tech sovereignty? *North Atlantic Population Forum*. [Policy brief]. <https://www.napforum.org/policy-briefs/can-asml-secure-europe-s-tech-sovereignty>
- Huang, R., & Lin, L. (2025). Chinese AI companies dodge U.S. chip curbs by flying suitcases of hard drives abroad. *The Wall Street Journal*, <https://www.wsj.com/tech/china-ai-chip-curb-suitcases-7c47dab1>

- Huawei. (2025). *Innovation and intellectual property*. <https://www.huawei.com/en/ipr>
- Huawei Technologies. (2025). *5G-advanced innovations at MWC Shanghai 2025*. [Huawei White Paper]. <https://www.huawei.com/en/news/2025/6/5g-advanced-mwc-shanghai>
- IEEE. (2025). *About IEEE standards association*. [Standards / Technical reports]. <https://standards.ieee.org/about/>
- International Association of Privacy Professionals. (2025). *Preparing for compliance: Key differences between EU, Chinese AI regulations*. <https://iapp.org/news/a/preparing-for-compliance-key-differences-between-eu-chinese-ai-regulations>
- International Telecommunication Union. (2023). *ITU world radiocommunication conference 2023 (WRC-23)*. <https://www.itu.int/wrc-23/>
- International Telecommunication Union. (2025a). *Radiocommunication study groups. Radiocommunication Bureau of the ITU*. <https://www.itu.int/en/ITU-R/study-groups>
- International Telecommunication Union. (2025b). *IMT-2030 framework and technical performance requirements (ITU-R M.2516)*. [Standards / Technical reports]. https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2516-2022-PDF-E.pdf
- ISO. (2017). *ISO celebrates 70 years*. <https://www.iso.org/news/2017/02/Ref2163.html>
- ISO. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems*. [Standards / Technical reports]. <https://www.iso.org/standard/27001>
- ISO. (2025). *Summit*. <https://www.iso.org/aisummit>
- Kharpal, A. (2025). *China says Nvidia violated anti-monopoly law after preliminary probe*. CNBC. <https://www.cnbc.com/2025/09/15/china-nvidia-violated-anti-monopoly-law-will-continue-investigation.html>
- Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.
- Keohane, R. O., & Nye, J. S. (2012). *Power and interdependence* (4th ed.). Longman.
- Keohane, R. O., & Victor, D. G. (2011). The regime complex for climate change. *Perspectives on Politics*, 9 (1), 7–23. <https://doi.org/10.1017/S1537592710004068>
- Korean Agency for Technology and Standards. (2025). *2025 international AI standards summit report*. KATS Publications.
- Khan, S. (2025). Who controls the chips, controls the world: The silicon cold war. *Modern Diplomacy*. <https://moderndiplomacy.eu/2025/08/30/who-controls-the-chips-controls-the-world-the-silicon-cold-war>
- Kirton, D. & Cherney, M. (2023). *Huawei's new chip breakthrough likely to trigger closer U.S. scrutiny*. Reuters. <https://www.reuters.com/technology/huaweis-new-chip-breakthrough-likely-trigger-closer-us-scrutiny-analysts-2023-09-05>
- Kitchen, K. (2020). U.S.- China 5G battle portends a divided internet. *Geopolitical Intelligence Services*. <https://www.gisreportsonline.com/r/usa-china-5g/>

- Koskenniemi, M. (2005). *From apology to utopia: The structure of international legal argument*. Cambridge University Press.
- Körömi, C. (2025). Trump: China's DeepSeek AI is a wake-up call for US tech. *Politico*. <https://www.politico.eu/article/donald-trump-china-deepseek-wake-up-call-for-us-tech/>
- Leicht, A. (2025). In the race for AI supremacy, can countries stay neutral? *AI Frontiers*. <https://aifrontiers.com/article/in-the-race-for-ai-supremacy-can-countries-stay-neutral>
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
- Lee, N.T. (2020). Navigating the U.S.- China 5G competition. Policy brief. *Brookings Institution*. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_5g_competition_turner_lee_v2.pdf
- Lee, H. (2021). The battle to set digital technical standards. *Global Asia*. 16 (4), 42-46, https://www.globalasia.org/v16no4/cover/the-battle-to-set-digital-technical-standards_heejin-lee
- Lue, H. T. &, Chen S. H. & Shih, Y. H. & Hsieh, K. Y. & Lu, C. Y. (2012). Overview of 3D NAND Flash and progress of vertical gate (VG) architecture. *2012 IEEE 11th International Conference on Solid-State and Integrated Circuit Technology*, Xi'an, China, 2012, <https://ieeexplore.ieee.org/document/6466681>
- Malaysia SME. (2025). *ASEAN Technology Summit 2025 to drive regional innovation and cross-border collaboration*. <https://www.malaysiasme.com.my/asean-technology-summit-2025-to-drive-regional-innovation-and-cross-border-collaboration>
- Maskus, K. E. (2000). *Intellectual property rights in the global economy*. Institute for International Economics.
- Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W. W. Norton & Company.
- MIKTA. (2025). *What is MIKTA?* <http://mikta.org/about/what-is-mikta/>
- Miller, C. (2022). *Chip war: The fight for the world's most critical technology*. Scribner.
- Milne, C. & Wang, J. (2022). The Geopolitics of global technology standards: Key issues and solutions. *Oxford Global Society*. Policy report. <https://oxgs.org/2022/11/25/report-the-geopolitics-of-global-technology-standards-key-issues-and-solutions/>
- Milmo, D. (2025). Apple appeals against “unprecedented” €500m EU fine over App Store. *The Guardian*. <https://www.theguardian.com/technology/2025/jul/07/apple-appeals-eu-fine-app-store>
- Mokyr, J. (2002). *The gifts of Athena: Historical origins of the knowledge economy*. Princeton University Press.
- Muhammad, J. (2024). *Nigeria's AI strategy: Insights from the national framework*. *African Leadership Magazine*. <https://www.africanleadershipmagazine.co.uk/nigerias-ai-strategy-insights-from-the-national-framework/>
- National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. <https://doi.org/10.6028/NIST.CSWP.29>

- Nemko Digital. (2025). *EU AI Act 2025 update: GPAI rules & compliance*. <https://digital.nemko.com/insights/eu-ai-act-rules-on-gpai-2025-update>
- Nestoras, A., & Cappelletti, F. (2022). 5G Geopolitics and European strategic autonomy: Security, standardisation, and the promise of open RAN. *Future Europe Journal*, 1(1), 89–95. <https://feu-journal.eu/issues/issue-1/5g-geopolitics-and-european-strategic-autonomy/>
- Nye, J. S. (2011). *The future of power*. Public Affairs.
- ORCA Asia. (2025). *Shaping next-generation technology*. <https://orcasia.org/article/1215/shaping-next-generation-technology>
- OECD. (2024a). *AI principles*. [Policy frameworks]. <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>
- OECD. (2024b). *AI incident reporting framework*. [Policy frameworks]. <https://www.oecd.org/going-digital/ai/ai-incident-reporting-framework.htm>
- OECD. (2024c). *OECD digital economy outlook*. [Policy frameworks]. https://www.oecd.org/en/publications/serials/oecd-digital-economy-outlook_16c2967d.html
- OECD. (2025a). *Towards a common reporting framework for AI incidents*. [Policy frameworks]. https://www.oecd.org/en/publications/towards-a-common-reporting-framework-for-ai-incidents_f326d4ac-en.html
- OECD. (2025b). *AI initiatives from Israel*. <https://oecd.ai/en/dashboards/national/israel>
- OECD. (2025c). *AI initiatives from Mexico*. <https://oecd.ai/en/dashboards/national/mexico?utm=>
- Özkan, Y. (2024). *Avrupa Adalet Divanı, Google'a 2,4 milyar euroluk rekor cezayı onayladı*. BBC News Türkçe. <https://www.bbc.com/turkce/articles/c20rqkee2l1do>
- Parola Analytics. (2025). *5G standard essential patents: Key players and trends in 2025*. <https://parolaanalytics.com/blog/5g-standard-essential-patentskey-players-and-trends-in-2025>
- PIPL. (2022). *Personal information protection law of the People's Republic of China*. [Official document]. <https://personalinformationprotectionlaw.com/>
- PS Centre. (2025). *ASEAN: Deepening regional integration and global partnerships*. <https://pscentre.com.sg/index.php/2025/09/10/asean-deepening-regional-integration-and-global-partnerships/>
- Reuters. (2024). *UAE-based G42 working with US to meet AI standards amid China concerns*. <https://www.reuters.com/technology/uae-based-g42-working-with-us-meet-ai-standards-amid-china-concerns-2024-08-01/>
- Reuters. (2025). *Trump wants to kill \$52.7 billion semiconductor chips subsidy law*. <https://www.reuters.com/technology/trump-wants-kill-527-billion-semiconductor-chips-subsidy-law-2025-03-05/>

- Rijksoverheid. (2025). *Minister Beljaarts start publiek-privaat overlegplatform halfgeleidersector op*. <https://www.rijksoverheid.nl/actueel/nieuws/2025/01/29/minister-beljaarts-start-publiek-privaat-overlegplatform-halfgeleidersector-op>
- Ruck, J. (2024). A geoeconomic fix? European industrial policy on semiconductors. *Journal of Common Market Studies*. 62 (4), 1–20. <https://doi.org/10.1111/jcms.13710>
- Sandys, A. (2023). Huawei and Ericsson renew global 5G patent licensing deal. *JUVE Patent*. <https://www.juve-patent.com/people-and-business/huawei-and-ericsson-renew-global-5g-patent-licensing-deal/>
- Saniuk-Heinig, C. (2025). Examining western cyber policy reactions to China's rise in the digital age. *International Association of Privacy Professionals (IAPP)*. <https://iapp.org/news/a/examining-western-cyber-policy-reactions-to-chinas-rise-in-the-digital-age>
- Seaman, J. (2020). China and the new geopolitics of technical standardization. *Ifri*. <https://www.ifri.org/en/papers/china-and-new-geopolitics-technical-standardization>
- Semiconductor Engineering. (2025). *Gate-all-around FET (GAA FET)*. https://semiengineering.com/knowledge_centers/integrated-circuit/transistors/3d/gate-all-around-fet/
- Seeking Alpha. (2025). *ASML: The monopoly at the heart of the AI revolution*. <https://seekingalpha.com/article/4825386-asml-the-monopoly-at-the-heart-of-the-ai-revolution>
- Synopsys. (2025). *Synopsys collaborates with TSMC to drive the next wave of AI and multi-die innovation*. <https://news.synopsys.com/2025-09-24-Synopsys-Collaborates-with-TSMC-to-Drive-the-Next-Wave-of-AI-and-Multi-Die-Innovation>
- Synopsys. (2025). *What is EDA (Electronic Design Automation)?* <https://www.synopsys.com/glossary/what-is-electronic-design-automation.html>
- Staglianò, G. (2024). Chip war: The fight for the world's most critical technology. *Geopolitica*. <https://www.geopolitica.info/fight-microchips-technology/>
- Taiwan Semiconductor Manufacturing Company (TSMC). (2025a). *2nm technology*. https://www.tsmc.com/english/dedicatedFoundry/technology/logic/1_2nm
- TSMC. (2025b). *3nm technology*. https://www.tsmc.com/english/dedicatedFoundry/technology/logic/1_3nm
- TSMC. (2025c). *A16 technology*. https://www.tsmc.com/english/dedicatedFoundry/technology/logic/1_A16
- Tech in Asia. (2025). *Samsung said to delay Texas chip plant to 2026*. <https://www.techinasia.com/news/samsung-said-to-delay-texas-chip-plant-to-2026>
- Teng, T. (2024). *Nvidia, ABD'nin ticaret kısıtlamalarına misilleme olarak Çin soruşturmasıyla karşı karşıya*. Euronews. <https://tr.euronews.com/business/2024/12/10/nvidia-abdnin-ticaret-kisitlamalarina-misilleme-olarak-cin-sorusturmasiyla-karsi-karsiya>

- The Federal Government. (2025). *Federal government report on the High-Tech Strategy 2025: The high-tech strategy – a successful model for Germany as a strong country of innovation*. [Strategy document]. https://www.bmfr.bund.de/SharedDocs/Publikationen/DE/FS/657232_Bericht_zur_Hightech-Strategie_2025_en.pdf?blob=publicationFile&v=5
- The White House. (2019). *Executive order on securing the information and communications technology and services supply chain*. [Government report]. <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>
- The White House. (2021). *Building resilient supply chains, revitalizing American manufacturing, and fostering broad-based growth*. From the series 100-day reviews under Executive Order 14017. [Government report]. <https://bidenwhitehouse.archives.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf>
- The White House. (2022). *National security strategy of the United States of America*. [Strategy document]. <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>
- The White House. (2025). *Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok* [Presidential action]. <https://www.whitehouse.gov/presidential-actions/2025/01/application-of-protecting-americans-from-foreign-adversary-controlled-applications-act-to-tiktok/>
- Thomson Reuters Foundation. (2025). *AI governance in South Africa*. <https://www.trust.org/toolkit/part-2-emerging-ai-governance-in-africa/ai-governance-in-south-africa>
- Tobin, L. (2018). Xi's vision for transforming global governance: A strategic challenge for Washington and its allies. *Texas National Security Review*, 2(1), 154–166. <https://tnsr.org/2018/11/xis-vision-for-transforming-global-governance-a-strategic-challenge-for-washington-and-its-allies/>
- TrendForce. (2025). *Intel rumored to purchase more ASML High-NA EUV equipment*. <https://www.trendforce.com/news/2025/10/02/news-intel-rumored-to-purchase-more-asml-high-na-euv-equipment/>
- TweakTown. (2025). *Samsung to use more ASML High-NA EUV lithography tools to speed up 2nm GAA wafer production*. <https://www.tweaktown.com/news/107523/samsung-to-use-more-asml-high-na-euv-lithography-tools-to-speed-up-2nm-gaa-wafer-production/index.html>
- United Nations General Assembly. (2024). *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (A/78/L.49)*. <https://undocs.org/en/A/78/L.49>
- UNESCO. (2024a). *Chile launches a national AI policy and introduces an AI bill following UNESCO's recommendations*. <https://www.unesco.org/en/articles/chile-launches-national-ai-policy-and-introduces-ai-bill-following-unescos-recommendations-0>

- UNESCO. (2024b). *Recommendation on the ethics of artificial intelligence*. <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>
- US Department of Commerce National Institute of Standards & Technology. (2019). *US leadership in AI: A plan for federal engagement in developing technical standards and related Tools*. [Official document]. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf
- Wang, P. (2011). A brief history of standards and standardization organizations: a Chinese perspective. *East-West Center*. <https://www.eastwestcenter.org/publications/brief-history-standards-and-standardization-organizations-chinese-perspective>
- Wei, K. H. (2022). China's national standardization development outline: Policy implications and future directions. *Institute for Future Initiatives (IFI), Security Studies Unit (SSU), University of Tokyo*. https://ifi.u-tokyo.ac.jp/en/wp-content/uploads/2022/03/SSUessay_5_Wei20220209_EN.pdf
- Wendt, A. (1999). *Social theory of international politics*. Cambridge University Press.
- White&Case. (2025). *AI Watch: Global regulatory tracker – Brazil*. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-brazil>
- WilmerHale. (2025). *Latest DOJ export control enforcement action highlights China risks*. <https://www.wilmerhale.com/en/insights/client-alerts/20250806-the-latest-doj-export-control-enforcement-action-highlights-china-risks>
- World Trade Organization. (2025) *Agreement on trade-related aspects of intellectual property rights (TRIPS)* [Legal document]. https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm
- Wu, Y. (2022). China standards 2035 strategy: Recent developments and implications for foreign companies. *China Briefing*. <https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/>
- Yahoo Finance. (2024). *TSMC: 1.6nm process is on track for 2026*. <https://www.yahoo.com/tech/tsmcs-1-6nm-process-remains-120000844.html>
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.
- Zhang, I. (2025). China's new AI plan. *ChinaTalk*. <https://www.chinatalk.media/p/chinas-new-ai-plan>
- Zúñiga, N., Datta Burton, S., Blancato, F., & Carr, M. (2024). The geopolitics of technology standards: Historical context for US, EU and Chinese approaches. *International Affairs*, 100(4), 1635–1652. <https://doi.org/10.1093/ia/iaae124>