2BLACKDOT..

“Esasen konu hep 2 nokta arasındadır”

Haftalık

Politik ve Jeopolitik

Gelişmeler

8 Haziran 2026 – Sayı 112

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:

SAVAŞIN YENİ YÜZÜ: ALGORİTMA ZAYIATI VE HUKUKİ SORUMLULUK

Yapay Zekâ'nın Modern Çatışmalardaki Rolü ve Uluslararası Hukuk Kapsamında Devlet Sorumluluğu Üzerine Geniş Kapsamlı Yönetici Özeti

1. Savaş Paradigmasında Değişim ve Algoritma Zayıatı

KARAR MİMARİSİNDE DÖNÜŞÜM

Algoritma Zayiatı
Karar süreçlerinin algoritmikleşmesiyle sivil ölümlerinin etik mesafeden uzaklaşarak teknik bir veri haline gelmesi.

Karar Vericiden Denetleyiciye Dönüşüm
İnsan, "ateş emrini veren" özne statüsünden, makinenin ürettiği hedef listelerini hızla onaylayan bir denetleyiciye dönüşüyor.

2.72 TRİLYON DOLAR REKOR HARCAMA
2024 yılı itibarıyla küresel askeri harcamalar rekor kırarken, stratejik güç odağı silah fabrikalarından veri merkezlerine kayıyor.

2. Saha Deneyimlerinden Acı Dersler

GAZZE: LAVENDER VE HABSORA SİSTEMLERİ

20 sn | **1 alt düzey üye : 15-20 sivil ölüm**

Askeri personelin hedef başına sadece 20 saniye ayırdığı, otomatik onayla büyük yıkıma yol açan sistemler.

"WHERE'S DADDY?" TAKİP YAZILIMI

Hedeflerin cephe yerine aileleriyle evlerine girdikleri an vurulmasına odaklanılması, konutlarda kitlesel sivil ölümlerine neden oluyor.

UKRAYNA VE İRAN: ÖNGÖRÜLEMEZ RİSKLER

3. Uluslararası Hukukta Devlet Sorumluluğu

SORUMLULUK DEVREDİLEMEZ
ICRC ve BM'ye göre, yaşam ve ölüm kararlarındaki hukuki hesap verebilirlik asla bir algoritmaya veya makineye devredilemez.

- **Komutanın Sorumluluğu (Roma Statüsü Md. 28)**
  "Sistemi anlamıyordum" savunması geçersizdir. komutan, sahaya sürdüğü YZ sisteminin risklerini bilmek ve öngörmekle yükümlüdür.
- **ARSIWA ve Atfedilebilirlik**
  Bir fiilin devlete atfedilmesi için teknik hata değil, mimariyi kimin onaylayıp sahaya sürdüğü esastır; algoritmik hata devleti sorumluluktan kurtarmaz.

4. Devletler İçin Asgari Yükümlülük Seti

HUKUKİ İNCELEME	DENETİM İZİ	YÜKSEK RİSKLİ ALANLAR	TAZMİN VE ONARIM
Yeni silahlar sahaya sürülmeden önce Madde 36 uyarınca disiplinler arası inceleme yapılmalıdır.	Hedefleme sistemlerinde zorunlu kayıt (log) ve şeffaf denetim mekanizmaları kurulmalıdır.	Konut, okul ve hastane gibi korunan alanlar için "yükseltilmiş insan doğrulaması" şarttır.	İhlal durumunda, devlet iç hukukuna sığınmadan maddi ve manevi zararı tam tazmin etmelidir.

NotebookLM

YAPAY ZEKÂ VE DEĞİŞEN SAVAŞ PARADİGMASI

“Savaşta Yapay Zekâ Uygulamaları ve Uluslararası Hukukta Devlet Sorumluluğu”

Kapsam ve temel argüman

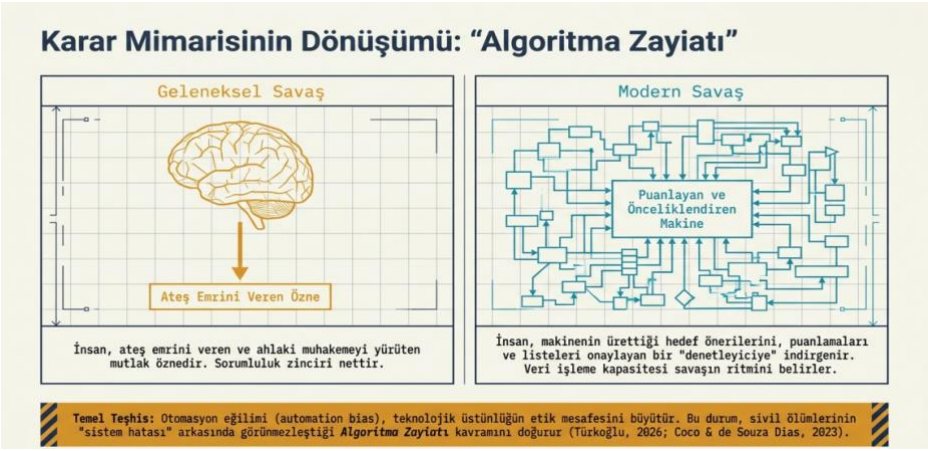
Bu rapor, Tanol Türkoğlu’nun “Algoritma Zayiatı” başlıklı yazısını merkez alarak yapay zekânın savaşın doğasını nasıl dönüştürdüğünü güvenlik, askerî ve küresel jeopolitik perspektiflerden inceleyerek; ardından bu dönüşümü uluslararası hukukta devlet sorumluluğu, özellikle de **Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Doğan Sorumluluğu Hakkında Maddeler** çerçevesinde değerlendirmektedir. Türkoğlu’nun iddiası şudur: savaşta değişen yalnızca silahlar değildir; karar mimarisi de insanın aleyhine algoritmikleşmektedir ve bunun sonucu “algoritma zayiatı” olarak görünür olmaya başlamaktadır (Türkoğlu, 2026). Bu iddia, son yıllarda Gazze, İran ve Ukrayna sahalarındaki uygulamalar ile ICRC, NATO, Pentagon, SIPRI ve BM kaynaklarının ortak biçimde işaret ettiği olguyla uyumludur:

> *“Yapay zekâ artık savaşın kenarında değil, istihbarat füzyonu, hedef üretimi, hava savunması, insansız sistemler, bilgi savaşı ve tedarik zinciri yönetiminin merkezindedir (International Committee of the Red Cross [ICRC], 2026a; Le Poidevin, 2026).“*

Bununla birlikte, mevcut saha verileri “tam otonom savaşın” her yerde gerçekleştiğini göstermemektedir. Daha isabetli teşhis, insan kararının yerini bütünüyle makinenin aldığı değil; insan kararının, makinenin ürettiği öneri, puanlama, önceliklendirme ve hedef listeleri tarafından giderek yapılandırıldığı yönündedir. NATO da hukuka uygunluk, sorumluluk ve hesap verebilirlik, açıklanabilirlik/izlenebilirlik, güvenilirlik, yönetilebilirlik ve önyargı azaltımını kendi AI savunma ilkelerine yerleştirmiştir (NATO, 2024). Yani sorunun kendisi, teknolojiyi kullanan devletler tarafından da kabul edilmektedir; **tartışma, riskin var olup olmadığı değil, hangi hız ve hangi hukuk altında yönetileceğidir (NATO, 2024).**

> **TTDijital makalesinin analitik değeri:**
> *Türkoğlu’nun makalesinde insanın “ateş emrini veren özne” statüsünden, önüne gelen hedef önerilerini önceliklendiren bir denetleyiciye dönüşmeye başladığını; veri işleme kapasitesinin savaşın ritmini değiştirdiğini, algoritmik öneri üreten sistemlerin fiilen kararın yönünü tayin eder hale geldiğini savunurken teknolojik üstünlüğün etik mesafeyi büyüttüğünü ve sivil ölümlerini görünmezleştirdiğini çok güçlü biçimde ortaya koymaktadır (Türkoğlu, 2026).*

Bu gözlem, yabancı literatürde “automation bias” ve “complacency”[1] diye adlandırılan sorunlarla doğrudan örtüşmektedir. Oxford’daki bir çalışma, savaşta hedefleme dâhil karmaşık kararların makinelerce desteklenmesinin, insan operatörlerin makine tespitlerine aşırı güven duymasına ve çelişkili bilgileri gözden kaçırmasına neden olabileceğini; bunun da savaş suçu niteliği kazanabilecek fiillere yol açabileceğini tartışmaktadır (Coco & de Souza Dias, 2023). SIPRI’nin 2024 tarihli çalışması ise askerî yapay zekâdaki önyargının yalnızca teknik bir doğruluk sorunu olmadığını; ırk, cinsiyet, sınıf ve benzeri toplumsal önyargıları yeniden üreterek tehdit ve tehdit olmayanı yanlış sınıflandırabildiğini, bunun da hedeflerin yanlış teşhisinden insani ihtiyaçların hatalı değerlendirilmesine kadar uzanan sonuçlar doğurabileceğini göstermektedir (Blanchard & Bruun, 2024). “Algoritma Zayiatı” kavramı akademik literatürde ampirik ve normatif bir karşılık bulmaktadır (Blanchard & Bruun, 2024; Coco & de Souza Dias, 2023).



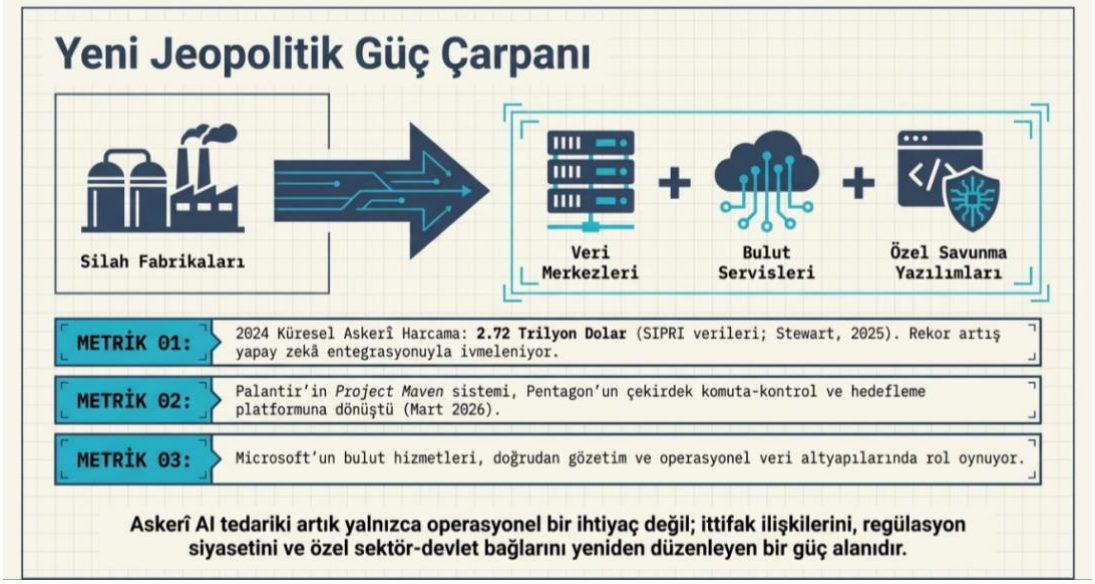
[1] Automation bias (Otomasyon Eğilimi) ve complacency (Rehavet/Kanıksama), insanların yapay zeka ve otomasyon sistemleriyle çalışırken düştükleri en kritik iki psikolojik yanılgıdır.

Savaş paradigmasının değişimi

Askerî açıdan yapay zekânın en önemli etkisi, öldürme zincirini hızlandırması ve ölçeklendirmesidir. Palantir'in Pentagon içindeki Maven sistemi,[2] uydu, drone, radar, sensör ve istihbarat akışlarından gelen çok büyük veri setlerini analiz ederek potansiyel tehdit ve hedefleri işaretleyebilen bir komuta-kontrol platformu olarak tanımlanmıştır; Reuters'a göre sistem Mart 2026 itibarıyla Pentagon'un çekirdek programlarından biri hâline getirilmektedir (Jeans, 2026). NATO da AI kullanımını hızlandırmakla birlikte test, doğrulama, standardizasyon ve sorumlu kullanım ilkelerini kurumsallaştırmaya çalışmaktadır (NATO, 2024). Bu tablo, yapay zekânın savaşta "yardımcı araç" olmaktan çıkıp operasyonel tempoyu belirleyen bir altyapıya dönüştüğünü göstermektedir (Jeans, 2026; NATO, 2024).

Jeopolitik açıdan daha sarsıcı olan ise savaş kapasitesinin artık yalnızca silah fabrikalarıyla değil, veri merkezleri, bulut servisleri, model tedarikçileri, görüntü işleme yazılımları ve savunma-teknoloji şirketleriyle birlikte düşünülmek zorunda olmasıdır. **SIPRI, askerî yapay zekâ tedarikinin artık devletlerin yalnızca operasyonel ihtiyacını değil, hukuki yükümlülüklerini ve yüksek düzeyli siyasi taahhütlerini de yerine getirmesi gereken bir alan olduğunu vurgulamaktadır** (Goussac & Boulanin, 2026).

CSIS, Project Maven'in çıktısı olan Maven Smart System'in yalnızca ABD savunma yapısında değil, NATO müttefiklerinde de yaygınlaştığını belirtmektedir; Microsoft'un 2025 ve 2025 sonrasındaki açıklamaları da özel sektör bulut ve AI hizmetlerinin doğrudan savaş ve gözetim altyapılarında rol oynayabildiğini ortaya koymuştur (Cancian, 2026; Microsoft, 2025a, 2025b). Silah fabrikalarının yerini veri merkezleri alıyor tezi bu nedenle abartılı değil, stratejik gerçekliğe oldukça yakındır (Türkoğlu, 2026; Goussac & Boulanin, 2026).



Bu dönüşüm aynı zamanda küresel bir silahlanma ve güvenlik rekabetini de hızlandırmaktadır. SIPRI verilerine dayanan Reuters haberi, 2024'te küresel askerî harcamaların 2,72 trilyon dolara çıkarak rekor kırdığını; artışın özellikle Avrupa ve Orta Doğu'daki gerilimlerden beslendiğini göstermektedir (Stewart, 2025). NATO'nun 2024 revizyonu ve ABD'nin 2026 Maven kararı, Batı blokunun "sorumlu AI" diliyle eşzamanlı bir operasyonel hızlanmaya gittiğini; Rusya'nın ise savaş ekonomisi içinde "egemen drone ekosistemi" ve uygulamalı AI özerkliği inşa etmeye çalıştığını göstermektedir (NATO, 2024; Bondar, 2026; Jeans, 2026).

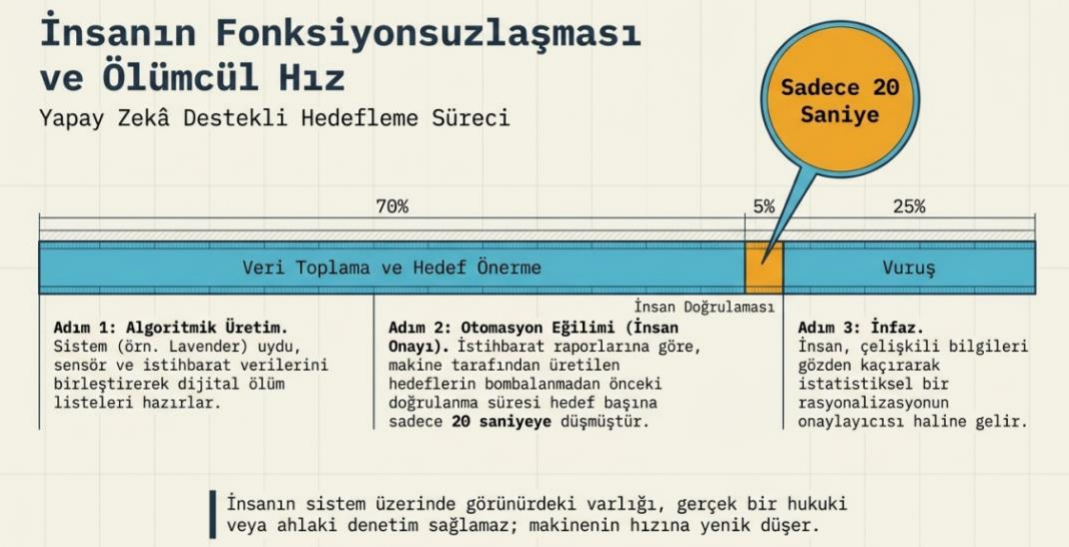
> *Sonuç olarak yapay zekâ, sadece muharebe alanını değil, ittifak ilişkilerini, tedarik zincirlerini, regülasyon siyasetini ve özel sektör-devlet bağlarını da yeniden düzenleyen jeopolitik bir kuvvet çarpanı haline gelmiştir (Bondar, 2026; NATO, 2024).*

[2] **Palantir'in Maven Sistemi (Maven Smart System), ABD Savunma Bakanlığı (Pentagon) tarafından resmi olarak tüm askeri birimlerin ana yapay zeka işletim sistemi ve komuta-kontrol platformu kabul edilen, yapay zekâ tabanlı bir algoritmik hedef tespit ve operasyon yönetim platformudur. Sistemin temel çalışma mantığı, rolü ve işleyişi kısaca şu şekildedir: (https://www.reuters.com/technology/pentagon-adopt-palantir-ai-as-core-us-military-system-memo-says-2026-03-20/)**

- **Çok Boyutlu Veri Entegrasyonu: Sistem; askeri uydulardan, insansız hava araçlarından (İHA), radarlardan, sahadaki sensörlerden ve istihbarat raporlarından gelen devasa miktardaki ham veriyi tek bir ekranda birleştirir.**
- **Algoritmik Hedef Belirleme (Targeting): Bilgisayarlı görü (computer vision) ve yapay zeka algoritmalarını kullanarak düşman askeri araçlarını, mühimmat depolarını, gizli sığınakları veya kişileri otomatik olarak saniyeler içinde tespit eder ve "hedef önerisi" olarak komuta kademesinin önüne koyar.**
- **Zaman Avantajı: Geleneksel yöntemlerle insan analistlerin saatler süren manuel tarama ve istihbarat eşleştirme süreçlerini saatlerden dakikalara (hatta saniyelere) indirger.**
- **Aktif Savaş Deneyimi: 2026 yılı itibarıyla Pentagon tarafından resmi bütçeli bir "kayıt programı" (program of record) haline getirilen Maven; Ukrayna cephesinde veri analitiğinde ve özellikle Ortadoğu'da yürütülen operasyonlarda binlerce hedefin eş zamanlı olarak vurulmasında ana harekat merkezi rolünü üstlenmiştir.**

Çatışma sahalarından çıkarılan dersler

Gazze sahası, algoritmik hedeflemenin hukukî ve ahlakî risklerini en çıplak haliyle gösteren örnektir. İsrail Savunma Kuvvetleri, Haziran 2024 açıklamasında Habsora ve Lavender[3] gibi araçların hedef tayinini insanın yerine yapmadığını, yalnızca analistlere veri düzenleme ve odaklanma desteği verdiğini, nihai hedefleme ve saldırı kararının insanlarca alındığını savunsa da (Israel Defense Forces [IDF], 2024) Human Rights Watch, İsrail'in Gazze'de kullandığı dijital araçların hatalı veriye ve "inexact approximations"a dayandığını, bunun ayrım gözetme ve saldırıda ihtiyat kurallarını ihlal ettiğini belirtmiştir.



Sahadan elde edilen istihbarat raporlarına ve uluslararası bağımsız incelemelere göre, bu sistemlerin kullanımı şu tehlikeli sonuçları doğurmuştur:

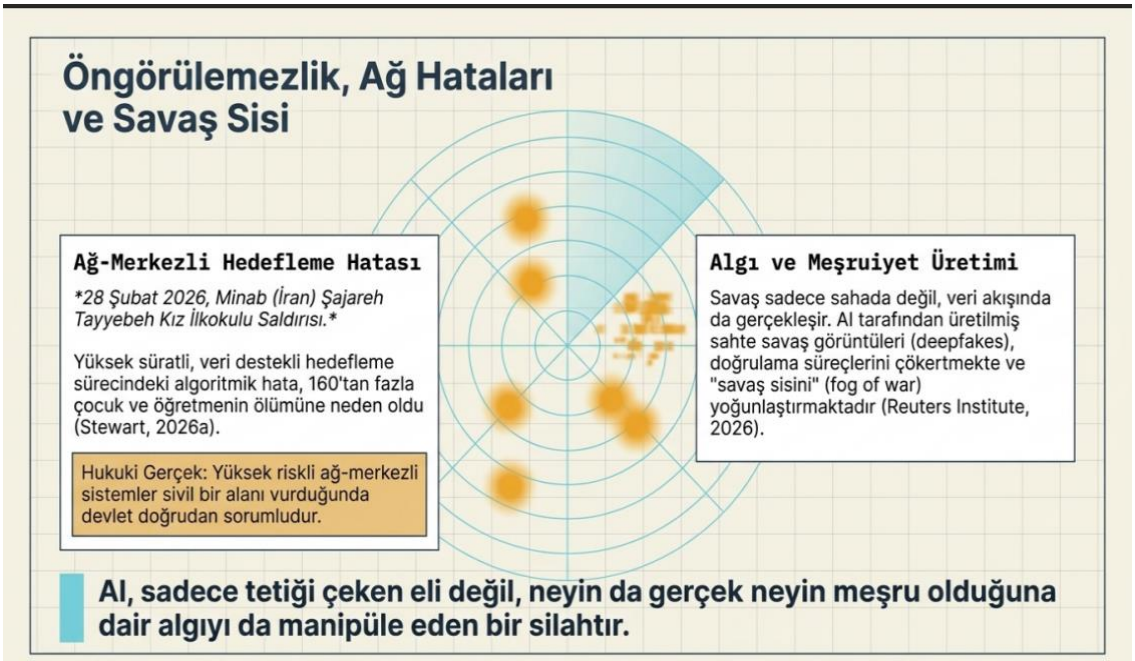
1. **İnsanın Fonksiyonsuzlaşması:** Askeri personelin Lavender'ın ürettiği insan hedeflerini bombalamadan önce doğrulamak için hedef başına sadece **20 saniye** harcadığı ortaya çıkmıştır(**otomasyon eğilimi**).
2. **"Where's Daddy?" (Baban Nerede?) Entegrasyonu:** Lavender tarafından listelenen hedefler, akıllı takip yazılımlarıyla izlenmiş; şahıslar cephede veya tünellerde askeri görevdeyken değil, **aileleriyle birlikte evlerine girdikleri an vurulmuştur.** Bu durum sivil yerleşim yerlerinde (konutlarda) kitlesel kadın ve çocuk ölümlerine yol açmıştır.
3. **Kabul Edilebilir Sivil Kayıp Limiti:** Sistemlerin ayarlarında, tek bir alt düzey Hamas üyesini öldürmek için **15 ila 20 sivilin**, üst düzey bir lider için ise **yüzlerce sivilin** öldürülmesine sistem tarafından otomatik olarak "orantılı hasar" onayı verildiği ifşa edilmiştir.

[3] Habsora (The Gospel) ve Lavender, İsrail Savunma Kuvvetleri (IDF) tarafından Gazze'deki askeri operasyonlarda hedef tespiti ve imha süreçlerini otomatikleştirmek için kullanılan, yapay zekâ tabanlı iki farklı algoritmik sistemdir.
Bu iki sistem, sivil zayiat oranlarının dramatik şekilde artması nedeniyle uluslararası hukukta ve askeri literatürde "algoritma zayiatı" kavramının en somut ve tartışmalı örnekleri olarak kabul edilir.
1. Habsora: Fiziksel Yapılar ve Altyapılar (Yere Dayalı Hedefleme) Dron görüntüleri, uydu fotoğrafları, sinyal istihbaratı ve siber verileri tarayarak Hamas veya İslami Cihad mensuplarının kullandığı iddia edilen binaları, komuta merkezlerini, mühimmat depolarını ve konutları tespit eder. Geleneksel yöntemlerle insan analistlerin yılda sadece birkaç yüz hedef belirleyebildiği süreçleri endüstriyel bir hızla makineleştirmiştir. Günde yüzlerce binayı "imha edilecek hedef" olarak üretebilen bir "hedef fabrikası" gibi çalışır.
2. Lavender: Canlı Kişiler (İnsan Hedefleme / Suikast Listeleri) Gazze'deki nüfusun telefon görüşmelerini, mesajlarını, sosyal medya hareketlerini, konum geçmişlerini ve temas ağlarını yapay zekâ algoritmalarıyla analiz eder. Kişilere 1 ile 100 arasında bir "terör militanı olma skoru" verir. Sistem, savaşın ilk aşamalarında yaklaşık 37.000 Filistinli erkeği "Hamas militanı" olarak potansiyel suikast listesine eklemiştir.

Özetle; Habsora binaları ve lojistik yapıları otomatik olarak yok etmek için hedefler üretirken; Lavender doğrudan insanları hedef alan dijital ölüm listeleri hazırlamaktadır. Her iki sistem de ahlaki muhakemeyi ve uluslararası insancıl hukuku istatistiksel bir rasyonalizasyon arkasına gizlemektedir.[4],[5]

OHCHR ise bu tür araçların geniş hedef tanımları ve müsamahakâr orantılılık uygulamalarıyla birleştiğinde sivil ölümleri ve sivil nesnelere zararı katlayıcı biçimde artırma riski taşıdığını yazmıştır (Human Rights Watch [HRW], 2024; Office of the United Nations High Commissioner for Human Rights [OHCHR], 2024a). Aynı OHCHR raporu, doğrulanmış ölümlerin çok önemli bir kısmının konutlarda gerçekleştiğini, bütün ailelerin barındıkları yerlerde öldüğünü ve bu durumun ayrım, orantılılık ve ihtiyat ilkeleri bakımından ciddi sorunlar doğurduğunu kaydetmiştir; UNICEF de Kasım 2024'te yalnızca bir ay içinde Gazze'de okula dönüştürülmüş sığınaklara yönelik en az 64 saldırı tespit edildiğini açıklamıştır (OHCHR, 2024a; UNICEF, 2024). Bu saha, "AI riski hassas vuruşu artırır" iddiasının kendiliğinden doğru olmadığını, veri ve model hatasının yoğun nüfuslu alanlarda sistematik sivil yıkıma evrildiğini göstermektedir (HRW, 2024; OHCHR, 2024a).

ABD-İsrail-İran hattı iki farklı ders üretmiştir. İlki, 13 Nisan 2024'te İran'ın füze ve drone saldırısına karşı ABD, İsrail ve diğer ortakların çok katmanlı hava savunma ve veri füzyonu yakalamasıdır; bu, algoritmik erken uyarı ve entegre hava savunmasının stratejik değerini ortaya koymuştur (Reuters, 2024a).



İkinci ders ise 28 Şubat 2026'da başlayan açık savaş safhasında görülmüştür:

> *Savaşın ilk gününde İran'ın Minab kentindeki Şajareh Tayyebeh kız ilkokuluna yönelik saldırıda 160'tan fazla çocuk ve öğretmen ölmüş, sonraki soruşturmalar olayda ABD kuvvetlerinin sorumluluğuna işaret etmiştir (Stewart, 2026a, 2026b). Bu olayda hukuken önemli nokta şudur: yüksek süratli, ağ-merkezli, veri destekli hedefleme süreçleri sivil okul gibi korunan alanları vurulduğunda, devlet otomatik olarak sorumludur.(OHCHR özel raportörleri, 2026; Stewart, 2026a, 2026b).*

[4] (Bu sistemlerin varlığını, Unit 8200 istihbarat subaylarının itiraflarını ve sahadaki "20 saniye" ile "Where's Daddy?" gibi operasyonel detaylarını dünya kamuoyuna ilk kez ifşa eden ana kaynaklardır):

[5] Ayrıca detaylı bilgi için bakınız:

- Abraham, Y. (2023, November 30). 'A mass assassination factory': Inside Israel's calculated bombing of Gaza. *+972 Magazine*. 972mag.com
- Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. *+972 Magazine*. https://www.972mag.com/lavender-ai-israeli-army-gaza/
- Davies, H. (2023, December 1). 'The Gospel': how Israel uses AI to select bombing targets in Gaza. *The Guardian*. https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets
- McKernan, B., & Davies, H. (2024, April 3). 'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets. *The Guardian*. https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes
- Alston, P. (2024). Algorithmic warfare and the erosion of human judgment: Critical reflections on the Gaza conflict. *Journal of International Humanitarian Legal Studies*, 15(2), 210-234.
- Boon, K. E. (2024, June 28). Israel – Hamas 2024 Symposium - The Gospel, Lavender, and the Law of Armed Conflict. *Lieber Institute West Point: Articles of War*. https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/ [1]
- Dorsey, J., & Bo, M. (2024). Speed and scale over substance: How AI-DSS compromised meaningful human control in the 2023-2024 Gaza War. *Opinio Juris*.
- Santos, S. (2025). The Use of 'Lavender' in Gaza and the Law of Targeting. *International Humanitarian Law Studies*, 16(2), 336-358. https://brill.com/view/journals/ihls/16/2/article-p336_003.xml [1]

Aynı savaşta Reuters ve Reuters Institute kaynakları, AI tarafından üretilmiş sahte savaş görüntülerinin doğrulama süreçlerini zorlaştırdığını ve savaş sisini kalınlaştırdığını da göstermiştir;

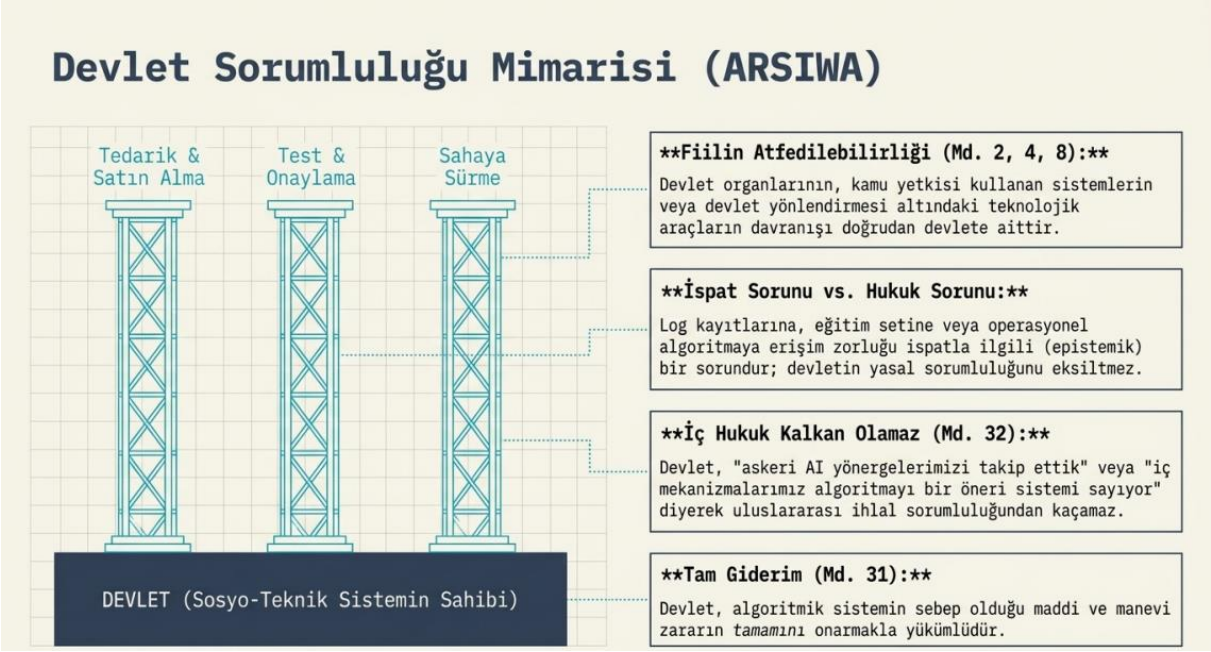
> *Dolayısıyla yapay zekâ yalnızca hedefleme değil, algı ve meşruiyet üretimi üzerinde de savaşın bir parçası haline gelmiştir (Reuters Fact Check, 2026; Reuters Institute for the Study of Journalism, 2026).*

Rusya-Ukrayna savaşı ise yapay zekânın bugünkü karakterini daha soğuk bir gerçekçilikle ortaya koymaktadır. CSIS'in 2025 raporu, Ukrayna'da tam otonom savaşın henüz genel kural olmadığını; buna karşın görüntü analizi, hedef tanıma, hedef takibi, "last-mile" navigasyon ve istihbarat çıkarımı gibi alanlarda kısmi otonominin hızla yayıldığını saptamaktadır (Bondar, 2025). Reuters da Kasım 2025'te, Ukrayna dronlarının görüntü tabanlı hedef kilitleme sayesinde yoğun elektronik karıştırma altında dahi bağlantı koptuktan sonra hedefe doğru otonom biçimde ilerleyebildiğini bildirmiştir (Reuters, 2025). Ancak 2026'ya gelindiğinde CSIS, Rusya'nın V2U tipi sistemlerle iletişim bileşeni olmadan hedef seçimi yapabilen daha ileri otonomi biçimlerine yaklaşmış olabileceğini yazmaktadır; bu, sahadaki teknolojik eşiklerin çok hızlı kaydığını göstermektedir (Bondar, 2026). Buna paralel olarak OHCHR, 2025 boyunca kısa menzilli dron saldırılarının sivil kayıplarda önemli pay aldığını; Reuters ise Rus elektronik harbinin Ukrayna dronlarını rotadan saptırarak Romanya limanı ve Baltık hava sahası gibi NATO alanlarına taşabildiğini aktarmıştır (OHCHR, 2025a, 2025b; Reuters, 2026).

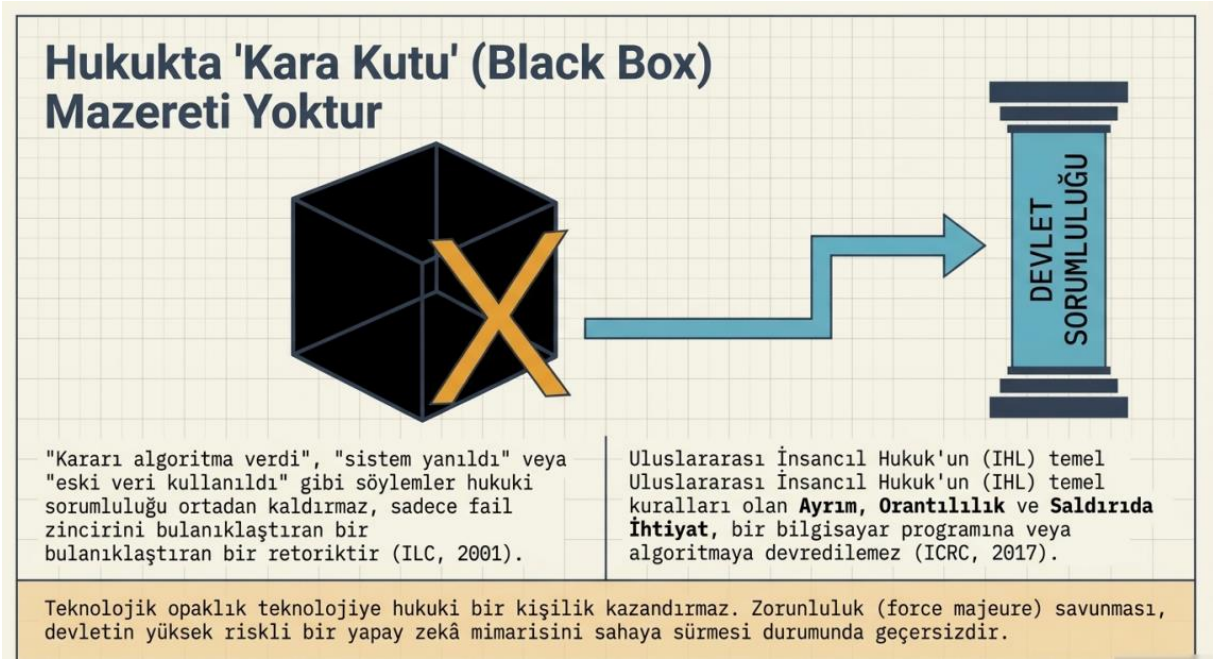
> *Ukrayna dersinin özü şudur: yapay zekâ bugünden savaşın tempo, maliyet ve erişim mantığını değiştirmiştir; ancak aynı zamanda öngörülemezlik ve sınır aşan hata riskleri üretmiştir (Bondar, 2025, 2026).*

Yapay zekâ uygulamaları ve uluslararası hukukta devlet sorumluluğu

Uluslararası insancıl hukuk bakımından temel nokta nettir: ayrım, orantılılık ve saldırıda ihtiyat kuralları yapay zekâ nedeniyle askıya alınmaz. ICRC, otonom silahlar ve ilgili sistemler bağlamında IHL yükümlülüklerinin ve bunlara ilişkin hesap verebilirliğin makineye, bilgisayar programına veya silah sistemine devredilemeyeceğini açıkça söylemektedir; ayrıca yeni silah, araç ve yöntemlerin silahlı kuvvetlere sokulmadan önce Ek Protokol I madde 36 uyarınca hukukî incelemeden geçirilmesi gerektiğini hatırlatmaktadır (ICRC, 2017, 2020). Aynı nedenle ICRC ve BM Genel Sekreteri, insan kontrolünün ölüm-kalım kararlarında korunmasını, öngörülemez etkiler doğuran otonom sistemlerin yasaklanmasını ve diğer sistemler için açık sınırlamalar getirilmesini talep etmektedir (ICRC, 2023).

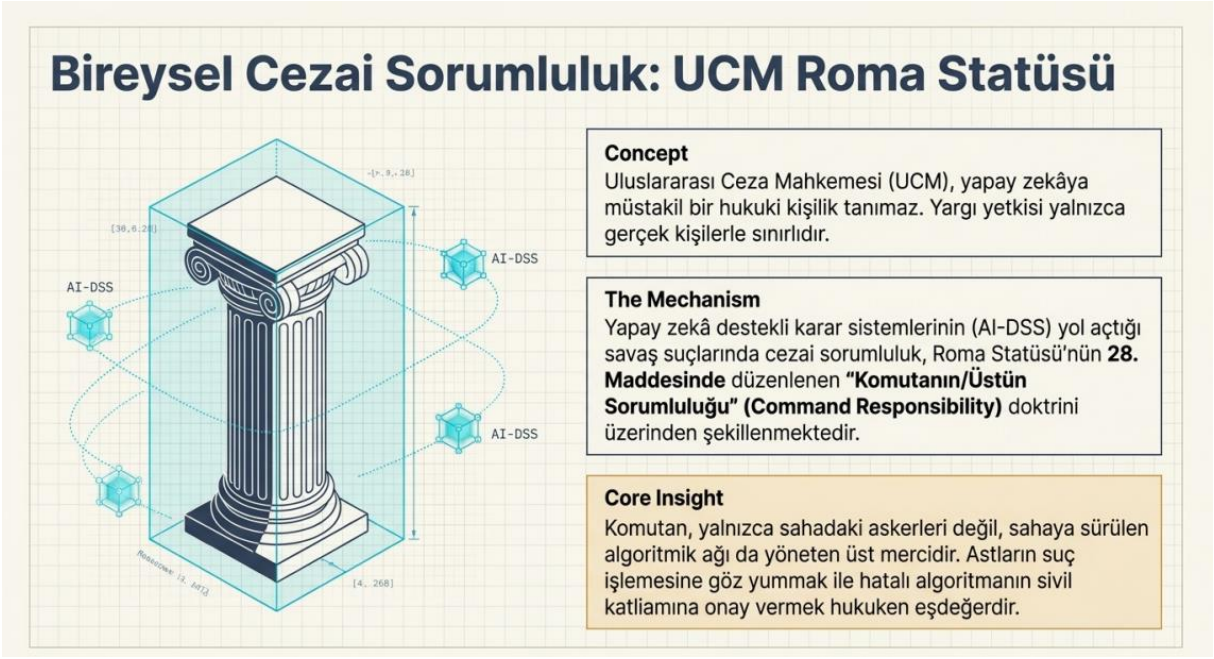


Mevcut hukuk, boşluklardan bağımsız olarak uygulanır; mesele, bu hukukun hız, opaklık ve çok-aktörlü dijital ekosistemler altında nasıl icra edileceğidir (ICRC, 2017, 2020, 2023).



ARSIWA bakımından da "AI yaptı" savunması normatif düzeyde ikna edici değildir. Uluslararası Hukuk Komisyonu'nun metnine göre bir devletin uluslararası hukuka aykırı fiilinden söz edebilmek için iki unsur yeterlidir: fiilin devlete atfedilebilir olması ve devletin bir uluslararası yükümlülüğünü ihlal etmesi (ILC, 2001, md. 2). Devlet organlarının davranışı devlete atfedilir (md. 4); kamu yetkisi kullanan fakat klasik anlamda organ olmayan kişi veya kuruluşların davranışı da belirli koşullarda devlete atfedilir (md. 5); organların talimatı aşması veya emre aykırı hareket etmesi atfedilebilirliği ortadan kaldırmaz (md. 7); devletin talimatı, yönlendirmesi veya kontrolü altındaki kişi ya da grupların davranışı da devlete bağlanabilir (md. 8) (ILC, 2001). Dolayısıyla atfedilebilirlik sorunu, çoğu durumda hukukî değil ispatî bir sorundur: log kayıtlarına, veri akışına, eğitim setine, kurumsal emir zincirine, tedarik sözleşmelerine ve operasyonel onay mekanizmasına erişim zor olabilir; ama bu güçlük teknolojiye bir tür hukukî kişilik kazandırmaz (ILC, 2001; ICRC, 2017).

Uluslararası Ceza Mahkemesi (UCM) Roma Statüsü, yapay zekaya (YZ) müstakil bir hukuki kişilik veya cezai ehliyet tanımadığı için UCM yargı yetkisi yalnızca gerçek kişilerle sınırlıdır. Bu bağlamda, yapay zeka destekli karar sistemlerinin (AI-DSS) veya otonom silahların yol açtığı savaş suçlarında bireysel cezai sorumluluğun tespiti, **Roma Statüsü'nün 28. maddesinde** düzenlenen **"Komutanın/Üstün Sorumluluğu" (Command/Superior Responsibility)** doktrini üzerinden şekillenmektedir.



Özellikle Gazze (Lavender, Habsora) ve Ukrayna gibi modern savaş arenalarından elde edilen hukuki çıktılarla birlikte, UCM savcılığı ve uluslararası hukuk doktrini 2026 yılı itibarıyla komutanların sorumluluğunu şu üç ana unsur ve güncel içtihat eğilimleri çerçevesinde ele almaktadır:

1. "Etkin Kontrol" (Effective Control) Kavramının Yeniden Yorumlanması

Geleneksel içtihatta (örneğin UCM'nin *Bemba* davası), bir komutanın sorumluluğu astları üzerinde **"fiili kontrol/etkin komuta"** yeteneğine sahip olmasına bağlanmıştır. Yapay zekâ çağında ise bu kavram "insan unsuru" dışına taşarak **teknolojik altyapı üzerindeki kontrolü** de kapsayacak şekilde genişlemektedir:

- **Makine Üzerinde Etkin Kontrol:** Eğer bir komutan, sahadaki otonom sistemin veya hedef önerme algoritmasının (AI-DSS) parametrelerini değiştirme, sistemi kapatma veya iptal etme (kill-switch/override) yetkisine sahipse, o sistem üzerinde "etkin kontrole" sahip kabul edilmektedir. [1]
- **Görünüşte Karar Verici Olmak:** Komutanlar, yapay zekanın sunduğu hedef önerilerini (örneğin Lavender listelerini) doğrulamak için sadece 20 saniye gibi çok kısa süreler ayırıp doğrudan onay veriyorlarsa, bu durum "etkin kontrolün" ihmal edildiği anlamına gelir. UCM savcılığının hazırlık çalışmalarındaki eğilim, sistemin körü körüne takip edilmesini komuta zaafiyeti ve görevi kötüye kullanma (failure to exercise control properly) olarak nitelendirmektedir.

2. Kusur Standardı: "Bilmeliydi" (Should Have Known) Kriteri

Roma Statüsü Madde 28(a)(i), komutanın astlarının suç işlediğini/işleyeceğini "bildiği veya eldeki koşullar uyarınca bilmesi gerektiği" durumları cezalandırır. Yapay zekâ sistemlerinde bu unsur "Algoritmik Öngörülebilirlik" üzerinden test edilmelidir.

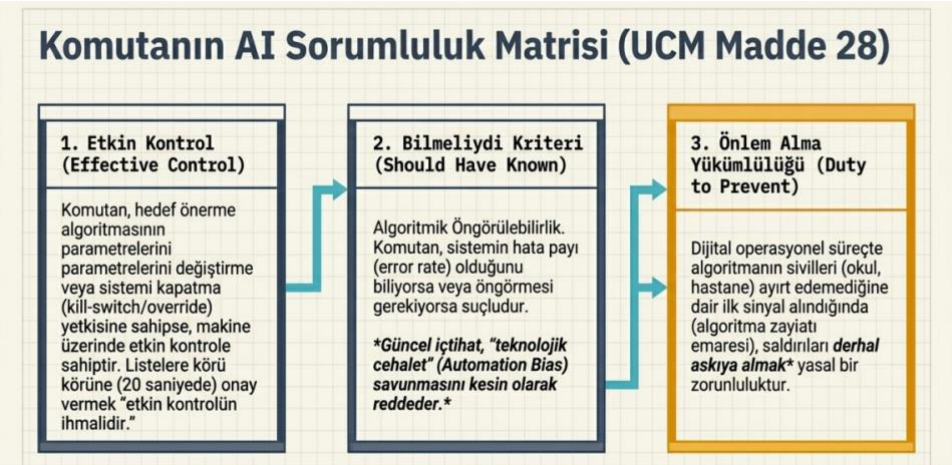
- **Kara Kutu (Black Box) ve Risk Kabulü:** Bir komutan, yapay zekanın "hata payı" (error rate) olduğunu ve sivil yerleşim yerlerinde yüksek zayiata neden olabileceğini (örneğin "Algoritmik Rasyonalizasyon" skorlarını) biliyor veya öngörebiliyorsa, sistemi sahaya sürmesi doğrudan kusur teşkil eder.
- **Teknolojik Cehalet Savunması:** Güncel UCM içtihat eğilimi, komutanların "Sistemin algoritmasını veya nasıl çalıştığını anlamıyordum, yapay zekâ hata yaptı" şeklindeki savunmalarını (automation bias / teknolojik cehalet) kesin olarak reddetmektedir. Komutan, konuşlandırdığı silah sisteminin doğuracağı sonuçları bilmekle ve "gerekli özeni" (due diligence) göstermekle yükümlüdür.

3. Gerekli ve Makul Önlemleri Alma Yükümlülüğü

Madde 28(a)(ii) uyarınca komutan, suçları önlemek, durdurmak veya yetkili makamlara bildirmek için "gerekli ve makul tüm önlemleri" almak zorundadır. Yapay zekâ kullanımında bu önlemler dijital operasyonel süreçleri kapsar:

- **Sistemi Kapatma Yükümlülüğü:** Algoritmanın sivil hedefleri (ilkokul, hastane, mülteci kampı) ayırt edemediğine dair ilk sinyal alındığında (yani bir "algoritma zayiatı" emaresi doğduğunda), komutanın saldırıyı derhal askıya alması veya iptal etmesi yasal bir zorunluluktur. [6]
- **Denetim Eksikliği:** Sistemin ürettiği hedef verilerinin doğruluğunu (insan istihbaratı gibi yan kaynaklarla) teyit etmeden doğrudan ateş emri verilmesi, "makul önlemleri almama" fiili olarak değerlendirilmekte ve komutanı bireysel olarak savaş suçundan mahkûm edebilmektedir.[7]

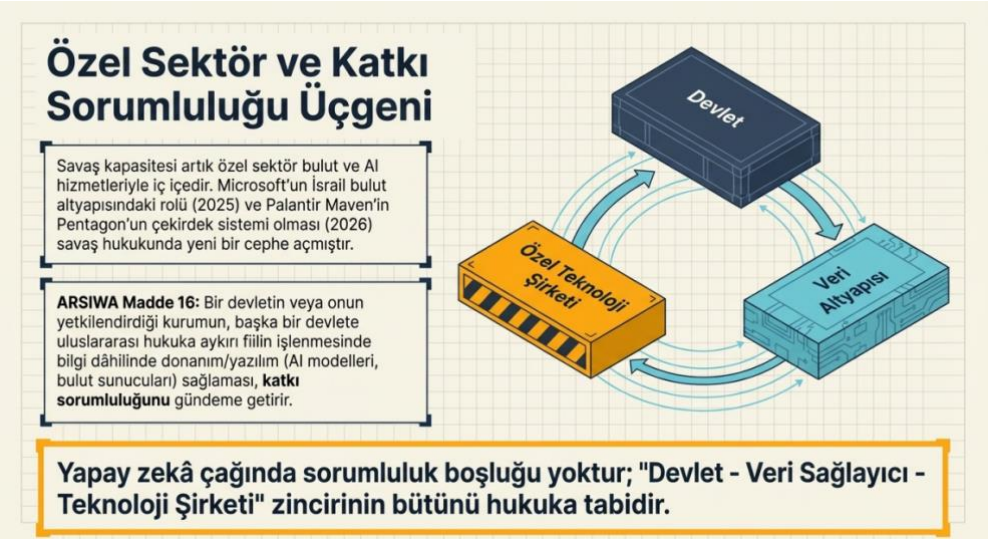
Bu nedenle, konutların, okulların veya sığınakların “algoritmik hata” sonucunda vurulduğu ileri sürüldüğünde, uluslararası hukuk bakımından asıl bakılması gereken teknikteki hata değil, o teknik mimariyi kimin kurduğu, test ettiği, onayladığı, satın aldığı, sahaya sürdüğü ve kullanma usullerini belirlediğidir. ARSIWA madde 31 uyarınca sorumlu devlet, doğan zararın tamamı için tam giderim sağlamak zorundadır; maddi ve manevi zarar bu kapsamdadır. Madde 30 ihlalin durdurulmasını ve tekrar etmeyeceğine dair güvence verilmesini, maddeler 34-37 ise iade, tazminat ve tatmini öngörür (ILC, 2001). Dahası, devlet kendi iç hukukunu veya kurumsal düzenini yahut “algoritma öneri sistemidir” gibi içsel kategorileri sorumluluktan kaçınmak için ileri süremez; madde 32 iç hukukun bu amaçla ileri sürülemeyeceğini açıkça söyler (ILC, 2001). Bu yüzden “kararı algoritma verdi” ifadesi, hukuken sorumluluğu ortadan kaldıran değil, olsa olsa fail zincirini bulanıklaştıran bir retoriktir (ILC, 2001; ICRC, 2017).



[6] https://www.icrc.org/sites/default/files/document/file_list/autonomous_weapon_systems_under_international_humanitarian_law.pdf
[7] Age.

Hatta devletin teknolojiye sığınarak “force majeure” veya “zorunluluk” benzeri söylemler üretmesi de çoğu durumda geçersizdir. ARSIWA madde 23, karşı konulamaz güç veya öngörülemez olay savunusunu devletin kendi davranışının duruma katkıda bulunduğu yahut riskin üstlenildiği hallerde daraltır; madde 25 ise devletin zorunluluk haline katkısı bulunduğunda bu savunmayı kapatır (ILC, 2001). Yüksek riskli, öngörülemezliği bilinen veya yeterli hukukî incelemeden geçmemiş bir AI destekli hedefleme mimarisini sahaya sürmek, devletin risk alanı içinde kalır. Bu yüzden algoritmik sistemlerin bulanıklığı devlet için bir mazeret değil; tam tersine ex ante test, doğrulama, kayıt tutma, insan denetimi ve ex post bağımsız soruşturma yükümlülüklerini daha da ağırlaştıran bir nedendir (ICRC, 2020; DoD, 2023).

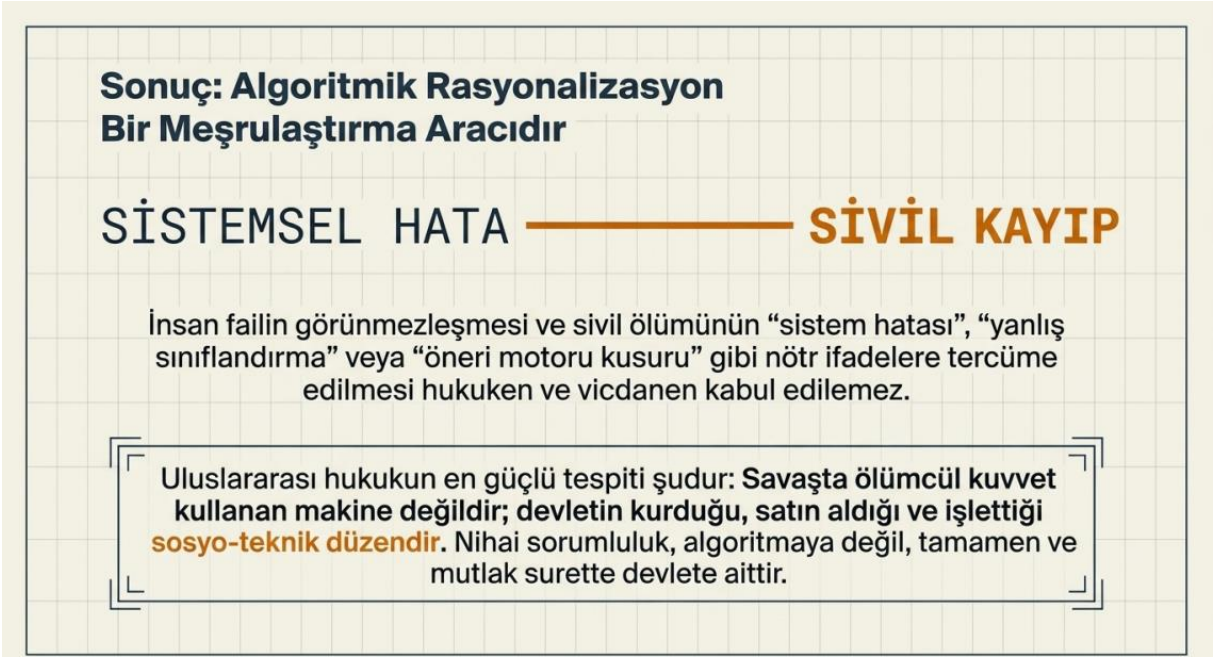
Özel şirketler ve üçüncü devletler meselesi de aynı sonuca çıkar. Microsoft’un 2025’te İsrail Savunma Bakanlığı’na bulut ve AI hizmetleri sunduğunu doğrulaması, ardından Eylül 2025’te bazı hizmetleri sivillerin kitlesel gözetimiyle ilişkili bulgular nedeniyle kesmesi; SIPRI’nin askerî AI tedarikini hukukî yükümlülüklerin icra mekanizması olarak görmesi; ve Reuters’ın Palantir Maven’i Pentagon’un çekirdek silah hedefleme altyapısı olarak tanımlaması, savaş hukukunda artık **“devlet - özel teknoloji sağlayıcısı - veri altyapısı”** bileşiminin dikkate alınması gerektiğini gösterir (Microsoft, 2025a, 2025b; Goussac & Boulanin, 2026; Jeans, 2026). ARSIWA madde 16 uyarınca bir devletin başka bir devlete uluslararası hukuka aykırı fiilin işlenmesinde bilgi dâhilinde yardım veya destek sağlaması halinde katkı sorumluluğu da gündeme gelebilir (ILC, 2001). Bu nedenle yapay zekâ çağında sorumluluk boşluğu yoktur; asıl boşluk şeffaflık, delillendirme ve zorunlu uluslararası standartlar alanındadır (ILC, 2001; Le Poidevin, 2026).



Sonuç

Sonuç olarak yapay zekâ, savaşı yalnızca daha hızlı ve daha “akıllı” kılmamaktadır; savaşın ahlaki mimarisini de dönüştürmektedir. Türkoğlu’nun sezgisel olarak işaret ettiği “algoritma zayiatı”, hukuk diliyle ifade edildiğinde, insan failin görünmezleşmesi ve sivil ölümünün “sistem hatası”, “yanlış sınıflandırma”, “eski veri”, “öneri motoru”, “değerlendirme kusuru” gibi nötrleşmiş ifadelere tercüme edilmesidir (Türkoğlu, 2026). Oysa Gazze’de konutlardaki aile ölümleri, okullara yönelik saldırılar ve Minab’daki kız okulunun vurulması bize aynı şeyi hatırlatmaktadır: sistemsel hataların bedelini algoritmalar değil, masum siviller ve çocuklar öder (OHCHR, 2024a; UNICEF, 2024; Stewart, 2026a). Bu koşullarda “algoritmik rasyonalizasyon”, hukuki ve vicdani sorumluluğun yerine geçmeye çalışan bir meşrulaştırma söylemidir; kabul edilmemelidir (Türkoğlu, 2026; ICRC, 2025).

Devletin sorumluluğu tam da burada merkezî hale gelir. Devlet, öldürücü veya hedefleme destekli AI sistemlerini yalnızca satın alan bir müşteri değil; bunların hukukî incelemesini yapan, harekât doktrinini belirleyen, insan-makine iş bölümünü tasarlayan, kayıt ve denetim rejimini kuran ve ihlal halinde soruşturma ile onarımı gerçekleştiren asli yükümlüdür. Bu nedenle devletler için asgari yükümlülük seti şunları içermelidir: gerçek anlamda bağımsız ve çok disiplinli madde 36 incelemeleri; hedefleme sistemlerinde zorunlu kayıt ve denetim izi; sivil zarar sonrası kamuya açıklanabilir olay kayıtları; konutlar, okullar ve hastaneler gibi korunan alanlar bakımından yükseltilmiş insan doğrulaması; özel sektör tedarik sözleşmelerine hukukî şeffaflık ve denetlenebilirlik şartları; ve ihlal halinde tam tazmin, tatmin ve tekrar etmeme güvenceleri (ICRC, 2020, 2023; DoD, 2023; Goussac & Boulanin, 2026; ILC, 2001). Bunlar tercihe bağlı "iyi uygulama"lar değil, devletin yapay zekâ çağında hukuka bağlı kalmasının ön koşullarıdır (ILC, 2001; Goussac & Boulanin, 2026).



Mevcut hukuk tüm soruları çözmemektedir. Reuters'ın da aktardığı üzere, 2026 itibarıyla birçok devlet IHL'nin uygulandığını kabul etse de otonom silahlar için bağlayıcı, ayrıntılı ve küresel standartlar fiilen yoktur; CCW müzakerelerinde ilerleme yavaştır ve yeni bir bağlayıcı araç hedefinin 2026 içinde tamamlanması gerçekçi görünmemektedir (Le Poidevin, 2026). Dahası, kamuya açık kayıtlar çoğu olayda model kartlarına, eğitim verilerine, hedef puanlama mantığına, operasyon günlüklerine ve kapalı hukukî inceleme dosyalarına erişim vermemektedir; bu da kesin hukukî nitelendirmeyi zorlaştırmaktadır. Fakat bu epistemik eksiklikler, atfedilebilirliği ve devlet sorumluluğunu ortadan kaldırmaz. Tam tersine, uluslararası hukuk bakımından en güçlü sonuç şudur: savaşta ölümcül kuvvet kullanan makine değil, devletin kurduğu ve işlettiği sosyo-teknik düzendir; dolayısıyla sorumlu olan da nihayetinde devlettir (ICRC, 2017; ILC, 2001; Le Poidevin, 2026).

Metin İçinde Geçen Kısaltmalar

- **ICRC: International Committee of the Red Cross**
- **SIPRI: Stockholm International Peace Research Institute**
- **CSIS: Center for Strategic and International Studies**
- **OHCHR: Office of the United Nations High Commissioner for Human Rights**
- **ILC: International Law Commission**
- **AI-DSS: Artificial Intelligence-Based Decision Support Systems**
- **ARSIWA: Articles on Responsibility of States for Internationally Wrongful Acts**
- **CCW: Convention on Certain Conventional Weapons**

Kaynakça

- **Blanchard, A., & Bruun, L. (2024). Bias in military artificial intelligence. Stockholm International Peace Research Institute.**
- **Bondar, K. (2025). Ukraine's future vision and current capabilities for waging AI-enabled autonomous warfare. Center for Strategic and International Studies.**
- **Bondar, K. (2026). How Russia is building a sovereign drone ecosystem for AI-driven autonomy. Center for Strategic and International Studies.**

- Cancian, M. (2026, June 2). What is Maven Smart System, and what does it do? Center for Strategic and International Studies.
- Coco, A., & de Souza Dias, T. (2023). Exploring the impact of automation bias and complacency on individual criminal responsibility in warfare. Journal of International Criminal Justice, 21(5), 1077–1096.
- Goussac, N., & Boulanin, V. (2026). Responsible procurement of military artificial intelligence. Stockholm International Peace Research Institute.
- Human Rights Watch. (2024, September 10). Gaza: Israeli military's digital tools risk civilian harm.
- International Committee of the Red Cross. (2017). Autonomous weapon systems under international humanitarian law.
- International Committee of the Red Cross. (2020). Legal review of new weapons.
- International Committee of the Red Cross. (2023, October 5). Joint call by the United Nations Secretary-General and the President of the International Committee of the Red Cross for States to establish new prohibitions and restrictions on autonomous weapon systems.
- International Committee of the Red Cross. (2025, May 12). Preserving human control over the use of force: A call to regulate lethal autonomous weapon systems under international law.
- International Committee of the Red Cross. (2026a, March 3). Autonomous weapon systems and international humanitarian law: Selected issues.
- International Law Commission. (2001). Responsibility of States for internationally wrongful acts.
- Israel Defense Forces. (2024, June 18). The IDF's use of data technologies in intelligence processing.
- Jeans, D. (2026, March 20). Pentagon to adopt Palantir AI as core U.S. military system, memo says. Reuters.
- Le Poidevin, O. (2026, March 3). Progress on rules for lethal autonomous weapons urgently needed, says chair of Geneva talks. Reuters.
- Microsoft. (2025a, May 15). Microsoft statement on the issues relating to technology services in Israel and Gaza.
- Microsoft. (2025b, September 25). Update on ongoing Microsoft review.
- NATO. (2024, July 10). Summary of NATO's revised Artificial Intelligence strategy.
- Office of the United Nations High Commissioner for Human Rights. (2024a). Six-month update report on the human rights situation in Gaza: 1 November 2023 to 30 April 2024.
- Office of the United Nations High Commissioner for Human Rights. (2025a). Protection of civilians in armed conflict — April 2025.
- Office of the United Nations High Commissioner for Human Rights. (2025b). Protection of civilians in armed conflict — September 2025.
- Reuters. (2024a, April 15). Israel says it shot down Iranian salvo "shoulder-to-shoulder" with U.S.
- Reuters. (2025, November 29). Ukrainian drone pilots look to AI for battlefield edge.
- Reuters Fact Check. (2026, March 10). Video of "Iran missile barrage" on Tel Aviv is AI-generated, say experts.
- Reuters Institute for the Study of Journalism. (2026, May 4). Trolling, memes and deepfakes: How AI is thickening the fog of war.
- Stewart, P. (2025, April 27). World military spending hits $2.7 trillion in record 2024 surge. Reuters.
- Stewart, P. (2026a, March 6). U.S. investigation points to likely U.S. responsibility in Iran school strike, sources say. Reuters.
- Stewart, P. (2026b, March 12). Bombed Iranian girls school had vivid website and yearslong online presence. Reuters.
- Türkoğlu, T. (2026, April 3). Algoritma zayiatı. TTDijital.
- UNICEF. (2024, November 8). Regular attacks put Gaza schools-turned-shelters on the frontlines of war.
- U.S. Department of Defense. (2020, February 25). DOD adopts 5 principles of artificial intelligence ethics.
- U.S. Department of Defense. (2023, January 25). DoD Directive 3000.09: Autonomy in weapon systems.
- U.S. Department of Defense. (2024). Responsible Artificial Intelligence strategy and implementation pathway.