2BLACKDOT..

“Esasen konu hep 2 nokta arasındadır”

Haftalık

Politik ve Jeopolitik

Gelişmeler

22 Haziran 2026 – Sayı 114

TEMA GRUP

Bu hizmet size **2blackdot** ve **Tema Grup** tarafından ücretsiz verilmektedir. **Bu yazılanlar yatırım tavsiyesi değildir.**

Hazırlayan: Hakan Çalışkantürk **2twoblackdots@gmail.com** **https://www.2blackdots.com**

2blackdot haftalık bülteni yönetici özeti:

Tekno-Faşizm:
Algoritmik Egemenlik ve Yeni Güvenlik Mimarisi

Tekno-Faşizm: Yeni Bir Yönetim Biçimi

Tekno-Faşizm: Teknik Rasyonalitenin Üstünlüğü
Demokratik siyasetin yerini veri tekelleri, algoritmik karar alma ve platform mimarileri üzerinden işleyen seesiz ama kapsayıcı bir kontrol biçiminin almasıdır.

Egemenliğin Veriyle Yeniden Kodlanması
Nüfus yönetimi ve tehdit sınıflandırması artık sadece hiyerarşik kurumlarla değil; ontolojiler, model çıktıları ve veri tabanları üzerinden yürütülmektedir.

Özel Şirketlerin Devlet Aygıtına İçkinleşmesi
Kamu otoritesinin karar kapasitesi bakımından teknoloji tedarikçilerine bağımlı hale gelmesiyle egemenlik ve lisanslı yazılını arasındaki sınır silikleşmektedir.

Karp Manifestosu ve Palantir'in Üç Sütunu

Yazılım Tabanlı "Sert Güç" Doktrini
Ales Karp'a göre caydıncılık artik nükleer silahlar üzerinden değli, yapay zeká ve otonom silah sistemleri üzerinden Inşa edilmektedir.

Palantir'in Sütunları

Gotham: İstihbarat ve Öldürme Zinciri
Farlılı veri kaynaklarını birleştirerek tehdit ağları oluştoran bu sistem, CIA ve Pentagon gibi kurunnarda operasyonel analizler için kullanılmaktadır.

Foundry: Süreçlerin Dijital İkizleri
Kurumsel ve kamussi süreçlerin (ömeğin Ingiltere NHS verileri) dijital modellerini oluşturarak algoritmik denetime açan platformdur.

AIP: Yapay Zekâ Destekli Komuta
Büyük dil modellerini (LLM) doğrudan askeri karar alma süreçlerine entegre ederek "öidürme zincirini" optimize etmeyi hedefler.

Küresel Vaka Analizleri ve Algoritmik Savaş

Gazze: Lavender ve Gospel Sistemleri
IDF tarafından kullanılan sistemlerin binlerce hedefi saniyeler içinde puanladığı ve sivil kayıpları artıran bir "hedefleme zinciri" oluşturduğu iddia edilmektedir.

ABD: ICE ve ImmigrationOS
Göçmen verilerinin plaka tanıma ve biyometrik verilerle birleştirilmesi, kişileri sınır dışı edilme önceliğine göre otomatik olarak sıralamaktadır.

Ukrayna: Dağıtık Algoritmik Model
Uydu görüntülerini ve saha verilerini hızla işleyen MetaConstellation gibi araçlar, savaşın hızını ve doğasını dijitalleştirmektedir.

Hukuki Boşluklar ve Çözüm Önerileri

%10'luk Algoritmik Hata Payı Riski
Lavender gibi sistemlerdeki hata payları ve "kara kutu" doğası, masum sivillerin hedef alınması riskini ve hesap verebilirlik boşluğunu büyütmektedir.

"Anlamlı İnsan Denetimi" Somutlaştırılmalı
Hedefleme süreçlerindeki insan onayının sadece formaliteye dönüşmemesi için asgari süre ve gerekçelendirme standartları getirilmelidir.

Uluslararası Hukukta Atfedilebilirlik Sorunu
Bir kararın algoritma mı, operatör mü yoksa yazılımcı şirket mi tarafından verildiğinin belirsiziiği, devlet sorumluluğu ilkesini zorlaştırmaktadır.

Bağımsız Algoritmik Denetim Organları
BM çatısı altında, aekeri ve göç yönetimi yapay zekâ sistemlerini ticari sı engeline takılmadan inceleyebilecek bir mekanizma kurulmalıdır.

NotebookLM

TEKNO-FAŞİZM[1]:

Kodların Devletin Sinir Sistemini Ele Geçirme Operasyonu

Alex Karp Manifestosu ve Palantir Örneğinde Yeni Nesil Dijital Totalitarizmin Kavramsal, Teknolojik ve Uluslararası Hukuk Bağlamında Çözümlemesi

1. Özet

21. yüzyılın ikinci çeyreğinde devletlerin güvenlik mimarisi, artık yalnızca ordular, istihbarat servisleri ve bürokratik kurumlar tarafından değil; özel sektörün ürettiği algoritmik altyapılar tarafından da şekillendiriliyor. Bu dönüşümün en somut ve en tartışmalı temsilcisi, ABD merkezli veri analitiği ve yapay zekâ şirketi Palantir Technologies ile şirketin kurucu ortağı ve CEO'su Alex Karp'tır. Karp'ın, kurumsal işbirlikçisi Nicholas Zamiska ile birlikte yazdığı ve "The Technological Republic: Hard Power, Soft Belief, and the Future of the West" başlıklı kitaptan derlenen 22 maddelik manifesto (Karp & Zamiska, 2025; Palantir Technologies, 2025), Silikon Vadisi'nin sadece tüketici teknolojisi üretmekle yetinmeyip, ulusal güvenlik ve savunma alanında doğrudan rol üstlenmesi gerektiğini savunan bir seferberlik çağrısı niteliği taşır.

Bu rapor, Alex Karp'ın The Technological Republic ekseninde şekillenen "Karp manifestosu"nu, yeni nesil dijital totalitarizmin güvenlik merkezli bir varyantı olarak okur ve "tekno-faşizm" kavramını bu çerçevede analitik bir araç olarak kullanır. Buradaki temel iddia şudur: sorun yalnızca daha fazla gözetim, daha güçlü yapay zekâ ya da daha yoğun veri toplama değildir; asıl mesele, devletin güvenlik aygıtları ile özel teknoloji şirketleri arasındaki sınırın bulanıklaşması, bu bileşimin demokratik meşruiyet ve hukuki hesap verebilirlik üretmekte giderek yetersiz kalmasıdır. Karp ve Nicholas Zamiska'nın metni, Silikon Vadisi'nin tüketici odaklı yenilikçiliğini eleştirip teknoloji sektörünü ulusal güç, caydırıcılık ve savunma hedeflerine yeniden bağlama çağrısı yapar; 2026'da dolaşıma giren 22 maddelik özet ise bu yaklaşımı daha çıplak ve siyasal bir dille formüle eder. Bu formül, "yazılım tabanlı sert güç", algoritmik yönetim, veri çıkarma, davranışsal yönlendirme ve güvenlik kisvesi altında otoriterleşme başlıkları etrafında bir çerçeve ortaya koymaktadır (Karp ve Zamiska, 2025)

Bu bağlamda "tekno-faşizm" tek başına bir slogan değil, belirli bir siyasal-tekno-ekonomik düzen tipini işaret eden bir kavramdır. Bu düzen tipinde egemenlik, artık yalnızca hukuk ve kurumlar yoluyla değil, sensör ağları, veri füzyonu, kimlik grafikleri, biyometrik eşleştirme, büyük dil modelleri, otonom veya yarı-otonom karar destek sistemleri ve sürekli davranışsal izleme üzerinden icra edilir. Zuboff'un "gözetim kapitalizmi" ve "araçsal iktidar" kavramları, McQuillan'ın anti-faşist AI eleştirisi, Naomi Klein'ın krizlerin siyasal ekonomisine ilişkin çözümlemeleri ve tarihsel "tekno-faşizm" tartışmaları, günümüz güvenlik devletinin neden artık yalnızca bürokratik değil, aynı zamanda **yazılımsal bir rejim biçimine dönüştüğünü** anlamak için güçlü teorik dayanaklar mevcuttur (Zuboff, 2019; McQuillan, 2022; Klein, 2007; Mimura, 2011; Chayka, 2025)

Teknolojik boyutta görülen temel hareket, dağınık veri kümelerinin "işletilebilir gerçeklik katmanları" hâline getirilmesidir. Palantir'in etrafında örülen tartışmaların merkezinde de bu vardır: farklı kurumlardan gelen yapılandırılmış ve yapılandırılmamış verilerin tek bir operasyonel ontoloji içinde birleşmesi, bunun üzerine makine öğrenmesi ve üretken yapay zekâ katmanlarının bindirilmesi, ardından da bu sonuçların istihbarat, sınır güvenliği, kriz yönetimi ve askerî komuta-kontrol süreçlerine geri verilmesi. Bu mimari, devletler için yüksek hız, daha fazla görünürlük, daha düşük koordinasyon maliyeti ve daha güçlü durumsal farkındalık üretir; ama aynı zamanda hata, önyargı, yanlış eşleştirme, hedef saptırma, kitlesel gözetim ve demokratik denetimin aşınması risklerini de büyütür. Son yıllarda NATO'nun Palantir'in Maven Smart System NATO sistemini satın alması, ABD Ordusu'nun Palantir ile 10 milyar dolara kadar ulaşabilen kurumsal sözleşme modeli kurması ve Fransa'nın 2026'da Palantir'den yerli bir sağlayıcıya geçme kararı alması, güvenlik ve egemenlik tartışmasının artık teorik değil, stratejik bir gerçeklik olduğunu gösterir. (NATO/Palantir gelişmeleri, 2025; ABD Ordusu, 2025; Fransa, 2026)

Vaka analizleri, bu eğilimin soyut değil somut olduğunu gösterir. Gazze'de AI destekli hedefleme sistemleri ve özel sektör destekli veri altyapıları, öldürme zincirinin hızını yükselttiği iddialarıyla uluslararası hukuki ve etik tartışmaların merkezine yerleşmiştir. Rusya-Ukrayna savaşında dijital komuta-kontrol, drone ekosistemi, veri tabanlı muharebe farkındalığı ve yazılımın "savaş alanı çarpanı" işlevi belirginleşti. Çin'in Sincan/Xinjiang bölgesinde ise karşı-terör söylemi ile öngörücü polislik, biyometrik toplama ve kitlesel veri füzyonu iç içe geçerek ayrımcı ve baskıcı bir güvenlik rejimi yarattı. ABD'de ICE'nin Palantir tabanlı göçmen takip ve deportasyon altyapıları

[1] Bu makale Sn.Mustafa KAYALI'nın https://utkvakfi.org/tekno-fasizm-palantir-alex-karp-manifestosu-ve-dijital-totalitarizmin-yukselisi/ adresinde yayınlanan 12 Mayıs 2026 tarihli makalesinde yer alan görüş ve kaynaklardan istifade edilerek AI destekli olarak yazarın öznel görüşleri doğrultusunda hazırlanmıştır.

da savaş dışı ama yüksek yoğunluklu bir iç güvenlik tekno-totalitarizminin örneği hâline geldi. Bu dört örnek birlikte okunduğunda ortaya çıkan şey, güvenliğin dijitalleşmesinden öte, dijital güvenliğin siyasallaşmasıdır.

Hukuki sonuç açıktır: mevcut uluslararası hukuk, devlet sorumluluğu ve insan hakları bakımından önemli ilkeler sunsa da güvenlik istisnası ile özel teknoloji altyapılarının birleştiği alanlarda ciddi boşluklar vardır. Uluslararası Hukuk Komisyonu'nun devlet sorumluluğu maddeleri ihlalin devlete atfedilebilirliği ve uluslararası yükümlülük ihlalini temel alsa da özel yazılım tedarikçileri, sınır-aşan veri akışları, model opaklığı ve otonom veya yarı-otonom karar destek sistemleri atfı, öngörülebilirliği ve delillendirmeyi zorlaştırdı. AB AI Act önemli bir dönüm noktası olmakla birlikte askerî ve ulusal güvenlik kullanımlarını büyük ölçüde kapsam dışı bırakır; Avrupa Konseyi AI Çerçeve Sözleşmesi ve BM'nin AI kararları ise ilke üretir ama güvenlik devletinin en sert tezahürlerini doğrudan dizginleyecek kadar ayrıntılı değildir. Bu nedenle rapor, devletler için zorunlu insan hakları etki değerlendirmesi, kamu tedarikinde denetlenebilirlik şartları, biyometrik ve öngörücü kolluk kullanımına keskin sınırlar, ölümcül otonom sistemler için bağlayıcı kırmızı çizgiler, savaş ve sınır güvenliği yazılımlarında olay kaydı ve bağımsız denetim zorunluluğu, ayrıca özel teknoloji şirketleri için güçlendirilmiş due diligence ve sorumluluk rejimleri önermektedir.

2. Kavramsal Çerçeve: Tekno-Faşizm Nedir?

"Tekno-faşizm" terimi, çağdaş tartışmalarda çoğu zaman polemik olarak kullanılsa da, tarihsel ve analitik bir çekirdeğe sahiptir. Tarihçi Janis Mimura'nın Japon savaş dönemi bürokrasisine ilişkin çalışmaları, teknik uzmanlığın askerî-bürokratik aygıtla birleşerek hesap vermez "üst-bakanlık" türü yönetim biçimleri üretebildiğini göstermiştir. Güncel yorumcular ise bu tarihsel çizgiyi, teknoloji elitlerinin devlet çekirdeğine doğru hareketiyle yeniden düşünmektedir. Dolayısıyla tekno-faşizm, en genel anlamıyla, teknik rasyonalitenin demokratik siyaset üzerindeki üstünlüğünün ilan edilmesi ve bunun güvenlik, düzen ve hız adına meşrulaştırılmasıdır. (Mimura, 2011; Chayka, 2025)

"Tekno-Faşizm" kavramı, klasik faşizmin kitlesel parti örgütlenmesi ve açık şiddet aygıtı yerine; veri tekelleri, algoritmik karar alma sistemleri ve platform mimarileri üzerinden işleyen, daha sessiz ama daha kapsayıcı bir kontrol biçimini tanımlamak için kullanılır (Coeckelbergh, 2026). Bu yeni düzenin ayırt edici özelliği, iktidarın artık yalnızca devletin elinde değil, devletle iç içe geçmiş özel teknoloji şirketlerinin elinde de toplanmasıdır. McQuillan (2022), bu süreci faşizan eğilimlerin yapay zekâ sistemlerinin "verimlilik" ve "optimizasyon" söylemleri arkasına gizlenerek yeniden üretilmesi olarak okur.

Çağdaş bağlamda bu kavramı işlevsel kılan dört kurucu unsur vardır. Birincisi, **egemenliğin veriyle yeniden kodlanmasıdır**: nüfus yönetimi, tehdit sınıflandırması ve davranış öngörüsü artık yalnızca polis, istihbarat ve ordu hiyerarşileriyle değil; veri tabanları, ontolojiler, model çıktıları ve skorlarla yürütülmektedir. İkincisi, **özel şirketlerin devlet aygıtına içkinleşmesidir**: kamu otoritesi, karar ve kapasite bakımından tedarikçiye bağımlı hâle geldikçe, egemenlik ile lisanslı yazılım arasındaki sınır silikleşir. Üçüncüsü, **güvenlik istisnasının norm haline gelmesidir**: savaş, terör, düzensiz göç, hibrit tehdit ve kriz, daimî veri toplama ve sürekli otomatik analiz için gerekçeye dönüşür. Dördüncüsü ise **insan eylemliliğinin aşınmasıdır**: karar süreçleri tamamen ortadan kalkmasa bile, insana çoğu zaman yalnızca algoritmanın ürettiği seçenekler arasından "onay verme" görevi bırakılır. (Zuboff, 2019; McQuillan, 2022; Leslie vd., 2022; Karp&Zamiska 2025)

Bu çerçeve, gözetim kapitalizmi ile tamamlanır. Zuboff'un gösterdiği gibi büyük teknoloji şirketlerinin ekonomik modeli yalnızca veri toplamak değil, insan davranışını öngörmek ve yönlendirmektir; bu da "araçsal iktidar" dediği, klasik totaliter rejimlerden farklı ama bireysel özerklik bakımından benzer derecede tehlikeli bir güç tipi üretir. Karp manifestosunun güvenlik merkezli yönü, bu ekonomik mantığı devletin zor kullanma kapasitesiyle eklemlediği ölçüde daha da kritik hale gelir: davranışsal veri çıkarımı piyasa için değil, istihbarat ve operasyon için de kullanılır hale gelir. Böylece sermaye mantığı ile güvenlik mantığı birbirini güçlendirir. (Zuboff, 2019; Time röportajları, 2020–2022)

Naomi Klein'ın "şok doktrini" çizgisi de burada önemlidir; çünkü krizler, normal zamanlarda kabul edilmeyecek kurumsal ve teknik dönüşümlerin hızlandırıldığı eşiklerdir. Savaş, terör saldırısı, büyük göç dalgası ya da hibrit tehdit söylemi, hukuki frenlerin aşılmasını ve olağanüstü önlemlerin rutinleşmesini mümkün kılar. Karp'ın savunduğu savunma-merkezli teknoloji seferberliği ile Klein'ın kriz anlarının siyasal ekonomisine dair çözümlemesi birleştiğinde, teknolojik olağanüstü hâlin hem yatırım hem de ideoloji bakımından nasıl kurumsallaşabildiği daha net görünür. (Klein, 2007; The Guardian, 2025; Washington Post, 2025)

Bu nedenle tekno-faşizm, üçlü bir tanımla kullanılmalıdır. **Kavramsal olarak,** teknokrasinin otoriterleşmiş biçimi; **teknolojik olarak,** gözetim, sınıflandırma ve yönlendirme kapasitesinin yapay zekâ ile ölçeklenmesi; **siyasal olarak,** güvenlik gerekçesiyle demokratik denetim ve hukuki sorumluluğun zayıflatılması. Bu tanım, kavramı gevşek bir hakaret olmaktan çıkarıp, belirli mimarileri, kurumsal ilişkileri ve hukuki riskleri inceleyen analitik bir araç haline getirir. (Chayka, 2025)

Özellikle teknolojik boyutunda; bugünün güvenlik odaklı dijital rejimleri, tek bir "süper algoritma" ile değil, katmanlı bir mimariyle çalışır. Bu mimarinin tipik bileşenleri; veri alımı, kimlik çözümleme, ontoloji/nesne modeli, analitik ve kestirim katmanı, operatör arayüzü, karar destek/senaryo üretimi, saha aktüasyonu ve geri besleme döngüsüdür. Palantir etrafındaki tartışmalarda öne çıkan "ontology" ve "digital twin" kavramları, tam da bu nedenle önemlidir: amaç, dağınık veriyi yalnızca depolamak değil, gerçek dünyadaki kişi, nesne, olay ve **ilişkilerin operasyonel bir modelini kurmaktır.** Büyük dil modelleri ve üretken AI da bu yapıya eklendiğinde, sistem yalnızca analiz sunmaz; özetler, önceliklendirir, öneri üretir ve **operatörün bilişsel yükünü yeniden düzenler.**

Bu mimari içindeki temel teknolojileri şöyle özetlemek mümkündür:

Teknoloji	Teknik işlev	Güvenlik getirisi	Temel demokratik risk
Gözetim sensörleri	Kamera, uydu, IoT, sinyal, konum ve meta-veri toplama	Geniş kapsama, sürekli izleme, olay sonrası delillendirme	Sürekli izleme, mahremiyetin aşınması, protesto ve muhalefetin bastırılması
Biyometrik tanıma	Yüz, yürüyüş, parmak izi, iris, ses	Hızlı eşleme, kimlik doğrulama, sınır ve erişim kontrolü	Irksal/cinsiyet temelli hata, yanlış eşleştirme, kitlesel fişleme
Büyük veri füzyonu	Kurumsal veri tabanlarını tek modelde birleştirme	Durumsal farkındalık, ağ analizi, ilişki keşfi	Amaç kayması, orantısız veri birikimi, devlet-şirket veri bağımlılığı
Makine öğrenmesi	Sınıflandırma, tahmin, anomali tespiti	Erken uyarı, önceliklendirme, operasyonel hız	Önyargı, yanlış pozitif, "kara kutu" meşrulaştırması
LLM/üretken AI	Dil tabanlı sorgu, özet, plan ve senaryo üretimi	Karar destek hızlanması, arayüz kolaylığı, bilgi yoğunluğunun yönetimi	Halüsinasyon, sahte güven, insan denetiminin biçimselleşmesi
Siber araçlar	Ağ istihbaratı, savunma/taarruz otomasyonu	Kritik altyapı koruma, hızlı müdahale	Tırmanma, atıf güçlüğü, sivil altyapıya yayılma
Dezenformasyon araçları	Deepfake, bot ağı, sentetik içerik	Psikolojik harekât, stratejik etki operasyonları	Kamusal alanın bozulması, kurumsal güven erozyonu

Bu çerçevenin arkasındaki veri ve güvenlik tartışmaları; AB'nin biyometrik öngörücü polislik yasağı/güçlü sınırlamaları, Europol'ün AI destekli suç ve hibrit tehdit uyarıları, günlük hayatta da LLM-tabanlı nudging ve davranışsal yönlendirme mimarilerinin üretime girmesiyle birlikte daha kritik hale gelmiştir.

Biyometrik veri, bu düzenin en kritik halkalarından biridir. Çünkü biyometri yalnızca "kim olduğunu" söylemez; devletin gözünde seni taşınabilir, doğrulanabilir ve en önemlisi karşılaştırılabilir bir nesneye dönüştürür. Ancak yüz tanıma ve benzeri sistemlerde eşit hata oranları ampirik olarak sağlanmış değildir; güvenlik eşiği yükseldikçe belirli demografik gruplar için hata ve dışlama risklerinin artabildiği yönünde güçlü bulgular vardır. Bu nedenle biyometrik güvenlik sistemleri, teknik olarak nötr değil, siyasal olarak yüksek etkili araçlardır. (AB AI Act sınırlamaları; yüz tanıma adalet literatürü)

Üretken yapay zekâ ve büyük dil modelleri ise yeni bir eşik açmıştır. Önceki analitik sistemler çoğunlukla uzman kullanıcılar için tasarlanmışken, LLM tabanlı katmanlar karmaşık veri altyapılarını "doğal dil arayüzü"ne dönüştürür. **Bu, savaş alanında ve iç güvenlikte hız kazancı getirir; fakat aynı zamanda yanlış özetleme, uydurma bağlam, aşırı güven ve karar zincirinde insanın giderek yalnızca "onay memuru"na dönüşmesi tehlikesini de beraberinde getirir.** Foundation model literatürü ve yüksek sonuçlu AI risk yönetimi çalışmaları, bu nedenle şeffaflık, kayıt tutma, olay bildirme ve kullanım-sonrası denetimin teknik tasarımın parçası olması gerektiğini vurgular.

Devlet Güvenliği Perspektifi

Devletler açısından bakıldığında bu teknolojiler baştan sona "mantıksız" ya da "otoriter" değildir; tersine, çoğu zaman rasyonel güvenlik ihtiyaçlarından doğarlar. İstihbarat kurumları için dağınık verileri birleştirmek, kolluk için çoklu veri tabanlarında hızlı ilişki analizi yapmak, sınır kurumları için hareket örüntülerini eşleştirmek, kriz yönetiminde lojistik ve kaynak dağıtımını optimize etmek ve savaş alanında komuta-kontrol zincirini hızlandırmak ciddi operasyonel avantajlar üretir. Ukrayna örneği, dijital dönüşüm ve insansız sistemlerin personel kıtlığı, bürokrasi ve mühimmat baskısı altında nasıl "hayatta kalma teknolojisi" işlevi gördüğünü açıkça göstermektedir. NATO ve ABD Ordusu'nun Palantir/Maven tabanlı sistemlere hızla yönelmesi de bunun başka bir tezahürüdür.

Bununla birlikte, güvenlik kazancı ile siyasi risk çoğu zaman aynı mimariden türemektedir. Yani sistemin fayda üretmesini sağlayan şey, aynı zamanda kötüye kullanım potansiyelini de büyütür. Daha çok veri, daha iyi tahmin imkânı sunar; fakat aynı zamanda daha büyük keyfilik kapasitesi de üretir. Daha hızlı karar destek, operasyonel etkinliği artırır; fakat hatanın daha geniş ölçekte çoğalmasına da neden olabilir. Daha güçlü ortak operasyon resmi, kurumsal koordinasyonu kolaylaştırır; fakat karar zincirindeki sorumluluğu dağıtabilir. Fransa'nın 2026'da Palantir'den çıkarak yerli bir sağlayıcıya yönelmesinin ardındaki temel düşünce de tam olarak budur: **güvenlik verimliliği ile stratejik bağımlılık arasındaki gerilim.**

Güvenlik alanı	Başlıca fırsat	Başlıca risk
İstihbarat	Çok kaynaklı veri füzyonu ve ağ analiziyle erken uyarı	Yanlış ilişkilendirme, hatalı hedefleme, gizli bütçe-gizli algoritma birleşmesi
İç güvenlik	Olay örüntülerinin hızlı saptanması, saha koordinasyonu	Öngörücü polislik, ayrımcı fişleme, protesto gözetimi
Sınır güvenliği	Kimlik doğrulama, visa/overstay takibi, akış yönetimi	Göçmenin daimi risk nesnesine dönüşmesi, usul güvencelerinin aşınması
Kriz yönetimi	Lojistik ve kaynak dağıtımında optimizasyon	Kriz bahanesiyle kalıcı veri rejimleri kurulması
Askerî kullanım	Hızlı durumsal farkındalık, hedef önceliklendirme, düşük koordinasyon maliyeti	Tırmanma, sivil zarar, insan denetiminin şekli hale gelmesi

2.1 Gözetim Kapitalizminden Tekno-Faşizme

Shoshana Zuboff'un (2019) "Gözetim Kapitalizmi" (Surveillance Capitalism) kavramı, insan deneyiminin hammaddeye dönüştürülüp veri olarak çıkarılması, davranışsal tahmin ürünlerine işlenmesi ve nihayetinde reklam ile etki piyasalarında satılması sürecini tanımlar. **Tekno-faşizm, bu mantığı bir adım öteye taşır: artık hedef sadece tüketici davranışını yönlendirmek değil, devletin güvenlik, göç ve savaş politikalarını da algoritmik karar destek sistemleri üzerinden biçimlendirmektir.** Naomi Klein'ın analiz ettiği "krizlerin fırsata çevrilmesi" mantığı da bu noktada devreye girer: savaş, pandemi veya göç krizleri, denetimsiz veri toplama ve algoritmik müdahale için birer kapı aralayıcı işlev görür.

2.2 Tekno-Feodalizm: Yeni Bir Tabakalaşma

Yanis Varoufakis'in (2023) "Tekno-Feodalizm" tezi, dijital platformların artık geleneksel kapitalist pazar mantığından çıkıp, kullanıcıları "dijital serfler" konumuna indiren bir kira (rent) ekonomisi kurduğunu öne sürer. Bu çerçevede birey, kendi kararlarını verdiğini düşünen ama aslında davranışsal "dürtme" (nudging) mekanizmalarıyla her adımı önceden hesaplanmış bir veri noktasına dönüşür. Palantir'in Foundry ve AIP gibi ürünleri aracılığıyla kurumsal ve devlet süreçlerine nüfuz etmesi, bu yeni dijital kast sisteminin kurumsal düzeydeki yansımasıdır.

3. Karp Manifestosu: "Teknolojik Cumhuriyet"in Felsefi Mimarisi

3.1 22 Maddelik Manifesto ve Sert Güç Doktrini

Palantir'in resmi X hesabından paylaştığı 22 maddelik manifesto, şirketin kurumsal bir bildirisinin ötesinde bir dünya görüşü ilanı olarak okunmaktadır (AA Analiz, 2026; SETA, 2026). Metnin ilk maddesi, Silikon Vadisi'nin ABD'ye

"ahlaki bir borcu" bulunduğunu ve ulusun savunmasına katılma yükümlülüğü taşıdığını ileri sürer (Fikir Coğrafyası, 2026). Manifestonun merkezi tezi, yumuşak gücün (soft power) 21. yüzyılın rekabetçi ortamında artık yeterli olmadığı, Batı medeniyetinin yazılım tabanlı bir "sert güç" ile yeniden inşa edilmesi gerektiğidir. Karp'a göre caydırıcılık bundan böyle nükleer silahlar üzerinden değil, yazılım, yapay zekâ ve otonom silah sistemleri üzerinden inşa edilecektir; metinde atom çağının sona yaklaştığı ve yapay zekâ temelli yeni bir caydırıcılık döneminin başladığı savunulmaktadır (Yeni Çağ Gazetesi, 2026).

Manifestonun en çok tartışılan yönlerinden biri, yapay zekâ destekli silahların geliştirilip geliştirilmeyeceğinin artık bir etik tartışma konusu değil, "kim tarafından ve hangi amaçla" yapılacağına dair stratejik bir zorunluluk olarak çerçevelenmesidir (Euronews, 2026; SETA, 2026). Bu yaklaşım, Hannah Arendt'in "kötülüğün sıradanlığı" kavramını hatırlatan bir mantık üretir: karmaşık bürokratik ve teknolojik sistemler içinde bireysel ahlaki sorumluluk buharlaşır, kararlar "sistemin gerekliliği" adına meşrulaştırılır.

3.2 Anti-Woke Söylem ve Kültürel Üstünlükçülük

Manifesto, "uyanış" (wokeness) ideolojisinin Batı'yı savunmasız bıraktığını, **bazı kültürlerin "vital ilerlemeler" ürettiğini, bazılarının ise "işlevsiz ve gerici" kaldığını öne sürerek açık bir kültürel üstünlükçülük (supremasism) söylemi inşa eder (Euronews, 2026).** Almanya ve Japonya'nın savaş sonrası "etkisizleştirilmesinin" sona ermesi çağrısı ve kamusal alanda dinin yeniden merkeze alınması talebi de bu çerçevenin parçasıdır. Bu söylem, teknokratik elitlerin müdahalesini meşrulaştırırken, kapsayıcılık ilkelerinin terk edilmesini "ulusal savunma" adına haklı çıkarmaya çalışır.

3.3 Thiel-Karp İttifakı: Zıt Kutupların Sentezi

Palantir, 2003 yılında libertaryen/sağ kanat yatırımcı Peter Thiel ile kendisini neo-sosyalist ve felsefe kökenli bir entelektüel olarak tanımlayan Alex Karp'ın ortaklığıyla kurulmuştur; şirketin ilk yatırımcıları arasında CIA'nin girişim sermayesi kolu In-Q-Tel de bulunmaktadır (Chafkin, 2021; AFSC Investigate, 2026). Şirketin adı, Tolkien'in evrenindeki her şeyi gören ama aynı zamanda kullanıcısını manipüle edebilen "palantir" taşlarından gelir — bu adlandırma, şirketin hem mutlak gözetim vaadini hem de bu gücün kötüye kullanılma potansiyelini sembolik biçimde taşır. **Thiel'in "Zero to One" (Thiel & Masters, 2014) adlı kitabında savunduğu radikal yenilikçilik ve tekelleşme anlayışı, Karp'ın felsefi söylemiyle birleşerek Palantir'i ideolojik ve ticari açıdan agresif bir aktöre dönüştürmüştür.**

4. Palantir'in İş Modeli: Teorinin Ete Kemiğe Bürünmesi

Palantir'in iş modeli, Karp'ın manifestosunun soyut önermelerinin somutlaşmış hâli olarak okunabilir. Şirketin üç ana ürün hattı, gözetim, kurumsal denetim ve askeri karar almayı tek bir ekosistemde birleştirir (Elsen, 2025).

4.1 Gotham: İstihbarat ve Öldürme Zinciri

Gotham platformu, telefon kayıtlarından uydu görüntülerine kadar her türlü yapılandırılmamış veriyi birleştirerek "tehdit ağları" oluşturan, istihbarat ve savunma odaklı bir sistemdir. **CIA ve Pentagon dâhil çok sayıda kurumda uzun süredir kullanılan Gotham, son dönemde ABD ordusunun TITAN programı ve başlangıçta insansız hava aracı görüntülerine makine öğrenimi uygulamak üzere tasarlanan Project Maven ile entegre çalışacak şekilde genişletilmiştir (AA Analiz, 2026).**

4.2 Foundry: Ticari ve Kamusal Dijital İkizler

Foundry, Airbus, BP ve Merck gibi ticari devler ile İngiltere Ulusal Sağlık Hizmeti (NHS) gibi kamu kurumları için kurumsal süreçlerin "dijital ikizini" oluşturarak bu süreçleri algoritmik denetime açar. **NHS ile imzalanan ve içeriği büyük ölçüde sansürlenmiş 330 milyon sterlinlik sözleşme, on binlerce hastanın itirazına ve sağlık çalışanları sendikalarının örgütlü direnişine yol açmıştır (Al Jazeera, 2026; TechnoLogic, 2026).**

4.3 AIP: Yapay Zekânın Komuta Kademesine Entegrasyonu

Yapay Zekâ Platformu (AIP), büyük dil modellerini doğrudan askeri karar alma süreçlerine entegre ederek "öldürme zincirini" (kill chain) optimize etmeyi hedefler. **Karp'a göre yazılım, artık savaşı kazandıran asıl silahtır; CEO, 2026 başında şirketin silah yazılımının kendisinin bildiği her muharebe ortamında bulunduğunu kamuoyu önünde ifade etmiştir (AFSC Investigate, 2026).**

5. Devletlerin Güvenlik Boyutu: Sinir Sistemini Ele Geçirme Operasyonu

Tekno-faşizmin en kritik boyutu, devletin "sinir sistemi" olarak adlandırılabilecek karar alma, veri akışı ve uygulama mekanizmalarının özel şirketlerin altyapısına bağımlı hâle gelmesidir. Bu bağımlılık hem ulusal güvenliği hem de demokratik denetimi doğrudan etkiler.

5.1 ABD'de DOGE ve Bürokrasinin Tasfiyesi

Trump-Vance-Thiel-Karp ittifakı çerçevesinde kurulan Hükümet Verimliliği Departmanı (DOGE) projesi, devlet bürokrasisinin tasfiye edilip yerine Silikon Vadisi kökenli algoritmik sistemlerin ikame edilmesi girişimi olarak değerlendirilmektedir. **Bu süreç, "oligarkların önderlik ettiği bir devrim" söylemi altında demokratik denetim mekanizmalarının zayıflatılması riskini taşımaktadır.**

5.2 ICE ve ImmigrationOS: Göçmenin Veri Noktasına Dönüşümü

Palantir, 2011-2026 yılları arasında ABD Göçmenlik ve Gümrük Muhafaza Teşkilatı'ndan (ICE) toplam 435 milyon dolar değerinde sözleşme almıştır (AFSC Investigate, 2026). Şirketin "Investigative Case Management" (ICM) sistemi, her ICE memuruna kişilerin göçmenlik geçmişi, istihdam bilgileri, biyometrik kimlik verileri, aile ilişkileri ve plaka tanıma kayıtlarını birleştiren bir ağa erişim sağlamaktadır. Bu sistem sayesinde ICE'nin bir hedefi başarıyla bulma oranı yüzde 27'den yüzde 80'e yakın bir seviyeye çıkmıştır. Buna paralel olarak geliştirilen "ImmigrationOS" ürünü, pasaport verileri ve otomatik plaka tanıma kayıtlarını birleştirerek kişileri sınır dışı edilme önceliğine göre sıralamakta; **bu, IDF'nin soykırım amaçlı olarak Gazze'de kullandığı hedefleme mantığının ABD sınırları içindeki bir yansıması olarak okunmaktadır (Berkeley Political Review, 2026).**

5.3 NHS ve Avrupa'da Genişleme

İngiltere, Ocak 2026'da Palantir ile 240 milyon sterlinlik bir savunma sözleşmesi imzalamıştır; bu, NHS ile yapılan 330 milyon sterlinlik veri sözleşmesinin üzerine eklenen yeni bir genişlemedir (Al Jazeera, 2026). **Başbakan ve eski büyükelçinin şirket merkezine yaptığı, tutanağı tutulmamış ziyaret, şeffaflık endişelerini artırmış; muhalefet milletvekilleri şirketi "son derece sorgulanabilir bir organizasyon" olarak tanımlamıştır.**

5.4 Dijital Panoptikon ve Sivil Özgürlükler Mühendisliği

IBAN takibi, sinyal takibi ve plaka tanıma gibi araçların birleşik kullanımı, bireyi devlet-şirket kıskacında sürekli izlenebilir bir nesneye dönüştürmektedir. Bu durum, Jeremy Bentham'ın panoptikon metaforunun dijital bir versiyonunu üretir: gözetlenen, kendisini her an gözetleniyormuş gibi davranmaya koşullandırılır. **Amnesty International'ın (2020) ICE sözleşmeleri üzerine yürüttüğü araştırma, bu mühendisliğin insan hakları açısından doğurduğu riskleri erken dönemde belgelemiştir.**

6. Güncel Savaş Örnekleri: Algoritmik Savaşın Cepheleri

6.1 Gazze: Lavender, Gospel, Where's Daddy ve "Kötülüğün Sıradanlığı"

7 Ekim 2023 saldırıları sonrası Palantir, İsrail ordusu (IDF) ile iş birliğini Ocak 2024'te imzalanan "stratejik ortaklık" ile derinleştirmiştir (Al Jazeera, 2026). Gazze savaşının ilk haftalarında, İsrail istihbarat birimi Unit 8200'ün geliştirdiği "Lavender" adlı yapay zekâ destek sistemi, yaklaşık 37.000 bireysel hedef üreten bir liste oluşturmuştur (IISS, 2026). **Lavender, Gazze sakinlerini WhatsApp kayıtları, telefon numarası değişiklikleri ve adres hareketliliği gibi verilere dayanarak Hamas veya İslami Cihad üyeliği olasılığına göre 1'den 100'e kadar puanlamaktadır; sistemin yaklaşık yüzde 10'luk bir hata payı taşıdığı bildirilmektedir. Lavender'a ek olarak "Gospel" (bina hedefleme) ve "Where's Daddy" (hedefin evine girişini gerçek zamanlı izleyen) sistemleri, sivil kayıpları artıran soykırım amaçlı bir hedefleme zincirini tamamlamaktadır (Springer Nature, 2026).**

Palantir, Lavender ve Gospel sistemlerinin doğrudan geliştiricisi olduğunu resmi olarak yalanlamakta, ancak "İsrail'in savunma ve ulusal güvenlik misyonlarını başka program ve bağlamlarda desteklemekten gurur duyduğunu" açıklamaktadır (Business & Human Rights Centre, 2026). Karp ise kamuoyu önünde şirketinin Filistinlileri "büyük ölçüde teröristler" olarak öldürme sürecine dâhil olduğunu kabul etmiştir (AFSC Investigate, 2026). Birleşmiş Milletler bağımsız soruşturma komisyonu ve Uluslararası Soykırım Bilimcileri Derneği, İsrail'in Gazze'deki eylemlerini soykırım olarak tanımlamış; Uluslararası Adalet Divanı (ICJ) 2024'te bu iddiaların doğruluğuna hükmetmiştir. Bu çerçevede, teknolojik "tarafsızlık" söyleminin, ölçeklenebilir öldürme süreçlerini gizleyen bir perde işlevi gördüğü öne sürülmektedir (Novara Media, 2025).

6.2 Ukrayna ve MetaConstellation: Dağıtık Bir Model

Ukrayna cephesi, Palantir'in merkezileşmiş ve devlet süreçlerine derinlemesine entegre olmuş modeline kıyasla daha dağıtık bir teknolojik mimariyi temsil eder. Palantir'in MetaConstellation ve AIP araçları, uydu görüntülerini ve saha verilerini saniyeler içinde işleyerek hedef belirleme süreçlerini hızlandırmakta; **bu da "savaşın algoritmikleşmesi" tartışmasını uluslararası hukukun en güncel kör noktalarından biri hâline getirmektedir (TechnoLogic, 2026).** Uzmanlar, Ukrayna modelinin çoklu tedarikçi yapısı ve sahadan gelen geri bildirimle hızlı iterasyon imkânı sayesinde, Palantir'in merkezi ve bağımlılık yaratan modeline kıyasla daha adapte olabilir bir yapı sunduğunu belirtmektedir (Globalisler, 2026).

6.3 İran-İsrail Çatışması ve Maven Smart System

ABD ordusunun Palantir'in Maven Smart System'i — ki bu sistem Anthropic'in Claude modelini de entegre etmektedir — üzerinden yürüttüğü hedefleme süreçleri, İran'a yönelik saldırılarda okul, sağlık tesisi ve konut gibi sivil yapıların da vurulmasına neden olmuştur (IISS, 2026). İran'ın buna karşılık Birleşik Arap Emirlikleri ve Bahreyn'deki Amazon veri merkezlerini hedef alması, bu altyapının askeri istihbarat faaliyetlerini desteklediği değerlendirmesine dayanmaktadır. **Bu örnek, ticari bulut altyapısının artık fiilen askeri hedef hâline gelebildiğini göstermektedir.**

7. Uluslararası Sorumluluk Bağlamında Devletin Sorumluluğu

7.1 Mevcut Hukuki Çerçeve ve Açıklar

Uluslararası Hukuk Komisyonu'nun Devletlerin Uluslararası Haksız Fiillerden Sorumluluğuna İlişkin Maddeleri (ILC Articles on State Responsibility), bir devletin uluslararası hukuka aykırı bir fiilden sorumlu tutulabilmesi için fiilin devlete atfedilebilir olmasını ve bir uluslararası yükümlülüğün ihlalini şart koşar.

Uluslararası Hukuk Komisyonu'nun Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Doğan Sorumluluğuna İlişkin Maddeleri de bu temel mantığı kurar. Sorun şudur ki, güvenlik alanındaki yeni dijital mimariler bu iki eşiği pratikte karmaşıklaştırmaktadır. **Kararı algoritma mı verdi, operatör mü onayladı, modeli şirket mi eğitti, devlet mi parametreledi, veri kaynağı kamusal mı özel mi, sınır-aşan bulut altyapısı hangi devletin kontrolünde?** Bunların hepsi, atıf, öngörülebilirlik ve ispatı zorlaştırır; ama sorumluluğu ortadan kaldırmaz. Aksine, özel şirket aracılığıyla hareket etmek devletin hukukî yükümlülüklerini bertaraf etmez.

Algoritmik savaş ve gözetim sistemlerindeki bu değişim bu atfedilebilirlik zincirini ciddi biçimde bulanıklaştırmaktadır: bir hedefleme kararı, özel bir şirketin geliştirdiği model, devlet kurumunun operatörü ve nihayetinde otomatik öneriyi onaylayan bir asker arasında parçalanmış durumdadır. Yapay zekâ destekli sistemlerin sivil kayıplardaki payı ve "savaşın algoritmikleşmesi", **uluslararası hukukun en yeni kör noktalarından birini oluşturmaktadır (TechnoLogic, 2026).**

Uluslararası insancıl hukuk (IHL), orantılılık ve ayırt etme ilkelerini **insan karar vericiye atfen tasarlanmıştır;** oysa Lavender benzeri sistemlerde insan onayı, saniyeler içinde verilen ve fiilen otomatikleşmiş bir formaliteye dönüşmektedir. Bu durum, "anlamlı insan denetimi" (meaningful human control) ilkesinin pratikte aşındığı bir boşluk yaratmaktadır. Aynı şekilde, **otonom deniz ve hava araçlarına yönelik siber müdahalelerde sorumluluğun kime ait olacağı sorusu da mevcut uluslararası deniz ve silahlı çatışma hukuku çerçevesinde net bir karşılık bulamamaktadır.**

Diğer taraftan insan hakları boyutunda hak ihlalleri çoğunlukla dört eksende yoğunlaşır: **mahremiyet ve veri koruma, ayrımcılık yasağı, adil/usule uygun işlem güvenceleri ve yaşam hakkı.** Biyometrik ve öngörücü kolluk sistemlerinde yanlış pozitifler ile ayrımcı veri setleri, eşitlik ve ayrımcılık yasağına temas eder. Göçmen izleme ve deportasyon platformları, etkili başvuru hakkı ve usul güvencelerini aşındırabilir. Savaş alanında hedef önceliklendirme ve yarı-otonom karar destek katmanları da ayrım, orantılılık ve askeri gereklilik ilkeleriyle doğrudan çatışabilir. OHCHR'nin Xinjiang değerlendirmesi, Gazze'de AI destekli hedefleme etrafındaki tartışmalar ve AB'nin biyometrik öngörücü polisliğe getirdiği yasak/sınırlamalar birlikte düşünüldüğünde, **uluslararası ve bölgesel hukuk bu riskleri görmektedir; ancak uygulama ve bağlayıcılık düzeyi eşit değildir.**

7.2 Şirket-Devlet Ortaklığında Sorumluluğun Bulanıklaşması

Birleşmiş Milletler İş Dünyası ve İnsan Hakları Rehber İlkeleri (UNGPs), şirketlere insan haklarına saygı gösterme sorumluluğu yükler; ancak bu rehber ilkeler bağlayıcı değildir ve uygulanması büyük ölçüde gönüllülük esasına dayanır. Palantir örneğinde görüldüğü gibi, şirketler kendi "insan hakları durum tespiti" (human rights due diligence) süreçlerini kendileri tanımlayıp kamuoyuna açıklamakta, **böylece hem savunma hem de meşrulaştırma işlevini aynı anda üstlenmektedir** (Business & Human Rights Centre, 2026). İrlanda Sivil Özgürlükler Konseyi'nin Microsoft'un Filistinlilere yönelik toplu gözetim verisi işlemesi konusunda yürüttüğü şikâyet süreci ve hukuk savunuculuğu gruplarının Microsoft'a yönelttiği cezai ve hukuki sorumluluk uyarıları, bu alanda iç hukuk yollarının (domestic litigation) bir denetim aracı olarak öne çıkabileceğini göstermektedir (IISS, 2026). Bu tablo, üç temel açığı görünür kılmaktadır:

(i) **Atfedilebilirdik açığı** — bir zararın devlete mi, şirkete mi, yoksa ikisinin ortak ürettiği bir sisteme mi bağlanacağı belirsizdir;

(ii) **Şeffaflık açığı** — algoritmik sistemlerin iç işleyişi ticari sır kapsamında korunduğundan bağımsız denetim fiilen imkânsızlaşmaktadır;

(iii) **Yaptırım açığı**— mevcut uluslararası mekanizmalar (ICJ, ICC, BM özel raportörlükleri) şirketleri doğrudan yargılayamadığından, **sorumluluk devlet düzeyinde sıkışıp kalmakta, devlet de "teknik tedarikçi" savunmasının ardına saklanabilmektedir.**

Mevcut düzenleyici çerçevelerin en büyük açığı, güvenliğin tam kalbinde ortaya çıkar. AB AI Act, dünya çapında en gelişmiş risk-temelli AI düzenlemelerinden biri olsa da askerî ve ulusal güvenlik kullanımlarını büyük ölçüde kapsam dışı bırakır; yani devletin en yüksek müdahale kapasitesine sahip olduğu alanların büyük kısmı doğrudan bu çerçevenin dışındadır. 2 Şubat 2025'te yasaklı uygulamalara ilişkin ilk hükümler devreye girmiş, 2 Ağustos 2026 ise daha geniş uygulama bakımından kritik eşik olmuştur; fakat ulusal güvenlik istisnası sorunu devam etmektedir. Avrupa Konseyi'nin 2024 tarihli AI Çerçeve Sözleşmesi küresel ölçekte ilk bağlayıcı anlaşma niteliğinde olsa da, ilkeler düzeyindedir ve yaptırım gücü sınırlıdır. BM Genel Kurulu'nun 2024 AI kararı da önemlidir; ancak o da bağlayıcı değildir. Bu tablo, güvenlik alanında "norm var, güç yok" sorununu ortaya koymaktadır.

Ölümcül otonom sistemler ve savaş AI'sı bakımından boşluk daha da büyüktür. 2014'ten beri BM Belirli Konvansiyonel Silahlar Sözleşmesi (CCW) bünyesinde yürüyen görüşmeler, 2025 itibarıyla hâlâ bağlayıcı ve ayrıntılı bir küresel rejim üretebilmiş değildir. Reuters'ın 2025 raporuna göre, Ukrayna ve Gazze'de AI destekli ve otonomi düzeyi yükselen sistemlerin yaygınlaşmasına rağmen devletler arasında açık "kırmızı çizgiler" üzerinde uzlaşma oluşmamıştır. Bu koşullarda **"anlamlı insan denetimi"** söylemi çoğu zaman normatif bir slogan olarak kalmakta; teknik tanım, ölçülebilir kayıt, denetim protokolü ve ihlal hâlinde yaptırım eksik kalmaktadır.

Şirket sorumluluğu cephesinde ise BM İş Dünyası ve İnsan Hakları Rehber İlkeleri hâlâ temel referanstır. Bu ilkeler devletin koruma yükümlülüğü, şirketlerin saygı sorumluluğu ve mağdurlar için giderim hakkını üç sütun halinde düzenler. Ancak UNGP'ler[2] büyük ölçüde soft-law niteliğindedir; yani normatif gücü yüksek, yaptırım gücü zayıftır. Palantir-ICE tartışmaları, AP'nin Çin soruşturması ve Gazze bağlamında şirketlerin rolüne ilişkin BM raportörü değerlendirmeleri bize şunu göstermektedir: **güvenlik teknolojileri için sıradan "kurumsal sosyal sorumluluk" dili yetersizdir. Çatışma, sınır ve kitlesel gözetim teknolojilerinde zorunlu insan hakları durum tespiti, denetlenebilir kayıt ve bazı kullanım alanlarında lisans öncesi bağımsız gözden geçirme gereklidir.**

7.3 Şirket-Devlet Ortaklığında Sorumluluğun Bulanıklaşması

Tekno-Faşizm ve yukarıda bahsedilen "şirket-devlet kıskacı" bağlamında UNGP, 3 temel sütun (Three Pillars) üzerinden aslında devletlerin ve Palantir, Meta, X gibi teknoloji devlerinin yasal/ahlaki sınırlarını çizer:

I. KORUMA Yükümlülüğü (*State Duty to Protect*)

- **Ne Anlama Gelir?** Devletler, kendi yetki alanları içindeki üçüncü tarafların (şirketlerin) insan hakları ihlallerine karşı bireyleri korumakla yükümlüdür.[3]
- **Tekno-Faşizm Açığı:** Devletler, Palantir gibi şirketlerden yapay zeka tabanlı istihbarat ve "gözetim" hizmeti (örneğin LASER veya Gotham) satın alarak [Amnesty International, 2020], vatandaşlarını şirketlerin algoritmik tiranlığına karşı **koruma yükümlülüğünü bizzat ihlal etmektedirler**.
- **II. SAYGI Sorumluluğu (*Corporate Responsibility to Respect*)**
- **Ne Anlama Gelir?** Şirketler, büyüklükleri veya sektörleri ne olursa olsun, insan haklarına saygı göstermek ve operasyonlarının yol açabileceği olumsuz etkileri önlemek için **"Haklara Uygunluk Denetimi" (*Human Rights Due Diligence*)** yapmak zorundadır.[4]
- **Tekno-Faşizm Açığı:** Palantir, AIP gibi platformlarla savaş sahasındaki "öldürme zincirini" optimize ederken ya da İsrail ordusuna (IDF) Gazze'deki operasyonlar için yapay zeka desteği sağlarken UNGP'nin bu maddesini tamamen bypass etmektedir [González, 2026]. Yazılımlarının yaşam hakkı ihlallerine olan doğrudan etkisini "biz sadece kod satıyoruz" diyerek reddetmektedirler.
- **III. TELAFİ / Çözüm Mekanizmaları (*Access to Remedy*)**
- **Ne Anlama Gelir?** Şirket faaliyetleri nedeniyle hakları ihlal edilen mağdurların, hem adli hem de adli olmayan mekanizmalar aracılığıyla etkin bir telafiye ve hak aramaya erişimi olmalıdır. [5]
- **Tekno-Faşizm Açığı:** Algoritmik önleyici baskı (Minority Report modelleri) veya dijital ırkçılık (LASER programı) yüzünden fişlenen, özgürlüğü kısıtlanan ya da otonom silahlarla hedef alınan bireylerin karşısında muhatap yoktur [Amnesty International, 2020]. Algoritmaların kara kutu (*black box*) doğası gereği, mağdurlar uğradıkları haksızlığı mahkemede kanıtlayacak **şeffaf veriye erişemezler**.

[2] UNGP (United Nations Guiding Principles on Business and Human Rights), küresel ekonomideki şirketlerin insan hakları ihlallerini önlemek, tespit etmek ve gidermek amacıyla 2011 yılında Birleşmiş Milletler İnsan Hakları Konseyi tarafından oy birliğiyle kabul edilen ilk küresel standartlar bütünüdür.
[3] https://www.ungpreporting.org/resources/the-ungps/
[4] https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
[5] https://johnruggie.scholars.harvard.edu/un-guiding-principles

7.4 Yapılması Gereken Düzenlemeler

- **Atfedilebilirlik standardının güncellenmesi:** Algoritmik karar destek sistemlerinin devlet adına icra ettiği fonksiyonların, ILC maddelerindeki "devlet yetkisi kullanan özel aktör" kategorisi kapsamında açıkça tanımlanması ve **bu sistemleri tedarik eden şirketlerin de devletle birlikte müşterek sorumluluk rejimine dâhil edilmesi.**
- **Bağlayıcı insan hakları durum tespiti yükümlülüğü:** UNGPs'in gönüllülük esasından çıkarılarak, savunma ve güvenlik alanında faaliyet gösteren yapay zekâ şirketleri için bağımsız, dışsal denetime açık ve yaptırım gücü olan bir durum tespiti rejiminin (AB'nin tedarik zinciri durum tespiti yönergelerine benzer biçimde) uluslararası düzeyde kabul edilmesi.
- **Anlamlı insan denetiminin somutlaştırılması:** Hedefleme ve öldürme zincirinde "insan onayı" aşamasının asgari süre, gerekçelendirme ve itiraz mekanizması içerecek şekilde uluslararası insancıl hukuk metinlerine teknik olarak gömülmesi; salt formaliteye dönüşen onay adımlarının hukuki geçerliliğinin tartışmaya açılması.
- **Bağımsız algoritmik denetim organları:** BM çatısı altında, ticari sır iddialarını aşabilen, askeri ve göç yönetimi yapay zekâ sistemlerini inceleyebilen, sonuçlarını kamuoyuyla paylaşabilen kalıcı bir denetim mekanizmasının kurulması.
- **Şirket sorumluluğunun uluslararası yargıya açılması:** Uluslararası Ceza Mahkemesi'nin yetki alanının, savaş suçlarına doğrudan teknolojik katkı sağlayan şirket yöneticilerini de kapsayacak şekilde yorumlanması veya bu amaçla yeni bir protokolün müzakere edilmesi.
- **Veri egemenliği ve yedeklilik zorunluluğu:** Kritik kamu hizmetlerinde (sağlık, göç, savunma) tek bir özel tedarikçiye bağımlılığı sınırlayan, çoklu tedarikçi ve devlet kontrolünde yedek sistem bulundurma zorunluluğu getiren ulusal mevzuatların yaygınlaştırılması.

Özetle: Uluslararası hukuk açısından başlangıç noktası nettir: bir devletin uluslararası sorumluluğu için genellikle iki unsur gerekir; fiilin devlete atfedilebilir olması ve uluslararası bir yükümlülüğün ihlal edilmesi. Uluslararası Hukuk Komisyonu'nun Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Doğan Sorumluluğuna İlişkin Maddeleri de bu temel mantığı kurar. Sorun şu ki, güvenlik alanındaki yeni dijital mimariler bu iki eşiği pratikte karmaşıklaştırmaktadır. Kararı algoritma mı verdi, operatör mü onayladı, modeli şirket mi eğitti, devlet mi parametreledi, veri kaynağı kamusal mı özel mi, sınır-aşan bulut altyapısı hangi devletin kontrolünde? Bunların hepsi, atıf, öngörülebilirlik ve ispatı zorlaştırır; ama sorumluluğu ortadan kaldırmaz. Aksine, özel şirket aracılığıyla hareket etmek devletin hukukî yükümlülüklerini bertaraf etmez.

8. Sonuç

Sonuç olarak, tekno-faşizmin önüne geçilmesi, ne salt teknolojiye karşı bir direniş ne de teknolojiyi olduğu gibi kabullenme arasında bir tercih meselesidir. Asıl mesele, demokratik denetimin, insan haklarına dayalı durum tespitinin ve bağlayıcı uluslararası yükümlülüklerin, algoritmik karar alma hızına ayak uyduracak şekilde yeniden tasarlanmasıdır. Karp'ın manifestosunun ortaya koyduğu "kodu kim yazarsa, kuralları o koyar" mantığına karşı en güçlü cevap, kodun yazılma ve uygulanma sürecini insan haklarına, şeffaflığa ve hesap verebilirliğe açık hâle getirecek kurumsal ve hukuki mekanizmaların inşa edilmesinden geçmektedir. Bu inşa gerçekleşmediği takdirde, devletin sinir sistemini ele geçirme operasyonu, sessizce ve büyük ölçüde meşrulaştırılmış biçimde tamamlanmış olacaktır.

Karp manifestosu etrafında şekillenen tartışma, yüzeyde Silikon Vadisi'nin savunma sektörüne dönüşü gibi görünebilir; ama daha derinde çok daha büyük bir kırılmaya işaret eder. Bu kırılma, devletin kendisini artık yalnızca hukuk, kurum ve bürokrasi olarak değil; veri ağları, yazılım katmanları, model davranışları ve özel teknoloji ekosistemleri üzerinden yeniden kurmasıdır. Tekno-faşizm dediğimiz şey tam da burada belirir: siyasal iktidarın teknik görünmezlik kazanması, teknik operasyonun siyasal bağışıklık elde etmesi ve vatandaşın hak öznesi olmaktan çıkarak işlenebilir, önceliklendirilebilir, sınıflandırılabilir bir güvenlik girdisine dönüşmesi. (Karp/Zamiska; Zuboff; Chayka; ekli belge)

Bu raporun temel bulgusu, tekno-faşizmin tek bir rejime, tek bir ülkeye ya da tek bir şirkete indirgenemeyeceğidir. Gazze'de yüksek hızlı hedefleme ve soykırım, İran savaşı örnekleri, Ukrayna'da yazılımlaşmış savaş, Xinjiang'da öngörücü baskı ve ABD'de veri-temelli deportasyon rejimi aynı fenomenin farklı yoğunluklardaki tezahürleridir. Bunların ortak paydası, güvenliğin gittikçe daha fazla veri füzyonu, algoritmik önceliklendirme ve özel tedarikçi bağımlılığı ile yürütülmesidir. Bu nedenle mesele, "demokratik devletler de teknoloji kullanıyor" itirazıyla kapanmaz; **asıl soru, bu teknolojilerin hakları askıya alan bir istisna rejimi mi, yoksa hakları koruyan bir anayasal mimari mi ürettiğidir.**

Devletlerin güvenlik ihtiyaçları gerçektir. Hibrit tehditler, siber saldırılar, savaşın hızlanması, kitlesel göç yönetimi, terör ve sınır-aşan suç ağları da gerçektir. Bu nedenle rapor, anti-teknolojik bir romantizm savunmamaktadır. **Sorun,**

teknolojinin varlığı değil; güvenlik adı altında *denetimsiz teknik egemenlik* kurulmasıdır. Teknoloji devlet kapasitesini artırabilir; ama hukuk, hesap verebilirlik ve insan haklarıyla bağlı kılınmadığında aynı kapasite, demokratik siyasal topluluğun sinir sistemini felç edebilir. Fransa'nın 2026'daki "dijital egemenlik" tepkisi, AB'nin biyometrik öngörücü polisliğe sınır koyma çabası ve küresel AI yönetişimi girişimleri, bu yüzden yalnızca düzenleyici ayrıntılar değil, rejim tipi tartışmalarıdır.

Son tahlilde Karp manifestosu, çok önemli bir gerçeği açığa çıkarıyor: 21. yüzyılın sert gücü, tanklarla ve füzelerle olduğu kadar veritabanları, model ağırlıkları, ontolojiler ve kullanıcı arayüzleriyle de kurulacaktır. Dolayısıyla demokrasi için asıl mücadele yalnızca sandıkta ya da sokakta değil; model kartlarında, veri minimizasyon kurallarında, olay günlüklerinde, sınır sistemlerinde, savaş hukukunun teknik protokollerinde ve özel teknoloji şirketlerinin sorumluluk rejimlerinde verilecektir. Eğer devletler bu alanları "ulusal güvenlik" etiketiyle bütünüyle istisna bölgesi haline getirirse, **dijital totalitarizm istisna olmaktan çıkar ve küresel yönetişimde yeni norm haline gelir.** Eğer tam tersine, güvenlik teknolojilerini anayasal bağlılık, insan hakları, bağımsız denetim ve uluslararası sorumluluk eksenine yerleştirebilirlerse, o zaman teknoloji küresel totaliterleşmenin değil, kamusal güvenliğin demokratikleşmesinin de aracı olabilir. **Bu raporun vardığı sonuç budur: geleceğin siyasal sorusu, "AI kullanılacak mı?" değil, "AI ile kurulan egemenlik kime karşı, kim adına ve hangi hukuk altında işletilecek?" sorusudur.**

Kaynakça:

- Amnesty International. (2020). Failing to Do Right: Palantir's ICE Contracts and Human Rights.
- American Friends Service Committee (AFSC) Investigate. (2026). Palantir Technologies Inc. https://investigate.afsc.org/company/palantir
- Anadolu Ajansı (AA) Analiz, Elmalı, B. (2026). Palantir'in 22 maddelik manifestosu yapay zeka savaşlarını nasıl şekillendirecek? https://www.aa.com.tr
- BDS Movement. (2026). Palantir. https://bdsmovement.net/palantir
- Berkeley Political Review. (2026). Lavender AI, Palantir, and the Israelification of "Homeland Security". https://bpr.studentorg.berkeley.edu
- Business and Human Rights Centre. (2026). Palantir response to allegations over its complicity in war crimes amid Israel's war in Gaza. https://www.business-humanrights.org
- Chafkin, M. (2021). The Contrarian: Peter Thiel and Silicon Valley's Pursuit of Power. Penguin Press.
- Chayka, K. (2025). Techno-fascism Comes to America. The New Yorker.
- Coeckelbergh, M. (2026). Technofascism: AI, Big Tech, and the New Authoritarianism. AI & Society, Springer Nature.
- David Leslie, Christopher Burr, Mhairi Aitken, Michael Katell, Morgan Briggs, Cami Rincon. "Human rights, democracy, and the rule of law assurance framework for AI systems: A proposal." 2022.
- Drop Site News / Alliance for Water Justice in Palestine. (2026). Palantir's AI Is Already Playing a Major Role in Tracking Gaza Aid Deliveries. https://www.waterjusticeinpalestine.org
- Elsen, J. H. (2025). Inside Palantir: How a Secret Tech Titan is Shaping the Future.
- Euronews. (2026). AI weapons, national service, and 'inferior cultures': Palantir's controversial manifesto explained. https://www.euronews.com
- Fikir Coğrafyası, Baydar, S. C. (2026). Palantir'in Manifestosu Ne Anlatıyor? https://fikircografyasi.com
- Globalisler. (2026). Palantir olayından dersler: Yapay zekâ artık milli güvenliğin temel unsurlarından. https://www.globalisler.com
- González, R. J. (2026). The Rise of the Techno-Tyrants. Transnational Institute (TNI).
- https://utkvakfi.org/tekno-fasizm-palantir-alex-karp-manifestosu-ve-dijital-totalitarizmin-yukselisi/
- International Institute for Strategic Studies (IISS). (2026). The proliferation of AI-enabled military technology in the Middle East. https://www.iiss.org
- Karp, A. C. & Zamiska, N. W. (2025). The Technological Republic: Hard Power, Soft Belief, and the Future of the West. Crown Currency.
- Janis Mimura. Planning for Empire: Reform Bureaucrats and the Japanese Wartime State. Cornell University Press, 2011.
- Lewis, B. (2025). Headed for Technofascism: The Rightwing Roots of Silicon Valley. The Guardian.
- McQuillan, D. (2022). Resisting AI: An Anti-Fascist Approach to Artificial Intelligence. Bristol University Press.
- Mersin Haber. (2026). Yapay zeka destekli gemilere yapılabilecek siber saldırılara yönelik hukuki boşluğu NATO gündemine taşıdı. https://www.mersinhaber.com
- Novara Media. (2025). Palantir Technologies and the Age of Automated Genocide. https://novaramedia.com
- Palantir Technologies. (2025). 22-Point Manifesto: Summary of The Technological Republic. X (Twitter).
- SETA Foundation at Washington DC. (2026). Palantir'den Tepki Çeken "Manifesto". https://setadc.org
- Springer Nature. (2026). AI at War. https://link.springer.com
- TechnoLogic. (2026). Dijital ikizlerden savaş alanına: Palantir neden eleştirilerin odağında? https://www.technologic.com.tr
- The Executives. (2026). Palantir Nedir? Ne İşe Yarar? Verilerimiz... (YouTube Analizi).
- Thiel, P. & Masters, B. (2014). Zero to One: Notes on Startups, or How to Build the Future. Crown Business.
- Varoufakis, Y. (2023). Technofeudalism: What Killed Capitalism. Vintage.
- Yeni Çağ Gazetesi. (2026). Palantir'den dünyaya yeni mesaj: Yeni savaş dönemi yapay zekâ ile şekillenecek. https://www.yenicaggazetesi.com
- Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.
- Demokrasinin "Fişini Çeken" Milyarderler: PayPal Mafyası ve Palantir Operasyonu. (YouTube Belgeseli).(2025)