2BLACKDOT••

“Esasen konu hep 2 nokta arasındadır”

Haftalık

Politik ve Jeopolitik

Gelişmeler

7 Eylül 2026 – Sayı 125

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:

Haftalık Politik ve Jeopolitik Gelişmeler
7 Eylül 2026 • Sayı 125

DAHA
GENİŞ PERSPEKTİF
DAHA SAĞLAM
KARARLAR

LEIPZIG SALDIRI GİRİŞİMİ: HİBRİT SAVAŞTAN OTONOM SİLAHLARA

GÜVENLİK
HUKUK
TEKNOLOJİ
İSTİKRAR

DAHA GÜVENLİ YARINLAR İÇİN, VERİYE DAYALI ANALİZ

ANA MESAJ

Leipzig/Halle vakası yalnızca bir havalimanı güvenliği olayı değil; failin gizlendiği, ticari teknolojinin askerîleştirildiği ve sorumluluğun devlet–şirket–algoritma arasında parçalandığı yeni savaş mimarisinin uyarısıdır.

OLAYIN SEYRİ

1. **4–5 Ağu.** Patlayıcı yüklü İHA bulundu; uçuşlar yaklaşık 2 saat durdu.
2. **7 Ağu.** Alman Ulusal Güvenlik Konseyi toplandı.
3. **1–4 Eyl.** Almanya, çok kaynaklı inceleme sonrası Rusya'yı sorumlu tuttu.
4. **6 Eyl.** Açik kaynaklarda komuta ve etkin kontrol zinciri henüz bütünüyle görünür değil.

HUKUKİ EŞİK

ARSIWA m. 8'e göre benzer yöntem veya Rus ekipmanı tek başına yetmez; talimat, yönlendirme ya da etkin kontrol gösterilmelidir.

Atıf ≠ ihlal ≠ silahlı saldırı ≠ NATO Madde 5

OTONOM SİLAHLARA GEÇİŞ

Ukrayna savaşı; bağlantısız uçuş, makine görüşü, otomatik takip ve hedef seçimine yaklaşan sistemleri hızlandırıyor.

Her drone LAWS değildir. Kritik ayrım: hedefi kim seçiyor ve insan saldırıyı gerçekten iptal edebiliyor mu?

DÜZENLEME BOŞLUĞU

BM'de bağlayıcı ve evrensel insan-kontrollü sınırı henüz yok.

Mevcut hukuk; ayrım, orantılılık, tedbir, devlet sorumluluğu ve yeni silah incelemesini zaten gerektiriyor.

5 KRİTİK RİSK

Ayrım hatası • Orantısız zarar • Sistematik ölçek hatası • Hızlı tırmanma • Hesap verebilirlik boşluğu

KARAR VERİCİ İÇİN 5 ÖNCELİK

1. Kamuya açıklanabilir asgari atıf dosyası
2. NATO için ortak hukuki eşik matrisi
3. Anlamlı insan kontrolü ve etkin iptal yetkisi
4. Her önemli yazılım/model güncellemesinde m. 36 incelemesi
5. Değiştirilemez görev logları ve tedarik zinciri durum tespiti

> ***Merkezi soru: Drone kime aitti değil; hedefi kim seçti, kim emretti, kim kontrol etti ve kime hesap sorulabilir?***

2blackdot & Tema • Yatırım tavsiyesi değildir.

DAHA İSTİKRARLI BİR DÜNYA MÜMKÜN

Jeopolitik ve Küresel Gelişmeler:

4–5 AĞUSTOS 2026 LEİPZİG/HALLE İHA SALDIRI GİRİŞİMİ RUSYA–UKRAYNA SAVAŞI VE ÖLÜMCÜL OTONOM SİLAH SİSTEMLERİNE DOĞRU GİDİŞ:

Hibrit Savaş, Küresel Savunma Sermayesi ve Devlet Sorumluluğu

Yönetici Özeti

Leipzig/Halle Havalimanı'nda 4–5 Ağustos 2026 gecesi bulunan patlayıcı yüklü insansız hava aracı, yalnızca Almanya bakımından bir havaalanı güvenliği vakası değildir.

> ***"Olay, klasik devletlerarası kuvvet kullanımının altında kalacak şekilde tasarlanan, göndericiyi gizleyen, aracılar ve ticari teknolojiler kullanan "inkâr edilebilir" operasyonların devlet sorumluluğu hukukunda nasıl değerlendirileceğine ilişkin güncel bir örnek oluşturmaktadır"***

Alman Federal Hükümeti, 1 Eylül 2026'da yaptığı siyasi-hukuki atıfta saldırı girişiminden **Rusya'yı açık biçimde sorumlu tutmuş**; 4 Eylül'de yayımlanan resmî açıklamada bu sonucun polis soruşturmaları, saldırı örüntüsü ve istihbarat bulgularının birlikte değerlendirilmesine dayandığını belirtmiştir (Bundesregierung, 2026a, 2026b).
Bununla birlikte, Alman Hükümeti kamusal atıf için kendisini yeterince emin gördüğünü açıklamış olsa da faillere ilişkin kimlikler, komuta/talimat zinciri, mali ve haberleşme bağlantıları, istihbaratın kaynağı ve adli materyalin tamamı kamuya açıklanmamıştır. Hükümet sözcüsü 2 Eylül'de özellikle hibrit operasyonların göndericiyi gizlemek üzere tasarlandığını, değerlendirmelerinin üç ayrı boyutta Rusya'ya işaret ettiğini, ancak devam eden soruşturma ile istihbarat kaynaklarının korunması nedeniyle tüm ayrıntıların açıklanamayacağını belirtmiştir (Bundesregierung, 2026b).

Devlet sorumluluğu açısından temel çerçeve, Uluslararası Hukuk Komisyonu'nun **Devletlerin Uluslararası Hukuka Aykırı Fiillerden Sorumluluğuna İlişkin Maddeleri**dir (ARSIWA). BM Genel Kurulu 56/83 sayılı kararla bu metni dikkate almış ve devletlerin dikkatine sunmuştur; metin henüz bağımsız bir sözleşme haline gelmemiştir ancak çok sayıda hükmü uluslararası teamül hukukunun kodifikasyonu veya gelişimi olarak mahkemelerce ve devletlerce kullanılmaktadır (BM Genel Kurulu, 2001; ILC, 2001). ARSIWA m. 2 uyarınca sorumluluk için iki soru birlikte cevaplanmalıdır: **Davranış devlete atfedilebilir mi ve bu davranış devletin uluslararası yükümlülüğünü ihlal etmiş midir?**

Leipzig vakasında kritik norm ARSIWA m. 8'dir. Fail doğrudan Rus devlet organı değil de istihbarat servisleri tarafından kullanılan düşük profilli bir aracı veya vekil ise, failin yalnızca "Rusya yanlısı" olması, Rus ekipmanı kullanması ya da operasyonun Rus yöntemlerine benzemesi hukuki atıf için tek başına yeterli değildir. Devletin **talimatı, yönlendirmesi veya kontrolü** gösterilmelidir. Uluslararası Adalet Divanı'nın *Nicaragua* ve *Bosnia Genocide* kararları, belirli hukuka aykırı operasyon bakımından "etkin kontrol" bağlantısının önemini ortaya koymaktadır (ICJ, 1986, 2007).

Bu nedenle mevcut açık kaynaklarla en savunulabilir sonuç şudur: **Rus sorumluluğuna ilişkin Alman atfı ciddi ve çok kaynaklıdır; fakat ARSIWA m. 8 anlamında yargısal ispata elverişli "etkin kontrol/talimat" zincirinin tamamı kamusal dosyada henüz görülmemektedir.** Kamuya kapalı Alman istihbaratı gerçekten ilgili kişilerin Rus devlet makamları adına hareket ettiğini ve belirli Leipzig operasyonunun yönlendirildiğini ortaya koyuyorsa, m. 8 eşiğinin aşılması mümkündür. Buna karşılık yalnızca kullanılan bileşenlerin, patlayıcının veya operasyonel yöntemin daha önce Rus faaliyetlerinde görülmüş olması hukuken tek başına yeterli değildir. BM'nin siber alanda geliştirdiği atıf yaklaşımı da analoji yoluyla önemlidir: bir operasyonun belirli bir devletin topraklarından veya altyapısından kaynaklanması tek başına devlet atfı için yeterli olmayabilir ve suçlamalar temellendirilmelidir (BM GGE, 2015, A/70/174).

Leipzig operasyonunun Rusya'ya atfedilmesi halinde ikinci mesele ihlal edilen "birincil kural"dır. Bir başka devletin topraklarında patlayıcı yüklü İHA aracılığıyla kritik sivil/çift kullanımlı havacılık altyapısına saldırı yürütülmesi Almanya'nın **egemenliğine aykırılık** oluşturur; koşullara göre BM Şartı m. 2(4) anlamında **kuvvet kullanımı** olarak da nitelendirilebilir. Bununla birlikte "kuvvet kullanımı" ile m. 51 anlamındaki daha yüksek eşikli **silahlı saldırı** aynı değildir. Başarısız bırakılmış ve sınırlı fiziksel etkiye sahip tek Leipzig operasyonunun mevcut açık bilgilerle Almanya'ya silahlı kuvvet kullanarak meşru müdafaa hakkı veren bir "silahlı saldırı" eşiğine ulaştığını söylemek güçtür. NATO da hibrit faaliyetlerin bazı şartlarda silahlı saldırı seviyesine ulaşabileceğini, fakat bunun **vaka bazında** değerlendirileceğini belirtmektedir (NATO, 2023, 2025).

> ***"Otonom silahlar bakımından Rusya–Ukrayna savaşı, uzaktan kumandalı İHA savaşından sensör-temelli seyrüsefer, makine görüşü, elektronik harp altında bağlantısız uçuş, otomatik hedef takibi ve giderek hedef seçimine yaklaşan sistemlere geçişi hızlandırmaktadır"***

Ancak bütün dronları "LAWS"[1] olarak nitelendirmek yanlıştır. Ukrayna'nın 2026'da savaşta denediğini açıkladığı bazı önleme sistemlerinde operatör hedefi seçmekte, sistem uçuş ve son yaklaşmayı otomatik gerçekleştirmekte, insan ise saldırıyı iptal edebilmektedir; bu, yüksek otomasyon ve gözetimli otonomi olmakla birlikte, insanın hedef seçme kararından tamamen çıkarıldığı bir sistem değildir (Brave1, 2026). Rus V2U gibi sistemlerde ise açık kaynak değerlendirmeleri, yerleşik bilgisayarlı görü ile hedef arama, tanıma ve seçme kabiliyetlerinin daha ileri bir otonomiye yaklaştığını öne sürmektedir; fakat bu performans iddialarının bir bölümü Ukrayna kaynakları ve savaş alanı adli incelemelerine dayandığından bağımsız doğrulama sorunu vardır (Bondar, 2026)[2].

BM düzeyindeki normatif eğilim açıktır. Genel Kurul 2023'te A/RES/78/241, 2024'te A/RES/79/62 ve 2025'te A/RES/80/57 kararlarıyla otonom silahların risklerini gündemde tutmuştur. A/RES/80/57, 164 lehte, 6 aleyhte ve 7 çekimser oyla kabul edilmiş; Rusya ve ABD aleyhte oy kullanan devletler arasında yer almıştır. Bu oy davranışı tek başına bu devletlerin "otonom öldürmeyi desteklediği" anlamına gelmese de metin ve düzenleme yöntemi üzerindeki devlet farklılıkları nettir. BM Genel Sekreteri ise insan kontrolü olmaksızın yaşam ve ölüm kararı veren sistemleri kabul edilemez görerek **2026'ya kadar hukuken bağlayıcı bir araç** oluşturulması çağrısını yinelemiştir (BM Genel Kurulu, 2023, 2024, 2025; UNODA, 2025).

6 Eylül 2026 itibarıyla CCW (Birleşmiş Milletler bünyesinde 1980 yılında imzaya açılan ve tam adı **Certain Conventional Weapons** olan **Belirli Konvansiyonel Silahlar Sözleşmesi**) bünyesindeki LAWS Hükümet Uzmanları Grubu'nun ikinci 2026 oturumu henüz **4 Eylül'de sona ermiştir**. Resmi UNODA(Birleşmiş Milletler bünyesinde faaliyet gösteren **United Nations Office for Disarmament Affairs** yani **Birleşmiş Milletler Silahsızlanma İşleri Ofisi)** sayfasında araştırma kesim tarihi itibarıyla yeni bir bağlayıcı protokol yürürlüğe girmiş görünmemektedir; süreç 2026 CCW Gözden Geçirme Konferansı yönünde ilerlemektedir (UNODA, 2026). Ayrım, orantılılık, saldırıda tedbir, insan hakları, devlet sorumluluğu ve yeni silahların hukuki incelemesi yükümlülükleri halihazırda uygulansa da asıl boşluk, otonom hedef seçimine **özel, açık ve evrensel insan-kontrolü sınırların** henüz bağlayıcı biçimde kodifiye edilmemiş olmasıdır.

---

[1] **LAWS, uluslararası güvenlik ve askeri literatürde Lethal Autonomous Weapons Systems (Ölümcül Otonom Silah Sistemleri) ifadesinin kısaltmasıdır. Halk arasında "Katil Robotlar" (Killer Robots) olarak da bilinen bu sistemler, yapay zekâ algoritmaları kullanarak, insan müdahalesi veya onayı olmadan hedefleri seçme, tespit etme ve üzerlerine ölümcül kuvvet uygulama yeteneğine sahip silahlardır.**

[2] **İnsan Kontrolünün Dereceleri (Human Control)**

Sistemler, insanın karar mekanizmasındaki yerine göre üç gruba ayrılır:

- **Human-in-the-Loop (Döngüde İnsan): Silah hedefi seçer ancak ateş etme/vurma kararını ve son onayı mutlaka bir insan verir (Örn: Bayraktar TB2/TB3 veya MQ-9 Reaper gibi uzaktan kumandalı İHA'lar).**
- **Human-on-the-Loop (Döngü üstünde İnsan): Silah otonom olarak çalışır, hedefi bulur ve vurur; ancak insan sistemi izler ve bir hata durumunda operasyonu iptal etme (müdahale etme) yetkisine sahiptir (Örn: Patriot veya SAMP/T hava savunma sistemleri).**
- **Human-out-of-the-Loop (Döngü Dışında İnsan - Gerçek LAWS): İnsanın sistem üzerinde hiçbir denetimi veya iptal yetkisi yoktur. Yapay zekâ algoritması kendi algoritmasıyla hedefi seçer, kilitlenir ve imha eder.**

Ukrayna sahasında yoğun olarak kullanılan elektronik harp (sinyal karıştırma) yöntemleri, dronların merkezle (insan operatörle) olan bağını kopardığı için iki taraf da zorunlu olarak Human-out-of-the-Loop sistemlere geçiş yapmıştır. Ukrayna'da kullanılan "Linza 3.0" [2] veya müttefiklerin geliştirdiği derin taarruz İHA'ları, sinyal kopsa dahi nesne tanıma (object recognition) algoritmalarıyla hedefi bulup otonom olarak vurabilmektedir. Uluslararası Hukuk ve Etik Tartışmalar

Birleşmiş Milletler (BM) Genel Kurulu'nun kabul ettiği A/RES/79/152 sayılı kararla, LAWS sistemlerine yönelik tanımlamalar sıkılaştırılmıştır:

- **Ayırt Etme (Distinction) İhlali: Yapay zekanın savaşçı ile sivili, teslim olan asker ile savaşmaya devam edeni ayırt etme yeteneğinin kusursuz olmadığı savunulmaktadır.**
- **Ahlaki Sorumluluk: Bir makinenin insan hayatı üzerinde ölüm kararı vermesi BM Genel Sekreteri António Guterres tarafından "ahlaken kabul edilemez" olarak nitelendirilmiş ve en geç 2026 yılına kadar bu silahların tamamen otonom olanlarının yasaklanması çağrısı yapılmıştır.**

Olayın Maddi Arka Planı[3],[4]

Alman Federal Hükümeti'nin güncellenmiş resmi anlatımına göre Leipzig/Halle Havalimanı'ndaki güvenlik olayı 4 Ağustos'u 5 Ağustos 2026'ya bağlayan gece gerçekleşmiştir. Patlayıcı taşıyan bir İHA'nın bulunması üzerine güvenlik operasyonu yürütülmüş; 5 Ağustos'taki ilk hükümet basın toplantısında havaalanındaki uçuş faaliyetlerinin yaklaşık 01.55'ten itibaren yaklaşık iki saat kesildiği, kuzey pistinin daha sonra açıldığı, güney pistinde Federal Polis çalışmalarının devam ettiği bildirilmiştir. İlk saatlerde hükümet olayın niteliği konusunda ihtiyatlı davranmış; sonraki resmî açıklamalarda İHA'nın patlayıcı yüklü olduğu teyit edilmiştir (Bundesregierung, 2026c).

[3] Olay Gecesi Ne Yaşandı? (4-5 Ağustos 2026)

- Antonov An-124 Yakınında Keşif: Havalimanı pistinde, Ukrayna ordusu ve NATO adına stratejik taşımacılık yapan Ukrayna'ya ait bir Antonov An-124 askeri nakliye kargo uçağının hemen yakınında patlayıcı yüklü, özel yapım bir quadcopter drone bulundu.
- Kıl Payı Atlatılan Felaket: Yapılan teknik incelemede, İHA'nın içine yerleştirilen askeri patlayıcının (Semtex/Hexogen) detonatöründeki (ateşleyici) teknik bir arıza sebebiyle patlamadığı, saldırının şans eseri başarısız olduğu anlaşıldı.
- Uçakla Çarpışma ve Kapanma: İlk dronun bulunmasının ardından havalimanı hava sahası sivil trafiğe kapatıldı. Kapatma kararı üzerine pas geçmek zorunda kalan bir DHL / Boeing 757 kargo uçağının, havada ikinci bir şüpheli cisimle/drone ile çarpıştığı ve hafif hasarla Hannover'e acil iniş yaptığı bildirildi.
- Üçüncü Drone: 14 Ağustos 2026'da havalimanının batı sınırında 50 gram askeri patlayıcıyla donatılmış üçüncü bir drone daha ele geçirildi.

[4] Bulgular ve Rusya'nın Suçlanması: Alman federal hükümeti ve istihbarat birimleri (BKA ve BfV), 1 Eylül 2026'da yaptıkları resmi açıklamada saldırı girişiminden doğrudan Rus askeri istihbaratı GRU'yu sorumlu tuttu.

- DNA İzleri Konserve Kutusunda: Olay yerinde ve İHA üzerindeki sinyal güçlendirici anten ile patlayıcının yerleştirildiği konserve kutusunun iç kısmında bulunan DNA örnekleri, faillerin kimliğini deşifre etti.
- İki Şüpheli Belirlendi: Zanlılardan birinin Letonya pasaportlu bir Rus vatandaşı (lojistik destek ve İHA eğitimi veren), diğerinin ise İtalya'dan aldığı turist vizesiyle Avrupa'ya sızan bir Belarus vatandaşı olduğu açıklandı.

Hükümetin resmi soru-cevap belgesine göre 7 Ağustos'ta Federal Şansölye başkanlığındaki Ulusal Güvenlik Konseyi olay üzerine telefonla toplanmıştır. Bu tarih önemlidir: Rusya'ya atıf olaydan hemen sonra yapılmamış, yaklaşık dört haftalık adli ve istihbari inceleme süreci beklenmiştir. 1 Eylül'de İçişleri Bakanı Alexander Dobrindt ve Dışişleri Bakanı Johann Wadephul, Federal Hükümetin Rusya'yı sorumlu tuttuğunu açıklamış; 2 Eylül hükümet basın toplantısında atfın yöntemsel temeli açıklanmış; 4 Eylül'de Federal Hükümet bunu kurumsal internet sayfasında **"Rusya'nın sorumlu olduğu hibrit saldırı"** olarak kesin biçimde kayda geçirmiştir (Bundesregierung, 2026a–c).

Federal Hükümetin açıkladığı atıf metodolojisi üç kümeye ayrılabilir.

- Birincisi, İHA'nın **teknik ve fiziksel özellikleri**dir: kullanılan araçlar, bileşenler, patlayıcı ve ateşleme/infial tekniği.
- İkincisi, bu yöntemin Avrupa'daki diğer Rus hibrit operasyonları ve Ukrayna savaşındaki yöntemlerle karşılaştırıldığı **operasyonel örüntü analizidir**.
- Üçüncüsü ve hukuken en önemlisi, olayda görev alan veya organizasyona katılan kişilerin Rus devlet aktörleri adına hareket ettiğine işaret ettiği söylenen **istihbarat bulgularıdır**. Alman makamları bu üç boyutun birlikte "açık" atıf sağladığını savunmaktadır (Bundesregierung, 2026a, 2026b).

Bununla birlikte açık kaynak dosyasında önemli belirsizlikler vardır. Alman makamları kamuoyuna fail kişilerin isimlerini, Rus kurumlarıyla irtibat kanallarını, talimat belgelerini, haberleşme kayıtlarını veya ödeme akışını açıklamamıştır. Hükümet bunu devam eden soruşturmaların ve istihbaratın kaynak-yöntem güvenliğinin korunmasıyla gerekçelendirmektedir. Dolayısıyla kamusal dosya **atfın gerekçesini** gösterirken, tüm **ispat materyalini** göstermemektedir.

Olayın hedefi konusunda da disiplinli bir ayrım gereklidir. Bazı medya haberleri saldırı girişimini havalimanındaki Ukrayna bağlantılı kargo/askerî lojistik faaliyetleriyle ilişkilendirmiştir; ancak kamuya açık resmi Alman metinleri olayın hedef seçme istihbaratının bütününü yayımlamamıştır. Bu nedenle "Ukrayna'ya silah taşıyan belirli bir Antonov'un kesin olarak hedef alındığı" önermesi, resmî açıklamaların ötesine geçen bir iddiadır. Rusya isnadı reddetmiştir.

Leipzig olayının bağlamının "Rus drone'u–Alman havaalanı" ikiliğinden ibaret olmadığını görmek gerekir. Rusya'nın Ukrayna'ya karşı kitlesel İHA kullanımı; Ukrayna'nın Batı ülkeleriyle ortak üretim, finansman ve teknoloji transferi;[5] NATO ülkelerindeki anti-drone yatırımları ve savunma teknoloji şirketlerinin hızla genişlemesi, **İHA üretimi–karşı-İHA–AI otonomisi–elektronik harp** ekseninde karşılıklı hızlanan bir güvenlik ikilemi yarattığı anlaşılmalıdır. Bu bağlamsal ilişki, Leipzig'in sorumluluk analizini değiştirmez; fakat neden böyle bir havaalanının hibrit sabotaj açısından stratejik değer taşıyabileceğini açıklamaya yardımcı olur.

Uluslararası Hukukta Devlet Sorumluluğu ve Birincil Kurallar

Devlet sorumluluğunda ilk yapılması gereken ayrım, **"atıf" ile "ihlal"i birbirinden ayırmaktır**. Bir devletin bir olaya politik olarak karışmış olması veya saldırganı desteklemiş olması otomatik olarak bütün davranışı o devlete atfetmez. ARSIWA m. 2'ye göre uluslararası hukuka aykırı devlet fiili, hem davranışın uluslararası hukuka göre devlete atfedilebilir olmasını hem de davranışın devletin uluslararası yükümlülüğüne aykırı olmasını gerektirir (ILC, 2001).

ARSIWA, 2001'de BM Genel Kurulunun **56/83 sayılı kararıyla** devletlerin dikkatine sunulmuştur. Genel Kurul daha sonraki 59/35, 62/61, 65/19, 68/104, 71/133, 74/180 ve 77/97 gibi kararlarla konuyu gündemde tutmuş; ancak 6 Eylül 2026 itibarıyla ARSIWA'nın tamamını bağlayıcı birçok taraflı sözleşmeye dönüştüren yeni bir antlaşma yürürlüğe girmemiştir. Bu sebeple maddelerin hukuki ağırlığı, ilgili hükmün teamül hukukunu ne ölçüde yansıttığına göre değerlendirilmektedir(BM Genel Kurulu, 2001; UN Sixth Committee, 2025).

ARSIWA m. 4 devlet organlarının davranışını doğrudan devlete bağlar. M. 5, devlet yetkisi kullanmak üzere yetkilendirilen kişi veya kuruluşları kapsar. Leipzig gibi gizli/vekâlet operasyonları bakımından merkezî hüküm m. 8'dir: özel kişi veya grubun davranışı, belirli davranışı gerçekleştirirken devletin **talimatları, yönlendirmesi veya kontrolü** altında ise devlete atfedilebilir. m. 11 ise başlangıçta özel bir kişi tarafından gerçekleştirilen davranışın daha sonra devlet tarafından kendi davranışı olarak açıkça kabul edilip benimsenmesi halinde atıf imkânı sağlar. m. 16, bir devletin başka bir devletin hukuka aykırı fiiline yardım veya destek sağlamasından doğan ayrı bir sorumluluk rejimi öngörmektedir (ILC, 2001).

[5] Ukrayna Cumhurbaşkanlığı, Şubat 2026'da Münih'teki Quantum Frontline Industries tesisini ilk Ukrayna–Almanya seri üretim ortak girişimi olarak tanımlamış ve yıl içinde 10.000 AI destekli saldırı İHA'sı üretme planını açıklamıştır (President of Ukraine, 2026a). Benzer şekilde 15 Temmuz 2026'da Ukrayna ve Avrupa Komisyonu bir "Drone Deal" yönünde ilk belgeyi imzalamış; 22 Temmuz'da Kiev, ABD ile gelecekteki Drone Deal üzerindeki çalışmanın sürdüğünü resmen açıklamıştır. Reuters da 24 Temmuz 2026'da Zelenskiy'nin ABD'de Ukrayna teknolojisiyle üretim tesisi oluşturma niyetini ve Ukraynalı üreticilerin Pentagon'un "Drone Dominance" programına katılımı üzerinde çalışıldığını bildirmiştir.

Sorumluluk doğduğunda m. 30 devam eden ihlalin durdurulmasını ve uygun koşullarda tekrar etmeme güvencelerini; m. 31 ise zararın tam giderimini öngörür. Giderim eski hale getirme, tazminat ve tatmin biçimleri alabilir. ARSIWA m. 49–54 karşı önlemleri düzenler; fakat karşı önlemler hukuka aykırı fiili sona erdirmeye ve yükümlülüğe dönüş sağlamaya yönelmeli, orantılı olmalı ve **kuvvet kullanma yasağını ihlal edilmemelidir** (ILC, 2001).

BM Şartı m. 2(4), devletlerin başka bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı tehdit veya kuvvet kullanmasını yasaklar; m. 51 ise "silahlı saldırı" halinde bireysel veya kolektif meşru müdafaa hakkını tanır. BM Genel Kurulunun **2625 (XXV) Dostane İlişkiler Bildirisi**, kuvvet kullanmama ve müdahale etmeme ilkelerini geliştirirken, **3314 (XXIX) Saldırganlığın Tanımı Kararı**, bir devlet adına silahlı grupların gönderilmesi veya devletin belirli ağırlıktaki silahlı eylemlere önemli ölçüde katılması gibi dolaylı yöntemleri de kuvvet kullanımı tartışmasının içine taşımıştır (BM Genel Kurulu, 1970, 1974).

Burada 3314 sayılı karar ile ARSIWA m. 8'i birbirine karıştırmamak gerekir. 3314'ün özellikle m. 3(g) yaklaşımı **saldırganlık/silahlı kuvvet** nitelemesine yardım eder; ARSIWA m. 8 ise davranışın devlete **hukuken atfedilip atfedilemeyeceğine** ilişkindir. Aynı olayda iki test kullanılabilir fakat aynı soruyu cevaplamazlar (ICJ, 1986; ILC, 2001).

Rusya–Ukrayna savaşının genel jus ad bellum çerçevesinde BM Genel Kurulunun **A/RES/ES-11/1** sayılı 2 Mart 2022 kararı Rusya'nın Ukrayna'ya yönelik saldırganlığını kınamış ve kuvvetlerin çekilmesini talep etmiştir; karar 141 lehte, 5 aleyhte, 35 çekimser oyla kabul edilmiştir. BMGK, 27 Şubat 2022 tarihli **2623 (2022)** sayılı kararla, 11 lehte, 1 aleyhte ve 3 çekimser oyla Genel Kurulun Olağanüstü Özel Oturumunu toplamıştır. Bu kararlar Leipzig'i otomatik biçimde Rus saldırganlığının hukuki bir "parçası" yapmaz; fakat Rusya–Ukrayna uyuşmazlığının BM sistemindeki resmî hukuki bağlamını oluştururlar.

24 Mart 2022 tarihli **A/RES/ES-11/2** ise saldırganlığın insani sonuçlarını ele almış ve uluslararası insancıl hukuk yükümlülüklerini tekrar vurgulamıştır. Genel Kurul kararları, Güvenlik Konseyinin BM Şartı Bölüm VII kapsamındaki bağlayıcı kararlarıyla aynı normatif nitelikte değildir; fakat devletlerin hukuki pozisyonlarını, opinio juris değerlendirmelerini ve mevcut hukuk kurallarının yorumlanmasını gösterebilirler.

Uluslararası insancıl hukuk bakımından iki ayrı düzlem vardır. Rusya ile Ukrayna arasında tartışmasız biçimde uluslararası silahlı çatışma bulunmaktadır. Fakat Almanya'nın Ukrayna'ya silah, finansman veya eğitim desteği sağlaması **tek başına** Almanya'yı Rusya ile silahlı çatışmanın tarafı haline getirmez. Leipzig operasyonunun Rus devletine atfedilen doğrudan bir silahlı kuvvet kullanımı olduğunun ortaya çıkması halinde Almanya–Rusya arasında uluslararası silahlı çatışma sınıflandırmasının doğup doğmadığı ayrıca değerlendirilmelidir; Cenevre Sözleşmeleri Ortak Madde 2'nin devletlerarası silahlı kuvvet kullanımına ilişkin düşük eşiği nedeniyle konu yalnızca Alman hükümetinin siyasi olarak "savaşta değiliz" demesiyle sonuçlandırılamaz. Alman Hükümeti 2 Eylül'de siyasi bağlamda Almanya'nın "savaşta olmadığını" özellikle vurgulamıştır; bu açıklama uluslararası insancıl hukuk sınıflandırmasının yerine geçen bir yargısal tespit değildir.

Otonom silahlar bakımından Ek Protokol I m. 36 özel önem taşır. Yeni bir silah, savaş aracı veya yöntemi araştıran, geliştiren, edinen ya da kabul eden taraf, kullanımının Ek Protokol veya kendisini bağlayan diğer uluslararası hukuk kuralları tarafından yasaklanıp yasaklanmadığını belirlemek zorundadır.

> ***"Bu nedenle yapay zekâ destekli hedefleme sistemleri için hukuki inceleme yalnızca seri üretimden sonra değil, tasarım–eğitim verisi–test–tedarik–yazılım güncellemesi–operasyonel kullanım yaşam döngüsünün tamamına yayılmalıdır (ICRC, 1977/2026)"***

Uluslararası insan hakları hukuku ise özellikle silahlı çatışma dışındaki ölümcül güç kararlarında ve kritik altyapı güvenliğinde önem taşır.

> ***"Medeni ve Siyasi Haklar Uluslararası Sözleşmesi m. 6 keyfî yaşamdan yoksun bırakmayı yasaklar. İnsanların sensör verileri ve algoritmik sınıflandırma üzerinden hedef seçildiği otonom sistemlerde yanlış pozitif, önyargılı eğitim verisi, bağlamı anlayamama ve insanın karar zincirinden uzaklaştırılması yaşam hakkı risklerini artırmaktadır (OHCHR, ICCPR m. 6; ICRC, 2026)"***

Atıf, İspat ve Leipzig Olayına Uygulama

Uluslararası hukukta "atıf standardı" ile "ispat standardı" aynı kavram değildir. **Atıf standardı, hangi bağlantının özel kişinin davranışını devlete bağladığını söyler; ispat standardı, mahkemenin o bağlantının gerçekleştiğine hangi derecede ikna edilmesi gerektiğini ifade eder. Buna bir de devletlerin dış politika amacıyla yaptıkları kamusal/siyasi atıf eklenir.** Hibrit operasyon tartışmalarındaki karışıklığın önemli bölümü bu üç katmanın birbirine karıştırılmasından kaynaklanmaktadır.

Military and Paramilitary Activities in and against Nicaragua davasında UAD, ABD'nin Contras'ı finanse etmesi, eğitmesi, donatması veya bazı operasyonel faaliyetlerle bağlantısının, Contras'ın gerçekleştirdiği her ihlali ABD'ye atfetmeye tek başına yetmediğini belirlemiş; ilgili operasyonlar üzerinde **etkin kontrol** aranmıştır (ICJ, 1986).

UAD, *Bosnia and Herzegovina v. Serbia and Montenegro* kararında da devlet sorumluluğu bakımından bu yaklaşımı korumuş ve ICTY'nin farklı amaçla kullandığı daha geniş "overall control/genel kontrol" ölçütünün ARSIWA m. 8 bakımından devlet sorumluluğunun genel standardının yerini almadığını göstermiştir (ICJ, 2007). Buna karşılık *Tehran Hostages* davasında İran makamlarının başlangıçta özel kişilerin gerçekleştirdiği elçilik işgalini daha sonra onaylayıp sürdürmesi, davranışın devlete mal edilmesinde devletin **benimseme** davranışının ne kadar önemli olabileceğini göstermiştir (ICJ, 1980).

Hibrit ve siber operasyonlarda teknik izlerin kolayca taklit edilebilmesi bu hukukî testi daha da önemli kılar. BM GGE'nin 2015 tarihli A/70/174 raporu, mevcut uluslararası hukukun devletlerin ICT kullanımına uygulandığını kabul etmiş; bir ICT faaliyetinin belirli bir devletin ülkesinden veya altyapısından kaynaklanmasının tek başına atıf için yetersiz kalabileceğini ve devletlere yöneltilen isnatların temellendirilmesi gerektiğini belirtmiştir (BM GGE, 2015). Bu kural doğrudan fiziksel İHA saldırıları için yazılmamıştır, ancak Leipzig gibi teknik imza, vekil aktör ve inkâr edilebilirliğin bir araya geldiği vakalara güçlü bir **metodolojik analoji** sunmaktadır.

Bu çerçevede Leipzig delilinin katmanları şöyle değerlendirilebilir:
Fiziksel/adli katman. İHA gövdesi, uçuş kontrolcüsü, elektronik parçalar, seri numaraları, GNSS/inertial sistemler, patlayıcı bileşenleri, infilak düzeneği ve üretim zinciri fail ağı hakkında önemli ipuçları sağlayabilir. Alman Hükümeti kullanılan materyal ve teknik unsurların daha önce Rus hibrit faaliyetleri ve Ukrayna savaşında görülen yöntemlerle bağlantılı olduğunu açıklamıştır. Bu bulgu **destekleyici delildir**, fakat ticari veya yaygınlaştırılmış komponentlerin taklit edilebilir olması nedeniyle tek başına m. 8'i ispatlamaz (Bundesregierung, 2026a, 2026b).

Örüntü katmanı. NATO, Mayıs 2024'ten beri Rusya'nın Müttefik topraklarında sabotaj, şiddet, elektronik müdahale, siber faaliyetler ve vekil aktör kullanımını içeren yoğunlaşan bir hibrit faaliyet kampanyası yürüttüğünü resmî olarak belirtmektedir. AB de Rusya bağlantılı sabotaj, kritik altyapı, siber ve enformasyon operasyonlarına yönelik yaptırım rejimini genişletmiştir (NATO, 2024; Council of the EU, 2024, 2025). Bu geniş örüntü Leipzig atfının bağlamını güçlendirir, ancak **geçmişteki benzer olaylar yeni olayın failini hukuken otomatik olarak kanıtlamaz.**

İnsan/istihbarat katmanı. Hukuken belirleyici katman budur. Alman Hükümeti 2 Eylül'de yalnızca teknik benzerliklerden değil, olayın arkasındaki aktörlerle Rus devlet unsurları arasındaki ilişkiyi gösterdiğini söylediği istihbarattan söz etmiştir. Eğer söz konusu istihbarat, Rus devlet makamlarının belirli saldırıyı emrettiğini, hedefi belirlediğini, operasyonu finanse ettiğini ve icrasını yönlendirdiğini gösterebiliyorsa m. 8 bağlantısı kuvvetlidir.
Bu nedenle "Alman makamlarının atfı yetersizdir" demek de "hukuki sorumluluk kesin kanıtlanmıştır" demek kadar erken olur. Doğru hukuki formül şudur:

> ***"Almanya çok kaynaklı ve resmî bir devlet atfında bulunmuştur; açık kaynak delili bu atfı makul ve ciddi göstermektedir; m. 8'in yargısal standardını karşıladığı sonucunun nihai teyidi ise kamuya kapalı delilin içeriğine bağlıdır"***

Alternatif hipotezlerin de test edilmesi gerekir. Bunlar;

- Bağımsız Rusya yanlısı aşırıcıların veya suçluların eylemi;
- Rus yöntemlerini taklit eden üçüncü bir aktör;
- Saldırı hedefinin Ukrayna lojistiği değil doğrudan Alman havacılık altyapısı olması;
- Operasyonun amacı fiziksel yıkımdan ziyade korkutma/aksatma yaratmak olmasıdır. Bu hipotezlerin varlığı Rus atfını çürütmez; yalnızca **iyi bir atıf analizinin rakip açıklamaları dışlaması gerektiğini** gösterir. Alman Hükümeti, teknik materyalin üçüncü taraflarca taklit edilebileceği itirazıyla 2 Eylül'de doğrudan karşılaşmış ve tam da bu nedenle üç ayrı delil boyutunun birlikte değerlendirildiğini söylemiştir.

Rus sorumluluğu m. 8 temelinde kurulursa, Leipzig'e patlayıcı yüklü İHA göndermek Almanya'nın ülkesel egemenliğinin ihlali olarak güçlü biçimde nitelendirilebilir. Ayrıca fiziksel zarar vermek amacıyla silahlı/patlayıcı araç sevk edilmesi, BM Şartı m. 2(4) bakımından "kuvvet kullanımı" niteliğine yaklaşır. Burada "bomba patlamadı, dolayısıyla kuvvet kullanılmadı" şeklinde mekanik bir sonuç isabetli değildir: bir saldırı aracının yabancı ülke topraklarında operasyonel biçimde konuşlandırılması ve hedefe yöneltilmesi de eylemin niteliğinin değerlendirilmesinde önemlidir. Bununla beraber bu, analitik bir yorumdur ve somut hedefleme/aktivasyon verisi belirleyici olacaktır.

Buna karşılık **m. 51 silahlı saldırı eşiği daha yüksektir.** UAD içtihadı bütün kuvvet kullanımlarının eşit ağırlıkta olmadığını kabul etmektedir. Leipzig'de büyük can kaybı veya geniş çaplı fiziksel yıkım meydana gelmemiş olması, tek olay bakımından silahlı saldırı iddiasını zayıflatır. Bir dizi koordineli sabotajın "birikimli olaylar" şeklinde değerlendirilmesi doktrinde tartışılsa da kümülatif yaklaşımın sınırları devlet pratiğinde kesin değildir.

"Dolayısıyla mevcut dosya Almanya'ya Rusya'ya karşı doğrudan silahlı kuvvet kullanma hakkı doğduğunu göstermek için yeterli değildir"

Bu ayrım NATO bakımından özellikle önemlidir. NATO'nun 2023 Vilnius Bildirisi ve güncel kolektif savunma açıklamaları, **önemli siber veya hibrit saldırıların silahlı saldırı seviyesine çıkabileceğini ve Madde 5 kararına yol açabileceğini**, fakat değerlendirmenin vaka bazında yapılacağını belirtmektedir. 5 Eylül 2026'da ABD'nin NATO nezdindeki Büyükelçisi de Leipzig olayını daha önceki istenmeyen hava sahası ihlallerinden daha kaygı verici bir kasıtlı hibrit faaliyet örneği olarak değerlendirmiştir. Bu siyasi dayanışma, hukuken otomatik Madde 5 tetiklenmesi anlamına gelmez.

Almanya'nın şimdiye kadarki cevabı, bu eşik ayrımına uygundur. Hükümet, Rusya'nın Bonn Başkonsolosluğu'nun kapatılması, Berlin'deki Rus Evi'ne ilişkin düzenlemelerin sona erdirilmesi, AB düzeyinde yaptırım girişimleri ve başka istihbari/diplomatik tedbirler duyurmuş ve cevabı açıkça **orantılı ve tırmandırıcı olmayan** bir yaklaşım olarak sunmuştur (Auswärtiges Amt, 2026; Bundesregierung, 2026a). Bunların önemli bir bölümü, başka bir hukuka aykırılıkla meşrulaştırılması gerekmeyen **retorsiyon** tedbirleridir. Eğer Almanya gelecekte normalde uluslararası yükümlülüklerine aykırı olacak bir karşı önleme başvurursa, ARSIWA'nın karşı önlem koşulları ayrıca yerine getirilmelidir.

Rusya–Ukrayna Savaşında Otonomlaşma ve LAWS

"Otonom sistem" ile "uzaktan kumandalı drone" arasındaki sınır, platformun üzerinde AI etiketi bulunup bulunmadığına göre çizilemez. ICRC(**International Committee of the Red Cross** yani **Uluslararası Kızılhaç Komitesi**) ye göre otonom silahın ayırt edici niteliği, **aktive edildikten sonra hedefi sensör bilgileri ve önceden belirlenmiş bir hedef profili üzerinden seçip saldırabilmesi**, böylece kullanıcının saldırının kesin hedefini, zamanını veya yerini tek tek belirlememesidir (ICRC, 2026).

Savaşın otonomiyi hızlandıran temel mekanizması **elektronik harptir**. İHA ile operatör arasındaki veri bağlantısı, GNSS ve radyo komuta kanalları karıştırıldıkça platformların çevreyi yerleşik sensörlerle algılamasına, konumunu bağımsız hesaplamasına ve hedefe haricî bağlantı olmaksızın son yaklaşma yapmasına duyulan ihtiyaç artmaktadır. RUSI'nin[6] Ukrayna'daki elektromanyetik operasyon analizi ile teknik çalışmalar, elektronik harp ve karşı tedbir döngüsünün taktik adaptasyonun merkezinde bulunduğunu göstermektedir (Iorillo & Simonetti, 2025).

[6] RUSI, İngilizce Royal United Services Institute ifadesinin kısaltması olup Türkçe karşılığı Kraliyet Birleşik Hizmetler Enstitüsü'dür. 1831 yılında Waterloo kahramanı Wellington Dükü tarafından Londra'da kurulan RUSI, dünyanın en eski, Birleşik Krallık'ın ise en prestijli savunma, askeri strateji ve güvenlik düşünce kuruluşudur.

"Ukrayna tarafında ölçek olağanüstüdür. Ukrayna Savunma Bakanlığı 2024'te 1,5 milyondan fazla İHA tedarik edildiğini; 2025 için sanayinin yaklaşık 4,5 milyon FPV drone üretim kapasitesinin tamamının satın alınmasının planlandığını açıklamıştır. Bakanlık ayrıca 2024'te 330'dan fazla yerli insansız sistemin kullanımına onay verildiğini ve cephede kullanılan İHA'ların yüzde 95'ten fazlasının yerli üretim olduğunu bildirmiştir (Ministry of Defence of Ukraine, 2025a, 2025b)"

Sayısal büyüme tek başına otonomi anlamına gelmez; fakat ölçek insan operatörü darboğaz haline getirir. CSIS'in Ukrayna'nın otonom harp kapasitesine ilişkin araştırmasına göre 2024'te AI destekli otonomi özelliklerine sahip yaklaşık 10.000 İHA'nın tedariki yönünde adımlar atılmış; makine görüşü, elektronik harp altında seyrüsefer ve hedefe terminal yaklaşma gibi fonksiyonlar öne çıkmıştır. Aynı araştırma, bunların hâlâ toplam drone hacminin küçük bir bölümünü oluşturduğunu özellikle göstermektedir (Bondar, 2025).

Haziran 2026'da Ukrayna'nın Brave1 savunma inovasyon kümesi, Shahed tipi hedeflere karşı bir önleyici drone sisteminin uçuş–önleme zincirinin yaklaşık yüzde 95'ini otomatikleştirdiğini duyurmuştur. Ancak burada kritik ayrıntı şudur: **operatör hedefi seçmekte ve saldırıyı her an iptal edebilmektedir**; AI ise hedefe yaklaşma sırasında onu tanıyıp kilitlenmektedir. Bu sistem, "insanın devreden tamamen çıkarıldığı LAWS" yerine **human-on-the-loop/gözetimli otonomi** örneği olarak sınıflandırılmaktadır (Brave1, 2026).

Ukrayna devletinin teknoloji politikasında daha ileri otonomi açık bir hedeftir. Eylül 2025'te Savunma ve Dijital Dönüşüm bakanlıklarının Brave1 yarışması, özellikle otonom dronlar, otonom yönlendirme modülleri, termal hedefleme, önleme AI'sı ve otonom savaş sistemleri için simülasyon ortamlarını finanse etmeye yönelmiştir (Ministry of Defence of Ukraine, 2025c).

Rusya tarafında da benzer, fakat kısmen farklı bir dönüşüm görülmektedir. Shahed/Geran ailesi önce düşük maliyetli tek yönlü uzun menzilli saldırı silahı olarak ölçeklendirilmiş; 2024–2026 arasında navigasyon, elektronik karşı tedbirler, motorlar, görev yükleri ve görev çeşitliliği hızla değiştirilmiştir. CSIS'in 4 Eylül 2026 tarihli güncel

değerlendirmesi, Geran platformlarında değişiklik döngülerinin yıllar değil haftalar düzeyinde gerçekleşebildiğini; yeni varyantların hız ve görev yüklerini değiştirdiğini göstermektedir (Bondar & Errera, 2026).

Rus **V2U** sistemi daha ileri bir kategoriye işaret etmektedir. Nisan 2026'da yayımlanan teknik değerlendirmede platformun Nvidia Jetson Orin sınıfı işlemci, bilgisayarlı görü ve YOLOv5 tabanlı tanıma modeli kullanarak bağlantısız seyrüsefer, görsel hedef arama, tanıma ve hedef seçme özelliklerine sahip olduğu ileri sürülmektedir (Bondar, 2026).

> ***"Fakat raporun önemli ölçüde Ukrayna savaş alanı incelemeleri ve Ukrayna istihbaratı/open-source verilerine dayanması nedeniyle, "tam otonom güvenilir hedef seçimi" iddiası operasyonel olarak bağımsız doğrulanmış kesin bir gerçek değil, ciddi fakat ihtiyatla değerlendirilmesi gereken teknik bulgudur"***

Bu gelişmelerden çıkarılabilecek daha temel sonuç, savaşın **"uzaktan pilotlu drone savaşı'nıntam otonom robot savaşı"** şeklinde tek sıçramayla ilerlemediğidir. Daha gerçekçi dönüşüm şu zincirde gerçekleşmektedir:

🔵 **Mavi (01-02):** Doğrudan insan kontrolü ve yarı otonom süreçler. Karar yetkisinin tamamen insanda olduğu uzaktan kontrol mekanizması ile yalnızca rota takibi (waypoint) yapan otopilot sistem.

🟡 **Sarı (03-05):** Algoritmik gözetim, hedef sınıflandırma ve yardımcı yapay zekâ mekanizmaları. Görsel Navigasyon aşamasına, elektronik harp altında çalışan SLAM ve optik akış algoritmalarıyla birlikte Baykar K2/Sivrisinek ve Estonya-Ukrayna ortaklığı ve Terminal Kilitlenme aşaması, iletişim kopsa dahi otonom dalışı sürdüren görsel kilit (pixel-lock) teknolojisi. Derin öğrenme ile insan ve araç ayrımını otonom yapabilen sistemler.

🔴 **Kırmızı (06-08):** İnsanın sadece "onay" verdiği aşamadan (human-on-the-loop), çoklu sürü orkestrasyonuna ve nihayetinde öldürme kararının makineye kalmasıyla oluşan ahlaki mesafeye geçiş. İnsanın sadece "onay/iptal" verdiği gözetimli hedef seçimi (human-on-the-loop) ve 15'li heterojen İHA

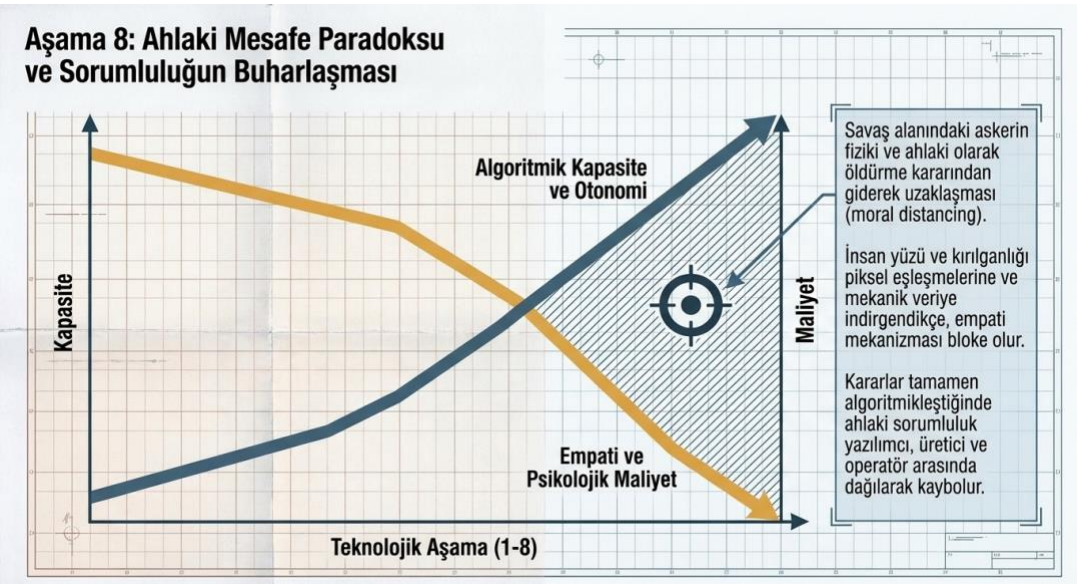
gruplarının kendi aralarındaki görev paylaşımını kapsayan otonom sürü orkestrasyonu. Son aşamada, kararların algoritmalara devredilmesinin insan hayatını "piksel eşleşmelerine" indirgediği, empatiyi engelleyerek ahlaki mesafeyi (moral distancing) artırdığı ve "sorumluluğun buharlaşması".

Teknolojik risk özellikle son iki basamakta artmaktadır. Tek bir platformun çok akıllı olmasından ziyade sensörler, istihbarat ağları, AI modelleri ve yüzlerce ucuz silahın **ortak komuta/yazılım katmanında orkestre edilmesi**, gelecekteki otonom savaşın belirleyici özelliği olabilir. Güncel çalışmalar da "platform otonomisi" ile bütün öldürme zincirini yöneten "network/kill-chain autonomy" arasındaki ayrımın önemini vurgulamaktadır.

Öngörülebilir zararlar yalnızca "robot yanlış kişiyi vurabilir" sorunundan daha geniştir.

- **Birinci risk ayrımdır: sivil/asker ayrımının görünüş, hareket ve sensör imzasına indirgenmesi bağlam bilgisini kaybedebilir.**
- **İkincisi orantılılıktır: algoritma hedefi tanıyabilse dahi beklenen sivil zarar ile somut ve doğrudan askerî avantajın normatif değerlendirmesi bağlama bağımlıdır.**
- **Üçüncüsü tedbir yükümlülüğüdür: dinamik sivil çevrede saldırının askıya alınması gerekebilir.**
- **Dördüncüsü ölçek riskidir: hata olasılığı küçük olsa bile binlerce sistemde aynı model/yazılım hatası sistematik zarara dönüşebilir.**
- **Beşincisi hız ve tırmanma riskidir: makine hızındaki hedef–karşı hedef döngüsü siyasi karar süresini daraltabilir.**

ICRC bu nedenle öngörülemez otonom silahların ve insanları doğrudan hedeflemek üzere tasarlanan otonom sistemlerin yasaklanması, diğerlerinin ise sıkı kısıtlanması yönünde bir yaklaşım savunmaktadır.



BM Genel Kurulu bu teknolojik dönüşümü artık iki ayrı fakat bağlantılı kanalda ele almaktadır. **A/RES/79/239**, "askerî alanda yapay zekâ" konusunda ilk Genel Kurul kararıdır ve uluslararası hukukun AI yaşam döngüsünün bütün aşamalarında uygulanabilirliğini teyit etmektedir. LAWS ise ayrıca A/RES/78/241, 79/62 ve 80/57 kararları ile CCW sürecinde ele alınmaktadır (BM Genel Kurulu, 2023–2025).

> ***"Bu ayrım önemlidir: Askerî AI = LAWS değildir. Bakım tahmini, hava savunma sensör füzyonu, lojistik optimizasyonu, rota planlama veya tehdit sınıflandırması AI kullanabilir fakat hedefi kendi başına seçip öldürmeyebilir. Hukukun en yoğun müdahale etmesi gereken nokta, AI'nın "kritik işlevlere", yani hedef seçme ve hedefe kuvvet uygulama kararlarına yaklaştığı yerdir"***

Devlet Dışı Aktörler, Teknoloji Şirketleri ve "Küresel Sermaye"

"Vatansız Para" veya "küresel sermaye" ifadesi, savunma sanayisinin ulusötesi finansman ve teknoloji ağlarını sorgulayan bir **eleştirel siyasal iktisat kavramı** olarak kullanılabilir; ancak uluslararası hukuk bakımından tek, merkezi iradesi olan veya ARSIWA kapsamında "devlet" gibi sorumluluk yüklenebilen bir hukuk öznesi değildir. Dolayısıyla analizin "küresel sermaye Rusya–AB arasında drone savaşını seçti" şeklinde nedenselliği peşinen kabul etmesi, hukuki kanıt standardını zayıflatır.

> **"Daha isabetli soru şudur: hangi şirket, yatırımcı, tedarikçi veya yüklenici hangi teknoloji/finansmanı hangi bilgi düzeyiyle sağladı; bu davranış hangi devlete veya belirli hukuka aykırı kullanıma bağlanabilir?"**

Bununla birlikte Rusya–Ukrayna savaşında özel sermayenin ve teknoloji şirketlerinin askerî kapasite üretimindeki ağırlığı tartışmasız biçimde büyümüştür. **Ukrayna'nın resmî Brave1 ekosistemi 2026'da binlerce savunma teknolojisi geliştirmesini, 500'ü aşkın İHA üreticisini ve 200'ü aşkın AI şirketini kapsayan bir inovasyon ağı tanımlamaktadır.** Brave1 ayrıca özel şirketlerin prototipten savaş alanı kullanımına geçişini devlet hibeleri ve yatırım turlarıyla hızlandırmaktadır.

Batı tarafında bu ekosistem yalnızca "devlet Ukrayna'ya silah gönderiyor" modelinden giderek uzaklaşmaktadır. Ukrayna ile Almanya'daki ortak üretim tesisleri, ABD'li şirketlerle **interceptor drone** üretimi, Avrupa ülkeleriyle **"Drone Deal"** anlaşmaları ve ABD ile teknoloji test/ortak üretim düzenlemeleri devlet finansmanı, özel sermaye, startup kültürü ve savaş alanı geri bildirimini aynı döngüde birleştirmektedir. **Ukrayna Cumhurbaşkanlığı Temmuz 2026'da Drone Deal modelinin güvenlik yardımı, ortak üretim finansmanı, yerelleştirme, teknoloji transferi, siber iş birliği ve kritik altyapı korumasını birlikte kapsadığını açıklamıştır.**

> ***"ABD'de de "drone dominance" yalnızca Ukrayna politikası değildir; 13 Ağustos 2026 tarihli Beyaz Saray belgesi yerli UAS üretim kapasitesini ulusal güvenlik sorunu olarak nitelendirmiş, belirli yabancı İHA ve bileşenlerine tarifeler koymuş ve ABD'de üretimi teşvik edecek "onshoring mekanizması"[7] öngörmüştür. Bu, İHA rekabetinin aynı anda askerî, endüstriyel, ticari ve teknoloji egemenliği meselesine dönüştüğünü gösterir"***

Bu bağlamda kullanıcının "küresel sermaye" tezinin ampirik açıdan güçlü tarafı, savunma teknolojisi değer zincirlerinin ulusal sınırlara sığmamasıdır: işlemciler bir ülkeden, optik sensörler başka bir ülkeden, yazılım başka bir şirketten, finansman başka bir fon veya hükümetten gelebilir; üretim ise savaş alanına yakın üçüncü bir ülkede gerçekleşebilir. **Rus V2U incelemelerinde de Batılı ve Çinli ticari bileşenlere rastlandığı rapor edilmektedir.** Bu durum yaptırımların, ihracat kontrolünün ve tedarik zinciri şeffaflığının önemini artırır (Bondar, 2026).

Ancak **bir şirketin bileşeninin bir silahın içinde bulunması, şirketi saldırıdan otomatik olarak sorumlu yapmaz.** Devlet sorumluluğu için şirket m. 5 kapsamında kamu yetkisi kullanıyor olabilir veya m. 8 anlamında devletin talimat/yönlendirme/kontrolü altında davranıyor olabilir. Bunlar yoksa şirketin faaliyeti özel davranış olarak kalır. **Devlet yine de şirketi yeterince düzenlememe, ihracatı kontrol etmeme veya hukuka aykırı fiile kendi davranışıyla yardım etme nedeniyle ayrı yükümlülükler altında bulunabilir (ILC, 2001).**

Özel askerî şirketler bakımından da aynı ayrım geçerlidir. Bir özel askerî şirketin varlığı kendi başına onu devlet organına dönüştürmez. Fakat mevzuatla kamu yetkisi verilmişse m. 5; belirli operasyon üzerinde devlet talimatı veya etkin kontrol varsa m. 8 devreye girebilir. Şirket personelinin uluslararası ceza hukuku bakımından bireysel sorumluluğu ise devletin ARSIWA sorumluluğundan ayrı bir sorudur.

Şirketlerin insan hakları yükümlülüğü açısından **BM İş Dünyası ve İnsan Hakları Rehber İlkeleri** önemli fakat büyük ölçüde soft-law nitelikli çerçevedir. "Koruma–saygı–telafi" modeli uyarınca devletlerin üçüncü kişilerin insan hakları ihlallerine karşı koruma görevi; işletmelerin insan haklarına saygı sorumluluğu, mağdurlar için etkili telafi mekanizmaları bulunması gerekir (OHCHR, 2011/2013). **Özellikle çatışmadan etkilenen bölgelerde şirketlerden daha yüksek insan hakları durum tespiti beklenmesi, AI silah tedarik zincirleri için önemlidir.**

"Savunma teknolojisine yatırım yapmak" ile "uluslararası hukuka aykırı saldırıya yardım etmek" de birbirinden ayrılmalıdır. Yatırım fonunun bir drone şirketine sermaye sağlaması tek başına belirli bir savaş suçuna veya uluslararası hukuka aykırı fiile iştirak anlamına gelmez. Hukuki sorumluluğun ağırlaşabilmesi için **bilgi, amaç, maddi katkı ve fiil ile nedensel bağlantı** gibi rejime özgü unsurlar aranır.

---

[7] Onshoring mekanizması (ülke içi üretim veya yerelleştirme); bir şirketin veya devletin, daha önce maliyet avantajı nedeniyle yurtdışına (offshore) devrettiği üretim, yazılım, teknoloji veya lojistik altyapısını kendi sınırları içerisine geri taşıması sürecidir. Ukrayna savaşıyla birlikte bu kavram, salt ekonomik bir tercih olmaktan çıkıp "savunma sanayii arz güvenliği ve egemenlik" mekanizmasına dönüşmüştür. Rapora temel teşkil eden transatlantik savunma ortaklıkları ve teknoloji transferleri bağlamında onshoring mekanizmasının işleyişi ve uluslararası hukuki boyutları şu şekildedir:

- Tersine Onshoring (Teknoloji Transferi): Ukrayna, dört yılı aşkın sıcak çatışma sahasında geliştirdiği ileri düzey İHA yazılımlarını ve elektronik harbe dayanıklı yapay zekâ kodlarını, güvenli lojistik bölgelere taşımaktadır. Ukrayna'nın gelişmiş teknolojisini kullanarak ABD topraklarında İHA fabrikası kurulması ve Pentagon'un *"Drone Dominance"* programına entegre edilmesi bu mekanizmanın en somut örneğidir.
- Lisans Altında Yerli Üretim: Fransa Cumhurbaşkanı Macron'un açıkladığı, Ukrayna'nın Fransız seyir füzelerini ve mühimmatlarını kendi ülkesinde lisans altında üretmesine (onshoring/yerelleştirme) izin verilmesi, lojistik bağımlılığı sıfırlamayı amaçlar.

Daha önemli yapısal tehlike, ekonomik teşviklerin **otonominin güvenlik testlerinden daha hızlı ilerlemesine** yol açmasıdır. Savaş alanı iterasyonu, startup finansmanı ve milyon adet ölçeğinde satın alma, geleneksel silah tedarik çevrimini kısaltmaktadır. UNODA'nın Mart 2026 CCW toplantısında "sorumlu askerî AI tedariki"ni özel bir konu olarak gündeme alması tam da bu problemi yansıtır: **insan–makine etkileşimi gereksinimleri, hukuki inceleme ve güvence testleri ancak tedarik sözleşmesinin başında teknik şart haline getirilirse etkili olabilir.**

> ***"Burada asıl uluslararası hukuk sorunu, aktörlerin çoğalmasıyla birlikte sorumluluk zincirinin parçalanmasıdır. Komutan "AI seçti", geliştirici "ordu kullandı", yatırımcı "yalnızca finansman sağladım", devlet "özel şirket geliştirdi" diyebildiğinde hesap verebilirlik boşluğu doğabilir. Mevcut hukuk bu aktörlerin her birine aynı tür sorumluluk yüklemese de sorumluluğun insandan makineye devredilemeyeceği temel ilke korunmalıdır. ICRC de otonom sistem kullanımında insanların uluslararası insancıl hukuk yükümlülüklerinden ve kararlarından sorumlu kalacağını vurgulamaktadır"***

Politika ve Hukuk Önerileri

Leipzig sonrası yapılması gereken;

- **İlk reform, kamusal atıf ile hukuki atıf arasında kurumsal bir köprü** kurmaktır. Almanya ve NATO ülkeleri her olayda tüm istihbarat kaynağını açamaz; ancak Rusya gibi suçlanan bir devletin "kanıtı gösterin" itirazını tamamen cevapsız bırakmak da uzun vadede atıf sisteminin meşruiyetini aşındırabilir. Bu nedenle "minimum kamuya açıklanabilir atıf dosyası" standardı geliştirilmelidir. Dosya, en azından olayın teknik analizi, alternatif hipotezlerin neden dışlandığı, atfın güven düzeyi, hukuki temel ve hangi delillerin güvenlik gerekçesiyle gizlendiğini sınıflandırılmış biçimde göstermelidir. BM GGE'nin atıfta bütün ilgili bilgilerin ve daha geniş bağlamın değerlendirilmesi gerektiği yönündeki yaklaşımı buna model olabilir.
- **İkinci olarak** NATO, **"fail atfı, devlet sorumluluğu, kuvvet kullanımı, silahlı saldırı, Madde 5"** basamaklarını aynı kavram gibi kullanmamalıdır. Bir sabotaj Rusya'ya hukuken atfedilebilir fakat silahlı saldırı eşiğine ulaşmayabilir; kuvvet kullanımı olabilir fakat Madde 5 kararı gerektirmeyebilir. **NATO'nun mevcut vaka-bazlı yaklaşımı korunmalı, fakat üyeler için ortak bir hukuki eşik matrisi ve olayların kümülatif etkisini değerlendirecek standart metodoloji oluşturulmalıdır.**
- **Üçüncü olarak** Almanya'nın **karşı-İHA savunması**, yalnızca kinetik vurma kapasitesine indirgenmemelidir. Federal Hükümet 2025–2026'da Federal Polis yetkilerini genişletmiş, ortak drone savunma merkezi ve özel Federal Polis anti-drone birimi oluşturmuş ve Luftsicherheitsgesetz'i değiştirmiştir. Bu yapı; RF tespiti, radar/elektro-optik füzyon, adli bileşen toplama, hava trafik yönetimi, siber istihbarat ve askeri destek arasındaki görev bölüşümünü hukukla netleştirmelidir (Bundesregierung, 2026d).
- **Dördüncü olarak** LAWS konusunda **iki katmanlı bağlayıcı rejim** izlenmelidir. Birinci katmanda kullanıcının öngöremeyeceği etkiler üreten sistemler ile insanları doğrudan sensör-profili üzerinden seçip öldürmek üzere tasarlanan sistemler yasaklanmalıdır. İkinci katmanda diğer otonom silahlar; hedef türü, coğrafi alan, görev süresi, sivil yoğunluk, insan gözetimi, abort/override, güvenilirlik, kayıt tutma ve m. 36 silah incelemesi koşullarına bağlanmalıdır. Bu yaklaşım ICRC'nin önerileri ve BM Genel Sekreterinin bağlayıcı araç çağrısıyla uyumludur.
- **Beşinci olarak** "**anlamlı insan kontrolü**" soyut slogan olmaktan çıkarılmalıdır. Asgari teknik-hukuki gereklilikler, insanın saldırının amaç ve bağlamını anlaması, hedef sınıfını ve operasyon bölgesini sınırlayabilmesi, sistemin hata/kararsızlık göstergelerini görebilmesi, yeterli müdahale süresine sahip olması ve saldırıyı etkili biçimde iptal edebilmesidir. Brave1'in insanın hedefi seçtiği ve iptal yetkisini koruduğu interceptor modeli, ölümcül işlevlerde bu ayrımın pratik olarak teknik tasarıma çevrilebileceğini göstermektedir.
- **Altıncı olarak** AI silahları için m. 36 incelemeleri "bir defalık sertifikasyon" olmamalıdır. Makine öğrenmesi modeli, eğitim verisi, sensör paketi veya hedef sınıflandırıcısı önemli ölçüde değiştirildiğinde **yeniden hukuki inceleme** gerekmelidir. Savaş sırasında haftalar içinde değiştirilen Geran varyantları ve sürekli güncellenen Ukrayna sistemleri, klasik "platformu bir kez onayla, yıllarca kullan" modelinin yetersizliğini göstermektedir.
- **Yedinci olarak** satın alma sözleşmelerine teknik hesap verebilirlik şartları eklenmelidir: değiştirilemez görev logları, hedefleme karar kayıtları, model/yazılım sürüm numarası, sensör girdilerinin saklanması, override kayıtları, güvenli güncelleme zinciri, sivil ortam performans testi ve olay sonrası bağımsız inceleme kapasitesi. Böylece "algoritma yaptı" savunmasının önüne geçilebilir. UNODA/SIPRI'nin 2026 gündemindeki sorumlu askerî AI tedariki tartışması bu yaklaşımı desteklemektedir.
- **Sekizinci olarak** şirket ve yatırımcılar için çatışma ortamlarında **güçlendirilmiş insan hakları ve tedarik zinciri durum tespiti** standartlaştırılmalıdır. Bir şirket yalnızca doğrudan silah üretmediği için sorumluluk değerlendirmesinden çıkmamalıdır; AI işlemcisi, hedef tanıma yazılımı, görüntü verisi, bulut/iletişim hizmeti

veya özel sensör sunan şirketlerin ürünlerinin öngörülebilir askerî kullanım riskleri de incelenmelidir. Ancak yükümlülükler nedensellik ve bilgi düzeyiyle bağlantılı tasarlanmalı; sırf savunma sanayisine yatırım yapıldığı için otomatik hukuki suçluluk yaratılmamalıdır (OHCHR, 2011/2013).

- **Dokuzuncu olarak** AB'nin Rus hibrit faaliyetlerine yönelik yaptırım rejimi, yalnızca doğrudan ajanları değil, doğrulanmış biçimde operasyonların **finansmanı, lojistiği veya teknolojik tedarikine** katılan kişi ve kuruluşları hedefleyebilir. AB 2025'te hibrit yaptırım çerçevesini finansal kolaylaştırıcıları ve maddi varlıkları kapsayacak şekilde genişletmiştir; bu araç, uygun delil ve usul güvenceleriyle Leipzig türü operasyonlara karşı kullanılabilir. Aynı tedbir başka ülkeler için de geçerlidir.
- **Onuncu olarak** BM sürecinde CCW konsensüsünün sonuç üretememesi halinde Genel Kurul hattı ihmal edilmemelidir. A/RES/78/241'den A/RES/80/57'ye uzanan büyük çoğunluk, en azından sorunun uluslararası düzenleme gerektirdiği yönünde geniş bir siyasal tabanın oluştuğunu göstermektedir. Ancak etkin bir rejim, yalnızca "AI iyidir/kötüdür" tartışması değil; **hangi hedefleme fonksiyonunun insandan makineye devredilemeyeceğini** tanımlayan teknik-hukuki hükümler içermelidir.

Sonuç:

Leipzig vakası, geleceğin savaşının yalnızca "otonom drone" teknolojisi sorunu olmadığını göstermektedir. Asıl dönüşüm, **failin kimliğinin gizlenebildiği, ticari bileşenlerin askerîleştirilebildiği, özel aktörlerin devletlerle iç içe geçtiği ve hedefleme kararının giderek yazılım katmanına taşındığı bir sorumluluk mimarisidir.** Bu mimaride uluslararası hukukun merkezi sorusu **"drone kime aitti?"** değil; **"kim hedefi seçti, kim operasyonu emretti veya kontrol etti, hangi devlet hangi yükümlülüğü ihlal etti, insan hangi aşamada hukuken anlamlı karar gücünü korudu ve zarar gerçekleştiğinde kime hesap sorulabilir?"** olmalıdır. ARSIWA, BM Şartı ve mevcut insancıl hukuk bu soruların büyük bölümüne temel sağlar; LAWS alanındaki yeni düzenlemenin görevi, insan sorumluluğunun algoritmik ve kurumsal katmanlar arasında **kaybolmasını önlemektir**.

Kaynakça:

Alman ve Avrupa resmî kaynakları

- Auswärtiges Amt. (2026, 1 Eylül). *Statement by Foreign Minister Wadephul on the Russian hybrid attack at Leipzig/Halle Airport and Germany's response*. Federal Foreign Office.
- Bundesregierung. (2026a, 4 Eylül). *Entschlossenes Vorgehen gegen hybriden Angriff: Versuchter Anschlag am Flughafen Leipzig/Halle*. Presse- und Informationsamt der Bundesregierung.
- Bundesregierung. (2026b, 2 Eylül). *Regierungspressekonferenz vom 2. September 2026*. Presse- und Informationsamt der Bundesregierung.
- Bundesregierung. (2026c). *Was tut die Bundesregierung gegen hybride Angriffe und Drohnenvorfälle? Fragen und Antworten*.
- Bundesregierung. (2026d, 17 Mart). *Stärkung der Drohnenabwehr*.
- Bundesregierung. (2026e, 26 Şubat). *Strengthening drone defence: Amendments to the Aviation Security Act*.
- Council of the European Union. (2024, 8 Ekim). *Russian hybrid threats: EU condemns Russia's continued hybrid campaigns*.
- Council of the European Union. (2025, 20 Mayıs). *Russian hybrid threats: EU sanctions individuals and entities and broadens restrictive measures*.
- Council of the European Union. (2025, 3 Ekim). *EU restrictive measures in view of Russia's destabilising activities: Extension of sanctions framework*.

Birleşmiş Milletler ve temel uluslararası hukuk belgeleri

- International Law Commission. (2001). *Draft articles on responsibility of States for internationally wrongful acts, with commentaries*. *Yearbook of the International Law Commission, 2001, Vol. II, Part Two*.
- United Nations General Assembly. (1970). *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations* (A/RES/2625[XXV]).
- United Nations General Assembly. (1974). *Definition of Aggression* (A/RES/3314[XXIX]).
- United Nations General Assembly. (2001). *Responsibility of States for internationally wrongful acts* (A/RES/56/83).
- United Nations Security Council. (2022). *Resolution 2623 (2022)* (S/RES/2623), 27 February 2022.
- United Nations General Assembly. (2022a). *Aggression against Ukraine* (A/RES/ES-11/1).
- United Nations General Assembly. (2022b). *Humanitarian consequences of the aggression against Ukraine* (A/RES/ES-11/2).
- United Nations General Assembly. (2023). *Lethal autonomous weapons systems* (A/RES/78/241).
- United Nations General Assembly. (2024a). *Lethal autonomous weapons systems* (A/RES/79/62).
- 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 General Assembly. (2025). *Lethal autonomous weapons systems* (A/RES/80/57).
- United Nations General Assembly. (2025). *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025* (A/RES/80/16).
- United Nations Group of Governmental Experts. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174).
- United Nations Office for Disarmament Affairs. (2025). *Lethal autonomous weapon systems*.
- United Nations Office for Disarmament Affairs. (2025). *Artificial intelligence in the military domain*.
- United Nations Office for Disarmament Affairs. (2026). *Convention on Certain Conventional Weapons – Group of Governmental Experts on Lethal Autonomous Weapons Systems, 2026*.
- United Nations Secretary-General. (2025, 12 Mayıs). *Secretary-General's remarks on autonomous weapons and human control*.
- United Nations. (1945). *Charter of the United Nations*, arts. 2(4), 51.

Uluslararası yargı ve insancıl hukuk kaynakları

- International Court of Justice. (1980). *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment*. *I.C.J. Reports 1980*.
- International Court of Justice. (1986). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment*. *I.C.J. Reports 1986*.

- International Court of Justice. (2007). *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment*. *I.C.J. Reports 2007*.
- International Committee of the Red Cross. (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949 (Protocol I), Article 36: New weapons*.
- International Committee of the Red Cross. (2019). *Autonomous weapon systems: Implications of increasing autonomy in the critical functions of weapons systems*.
- International Committee of the Red Cross. (2026). *Autonomous Weapon Systems and International Humanitarian Law: Selected Issues*.
- International Committee of the Red Cross. (2026). *ICRC position on autonomous weapon systems*.

NATO kaynakları

- North Atlantic Treaty Organization. (2023, 11 Temmuz). *Vilnius Summit Communiqué*.
- North Atlantic Treaty Organization. (2024, 2 Mayıs). *Statement by the North Atlantic Council on recent Russian hybrid activities*.
- North Atlantic Treaty Organization. (2025, 18 Temmuz). *Statement of condemnation by the North Atlantic Council concerning Russian malicious cyber activities*.
- North Atlantic Treaty Organization. (2025/2026). *Collective defence and Article 5*.
- North Atlantic Treaty Organization. (2026). *Countering hybrid threats*.
- North Atlantic Treaty Organization. (2025). *NATO Integrated Air and Missile Defence Policy*.

Ukrayna, ABD ve savunma teknolojisi birincil kaynakları

- Brave1. (2026, 8 Haziran). *Ukrainian drones are already shooting down Shaheds in autonomous mode*.
- Ministry of Defence of Ukraine. (2025a, 28 Nisan). *In 2024, the Ministry of Defence quadrupled the number of Ukrainian unmanned systems authorized for operational use*.
- Ministry of Defence of Ukraine. (2025b, 10 Mart). *In 2025, the Ministry of Defence plans to procure 4.5 million FPV drones*.
- Ministry of Defence of Ukraine. (2025c, 4 Eylül). *Up to UAH 100 million for breakthrough AI solutions: Ministry of Defence and Ministry of Digital Transformation launch Brave1 grant competition*.
- Office of the President of Ukraine. (2025, 3 Temmuz). *Memorandum between Ukraine and the U.S. company Swift Beat, LLC will enable scaling up production of interceptor drones*.
- Office of the President of Ukraine. (2026a, 13 Şubat). *President visits the first Ukrainian-German joint drone production venture in Munich*.
- Office of the President of Ukraine. (2026b, 7 Temmuz). *Ukraine and Denmark sign a Drone Deal*.
- Office of the President of Ukraine. (2026c, 15 Temmuz). *Ukraine and the European Commission sign document opening the path toward a Drone Deal*.
- Office of the President of Ukraine. (2026d, 22 Temmuz). *President discusses future defense cooperation and Drone Deal with the United States*.
- The White House. (2026, 13 Ağustos). *President Donald J. Trump bolsters national security and strengthens U.S. supply chains by imposing tariffs on drones and their parts and components*.

Teknik, akademik ve uzmanlık literatürü

- Asaro, P. (2012). On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross, 94*(886), 687–709.
- 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.
- Bondar, K., & Errera, N. (2026, 4 Eylül). *From Shahed to Geran: How Russia continues to reinvent the one-way attack drone*. Center for Strategic and International Studies.
- Crawford, J. (2002). *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge University Press.
- Crootof, R. (2015). The killer robots are here: Legal and policy implications. *Cardozo Law Review, 36*, 1837–1915.
- Eichensehr, K. E. (2020). The law and politics of cyberattack attribution. *UCLA Law Review, 67*, 520–598.
- Iorillo, P., & Simonetti, R. M. (2025). Electromagnetic operations in Ukraine. *The RUSI Journal, 170*(6/7).
- Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of cyber operations by non-state actors. *Journal of Conflict & Security Law, 21*(3), 405–428.
- Sharkey, N. (2012). The evitability of autonomous robot warfare. *International Review of the Red Cross, 94*(886), 787–799.
- Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict & Security Law, 17*(2), 229–244.
- Center for Strategic and International Studies. (2025). *Drone saturation: Russia's Shahed campaign*.
- Center for Strategic and International Studies. (2026). *Defining autonomy: Why software, not drones, will decide the next war*.
- Center for Strategic and International Studies. (2026). *Shahed-131 and -136*. Missile Defense Project.

İnsan hakları ve şirket sorumluluğu

- Office of the United Nations High Commissioner for Human Rights. (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (A/HRC/17/31).
- Office of the United Nations High Commissioner for Human Rights. (2013). *Protect, Respect and Remedy: A Guide on Business and Human Rights*.
- Office of the United Nations High Commissioner for Human Rights. (2024). *Access to remedy in cases of business-related human rights abuse: A practical guide for state-based judicial mechanisms*.

Medya ve tamamlayıcı güncel kaynaklar

- Reuters. (2026, 24 Temmuz). *Zelenskiy says US, Ukraine moving forward on joint drone production*.
- Reuters. (2026, Ağustos). *Germany investigates explosive drone incident at Leipzig/Halle Airport*.
- Reuters. (2026, 1 Eylül). *Germany attributes attempted Leipzig drone attack to Russia; Moscow denies allegation*.
- Reuters. (2026, 5 Eylül). *NATO will not tolerate hybrid actions against members, US envoy says*.
- Reuters. (2026, 6 Eylül). *Russian foreign minister rejects German Leipzig allegations*.