YAPAY ZEKA VE KÜRESEL GÜVENLİK MİMARİSİ: GÜÇ DAĞILIMININ MEKANİZMALARI VE YAPISAL DÖNÜŞÜM

Kürşat KAN[*]
ORCID ID: 0000-0003-2195-255

Declaration[**]

Özet

Bu çalışma, yapay zekanın küresel güvenlik mimarisi üzerindeki yapısal etkilerini ve güç dağılımını dönüştürme mekanizmalarını incelemektedir. Mevcut literatürde YZ'nin ürettiği nedensel zincirlerin ve kurumsal basıncın yeterince açıklanamaması temel araştırma problemini oluşturur. Makale, YZ'yi tekil bir araç yerine; hesaplama gücü (compute) yoğunlaşması, operasyonel hız ve modüler yönetişim üzerinden işleyen bir "çarpan teknoloji" olarak tanımlar. Araştırmada kuram güdümlü nitel bir tasarım benimsenmiş; yapılandırılmış belge analizi ve süreç izleme mantığına dayalı mekanizma temelli akıl yürütme yoluyla, güvenlik mimarisinin normatif, kurumsal ve operasyonel katmanlarında ortaya çıkan basınçlar ile uyum/gerilim dinamikleri izlenmiştir.

Bulgular, YZ'nin karar alma döngülerini sıkıştırdığını ve komuta-kontrol süreçlerini dönüştürdüğünü göstermektedir. Ancak bu teknolojik çarpanın etkisi homojen değildir. Hesaplama gücü, ileri çip üretimi ve veri merkezleri üzerindeki kontrol, devletler arasında sert bir hiyerarşi üretmektedir. Güç rekabeti artık model performansından ziyade altyapısal üstünlük ve kritik girdiler üzerinde denetim mücadelesine dönüşmüştür. Bu dönüşüm; BM, NATO ve silah kontrol rejimleri gibi çok katmanlı yapılar üzerinde yapısal bir baskı oluşturmaktadır. Bulgular; evrensel rejimlerin tıkandığı mevcut koşullarda, teknik standartlar ve ittifak içi düzenlemeleri kapsayan modüler araçların risk azaltımı için daha uygulanabilir bir yönetişim hattı sunduğuna işaret etmektedir.

Anahtar Kelimeler: Yapay zeka ve küresel güç dağılımı, Küresel güvenlik mimarisi, Stratejik istikrar ve tırmanma riski, Hesaplama gücü yoğunlaşması

[*] Dr. Öğr. Üyesi, Selçuk Üniversitesi, Uluslararası İlişkiler Bölümü
[*] AI language model (Claude) was minimally employed to help refine the writing style and clarity of certain sections in this paper.
[*] Bu çalışma Selçuk Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü tarafından 23401184'nolu proje kapsamında desteklenmiştir.

ARTIFICIAL INTELLIGENCE AND GLOBAL SECURITY ARCHITECTURE: MECHANISMS OF POWER DISTRIBUTION AND STRUCTURAL TRANSFORMATION

Abstract

This study examines the structural impact of artificial intelligence (AI) on the global security architecture and the mechanisms transforming the distribution of power. The core research problem is the lack of a clear causal chain explaining how AI-driven shifts exert pressure on norms, institutions, and operational tools. This article conceptualizes AI not as a singular capability but as a "multiplier technology" that redefines power competition through compute concentration, operational speed, and modular governance. Adopting a theory-driven qualitative design, the research utilizes structured document analysis and mechanism-based reasoning to trace structural pressures across the normative, institutional, and operational layers of the security architecture.

The findings indicate that AI compresses decision cycles and reshapes command-and-control and intelligence processes. However, the impact of this multiplier is not distributed uniformly. Concentration in computing power, advanced chips, and data centers produces a rigid strategic hierarchy. Consequently, power competition has evolved into an infrastructural struggle over critical inputs and the control of enabling infrastructures. This shift exerts structural pressure on the multi-layered security architecture, including the UN-centered collective security system, NATO, and arms control regimes. Given the deadlock in universal regimes caused by great power rivalry, the findings suggest that modular regulatory tools—such as technical standards and alliance-based arrangements—offer a more viable pathway for risk mitigation and governance.

Keywords: Artificial Intelligence and Global Power Distribution, Global Security Architecture, Strategic Stability and Escalation Risk, Compute Concentration

Giriş

Yapay zeka (YZ) bilimkurgu filmlerinin neredeyse yarım asırdır kullandığı objelerden biriydi. Sinemanın iyi veya kötü sanal karakteri, son on yıldır devletlerin ve insanların hayatına giren çok önemli bir karaktere evrildi. Bugün YZ sadece sinemanın bir karakterinden ötede, günlük yaşamın önemli bir parçası haline geldi. Bireysel hayatta bu kadar alan kaplayan bir unsurun devletlere etkisi de kaçınılmazdı. Ancak bu etki, on yıl önce konuşulan ve tartışılanlardan çok daha büyük ve asimetrikti. Bu etki kuramsal açıdan da pratikler açısından da yıkıcı ve yeniden inşa edici boyutlar taşımaktadır.

YZ, devletlerin göreli güç kazanımı arayışını hızlandırarak veri, hesaplama kapasitesi (compute) ve kritik altyapı üzerindeki yoğunlaşmayı stratejik üstünlüğün yeni ögelerine dönüştürmekte ve uluslararası eşitsizliği sert bir hiyerarşi şeklinde yeniden üretmektedir. Ayrıca karar süreçlerine asimetrik katılım ve düzenleme kapasitesindeki uçurumlar, teknolojik yönetişimi bazı aktörlerin lehine kurumsal bir eşitsizlik mekanizmasına çevirmektedir. YZ ekosisteminin küresel sermaye, platform gücü ve bilgi tekelleri etrafında örgütlenmesi, uluslararası ilişkilerde eşitsizliği yalnızca bir sonuç olarak değil; üretim ve denetim ilişkileri içinde süreklileşen yapısal bir tahakküm biçimi olarak da görünür kılmıştır.

Uluslararası sistem, tarih boyunca teknolojik dönüşümlerin yarattığı yapısal etkilerle defalarca yeniden şekillenmiştir. Sanayi Devrimi, buhar gücü, elektrik ve nükleer teknoloji; güç dengelerini dönüştürerek devletler arasındaki hiyerarşiyi derinden etkilemiştir. YZ günümüzde benzer bir dönüşüme öncülük eden teknolojidir.

YZ, devletlerin ekonomik kapasitesinden askeri yeteneklerine, toplumsal yapısından bilgi işleme kabiliyetine kadar uzanan geniş bir alanda yeni güç parametreleri üretmektedir. Akademik literatür, YZ'nin uluslararası rekabeti yeniden tanımladığını vurgulamaktadır (Horowitz, 2018; Johnson, 2019a; Sastry vd., 2024). Bu dönüşüm süreci, yalnızca askeri kapasite artışıyla sınırlı değildir. Rekabet; karar döngülerinin hızlanması ve komuta-kontrol sistemlerinin dönüşümü üzerinden şekillenmektedir. Ayrıca altyapısal yoğunlaşma, bu yeni güç mücadelesinin temel belirleyicilerinden biri olarak öne çıkmaktadır (Horowitz, 2018; Johnson, 2019a; Sastry vd., 2024).

Bu çalışmada YZ'nin küresel güç dağılımını nasıl dönüştürdüğü ve küresel güç ve güvenlik mimarisine etkisi ele alınacaktır. Bu çalışma, YZ'nin küresel güç dağılımını dönüştüren

mekanizmalarını kuramsal bir çerçevede belirlemeyi amaçlamaktadır. Bu mekanizmaların küresel güvenlik mimarisinin normatif, kurumsal ve operasyonel katmanlarındaki etkileri, süreç izleme ve yapılandırılmış belge analizi yöntemleriyle analiz edilmektedir.

Bu çalışma, YZ'nin küresel güç dağılımını hangi yapısal kanallar üzerinden dönüştürdüğünü sorunsallaştırmaktadır. Araştırmanın temel odağı, bu dönüşümün küresel güvenlik mimarisi üzerinde ürettiği dinamikleri analiz etmektir. Bu bağlamda, YZ'nin mimarideki farklı katmanlarda ne tür uyum ve gerilimlere yol açtığı incelenmektedir. Analitik çerçeve; BM merkezli kolektif güvenlik sistemi, bölgesel düzenlemeler ve silahların kontrolü rejimlerini kapsamaktadır. Ayrıca uluslararası insancıl hukuk ve ceza adaleti mekanizmaları da çalışmanın kapsamına dahil edilmiştir. Çalışma, YZ'yi tekil bir kapasite artışından ziyade; karar döngülerini sıkıştıran, bilgi işleme maliyetlerini düşüren ve komuta-kontrol/istihbarat/hedefleme süreçlerini dönüştüren bir "çarpan teknoloji" olarak ele alır.

Çalışmanın araştırma sorusu, birbirini tamamlayan üç temel hipotez üzerinden sınanmaktadır.

İlk hipotez, YZ kapasitesinin fiziksel altyapıdaki yoğunlaşmasına odaklanmaktadır. İleri düzey çipler, bulut sistemleri ve veri merkezleri bu kapasitenin temel bileşenleridir. Günümüzde güç rekabeti, model performansından ziyade bu kritik girdilerin ve hesaplama gücü akışlarının kontrolüne kaymaktadır. Söz konusu eğilim, uluslararası sistemdeki hiyerarşik yoğunlaşmayı derinleştiren temel bir unsurdur.

İkinci hipotez, YZ'nin karar alma süreçlerindeki hız ve otomasyon etkisini ele almaktadır. Daralan karar süreleri, kriz yönetiminde yanlış anlama ve hatalı hesaplama riskini belirgin şekilde artırmaktadır. Özellikle YZ-siber etkileşimi, komuta-kontrol süreçlerinde tırmanma riskini tetikleyerek stratejik istikrar üzerinde ciddi bir baskı oluşturmaktadır.

Üçüncü hipotez, küresel yönetişim mekanizmalarındaki yapısal dönüşümü incelemektedir. Büyük güç rekabeti ve mevcut kurumsal tıkanıklıklar, bağlayıcı evrensel rejimlerin inşasını giderek zorlaştırmaktadır. Bu süreçte güvenlik yönetişimi, daha kademeli ve modüler araçlara evrilmektedir. Teknik standartlar, ittifak içi düzenlemeler ve tedarik zinciri üzerinden kurulan fiili uyum baskıları, bu yeni dönemin temel yönetişim enstrümanlarıdır.

Bu çalışma, metodolojik olarak kuram güdümlü nitel bir araştırma tasarımı üzerine inşa edilmiştir. Araştırmada birbirini tamamlayan iki temel teknik kullanılmaktadır. Bunlar; yapılandırılmış belge analizi ve süreç-izleme (process tracing) mantığına dayalı nedensel akıl yürütmedir (Bowen, 2009; Beach & Pedersen, 2019; Bennett & Checkel, 2015).

Yapılandırılmış belge analizi, küresel güvenlik mimarisinin normatif ve kurumsal metinlerine odaklanır. Bu aşamada; YZ'ye ilişkin risk tanımları, düzenleme tercihleri ve önerilen yönetişim araçları sistematik olarak ayrıştırılmaktadır (Bowen, 2009).

Süreç-izleme mantığı ise teorik mekanizmalar ile ampirik çıktılar arasındaki nedensel bağları değerlendirir. Örneğin; hesaplama gücü yoğunlaşması veya otomasyon hızı gibi mekanizmaların, stratejik istikrar ve yönetişimde parçalanma gibi sonuçlarla tutarlılığı analiz edilmektedir (Beach & Pedersen, 2019; Bennett & Checkel, 2015).

Araştırmanın veri seti geniş bir yelpazeye dayanmaktadır. Resmi kurum metinleri ve politika belgeleri birincil kaynakları oluştururken; hakemli literatür ve araştırma raporları ikincil kaynaklar olarak kullanılmaktadır.

Araştırmanın yöntemsel geçerliliği üç temel dayanak üzerine inşa edilmiştir. Bu süreç; kavramların operasyonel olarak tanımlanmasını, veri setinin şeffaf sınırlandırılmasını ve bulguların literatürle üçgenlenmesini (triangulation) kapsamaktadır (Bowen, 2009; Beach & Pedersen, 2019).

Makalenin temel argümanı belirli bir analitik zincir doğrultusunda ilerlemektedir. İlk aşamada, YZ'nin güç dağılımını dönüştüren temel mekanizmaları kavramsal düzeyde belirlenmektedir. Bu kapsamda hesaplama gücü yoğunlaşması, otomasyon hızı ve ağ merkeziliği gibi unsurlar analiz edilmektedir. İkinci aşamada, bu mekanizmaların küresel güvenlik mimarisi üzerinde yarattığı baskılar sistematik olarak izlenmektedir. Analiz; mimarinin normatif, kurumsal ve operasyonel katmanlarında yoğunlaşmaktadır. Bu süreçte stratejik istikrar, hukuki uyum ve yönetişimde parçalanma gibi temel sorunlar ele alınmaktadır. Son aşamada ise bağlayıcı rejimlerin sınırları ve modüler düzenleme seçeneklerinin uygulanabilirliği tartışılmaktadır. Söz konusu tartışma, büyük güç rekabeti ve mevcut kurumsal tıkanıklıklar ekseninde yürütülmektedir. Bu kurgu, çalışmadaki tüm kavram ve bulguları hipotezlerin öngördüğü mekanizma-sonuç ilişkisi içinde konumlandırmayı amaçlamaktadır.

Bu makalenin özgün katkısı, YZ'yi yalnızca yeni bir askeri kapasite artışı olarak değil; bulut altyapısı, ileri çipler ve yüksek ölçekli veri-merkezleri üzerinden şekillenen bir "altyapısal çarpan" olarak kavramsallaştırmasında yatmaktadır. Bu çerçevede "hesaplama kapasitesi egemenliği", bir aktörün yüksek performanslı hesaplama kaynaklarına (ileri yarı iletkenler, bulut ve veri merkezi kapasitesi, kritik tedarik zincirleri) erişimi kontrol etme ve bu

kaynakları stratejik amaçlar doğrultusunda yönlendirme yeteneğini ifade eder. Dolayısıyla YZ rekabeti, model yeteneği kadar, bu yeteneği mümkün kılan altyapının yoğunlaşması ve boğaz noktalarının yönetimi üzerinden de güç dağılımını yeniden üretmektedir (Farrell & Newman, 2019; Hawkins vd., 2025; U.S. Department of Commerce, Bureau of Industry and Security, 2023).

Literatüre katkı üç düzlemde yapılandırılmıştır. Birincisi, güç tartışmasını salt "platform/algoritma" rekabeti düzeyinde bırakmak yerine, YZ'nin üretim ve kullanım koşullarını belirleyen altyapı-asimetriyi (hesaplama kapasitesi yoğunlaşması) gücün yapısal bir bileşeni olarak görünür kılar (Horowitz, 2018; Johnson, 2019a). İkincisi, bu altyapısal dönüşümün küresel güvenlik mimarisinin normatif, kurumsal ve operasyonel katmanlarında nasıl bir basınç ürettiğini mekanizma-temelli bir argüman zinciri içinde eşler. Üçüncüsü, bağlayıcı rejimlerin tıkanıklıklarını dikkate alarak, risk azaltımı ve uyum için "modüler düzenleme" yaklaşımını pratik bir yönetişim alternatifi olarak tartışır.

Bu çalışma, kuram güdümlü nitel bir araştırma tasarımı çerçevesinde, yapılandırılmış belge analizi ve süreç-izleme mantığıyla mekanizma-temelli bir değerlendirme yürütmektedir (Bowen, 2009; Beach & Pedersen, 2019; Bennett & Checkel, 2015). Dolayısıyla amaç, YZ'nin etkilerini tekil bir vaka üzerinden nedensel olarak "ölçmekten" ziyade; literatürde dağınık halde bulunan nedensel kanalları tutarlı bir analitik zincire bağlamak ve bu zincirin güvenlik mimarisinin katmanlarına nasıl yansıdığını göstermekti.

Ampirik kapsam, başlıca uluslararası örgüt belgeleri, strateji dokümanları, düzenleyici metinler ve alan raporları gibi açık kaynak metinlere dayanmaktadır. Bu tercih, bulguların genellenebilirliğini istatistiksel bir temsilden değil; kaynak çeşitliliği, kavramsal tutarlılık ve mekanizma-çıktı eşlemesinin izlenebilirliğinden türetir. Bu nedenle çalışma, firma düzeyinde performans kıyasları, model değerlendirme metrikleri veya ayrıntılı teknik doğrulama analizleri sunmamaktadır.

Siber alan bu makalede bağımsız bir alt disiplin veya "siber güç/siber düzen" literatürünün başlı başına bir inceleme alanı olarak ele alınmamaktadır. Bunun yerine siber alan, YZ'nin hız, otomasyon ve bilgi bütünlüğü üzerindeki etkilerinin somutlaştığı bir uygulama düzlemi olarak konumlandırılır ve YZ-siber etkileşimi stratejik istikrar ve bilgi güvenliği bağlamında tartışılır (Johnson, 2019b). Bu sınırlama, çalışmanın analitik odağını YZ'nin küresel güvenlik mimarisinin katmanlarında ürettiği yapısal basınçlara yoğunlaştırmak ve siber alanı bu basınçların görünürleştiği mekanizmalardan biri olarak ele almak amacıyla tercih edilmiştir.

Son olarak, çalışma öngörü (forecasting) iddiası taşımaz; belirli bir ülke veya bölgeye ilişkin ayrıntılı alan incelemesi yerine, büyük güç rekabeti bağlamında ortaya çıkan genel mekanizmaları ve yönetişim seçeneklerini tartışır. Bu nedenle vaka dışlamaları (ör. tekil savaş alanı uygulamaları veya kapalı veri setlerine dayalı değerlendirmeler) bilinçli bir tercih olup, makalenin kapsamını kavramsal bütünlük içinde sınırlamayı hedefler.

Gücün Doğası, Değişim ve Dönüştürücü Mekanizmalar

Bu bölüm, araştırmanın bağımsız değişkenini inşa etmektedir. YZ'nin güç üretimini dönüştürme süreçleri bu kısımda tanımlanmaktadır. Özellikle birinci ve ikinci hipotezlerde (H1 ve H2) öngörülen mekanizmalar kavramsal olarak temellendirilmektedir. Bu sayede, küresel güvenlik mimarisi üzerindeki baskı noktaları analitik olarak netleştirilmektedir. Analiz, teknolojik dönüşümün kurumsal yapılar üzerindeki etkisini anlamayı kolaylaştıran bir çerçeve sunmaktadır.

Uluslararası ilişkiler literatüründe güç, uzun süre askeri kapasite, ekonomik büyüklük ve teknolojik üretim gücüyle ölçülmüştür. YZ bu ölçütleri ortadan kaldırmaktan ziyade, onları yeniden işleyen bir ara katman üretir ve bunların etkinliğini artıran/azaltan bir çarpan işlevi görür. Karar alma döngülerini sıkıştırır, bilgi üretim maliyetlerini düşürür, üretimde otomasyon imkanlarını genişletir ve güvenlik alanında hedefleme-istihbarat-komuta-kontrol süreçlerini dönüştürür (Horowitz, 2018).

YZ'nin küresel güç dağılımı üzerindeki dönüştürücü etkisini belirgin kılan temel dinamik, bu teknolojinin homojen bir yayılım sergilememesidir. Aksine YZ ekosistemi; ileri nesil çipler, bulut altyapısı, yüksek kapasiteli veri merkezleri, araştırma ekosistemleri ve norm belirleyici kurumlar gibi stratejik odak noktalarında yoğunlaşma eğilimi göstermektedir. Bu yapısal yoğunlaşma merkezinde üzerine odaklanılması gereken soru şudur: YZ, küresel güç dağılımını hangi yapısal kanallar üzerinden dönüştürmekte ve bu süreç hangi aktörler lehine asimetrik bir güç yoğunlaşması üretmektedir?

Bu sorunsalın aciliyeti birbiriyle kesişen iki eğilimin yarattığı gerilimden doğmaktadır. İlk eğilim, hesaplama gücü talebindeki artışın endüstriyel yoğunlaşmayı hızlandırmasıdır. İleri seviye YZ modellerinde hesaplama gücü ihtiyacı hızla artarken, model geliştirme kapasitesinin büyük ölçüde özel sektör odaklı hale gelmesi dikkat çekicidir. Stanford AI Index 2025 raporu, 2024 yılı itibarıyla en öne çıkan modellerin ezici çoğunluğunun endüstri kaynaklı olduğuna işaret etmektedir (Maslej vd., 2025). İkinci eğilim ise jeopolitik rekabet ve

dışlayıcı erişim rejimleridir. YZ üretim zincirinin temel girdilerine (ileri seviye yarı iletkenler ve üretim ekipmanları) erişimin bir ulusal güvenlik ve stratejik rekabet unsuruna dönüşmesi; ihracat kontrolleri vasıtasıyla hesaplama ekosisteminin bir kısıtlama ve dışlama alanına evrilmesidir (U.S. Department of Commerce, Bureau of Industry and Security, 2023).

Bu iki eğilim birlikte okunduğunda, YZ'de rekabet avantajının salt yenilikçilikten ibaret olmadığı; sermaye yoğun altyapı, tedarik zinciri boğazları ve erişim rejimleriyle şekillenen daha sert bir hiyerarşi ürettiği görülür. Dolayısıyla güç mücadelesi, model performansının ötesinde, hesaplama gücü akışlarının kontrolü ve kritik girdilere erişim üzerinden kurumsallaşmaktadır.

YZ'nin ileri seviye modellerinde rekabet avantajı; yüksek ölçekli veri merkezleri, hızlandırıcı çipler ve bulut altyapısı gibi sermaye yoğun girdilere dayanır. Hesaplama gücü yönetişimi çerçevesi, bu girdinin yoğunlaşmış tedarik zinciri nedeniyle merkezi aktörlere yapısal avantaj sağladığını ve devletlerin hesaplama gücü akışlarını politika araçlarıyla etkileyebileceğini belirtir (Sastry vd., 2024). Bu tartışmayı somutlayan hesaplama gücü egemenliği literatürü, hesaplama gücünün yalnızca miktar değil, mülkiyet ve denetim boyutlarını da öne çıkarır. Bazı akademisyenler hesaplama gücü egemenliğini; (i) ülke sınırları içindeki hesaplama gücü kapasitesi, (ii) bu kapasiteye sahip bulut şirketlerinin milliyeti/mülkiyeti, (iii) hızlandırıcı çip ekosisteminin menşei gibi üç düzeyde ayrıştırır ve küresel bulut pazarının büyük kısmını temsil eden baskın sağlayıcılar üzerinden ampirik bir okuma önerir (Hawkins vd., 2025). Hesaplama gücü yoğunlaşması, YZ kabiliyet üretimini belli merkezlerde toplarken; çevrede kalan aktörleri maliyet, tedarik ve erişim kısıtları üzerinden bağımlı hale getirebilir.

Ayrıca Farrell ve Newman'ın (2019) ortaya koyduğu gibi, küresel ağlarda merkezi düğümlerin kontrolü devletlere zorlayıcı güç sağlayabilir. YZ bağlamında bu merkezi düğümler; bulut altyapısı, model dağıtım kanalları, veri akışları ve yarı iletken tedarik zincirleri olarak düşünülebilir. Buradaki kritik nokta, güç projeksiyonunun yalnızca askeri değil, erişimi sınırlamak, hizmeti kesmek, uyum maliyeti yaratmak veya izleme kapasitesi elde etmek gibi altyapısal olmasıdır. Özel sektörün notable model üretimindeki ağırlığına işaret eden bulgular, bu altyapı/kapasite birikiminin şirketleşmiş doğasını da görünür kılar (Maslej vd., 2025). Böylece güç dağılımı, yalnızca devletler arası rekabet olmaktan çıkarak devlet–şirket eklemlenmesi üzerinden hibrit bir form kazanmaktadır.

YZ askeri güç dengesini bir etkinleştirici teknoloji olarak etkileme potansiyeline sahiptir. Nitekim YZ istihbarat, hedefleme, lojistik ve komuta-kontrol alanlarında dönüşüm

yaratacaktır (Horowitz, 2018). Johnson (2019a), YZ'nin hızlı yayılımının belirsizlik ve kırılganlıklar üreterek stratejik istikrarsızlık ve büyük güç rekabetini keskinleştirebileceğini ileri sürer. Bu yaklaşımın ima ettiği temel sonuç, askeri gücün yalnızca daha fazla platform üretimiyle değil; daha hızlı karar, daha yoğun veri işleme ve operasyonel koordinasyonla yeniden tanımlanmasıdır. Bu dönüşüm, kriz anlarında tırmanma risklerini artırabilir.

YZ'nin ekonomik kazançlarının girdi yoğunlaşması ve ağ merkeziliği nedeniyle eşitsiz dağılmaya meyilli olduğu da görülmektedir. Emek piyasası düzeyinde otomasyon ağırlığına dönük tartışmalar (Acemoglu & Restrepo, 2020) ile kalkınma düzeyindeki uyarılar (Korinek & Stiglitz, 2021) birlikte okunduğunda, YZ'nin küresel güç farklarını artırma riski belirginleşmektedir (Acemoglu & Restrepo, 2020). Bu durum, özellikle orta ve gelişmekte olan ülkeler açısından iki stratejik zorunluluk üretir: hesaplama gücü erişimi ve bulut/altyapı seçeneklerini çeşitlendirmek; bununla eş zamanlı olarak veri yönetişimi ve yerli yetenek ekosistemini güçlendirmek.

Genel sonuç şudur: YZ, uygun politikalarla yaygın refah artışı potansiyeli taşısa da mevcut ekosistem yapısı (hesaplama gücü yoğunlaşması, şirketleşmiş kapasite ve tedarik zinciri boğazları) nedeniyle küresel güç birikimini hızlandırma ve eşitsizliği derinleştirme eğilimi taşır. Bu nedenle YZ çağında güç; askeri ve ekonomik stokların yanı sıra hesaplama gücü egemenliği, ağ merkeziliği, veri yönetişimi ve standart belirleme kapasitesinin bileşiminden oluşan yeni bir mimariye dayanmaktadır.

Bu noktada güç parametrelerindeki dönüşümün yalnızca rekabet ve kalkınma sonuçları üretmediği; bununla beraber uluslararası düzenin güvenlik üretme biçimini de yeniden şekillendirdiği görülür. Çünkü güçteki yeniden ölçeklenme, kriz yönetimi, caydırıcılık, silahların kontrolü ve uluslararası hukukun uygulanabilirliği gibi alanlarda kurumsal mimariyi doğrudan baskılayan bir etki yaratır. Dolayısıyla YZ'nin etkisini tam anlamak için, küresel güvenlik mimarisinin dayandığı normlar ve kurumlar ile bu mimarinin sahadaki işleyişine bakmak gerekmektedir.

Takip eden bölüm, araştırmanın bağımlı değişkeni olan güvenlik mimarisini tüm katmanlarıyla tanımlamaktadır. Bu tanımlama süreci, YZ'nin söz konusu katmanlarda yarattığı etkilerin incelenebileceği analitik bir zemin hazırlamaktadır. Böylece çalışmanın ilerleyen aşamalarında yapılacak değerlendirmeler için gerekli kuramsal çerçeve oluşturulmaktadır.

Küresel Güvenlik Mimarisi

Bu bölüm, küresel güvenlik mimarisini normatif, kurumsal ve operasyonel katmanlar şeklinde tasnif etmektedir. Bu yaklaşım, analizin ortak referans çerçevesini oluşturmaktadır. Temel amaç, YZ'nin etkilerini tekil örnekler üzerinden sunmak değildir. Bunun yerine, her bir etkinin ilgili katmanlarda ne tür bir uyum veya gerilim ürettiğini metodolojik olarak izlenebilir kılmaktır.

Küresel güvenlik mimarisi, devletlerin ve uluslararası örgütlerin barışı korumak, çatışmaları önlemek/sonlandırmak ve savaşın insani etkilerini sınırlamak amacıyla geliştirdiği normlar, kurumlar ve operasyonel araçlar bütününü ifade eder. Bu mimari tekil bir dünya hükümeti değil; BM merkezli kolektif güvenlik sistemi, bölgesel düzenlemeler, silahların kontrolü rejimleri, insancıl hukuk ve uluslararası ceza adaletinin iç içe geçtiği çok katmanlı bir yönetişim alanıdır.

Mimari, normatif çekirdeğini 1945 BM Şartı'ndan alır: devletlerin egemen eşitliği ve uluslararası ilişkilerde kuvvet kullanma/tehdit etme yasağı, savaşın meşru bir dış politika aracı olmasına sınır çizer (United Nations, 1945).

Kolektif güvenlik mantığı, saldırganlığın tüm uluslararası topluma karşı ihlal sayılması ve BM Güvenlik Konseyi'nin barışa tehdit/ihlal veya saldırı fiilini tespit ederek bağlayıcı tedbirlere karar verebilmesiyle işler. Şart'ın VII. Bölümü ekonomik yaptırımlar, iletişim/diplomatik ilişkilerin kesilmesi gibi zorlayıcı araçları; yetersiz kaldığında askeri tedbirleri öngörerek mimarinin hukuki omurgasını oluşturur (United Nations, 1945). Bu klasik normatif omurga, YZ'nin barış ve güvenlik boyutunu da kurumsal gündeme taşımaktadır. BM Genel Kurulu'nun güvenli, emniyetli ve güvenilir YZ odağındaki kararı (United Nations, 2024a), YZ'nin insan hakları, kapasite geliştirme ve yönetişim boyutlarını küresel düzeyde ilkesel bir çerçeveye bağlayarak güvenlik mimarisinin norm üretim katmanına somut bir ek yapmıştır.

Ayrıca BM sisteminin kendi içinde, YZ'nin kurumsal kullanımı için etik ilke setleri benimsemesi (United Nations System Chief Executives Board for Coordination, 2022), güvenlik mimarisinin yalnızca dışarıya dönük norm üretimiyle değil kurumsal örneklik üzerinden de yeniden güncellenmeye çalışıldığını göstermektedir.

Küresel güvenlik mimarisinin kurumsal çekirdeğinde BM bulunsa da güvenliğin fiili üretimi çoğu zaman bölgesel örgütler ve alt bölgesel mekanizmalar üzerinden gerçekleşir. Bu iş

bölümünün Avrupa-Atlantik ayağında NATO, kolektif savunma ve caydırıcılığı kurumsallaştırır. NATO'nun 2022 Stratejik Konsepti, İttifak'ın temel amacını kolektif savunma olarak tanımlarken caydırma ve savunma; kriz önleme ve yönetimi, işbirliğine dayalı güvenlik şeklinde üç temel görevi açık biçimde sıralar (NATO, 2022). NATO, bu görev setini teknoloji yönetişimi ile tamamlayarak savunmada YZ'nin sorumlu kullanımına ilişkin ilkeleştirme ve uygulama hedefleri geliştirmiş; 2024'te yayımlanan revize YZ stratejisinde Principles of Responsible Use ile birlikte birlikte-çalışabilirlik, YZ ekosisteminin genişletilmesi ve uygulama kapasitesinin artırılması gibi somut öncelikleri vurgulamıştır (NATO, 2024). Bu, küresel mimarinin bir parçası olarak yalnızca askeri savunma değil, kriz yönetimi ve ortak güvenlik ağlarıyla daha geniş bir güvenlik portföyü sunmaktadır.

Avrupa güvenlik düzeninin bir diğer normatif-kurumsal sütunu, 1975 Helsinki Nihai Senedi ile şekillenen ve bugün Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) çerçevesinde sürdürülen kapsamlı güvenlik yaklaşımıdır. Helsinki metni, katılımcı devletlerin eşit haklar ve halkların kendi kaderini tayin hakkına saygı ilkesini vurgular ve devletler arası işbirliğini uluslararası hukuka uyumla ilişkilendirir (Conference on Security and Co-operation in Europe, 1975). Bu kapsamlı güvenlik hattı, YZ kaynaklı güvenlik etkilerini de gündemine almaya başlamıştır: AGİT Parlamenter Asamblesi'nin 2024 Bükreş Deklarasyonu, YZ'nin güvenlik etkilerine ilişkin farkındalık/izleme vurgusu yapmış ve teknoloji kaynaklı risklerin demokratik denetim ve şeffaflık ilkeleriyle ele alınması gerektiğini belirtmiştir (Organization for Security and Co-operation in Europe Parliamentary Assembly, 2024).

Küresel mimarinin çok-merkezli niteliği Avrupa dışındaki bölgesel güvenlik düzeneklerinde de görülür. Örneğin Afrika Birliği bünyesindeki Barış ve Güvenlik Konseyi (PSC), çatışmaların önlenmesi-yönetimi-çözümü için kalıcı karar organı ve kolektif güvenlik/erken uyarı düzenlemesi olarak kurulmuştur (The African Union, 2002). Aynı protokol, PSC'yi kıtasal erken uyarı sistemi ve Afrika Daimi Hazır Gücü gibi araçlarla desteklenmiş bir mimari olarak tasarlar (The African Union., 2002). Bu bize küresel güvenliğin yalnızca BM merkezli değil, bölgesel kapasite inşası ile de şekillendiğini gösterir. Afrika Birliği bu kapasite inşasını teknoloji yönetişimine de genişletmiş; 2024'te Kıtasal YZ Stratejisini kabul ederek etik, kapsayıcılık, kapasite geliştirme ve yönetişim başlıklarında çerçeve oluşturmuştur (African Union, 2024). PSC ise 20 Mart 2025 tarihli toplantısında YZ'nin barış, güvenlik ve yönetişime etkilerini doğrudan gündem başlığı yaparak danışma/uzman desteği, kapasite geliştirme ve düzenleyici çerçevelerin güçlendirilmesi gibi

somut adımlar çağrısında bulunmuştur (African Union Peace and Security Council [AU PSC], 2025).

Küresel güvenlik mimarisinin sahadaki en görünür enstrümanlarından biri olan BM barış operasyonları, meşruiyetini 2008 tarihli Capstone Doktrininde tanımlanan üç temel ilke üzerine inşa etmiştir. Bu ilkeler; tarafların rızası, tarafsızlık ve meşru müdafaa ya da manda savunması haricinde kuvvet kullanımından kaçınılmasıdır (United Nations, 2008). Söz konusu normatif çerçeve, barış operasyonlarını klasik askeri çatışma modellerinden ayrıştırarak operasyonun başarısını saf askeri üstünlükten ziyade siyasi uzlaşı ve güven inşasına bağlar. Bununla eşzamanlı olarak BM Barış Operasyonları Dijital Dönüşüm Stratejisi ile (veri/analitik dahil) yeni teknolojilerin sahada kullanımını kapasite ve risk yönetimi mantığıyla ele alarak misyonların daha etkin ve güvenli biçimde yürütülmesine dönük somut bir kurumsal modernizasyon hattı açmıştır (United Nations, 2021).

Küresel güvenlik mimarisinin bir diğer temel katmanı, silahların kontrolü ve yayılmanın önlenmesi rejimleridir. Nükleer Silahların Yayılmasının Önlenmesi Antlaşması (NPT), nükleer silah sahibi devletlerin bu silahları devretmemesi ve nükleer silah sahibi olmayan devletlerin de nükleer silah edinmemesi yönünde çekirdek yükümlülükler getirir (United Nations, 1970). YZ'nin askeri alandaki yayılımı arttıkça, silah kontrolü katmanı da teknoloji yönetişimiyle kesişmektedir. BM Genel Kurulu'nun askeri alanda YZ ve uluslararası barış ve güvenlik gündemli kararı (United Nations, 2024b), uluslararası hukukun uygulanabilirliği, risklerin değerlendirilmesi ve kapsayıcı diyalog çağrısıyla bu alanı kurumsal bir müzakere hattına bağlamıştır.

Güvenlik mimarisi yalnızca çatışmayı önlemekle değil, çatışma çıktığında insani tahribatı sınırlamak ve ağır ihlaller için hesap verebilirliği güçlendirmekle de ilgilidir. Uluslararası insancıl hukuk (UİH), silahlı çatışmanın etkilerini sınırlamayı; çatışmaya katılmayan ya da artık katılmayan kişileri korumayı hedefler. Hesap verebilirlik boyutunda ise Uluslararası Ceza Mahkemesi'ni kuran Roma Statüsü önemlidir. Statü, Mahkemenin yargı yetkisini ve yargılamanın koşullarını düzenlerken, BMGK'nin VII. Bölüm kapsamında bir kararla soruşturma/kovuşturmayı belirli süreyle ertelemesine ilişkin mekanizmayı da içerir (United Nations, 1998). Bu, küresel güvenlik mimarisindeki siyasal güvenlik yönetimi ile ceza adaleti arasındaki gerilimli ama kurumsallaşmış ilişkiye işaret etmektedir.

Özetle küresel güvenlik mimarisi; Birleşmiş Milletler Şartı çerçevesindeki kuvvet kullanma yasağına dayalı kolektif güvenlik sistemi, NATO ve Afrika Birliği gibi bölgesel

düzenlemeler, barış operasyonları, NPT odaklı silahların kontrolü rejimleri ile uluslararası insancıl hukuk ve ceza adaleti mekanizmalarının iç içe geçtiği çok katmanlı bir yapıdır. Bu mimari, uluslararası barışın tesisi için müşterek bir hukuki-siyasi zemin sunsa da büyük güçler arası rekabet, veto mekanizmaları, asimetrik tehditler ve bölgesel kapasite farkları nedeniyle uygulama aşamasında sıklıkla yapısal tıkanıklıklar yaşamaktadır.

YZ'nin katmanlı mimari üzerindeki etkisi, araştırmanın hipotezlerinde tanımlanan üç mekanizma aracılığıyla incelenmektedir. İlk olarak, altyapı ve hesaplama gücü yoğunlaşması, mimarinin kurumsal kapasitesini ve asimetrik bağımlılık ilişkilerini derinleştirmektedir. İkinci olarak, hız ve otomasyon faktörleri, krize müdahale süreçleri ile stratejik istikrar pratikleri üzerinde baskı oluşturmaktadır. Büyük güç rekabeti koşullarında yaşanan yönetişim tıkanıklıkları ise bağlayıcı rejimler yerine modüler araçlara yönelimi teşvik etmektedir. Bu eğilim, güvenlik mimarisinin norm üretim kapasitesini parçalı bir biçimde dönüştürmektedir. Bu gerekçelerle izleyen bölüm, söz konusu etkileri üç temel analitik izlek üzerinden değerlendirmektedir. Bu izlekler; stratejik istikrar, hukuki uyum ve hesap verebilirlik ile YZ-siber güvenlik başlıklarından oluşmaktadır.

Yapay Zekanın Küresel Güvenlik Mimarisine Etkileri

Küresel güvenlik mimarisi; devletlerin askeri kapasiteleri kadar, NATO benzeri ittifak sistemleri, caydırıcılık ve stratejik istikrar pratikleri, silahların kontrolü/insancıl hukuk rejimleri, kriz yönetimi mekanizmaları ve giderek artan biçimde dijital altyapı güvenliği üzerinden işleyen bir kurumlar, normlar ve kapasiteler bütünüdür. YZ, bu mimarinin her katmanına aynı anda temas eden genel amaçlı bir teknoloji olduğu için, etkisi tekil bir silah sisteminin ötesine geçerek karar alma hızını, bilgi üstünlüğü üretimini, savaşın yürütülme biçimini ve silahların kontrolünün doğrulanabilirliğini dönüştürmektedir (Horowitz, 2018).

Bu dönüşüm iki nedenle mimariyi yeniden düzenleyici bir basınç üretmektedir. Birincisi, YZ'nin askeri alandaki yayılımı hız/otomasyon/entegre sensör-ağları üzerinden kriz zamanında yanlış hesap ve tırmanma risklerini büyütebilir (Johnson, 2019b; Zala, 2024). İkincisi, YZ'nin çift kullanımlı doğası, özel sektörün ve sivil ekosistemlerin savaş kapasitesi üretimindeki ağırlığını artırarak güvenlik mimarisinin geleneksel devlet merkezli araçlarını zorlar; bu da norm koyma ve denetimi kurumsal olarak güçleştirmektedir (Horowitz vd., 2020).

Analiz, söz konusu basıncı üç farklı düzlemde incelemektedir. İlk aşamada stratejik istikrar ve tırmanma dinamikleri ele alınmaktadır. Bu kapsamda karar sürelerinin daralması ve nükleer-konvansiyonel eklemlenme süreçleri tartışılmaktadır. İkinci düzlemde otonom sistemler aracılığıyla uluslararası insancıl hukuk ve hesap verebilirlik konuları değerlendirilmektedir. Özellikle "anlamlı insan kontrolü" kavramı üzerine yürütülen tartışmalara odaklanılmaktadır. Üçüncü düzlemde YZ ile siber alan arasındaki etkileşim analiz edilmektedir. Dezenformasyon ve deepfake kaynaklı bilgi güvenliği risklerinin güvenlik mimarisinin meşruiyeti üzerindeki etkileri gösterilmektedir. Son olarak, bu risklerin kriz yönetimi kapasitesini nasıl dönüştürdüğü ortaya koyulmaktadır.

Nükleer çağın güvenlik mimarisi; erken uyarı, ikinci vuruş kapasitesi, yanlış alarm yönetimi ve kriz iletişimi gibi stratejik istikrar varsayımları üzerine inşa edilmiştir. YZ bu istikrar ortamını iki temel eksende etkilemektedir: bir yandan erken uyarı ve istihbarat verilerini işleme kapasitesini artırarak karar vericilere daha kapsamlı bir farkındalık sunabilmekte; diğer yandan karar sürelerini daraltıp belirsizliği artırarak kriz anlarında yanlış hesaplama riskini yükseltmektedir (Johnson, 2020; Stockholm International Peace Research Institute [SIPRI], 2019). Johnson (2020), YZ'nin geliştirilmiş konvansiyonel kabiliyetlerinin nükleer kuvvetlere dolaylı baskı yaratabileceğini; nükleer ve konvansiyonel alanların iç içe geçmesinin istem dışı tırmanma olasılığını artırdığını savunur. Zala (2024) ise YZ'nin bazı senaryolarda ilk vuruş teşviklerini artırıp artırmayacağını, özellikle erken uyarı ve hedefleme alanındaki riskler üzerinden tartışmaktadır.

YZ'nin nükleer alanda kullanımı, insan hatasını azaltma ve bilgi kalitesini artırma gibi faydalarla gerekçelendirilebilse de güvenlik mimarisi açısından kritik soru şudur: karar otoritesi ve hesap verebilirlik kimde kalacaktır? Bu noktada anlamlı insan kontrolü ilkesi, nükleer komuta-kontrol için özellikle hassas hale gelir; çünkü otomasyonun hata payı kriz koşullarında geri döndürülemez sonuçlar doğurabilir (Johnson, 2020; Horowitz vd., 2020). Yakın dönem nükleer risk literatürü ayrıca görünürlük/görünmezlik yarışına işaret eder: YZ hem tespit etme kapasitesini artırabilir hem de aldatma/maskeleme tekniklerini güçlendirebilir. Bu, karşılıklı kırılganlık ve belirsizlik üzerinden güvenlik mimarisinin istikrar ayarlarını zorlayabilir (Allison & Herzog, 2025).

Michael Horowitz'in 2018 yılında Texas National Security Review dergisinde yayımlanan çalışması, YZ'nin modern askeri inovasyon literatüründeki konumunu tanımlamak açısından temel bir referans noktasıdır. Horowitz'e göre YZ, tek başına savaşın sonucunu tayin eden

müstakil bir silah sisteminden ziyade, mevcut askeri kabiliyetlerin etkinliğini artıran ve savaşın doğasından ziyade icra ediliş biçimini kökten değiştiren bir etkinleştirici veya genel amaçlı teknoloji olarak değerlendirilmelidir (Horowitz, 2018). Bu çerçeve, YZ'nin uluslararası güvenlik mimarisi üzerindeki etkilerini daha sistematik analiz edebilmek için taktik/operasyonel ve stratejik boyutları birlikte okumayı mümkün kılmaktadır.

Otonom silah sistemlerinin teknolojik bir gerçeklik olarak ortaya çıkışı, küresel güvenlik mimarisinin temel taşlarını oluşturan uluslararası insancıl hukuk ve silahların kontrolü rejimlerini ciddi bir sınamayla karşı karşıya bırakmaktadır. Akademik literatürdeki tartışmalar, bu sistemlerin hukuki statüsünü ve kullanım sınırlarını belirlemek amacıyla temelde iki eksen etrafında yoğunlaşmaktadır. Birinci eksen, geleneksel savaş hukukunun temel ilkeleri olan askeri hedefler ile sivilleri ayırma, orantılılık ve önleyicilik gibi kuralların, karar alma süreçlerinde insan müdahalesinin bulunmadığı otonom sistemlere nasıl uyarlanabileceğini sorgulamaktadır. İkinci eksen ise, makinelerin öldürücü güç kullanma yetkisine sahip olması durumunda ortaya çıkacak anlamlı insan kontrolü eksikliği ve buna bağlı gelişen hukuki ve cezai sorumluluk boşluklarını ele almaktadır.

Bu tartışma zeminini güçlendiren çalışmalar, otonom sistemlerin uluslararası insancıl hukuk ilkeleriyle yapısal uyumunu analiz etmektedir. Bu teknolojilerin savaş alanındaki karmaşık dinamikleri kavrayarak sivil–muharip ayrımını yapabilme kapasitesi ve saldırının beklenen askeri avantajla orantılı olup olmadığını değerlendirme yeteneği kritik sorun alanları olarak işaret edilmektedir (Güneysu, 2024). Öte yandan, öldürücü otonom silah sistemleri için küresel ölçekte bağlayıcı ve dirençli bir kontrol rejiminin tesis edilmesinin önündeki engeller de öne çıkmaktadır. Devletlerin stratejik çıkarlarından kaynaklanan siyasal dirençler ve yazılımsal tabanlı bu silahların doğrulama süreçlerindeki teknik zorluklar, uluslararası bir denetim mekanizmasının kurulmasını güçleştirmektedir (Qerimi, 2023).

Uluslararası hukuk perspektifinden güncel yaklaşımlar ise, otonom silah sistemlerinin doğası gereği hukuka aykırı olup olmadığı sorusuna odaklanmaktadır. Casey-Maslen'e göre bu sistemlerin varlığı kendi başına uluslararası hukukun ihlali sayılmasa da kullanılmaları durumunda her zaman uluslararası insancıl hukuk ve uluslararası insan hakları hukuku ile tam uyum içinde olmak zorundadır (Casey-Maslen, 2025). Bu durum, teknolojinin kendisinden ziyade bu teknolojinin savaş alanındaki uygulama biçimlerinin hukuki meşruiyeti belirleyeceğini göstermektedir. Sonuç olarak, YZ tabanlı silah sistemlerinin askeri doktrinlere entegrasyonu; mevcut hukuk normlarının yeniden yorumlanmasını ve sorumluluk

hiyerarşisinin bu yeni teknolojik gerçekliğe göre yeniden tanımlanmasını kaçınılmaz kılmaktadır.

YZ teknolojilerinin küresel güvenlik mimarisi üzerindeki derin etkilerinden biri de devletlerin savaşa girme kararı alma süreçlerindeki siyasal maliyet analizlerini ve stratejik enformasyon akışını dönüştürmesidir. Bu bağlamda askeri alanda sorumlu YZ kullanımına ilişkin tartışmalar ve beraberindeki riskler, savaş kararının geleceğine dair normatif ve siyasal sonuçlar çerçevesinde ele alınmaktadır (Erskine & Miller, 2024). YZ destekli sistemlerin sağladığı hız ve otomasyon, bir yandan karar vericilere operasyonel avantaj sunarken, diğer yandan savaşın insani ve siyasi maliyetini görünmez kılma eğilimi üzerinden demokratik hesap verebilirlik mekanizmalarını zayıflatma potansiyeli taşımaktadır. Dolayısıyla YZ, modern güvenlik ekosisteminde yalnızca bir kuvvet çarpanı değil; bunun yanı sıra devletin savaş ve barış arasındaki kritik kararı verme biçimini ve bu kararın meşruiyet zeminini etkileyen kurumsal bir dinamik olarak konumlanmaktadır.

AI-Siber Etkileşimi: Stratejik İstikrar ve Bilgi Güvenliği

YZ ve siber kapasitelerin birleşimi, modern güvenlik mimarisinin en belirsiz alanlarından biri olan gri bölge faaliyetlerini daha karmaşık ve öngörülemez bir boyuta taşımaktadır. Soğuk Savaş sonrası dönemde tırmanma yönetimini zorlaştıran siber tehditler, YZ algoritmalarının entegrasyonuyla birlikte stratejik istikrar üzerinde doğrudan bir risk unsuru haline gelebilir. Bu bağlamda YZ destekli siber kabiliyetlerin özellikle nükleer kuvvetlerin güvenilirliği, komuta-kontrol sistemleri ve operasyonel hazır bulunuşluk üzerinde dolaylı fakat derin etkiler yarattığını savunan görüşler ortaya çıkmıştır (Johnson, 2019b). Bu birleşme, sadece teknik sabotaj ihtimalini değil; yanlış anlama veya hatalı sinyal okuma nedeniyle ortaya çıkabilecek istem dışı tırmanma riskini de büyütebilir.

Güvenlik mimarisinin bir diğer kritik sütunu, askeri kapasitelerin ötesinde yer alan toplumsal meşruiyet ve algı yönetimidir. YZ destekli dezenformasyon faaliyetleri ve deepfake teknolojileri, kriz anlarında kamuoyu algısını manipüle ederek liderlerin karar alma mekanizmalarını ve müttefikler arası dayanışmayı hedef alabilmektedir. YZ'nin dezenformasyon üretimini devasa ölçeklere ulaştırma potansiyeli, güvenlik risklerini ulusal sınırların ötesine taşımakta ve koordineli bir uluslararası yanıtı zorunlu kılmaktadır (Kertysova, 2018). Hynek vd. (2025) ise deepfake uygulamalarının kurumsal güven erozyonu ve kriz manipülasyonu aracılığıyla uluslararası güvenlik sisteminin meşruiyet zeminini nasıl zayıflattığını ortaya koymaktadır. Bu nedenle geleceğin caydırıcılık ve kriz yönetimi

stratejileri, yalnızca silah sistemlerine değil; içerik menşei işaretleme ve hızlı teyit ağları gibi güçlü bir bilgi bütünlüğü altyapısına da dayanmak zorundadır.

YZ, siber saldırıları daha düşük maliyetle ve yüksek ölçekte otomatize ederken savunma kalkanlarını aşma hızını da artırmakta; bu hızlanma 'gri bölge' eylemlerinin tespit-atıf-yanıt döngüsünü sıkıştırarak diplomasiye bırakılan süreyi daraltmakta ve kriz iletişimi ile gerilimi düşürme kanallarını zayıflatmaktadır.

Sonuç

Çalışma kapsamında üç temel bulgu ön plana çıkmaktadır. İlk olarak YZ ekosistemindeki altyapı ve hesaplama gücü yoğunlaşması, uluslararası sistemdeki hiyerarşik yapıyı derinleştirmektedir. Güç rekabeti, model performansından ziyade kritik girdilere erişim rejimleri ve akış kontrolü etrafında şekillenmektedir. İkinci olarak hız ve otomasyon etkisi karar sürelerini daraltmakta ve belirsizliği artırmaktadır. Bu durum kriz anlarında yanlış hesaplama ve tırmanma riskini büyüterek stratejik istikrar pratiklerini baskılamaktadır. Üçüncü olarak çift kullanımlılık, özel sektör ağırlığı ve büyük güç rekabeti gibi unsurlar bağlayıcı rejimlerin inşasını zorlaştırmaktadır. Bu süreçte yönetişim araçları modüler ve parçalı bir hatta ilerlemektedir. Söz konusu eğilim, güvenlik mimarisinin doğrulama, hesap verebilirlik ve meşruiyet kapasitesini sınamaktadır. Bu üç temel bulgu makalenin ana argümanını doğrulamaktadır. YZ, tekil bir kapasite artışından ziyade güvenlik mimarisinin tüm katmanlarına eş zamanlı basınç uygulayan bir "çarpan teknoloji" niteliğindedir. Aşağıda, bu üç bulgunun (H1–H3) güvenlik mimarisinin normatif, kurumsal ve operasyonel katmanlarında ürettiği başlıca sonuçlar ve bunlara karşılık gelen risk azaltımı seçenekleri özetlenmektedir.

Birinci bulgu, güvenlik mimarisinin kurumsal katmanında karar ve kapasite üretimini dar bir sağlayıcı/ittifak ekosistemine bağımlı kılmakta; normatif katmanda ise "eşit egemenlik" ve "adil erişim" ilkeleriyle fiili altyapı hiyerarşisi arasındaki gerilimi görünürleştirmektedir.

İkinci bulgu, operasyonel katmanda karar döngülerini sıkıştırarak yanlış anlama ve tırmanma riskini büyütmekte; bu nedenle kriz yönetimi, caydırıcılık ve komuta-kontrol pratikleri üzerinde baskı üretmektedir.

Üçüncü bulgu, normatif ve kurumsal katmanlarda evrensel mutabakatın yerini standartlar, ittifak içi düzenlemeler ve tedarik zinciri üzerinden kurulan fiili uyum baskılarının aldığı daha parçalı bir yönetişim hattına işaret etmektedir.

Bu çerçevede risk azaltımı ve uyum için öneriler, doğrudan bulguların işaret ettiği mekanizmalara bağlanmalıdır. (H1) Altyapı/ hesaplama kapasitesi yoğunlaşmasına karşı, uluslararası düzeyde asgari şeffaflık ve karşılaştırılabilir raporlama (kritik girdiler, tedarik zinciri kırılganlıkları, büyük ölçekli veri-merkezi kapasitesi) ile kapasite geliştirme araçlarının birlikte tasarlanması; bağımlılıkları azaltırken "fiili hiyerarşi"nin meşruiyet maliyetini azaltma potansiyeli taşır. (H2) Hız ve otomasyon kaynaklı tırmanma riskine karşı, kriz iletişim hatlarının güncellenmesi, YZ destekli karar süreçlerinde "anlamlı insan kontrolü" eşiğinin operasyonel olarak tanımlanması ve olay/arıza bildirimi gibi güven artırıcı önlemler, stratejik istikrar pratiklerini destekleyebilir. (H3) Evrensel bağlayıcı rejimlerin tıkandığı koşullarda ise modüler düzenleme yaklaşımı daha uygulanabilir bir hat sunar: teknik standartlar, birlikte-çalışabilirlik ölçütleri, denetim/sertifikasyon ve ittifak içi ortak ilkeler yoluyla, en azından belirli risk sınıflarında doğrulama, hesap verebilirlik ve uyum kapasitesi artırılabilir. Bu modüler hat, parçalanmayı ortadan kaldırmasa da mimarinin 'işleyen asgari ortak zemini'ni üretmeye dönük pragmatik bir ara çözüm olarak görülebilir.

Dolayısıyla sonuçlar, YZ'nin güvenliği yalnızca yeni sistemler üzerinden değil; altyapı hiyerarşisi (hesaplama kapasitesi), karar hızlanması (otomasyon) ve yönetişim biçimi (modülerleşme) üzerinden eşzamanlı biçimde yeniden yapılandırdığını göstermektedir. Bu da makalenin ana iddiasıyla tutarlıdır: YZ, tekil bir askeri kapasite artışından ziyade güvenlik mimarisinin tüm katmanlarında basınç üreten bir çarpan teknolojidir; bu nedenle çözüm arayışı da tek bir rejime indirgenmekten çok, mekanizma-temelli ve katman-duyarlı bir risk azaltımı mimarisi olarak kurgulanmalıdır.

Bu bulgular, güvenlik mimarisinde uygulanabilir müdahale alanlarının ideal çözümlerden çok risk azaltımı ve doğrulanabilirlik odaklı, kademeli araçlara dayandığını göstermektedir. Bu yönelim, çalışmanın üçüncü hipotezinin (H3) işaret ettiği üzere, büyük güç rekabeti altında evrensel bağlayıcı rejimlerin sınırlı kalması nedeniyle yönetişimin daha çok modüler ve doğrulanabilir araçlara kaymasıyla uyumludur.

Bu yeni dönemde güvenlik mimarisini YZ'nin hız, ölçek ve belirsizlik etkilerine karşı dayanıklı kılmak, kuralların ve kurumsal süreçlerin yeniden yapılandırılmasının gerektiğine işaret etmektedir. Bu dayanıklılığı inşa etmenin ilk adımı, askeri YZ sistemleri için kullanım bağlamı sınırlarını, eğitim verisi standartlarını ve doğrulama kayıtlarını içeren kapsamlı bir yaşam döngüsü denetimi ve emniyet dosyası standardı geliştirmektir.

Bununla birlikte, kriz anlarında tırmanma riskini ve sistem davranışlarındaki belirsizliği azaltmak amacıyla güven artırıcı önlemlerin teknoloji odaklı bir yaklaşımla güncellenmesi ihtiyacını doğurmaktadır. Bu çerçevede; karşılıklı bilgi paylaşımı, ortak terminoloji oluşturulması ve kaza senaryolarına yönelik ortak tatbikatlar stratejik istikrarın korunmasında kritik rol oynamaktadır.

Güvenlik mimarisinin merkezindeki bir diğer unsur ise insan yargısının doktrin ve eğitimle kurumsallaştırılmasıdır. YZ'nin önerdiği hedefleme verilerinin kanıt standartlarının belirlenmesi ve komutan sorumluluğunu netleştiren raporlama mekanizmalarının tesisi, teknolojinin etik ve hukuki sınırlar içinde tutulmasını sağlar. Ayrıca, veri setlerindeki önyargıların uluslararası insancıl hukuk uyumunu sistemik olarak aşındırmasını önlemek için tedarik süreçlerinde bağımsız denetim mekanizmalarının kurulması ve hukuk uzmanları ile veri bilimcilerin eşgüdümlü çalışması önem kazanmaktadır.

Ne var ki çalışmanın önceki bölümlerinde vurgulanan büyük güçler arası rekabet ve veto kaynaklı kurumsal tıkanıklıklar, tam da bu tür yaşam döngüsü denetimi ve bağımsız denetim önerilerinin uygulanabilirliğini sınırlayan temel siyasal engeli oluşturmaktadır. Rekabet koşullarında denetim rejimleri, çoğu zaman ortak güvenlik ihtiyacından ziyade göreli kazanımlar mantığıyla okunmaktadır. Taraflar, denetimin, kendi inovasyon hızını yavaşlatırken rakibin kapasitesini görünür kılacak bir 'asimetrik şeffaflık' aracı olmasından çekinmektedir. Veto mekanizmaları ise evrensel ve bağlayıcı standartların -özellikle doğrulama, raporlama ve yaptırım boyutları olan rejimlerin- kabulünü geciktirerek denetimi en düşük ortak paydaya itmektedir. Bu nedenle önerilen denetim araçlarının hayata geçebilmesi, ideal tipte küresel mutabakattan çok, önce dar kapsamlı kademeli ve modüler düzenlemelerle ilerlemeye; ayrıca bağlayıcı rejimlerin tıkandığı yerde çok taraflı teknik standartlar, ittifak içi düzenlemeler ve tedarik zinciri üzerinden 'fiili' uyum baskısı üreten mekanizmaların devreye girmesine bağlıdır.

Nihayetinde dijital uçurum, yalnızca teknik kapasite eksikliği değil; YZ ekosistemindeki hesaplama gücü-veri-altyapı yoğunlaşmasının ürettiği sert hiyerarşi içinde çevre aktörleri kalıcı bağımlılığa iten ve karar/uyum alanlarını daraltarak egemenlik kaybı riskini büyüten yapısal bir tahakküm mekanizması olarak yorumlanabilir. Bu nedenle gelişmekte olan ülkelerin teknik ve hukuki kapasitesinin desteklenmesi, küresel yönetişimin kapsayıcı ve kırılganlıktan uzak bir yapıya kavuşması için stratejik bir zorunluluk olarak öne çıkmaktadır.

Sonuç olarak bulgular, YZ'yi tamamen dışlamaya dayalı yaklaşımların yerine, teknik doğrulama kapasitesi ile şeffaflık/diyalog/çok taraflı iş birliği arasında denge kuran bir uyum hattının daha uygulanabilir olabileceğine işaret etmektedir.

KAYNAKÇA

Acemoglu, D., & Restrepo, P. (2020). The wrong kind of AI? Artificial intelligence and the future of labour demand. *Cambridge Journal of Regions, Economy and Society, 13*(1), 25–35. https://doi.org/10.1093/cjres/rsz022.

African Union Peace and Security Council. (2025, March 20). *Communiqué of the 1267th meeting of the Peace and Security Council on artificial intelligence and its impact on peace, security and governance in Africa.*

African Union. (2002). *Protocol relating to the establishment of the Peace and Security Council of the African Union*(Adopted July 9, 2002).

African Union. (2024). *Continental Artificial Intelligence Strategy* (Adopted July 2024).

Allison, D. M., & Herzog, S. (2025). Artificial intelligence and nuclear weapons proliferation: The technological arms race for (in)visibility. *Risk Analysis, 45*(11), 3839–3859. https://doi.org/10.1111/risa.70105

Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines* (2nd ed.). University of Michigan Press.

Bennett, A., & Checkel, J. T. (Eds.). (2015). *Process tracing: From metaphor to analytic tool*. Cambridge University Press.

Boulanin, V. (Ed.). (2019). *The impact of artificial intelligence on strategic stability and nuclear risk: Volume I—Euro-Atlantic perspectives*. Stockholm International Peace Research Institute (SIPRI).

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

Casey-Maslen, S. (2025). Autonomous weapons systems under international law. In K. S. Talves (Ed.), *Artificial intelligence in military technology* (pp. 161–179). Springer. https://doi.org/10.1007/978-3-031-95578-5_10.

Conference on Security and Co-operation in Europe. (1975). *Helsinki Final Act*. Organization for Security and Co-operation in Europe (OSCE).

Erskine, T., & Miller, S. E. (2024). AI and the decision to go to war: Future risks and opportunities. Australian Journal of International Affairs, 78(2), 135–147. https://doi.org/10.1080/10357718.2024.2349598.

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.

Güneysu, G. (2024). Autonomous weapon systems and the humanitarian principle of distinction. *Annales de la Faculté de Droit d'Istanbul, 74*, 133–153. https://doi.org/10.26650/annales.2024.74.0007

Hawkins, Z. J., Lehdonvirta, V., & Wu, B. (2025). AI compute sovereignty: Infrastructure control across territories, cloud providers, and accelerators. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5312977.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review, 1*(3), 36–57. https://doi.org/10.15781/T2639KP49.

Horowitz, M. C., Kahn, L., & Mahoney, C. (2020). The future of military applications of artificial intelligence: A role for confidence-building measures? *Orbis, 64*(4), 528–543. https://doi.org/10.1016/j.orbis.2020.08.003.

Hynek, N., Gavurová, B., & Kubák, M. (2025). Risks and benefits of artificial intelligence deepfakes: Systematic review and comparison of public attitudes in seven European countries. *Journal of Innovation & Knowledge, 10*(5), Article 100782. https://doi.org/10.1016/j.jik.2025.100782.

Johnson, J. (2019a). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis, 35*(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800.

Johnson, J. (2019b). The AI-cyber nexus: Implications for military escalation, deterrence and strategic stability. *Journal of Cyber Policy, 4*(3), 442–460. https://doi.org/10.1080/23738871.2019.1701693.

Johnson, J. (2020). Artificial intelligence: A threat to strategic stability. *Strategic Studies Quarterly, 14*(1), 16–39.

Kertysova, K. (2018). Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered. *Security and Human Rights, 29*(1–4), 55–81. https://doi.org/10.1163/18750230-02901005.

Korinek, A., & Stiglitz, J. E. (2021). *Artificial intelligence, globalization, and strategies for economic development*(NBER Working Paper No. 28453). National Bureau of Economic Research. https://doi.org/10.3386/w28453.

Maslej, N., Fattorini, L., Perrault, R., Gil, S., Parli, V., Kariuki, A., Capstick, M., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., Walsh, T., Hamrah, H., Santarlasci, S., … Oak, S. (2025). *The AI Index 2025 annual report*. Stanford University—Institute for Human-Centered Artificial Intelligence (HAI). https://doi.org/10.48550/arXiv.2504.07139.

North Atlantic Treaty Organization. (2022). *NATO 2022 Strategic Concept* (Madrid Summit, 29 June 2022).

North Atlantic Treaty Organization. (2024, July 10). *Summary of NATO's revised artificial intelligence (AI) strategy.*

Organization for Security and Co-operation in Europe Parliamentary Assembly. (2024). *Bucharest Declaration* (2024 Annual Session).

Qerimi, Q. (2023). Controlling lethal autonomous weapons systems: A typology of the position of states. *Computer Law & Security Review, 50*, Article 105854. https://doi.org/10.1016/j.clsr.2023.105854.

Sastry, G., Heim, L., Belfield, H., Andres, M., Chan, B., Baker, M., Anderljung, M., Hecht, F., & Coyle, D. (2024). *Computing power and the governance of artificial intelligence* (arXiv:2402.08797) [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2402.08797.

Stockholm International Peace Research Institute. (2019). *The impact of artificial intelligence on strategic stability and nuclear risk: Volume I—Euro-Atlantic perspectives*. Stockholm International Peace Research Institute. [Rapor].

U.S. Department of Commerce, Bureau of Industry and Security. (2023, October 25). *Export controls on semiconductor manufacturing items* (88 FR 73424). *Federal Register*.

United Nations. (1945). *Charter of the United Nations.*

United Nations. (1970). *Treaty on the Non-Proliferation of nuclear weapons (NPT).*

United Nations. (1998). *Rome Statute of the International Criminal Court.*

United Nations. (2008). *United Nations Peacekeeping Operations: Principles and Guidelines* (Capstone Doctrine).

United Nations. (2021). *Strategy for the digital transformation of UN peacekeeping.* https://peacekeeping.un.org/en/strategy-digital-transformation-of-un-peacekeeping.

United Nations General Assembly. (2024a). *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development* (A/RES/78/265).

United Nations General Assembly. (2024b). *Artificial intelligence in the military domain and its implications for international peace and security* (A/RES/79/239).

United Nations System Chief Executives Board for Coordination. (2022). *Principles for the ethical use of artificial intelligence in the United Nations system.* https://unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system.

Zala, B. (2024). Should AI stay or should AI go? First strike incentives & deterrence stability. *Australian Journal of International Affairs, 78*(2), 154–163. https://doi.org/10.1080/10357718.2024.2328805.