9 Kasım 2026 -Sayı 134

TEMA GRUP

2BLACKDOT··

''Esasen konu hep 2 nokta arasındadır''

Haftalık
Politik ve Jeopolitik
Gelişmeler

Bu hizmet size 2blackdot ve Tema Grup tarafından ücretsiz verilmektedir. Bu yazılanlar yatırım tavsiyesi değildir.
Hazırlayan: Hakan Çalışkantürk 2twoblackdots@gmail.com www.2blackdot.com

***** Yasal Uyarı:***** Burada yer alan yatırım bilgi, yorum ve tavsiyeleri yatırım danışmanlığı kapsamında değildir. Yatırım danışmanlığı hizmeti; aracı kurumlar, portföy yönetim şirketleri, yatırım ve kalkınma bankaları ile müşteri arasında imzalanacak yatırım danışmanlığı sözleşmesi çerçevesinde ve yetkili kuruluşlar tarafından kişilerin risk ve getiri tercihleri dikkate alınarak kişiye özel olarak sunulmaktadır. Burada yer alan yorum ve tavsiyeler ise genel niteliktedir. Bu yorum ve tavsiyeler mali durumunuz ile risk ve getiri tercihinize uygun olmayabilir. Bu nedenle sadece burada yer alan bilgilere dayanılarak yatırım kararı verilmesi beklentilerinize uygun sonuçlar doğurmayabilir. Gerek bu yayındaki gerekse bu yayında kullanılan kaynaklardaki hata ve eksikliklerden ve bu yayındaki bilgilerin kullanılması sonucundaki yatırımcıların ve/veya ilgili kişilerin uğrayabilecekleri doğrudan ve/veya dolaylı zararlardan, kâr yoksunluğundan, manevi zararlardan ve her ne şekilde ve surette olursa olsun üçüncü kişilerin uğrayabileceği her türlü zarardan dolayı 2blackdot ve Hakan Çalışkantürk sorumlu tutulamaz.

2blackdot haftalık bülteni yönetici özeti:

AVRUPA'DA TOPLUMSAL HAZIRLIK VE KRİZ REHBERLERİ



İsveç'ten 5.2 Milyon Kitapçık
İsveç, hanelere eiber saldırı ve dezenformasyon uyarıları içeren 32 sayfalik saveç rehheri dağıttı.



AB 72 Saatlik Stok
AB Hazırlikhlik Stratejisi 450 milyon vatandaşa 72 saatlik bağımsız gıda/su atoku taveiye etti.



Polonya 17 Milyon Hano
Polonya 8.1 milyar avroluk sivil koruma pianıyla tüm hanelere güvenlik rehberi gönderdi.



İskandinav Ülkeleri Alarında
Norveç stok süresini 7 güne çıkardı, Danünarka dğital gida ve ilaç tavsiyesi yayımladı.

SİVİL ALTYAPIYA YÖNELİK SOMUT HİBRİT SALDIRILAR

	Tarih	Saldırı / Olay	Atıf / Tespit Durumu	Alınan Tepki / Sunuş
	Kas 2025	10 ülkede gıda soğutma ve kan bonkasi aiber saldırıları	Rus yenlısr havhtlviotlar herlendi, resmi devlet atfı yok	Savcılik soruştorması ve AB bilgi paylaşımı
	Kas 2025	Polonya Varşava Lublin demiryolu battı patlaması	Rus isbhbaratı adına hareket eden iki Ukrayna vekili	Ceza soruştorması ve demiryolu operasyonu
	Eyl 2025	Kopenhag ve Oslo havalimanlarında drone ihldıleri	Denimarka tarafından "bibrh selchıı" tonunlaması	Have sehacı kıaıtlamaları
	Eyl 2025	Colline Acrospace yozıkmına fülye yazılım saldırısı	Siber suç akstvamu reemi devlet atfi yapılmadı	Manuel işleme geçiş ve gözeltı kararları
	Eyl 2024 - Ağast 2025	Birleşik Krallik'ta 204 olusel öneme sahip siber olay	NCSC: Ciddi sdidinlor önceki yılın ikl kotina çikü	Haftada ortalama 4 eiddi olay mübehalesi

ULUSLARARASI HUKUKTA ATIF VE DEVLET SORUMLULUĞU (ARSIWA)



Üç Farklı Atıf Katmanı
Siber alanda taknik, siysal ve hukuki atıf ayrılmakte; devletler hukuki atıftan kaçınmaktadır.



ARSIWA Madde 8 Sınırı
Nikaragua kararındaki "etkin kontrol" sortı siber vekillerin devlete bağlanmasını zorlaştırmaktadır.



ARSIWA Madde 5 Yetkisi
Siber savumnayı özel şirketlere devreden devletler, bu şirketlerin eylemlerinden doğrudan sorumludur.



Devletin Özen Yükümlülüğü
Karfu Kanalı iikesince devletler kendi topraklarının huksiz filllerde kullanımını önlemek zorundadır.

YENİ DEVLET DIŞI AKTÖRLER OLARAK TEKNOLOJİ ŞİRKETLERİ



Savunma Ortağı



Altyapı Sağlayıcı



Saldırı Aracı Üreticileri

Şirketler savunma ortağı, altyapı sağlayıcı ve saldırı aracı üreticileri olarak smıflandırılır.



Microsoft Azure Vokası
İsrali sekeri istifibarat verilerinin Hollanda bulutunda tutulması toprak devletinin özenini tartışmaya açtı.

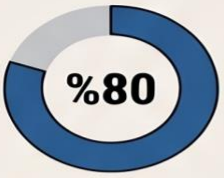


Siber Paralı Askerler Riskleri
Pogasus banseri cesus yazıkmların ihrasatı, ev sehibi devletin m. 16 yarıtım sorumluluğunu doğurabilir.

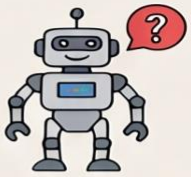


Çift Kullanımlı Altyapı Riski
Askeri verilerin eivil hulutta barıntılınması sizil veri memazlerini meşru askeri hedef yapabilir.

STRATEJİK BİR SİLAH OLARAK YAPAY ZEKÂ



Yapay Zekâh Oltalama %80
ENiSA 2023 verilerine göre küresel susyal mühendisliğin %80'den fazlası yapay zeka desteklidir.



Sorumluluk Doşluğu Yanılsaması
Devlet sorumluluğu kusur gerektırmediğinden, otonom sistem hataları doğrodan devlete etfedilk.



Ek Protokol I Denetimi
Madde 35 gereğince yapay zekalı yeni silah ve yöntemlerin hukuka uygunluğu önceden incelemnehilir.



BM Otonom Silah Oylaması
2035 BM kararı (A/RES/80/57) 164 lehte oyla kabul edilmiş, ARD oleyhte oy kullanmıştır.

HUKUKİ VE KURUMSAL REFORM ÖNERİLERİ



Talimat Kavramının Genişletilmesi
ARSiWA m. 8 talimat kavramı vekillere verilen yazılım şartnamelerini kapsayacak şekiide okunmalıdır.



Bağımsız Uzmenler Paneli
BM bünyesinde istihbaratı riske atmadan teknik eiber atıf deiilerini inceleyecek panel kurulmalıdır.



Şirketlere Artırılmış Özen
Çatısma bölgelerinde hizmet veren teknoloji şirketlerine zorunlu insan hakları özeni getirilmelidir.



Askeri Yapay Zekâ Sözleşmesi
CCW Konferenei'nda askeri yapay zekâ kullanımını düzenleyen bağlayıcı uluslararası antlaşma yapılmalıdır.

Gemini Notebook

2blackdot haftalık bülteni yönetici özeti:

AVRUPA'DA SİBER SALDIRILAR:
"Yeni Devlet Dışı Aktörler; Teknoloji Şirketleri ve Stratejik Bir Silah Olarak Yapay Zekâ"

Öz

Avrupa, 2024-2026 döneminde siber saldırı, sabotaj, drone ihlali ve dezenformasyonun iç içe geçtiği bir "hibrit tehdit" ortamıyla karşı karşıya kalmıştır. Bu süreçte İsveç, Norveç, Danimarka, Finlandiya, Fransa ve Polonya hanelere kriz ve savaş rehberleri ulaştırmış; Avrupa Komisyonu ise vatandaşlardan en az 72 saat yetecek temel ihtiyaç stoku tutmalarını istemiştir. Saldırıların önemli bir kısmı doğrudan devlet organlarınca değil, "hacktivist" gruplar, suç örgütleri, "tek kullanımlık" ajanlar ve teknoloji şirketleri gibi devlet dışı aktörler eliyle gerçekleşmekte; bu da uluslararası sorumluluk hukukunun temel sorusunu, yani fiilin devlete atfını yeniden gündeme taşımaktadır. Çalışma önce Avrupa'daki tehdit algısını devletlerin kamuoyuna yönelik uyarıları ve somut olaylar üzerinden ortaya koymakta, ardından uluslararası hukukta devlet dışı aktör kavramını tanım, literatür ve tipoloji bakımından incelemektedir. Devamında Uluslararası Hukuk Komisyonu'nun Devletlerin Uluslararası Haksız Fiillerinden Doğan Sorumluluğuna İlişkin Taslak Maddeleri (ARSIWA) çerçevesinde atıf kuralları ve özen yükümlülüğü değerlendirilmekte; teknoloji şirketlerinin "yeni devlet dışı aktörler" olarak konumu ve yapay zekânın stratejik bir silah olarak kullanımı bu çerçeveye yerleştirilmektedir. Çalışmanın temel iddiası, mevcut sorumluluk hukukunun kural düzeyinde büyük ölçüde yeterli olduğu; asıl boşluğun etkin kontrol eşiğinin ispatında, özen yükümlülüğünün içeriğinin belirsizliğinde ve devletlerin siyasi atıfı hukuki sorumluluk talebine dönüştürmekten kaçınmasında yattığıdır.

Anahtar Kelimeler: Devletin uluslararası sorumluluğu, devlet dışı aktörler, atıf (isnat), siber operasyonlar, teknoloji şirketleri, askerî yapay zekâ, özen yükümlülüğü, hibrit tehditler

Abstract

Between 2024 and 2026, Europe has faced a "hybrid threat" environment in which cyber operations, sabotage, drone incursions and disinformation increasingly overlap. Several European states have distributed crisis and war preparedness guides to every household, and the European Commission has urged citizens to keep essential supplies for at least 72 hours. Many of these operations are carried out not by state organs but by non-state actors such as "hacktivist" groups, criminal networks, "disposable" agents and technology companies, which brings the core question of the law of state responsibility, attribution, back to the fore. This article first maps the European threat perception through public warnings and concrete incidents, then examines the concept of non-state actors in international law, and finally analyses attribution and due diligence under the ILC Articles on State Responsibility (ARSIWA) in relation to technology companies and the strategic use of artificial intelligence. It argues that the existing rules are largely adequate; the gap lies in proving effective control, in the indeterminate content of due diligence, and in the reluctance of states to turn political attribution into legal claims of responsibility.

Keywords: State responsibility, non-state actors, attribution, cyber operations, technology companies, military artificial intelligence, due diligence, hybrid threats

Giriş

Kasım 2026'nın ilk haftası, Avrupa kamuoyuna siber tehdidin artık yalnızca bilgisayar uzmanlarını ilgilendiren teknik bir sorun olmadığını açıkça gösterdi. 2 Kasım'dan itibaren neredeyse her gün gelen sahte bomba ihbarları nedeniyle Londra'dan Bulgaristan'a giden bir yolcu uçağı Budapeşte'ye inmek zorunda kaldı; perşembe günü yirmiden fazla uçuş hedef alındı ve İtalya'dan Birleşik Krallık'a kadar on altı ülkeyi bağlayan seferler etkilendi (Schneid, 2026). Aynı hafta Belçika, Lüksemburg, İsveç, Almanya, Yunanistan, İrlanda, İtalya, Estonya, Hollanda ve Finlandiya'daki süpermarketlerde soğutma sistemlerinin uzaktan ele geçirildiği, dondurucu sıcaklıklarının yükseltildiği ve büyük miktarda gıdanın imha edildiği bildirildi. Fransa'da ise Ulusal Kan Kurumu'nun (EFS) bazı bölge tesislerindeki soğuk oda izleme ve kontrol sistemleri siber saldırıya uğradı; kan ürünleri alarm sistemleri sayesinde korunabildi (Reynolds ve Croft, 2026). Cuma günü İrlanda kamu yayıncısı RTÉ, Bulgaristan'ın Nova TV kanalı ve İngiliz Sky News'e bomba ihbarı içeren e-postalar gönderildi; İrlanda hükümeti olayların büyük olasılıkla koordineli bir kargaşa kampanyası olduğunu açıkladı.

Bu olaylarda dikkat çeken unsur, saldırıların neredeyse hiçbirinin bir devlet tarafından açıkça üstlenilmemesidir. Süpermarket saldırılarını iki Rusya yanlısı "hacktivist" grup üstlenmiş, Kremlin ise suçlamaları "saçma" ve "temelsiz" olarak nitelendirmiştir. İspanya Dışişleri Bakanı José Manuel Albares olayları hibrit saldırganlık ve psikolojik savaş girişimi olarak tanımlarken, Paris Cumhuriyet Savcılığı e-postaların yabancı güçlerle bağlantısını araştırmaya başlamıştır (Schneid, 2026).

Uzmanların ortak gözlemi şudur: Devlet düğmeye kendisi basmamakta, uyumlu vekillerin bunu yapmasına izin vererek "makul inkâr edilebilirlik" alanını korumaktadır (Reynolds ve Croft, 2026). Bu tablo, uluslararası hukuknun en temel sorularından birini, yani zararı doğuran fiilin hangi koşullarda bir devlete atfedilebileceğini, yeniden ve daha keskin biçimde gündeme getirmektedir.

Sorunu daha da karmaşık hâle getiren iki gelişme vardır. **Birincisi,** teknoloji şirketleri modern çatışmaların vazgeçilmez aktörlerine dönüşmüştür. Bulut altyapısı, uydu iletişimi, yapay zekâ destekli istihbarat analizi ve siber savunma hizmetleri artık büyük ölçüde özel şirketler tarafından sağlanmakta; bu şirketler kimi zaman bir devletin savunmasına destek veren, kimi zaman ise bir orduya hedefleme altyapısı sağlayan ya da saldırı yazılımı satan aktörler olarak ortaya çıkmaktadır. **İkincisi,** yapay zekâ hem siber saldırıların hem de askerî karar süreçlerinin hızını ve ölçeğini dönüştürmektedir. Avrupa Birliği Siber Güvenlik Ajansı (ENISA), 2025 başı itibarıyla küresel sosyal mühendislik faaliyetinin %80'inden fazlasının yapay zekâ destekli oltalama içerdiğini tespit etmiştir (European Union Agency for Cybersecurity [ENISA], 2025).

Sorulması gereken; Uluslararası Hukuk Komisyonu'nun 2001 tarihli Devletlerin Uluslararası **Haksız Fiillerinden Doğan Sorumluluğuna İlişkin Taslak Maddeleri'ndeki** (bundan sonra ARSIWA olarak kullanılacaktır) **atıf kuralları ve devletin özen yükümlülüğü, devletlerin teknoloji şirketleri, vekil gruplar ve yapay zekâ destekli sistemler aracılığıyla yürüttüğü ya da bunlara dayanarak gerçekleştirdiği siber ve askerî operasyonlardan doğan zararları kapsamaya yeterli midir? Yeterli değilse, boşluk birincil kurallarda mı, ikincil kurallarda mı, yoksa ispat ve siyasi irade düzleminde midir?**

Başlangıç itibariyle belirtilmesi gereken; sorumluluk hukukunun "yetersiz" değil, "işletilmeyen" bir hukuk olduğudur. Yeni bir antlaşmaya ihtiyaç duyulmaksızın, ARSIWA m. 5'in işlevsel yorumu[1],

Article 5
Conduct of persons or entities exercising elements of governmental authority

The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance.

m. 8'deki "talimat" kavramının sözleşmesel teknik şartnameleri de kapsayacak biçimde okunması[2],

Article 8
Conduct directed or controlled by a State

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

Özen yükümlülüğünün "bilmesi gereken" standardıyla somutlaştırılması ve m. 16'nın[3] bulut ve yapay zekâ hizmetlerinin sağlanmasına uygulanması büyük ölçüde yeterlidir.

---

[1] **Madde 5: Kamu gücü yetkilerini kullanan bir kişinin ya da bir birimin davranışı**
Madde 4 kapsamında devletin bir organı olmayan, fakat o devletin hukuku tarafından kamu gücü yetkilerini (hükümet yetkisinin unsurlarını) kullanmak üzere yetkilendirilmiş bir kişinin ya da bir birimin davranışı; söz konusu kişi ya da birimin olayda bu sıfatla hareket etmesi koşuluyla, uluslararası hukuk uyarınca devletin bir fiili olarak kabul edilir.

[2] **Madde 8: Bir Devlet tarafından yönlendirilen veya kontrol edilen davranış**
Bir kişinin ya da bir grup kişinin davranışı; söz konusu kişi ya da grup kişinin bu davranışı gerçekleştirirken o Devletin talimatları doğrultusunda veya onun yönlendirmesi ya da kontrolü altında hareket etmesi halinde, uluslararası hukuk uyarınca bir Devlet fiili olarak kabul edilir.

[3] **Madde 16**: Uluslararası hukuka aykırı bir fiilin işlenmesine yardım veya destek

Article 16

Aid or assistance in the commission of an internationally wrongful act

A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if:

(*a*) that State does so with knowledge of the circumstances of the internationally wrongful act; and

(*b*) the act would be internationally wrongful if committed by that State.

Asıl reform ihtiyacı atıf delilinin paylaşımı, askerî yapay zekâda anlamlı insan denetiminin normatif hâle getirilmesi ve teknoloji şirketlerinin çatışma bölgelerindeki özen yükümlülüğünün güçlendirilmesi alanlarındadır.

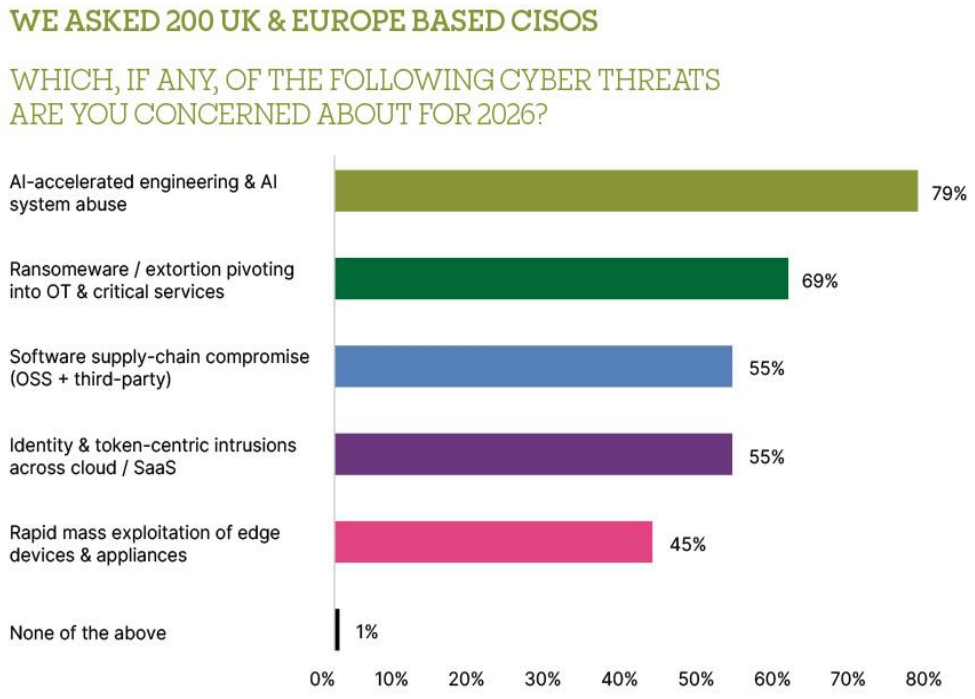
Terminoloji bakımından "atıf" (attribution) kavramı üç ayrı anlamda kullanılmaktadır:

- Saldırının kaynağını adli bilişim yöntemleriyle tespit eden **teknik atıf,**
- Bir devletin kamuoyu önünde başka bir devleti suçladığı **siyasi atıf**,
- ARSIWA ölçütlerine göre fiilin devlete isnat edilmesi anlamına gelen **hukuki atıf.**

Çalışmanın önemli bir bulgusu, Avrupa devletlerinin ilk ikisini giderek daha sık yaptığı hâlde üçüncüsünden kaçındığıdır. Çalışma yedi bölümden oluşmaktadır. Birinci bölüm Avrupa'daki tehdit algısını devletlerin kamuoyuna yönelik uyarıları ve somut olaylar üzerinden ortaya koymaktadır. İkinci bölüm devlet dışı aktör kavramını tanım, literatür ve tipoloji bakımından incelemektedir. Üçüncü bölüm devlet dışı aktörlerin fiillerinden doğan devlet sorumluluğunun doktrinel çerçevesini kurmaktadır. Dördüncü ve beşinci bölümler sırasıyla teknoloji şirketlerini ve yapay zekâyı bu çerçeveye yerleştirmektedir. Altıncı bölüm mevcut hukukun yeterliliğini değerlendirip öneriler sunmakta, sonuç bölümü ise bulguları özetlemektedir.

1. Avrupa'da Tehdit Algısı: "Kriz ya da Savaş Gelirse"

Avrupa devletleri son iki yılda vatandaşlarına Soğuk Savaş'tan bu yana görülmemiş bir açıklıkla şunu söylemektedir: Elektrik kesilebilir, internet çökebilir, ödeme sistemleri durabilir ve devlet ilk günlerde herkese aynı anda ulaşamayabilir. **Bu uyarıların ortak noktası, tehdidin yalnızca tanklar ve füzelerle değil, siber saldırılar, sabotaj ve dezenformasyon yoluyla da gelebileceğinin kabul edilmesidir.**



https://www.consultancy.uk/news/42036/business-leaders-warn-ai-threats-will-test-resilience-in-2026

Başka bir Devletin uluslararası hukuka aykırı bir fiil işlemesine yardım eden veya destek sağlayan bir Devletin, şu koşulların varlığı halinde bu davranışı nedeniyle uluslararası sorumluluğu doğar:

(a) Söz konusu Devletin fiilin koşullarının bilincinde olarak bunu yapması; ve

(b) Fiilin, yardım eden veya destek sağlayan Devlet tarafından doğrudan işlenmesi halinde de uluslararası hukuka aykırı olacak olması.

1.1. Hanelere Ulaşan Rehberler: Devletin Vatandaşla Yeni Sözleşmesi

Bu dönüşümün sembolü İsveç olmuştur. İsveç Sivil Olağanüstü Durumlar Ajansı (MSB), 18 Kasım 2024'ten itibaren iki hafta içinde 5,2 milyon haneye "Kriz ya da Savaş Gelirse" **(Om krisen eller kriget kommer)** başlıklı 32 sayfalık bir kitapçık göndermiştir. İkinci Dünya Savaşı'ndan bu yana beşinci kez yayımlanan rehberin 2024 sürümü, öncekilere göre savaşa hazırlığa çok daha fazla ağırlık vermekte ve ilk kez dezenformasyon ile dijital saldırı tehdidine ayrı başlık açmaktadır. Kitapçık, bir saldırı hâlinde İsveç'in asla teslim olmayacağını ve aksi yöndeki her bilginin yanlış kabul edilmesi gerektiğini vurgulamaktadır. Sivil Savunma Bakanı Carl-Oskar Bohlin, tehdit tablosunun artık siber saldırıları, etki operasyonlarını ve sabotaj riskini de kapsadığını açıklamıştır (Associated Press, 2024).

Komşu ülkeler benzer adımlar atmıştır. Norveç Sivil Koruma Müdürlüğü (DSB), Mayıs 2024'te hanelerin kendi kendine yetme süresine ilişkin tavsiyesini üç günden bir haftaya çıkarmış ve 2024 sonbaharında tüm hanelere yeni bir broşür göndermiştir **(Direktoratet for samfunnssikkerhet og beredskap [DSB], t.y.).** Danimarka Haziran 2024'te yetişkinlere e-posta yoluyla üç günlük su, gıda ve ilaç stoğu tavsiyesi ulaştırmış; Finlandiya ise Kasım 2024'te hazırlık bilgilerini toplayan bir internet portalı açmıştır.

Avrupa Birliği bu ulusal girişimleri birlik düzeyine taşımıştır. Avrupa Komisyonu ve Yüksek Temsilci, 26 Mart 2025'te ilk "Hazırlıklılık Birliği Stratejisi"ni **(Preparedness Union Strategy)** açıklamıştır. Otuz temel eylem içeren strateji, AB'de yaşayan yaklaşık 450 milyon kişiye olağanüstü durumlarda en az 72 saat kendine yetecek temel ihtiyaç stoğu tutmalarını tavsiye etmekte; gerekçe olarak jeopolitik gerilimleri, hibrit ve siber tehditleri, yabancı bilgi manipülasyonunu ve iklim kaynaklı afetleri saymaktadır (European Commission, 2025). Hazırlıklılık ve Kriz Yönetiminden Sorumlu Komiser Hadja Lahbib bu yaklaşımı "her şeye hazır olmak" şeklinde yeni bir Avrupa yaşam tarzı olarak tanımlamıştır.



Fransa, 20 Kasım 2025'te Başbakanlık ve Ulusal Savunma ve Güvenlik Genel Sekreterliği (SGDSN) tarafından hazırlanan **"Tous responsables"** (Herkes Sorumlu) rehberini yayımlamıştır. Rehber, nükleer kazadan siber saldırıya ve savaşa kadar geniş bir kriz yelpazesini ele almakta ve özellikle Fransa'ya düşman bir örgüt ya da devletin bir kriz anını düzensizliği artırmak için kullanabileceği uyarısını içermektedir (The Local France, 2025).



Polonya ise bir adım daha ileri giderek savunma ve içişleri bakanlıklarıyla Hükümet Güvenlik Merkezi'nin (RCB) ortak hazırladığı "Güvenlik Rehberi"ni **(Poradnik Bezpieczeństwa)** Ocak 2026 sonuna kadar ülkedeki 17 milyon hanenin tamamına basılı olarak ulaştırmıştır. Rehberin girişinde Polonya'nın karşı karşıya olduğu tehditlerin son yıllarda önemli ölçüde arttığı ve doğu sınırının ötesindeki savaşın güvenlik duygusunu doğrudan etkilediği belirtilmektedir (Notes from Poland, 2026). Rehber, 2026-2027 için 34 milyar zlotilik (yaklaşık 8,1 milyar avro) bir sivil koruma programının parçasıdır.



Almanya'da Federal Nüfus Koruma ve Afet Yardımı Dairesi (BBK) Başkanı Ralph Tiesler, Haziran 2025'te ülkenin olası bir silahlı tehdide karşı "zamana karşı yarış" içinde olduğunu açıklamış; metro istasyonları, tüneller ve otoparkların sığınağa dönüştürülmesini, siren ağının yenilenmesini ve NINA uyarı uygulamasının siber saldırılara karşı güçlendirilmesini önermiştir. Alman planlamasında 2029 yılı, Rusya'nın NATO'ya yönelik bir saldırı kapasitesine ulaşabileceği tarih olarak öne çıkmaktadır.

Açıkça devletler, kritik altyapıya yönelik siber saldırıları artık soyut bir ihtimal olarak değil, vatandaşın evinde su ve fener bulundurmasını gerektirecek kadar somut bir risk olarak tanımlamaktadır.

1.2. Güvenlik Yetkililerinin Açık Uyarıları

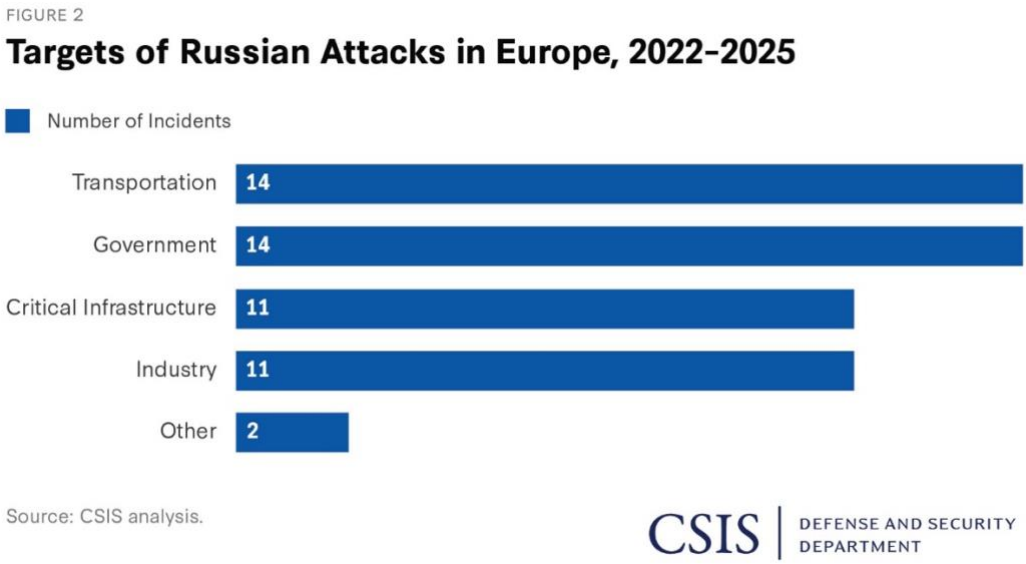
Rehberlere, güvenlik kurumlarının alışılmadık ölçüde açık uyarıları eşlik etmiştir. NATO Genel Sekreteri Mark Rutte, 11 Aralık 2025'te Berlin'de yaptığı konuşmada müttefiklerin Rusya'nın bir sonraki hedefi olduğunu ve şimdiden tehlikenin içinde bulunduklarını söylemiş; Avrupa'nın büyükannelerinin ve büyük büyükannelerinin yaşadığı ölçekte bir savaşa hazırlıklı olması gerektiğini vurgulamıştır (Reuters, 2025). Macaristan Dışişleri Bakanı Péter Szijjártó bu açıklamaları "pervasız" olarak nitelendirmiş, bu da tehdit değerlendirmesinin Avrupa içinde tartışmasız olmadığını göstermiştir.

Birleşik Krallık İç İstihbarat Servisi MI5'ın Genel Direktörü Ken McCallum



16 Ekim 2025 tarihli yıllık konuşmasında devlet kaynaklı tehdit faaliyeti nedeniyle soruşturulan kişi sayısının bir yılda yüzde 35 arttığını açıklamıştır. McCallum, Rusya ve İran'ın gözetleme, sabotaj, kundaklama ve fiziksel şiddet gibi daha önce terör örgütlerine özgü "çirkin yöntemlere" giderek daha fazla başvurduğunu ve Rusya'nın bu işler için ücretini dahi ödemediği "vekiller" kullandığını belirtmiştir (MI5, 2025).

Aynı dönemde Birleşik Krallık Ulusal Siber Güvenlik Merkezi (NCSC), Eylül 2024-Ağustos 2025 arasında 204 "ulusal öneme sahip" siber olayla ilgilendiğini açıklamıştır. Bu rakam **bir önceki yılın 89'unun iki katından fazla ve haftada ortalama dört ciddi saldırı anlamına gelmektedir** (National Cyber Security Centre [NCSC], 2025).



Hollanda Askerî İstihbarat ve Güvenlik Servisi (MIVD), 2024 yılına ilişkin raporunda ülkede ilk kez bir kamu hizmetinin dijital işletim sistemine yönelik ve sistemin kontrolünü ele geçirmeyi amaçlayan bir Rus siber sabotaj girişimi tespit ettiğini açıklamıştır. MIVD Direktörü Peter Reesink, savaş ile barış arasındaki **"gri bölgede"** çatışmanın artık bir gerçeklik olduğunu ifade etmiştir.

1.3. Somut Olaylar: Gündelik Hayatı Hedef Alan Saldırılar

Aşağıdaki tablonun dikkat çeken yönü, "tespit" sütununda devletlerin çoğunlukla siyasi açıklama düzeyinde kalmasıdır.

Tarih	*Olay*	*Tespit*	*Tepki*
2-7 Kasım 2026	*10 ülkede süpermarket soğutma sistemlerine saldırı, Fransa'da kan kurumu tesislerine siber saldırı, 16 ülkeyi etkileyen uçak ve yayın kuruluşu bomba ihbarları*	*Rusya yanlısı "hacktivist" gruplar üstlendi; resmî devlet atfı yok, Kremlin reddetti*	*AB havacılık güvenliği bilgi paylaşımı mekanizması; Paris savcılığının yabancı güç bağlantısı soruşturması (Schneid, 2026)*
15-16 Kasım 2025	*Polonya'da Varşova-Lublin demiryolu hattında patlama*	*Polonya: Rus istihbaratı adına hareket eden iki Ukrayna vatandaşı*	*Ceza soruşturması, demiryolu güvenlik operasyonu*
22-25 Eylül 2025	*Kopenhag, Oslo ve Danimarka'daki diğer havalimanlarında drone kaynaklı kapanmalar*	*Fail açıklanmadı; Danimarka "hibrit saldırı" olarak nitelendirdi*	*Hava sahası kısıtlamaları*
19-20 Eylül 2025	*Collins Aerospace check-in yazılımına fidye yazılımı saldırısı; Heathrow, Brüksel, Berlin ve Dublin havalimanlarında manuel işleme dönüş*	*Devlet atfı yok; siber suç*	*Birleşik Krallık Ulusal Suç Ajansı'nın gözaltı işlemi*
9-10 Eylül 2025	*Rus yapımı drone'ların Polonya hava sahasını ihlali*	*Polonya: Rusya (BM Güvenlik Konseyi'ne mektup, S/2025/572)*	*NATO m. 4 istişareleri, "Eastern Sentry" faaliyeti*
28 Mayıs 2025	*Çek Dışişleri Bakanlığı ağlarına 2022'den beri süren casusluk*	*Çekya: Çin bağlantılı APT31*	*Çin büyükelçisinin bakanlığa çağrılması*
29 Nisan 2025	*Yaklaşık bir düzine Fransız kuruluşunun 2021'den beri hedef alınması*	*Fransa: GRU'ya bağlı APT28*	*Resmî kınama, ANSSI teknik raporu*
Ağustos 2024 (atıf: 12 Aralık 2025)	*Alman hava trafik kontrol kuruluşu DFS'ye siber saldırı; Şubat 2025 seçimlerine "Storm-1516" kampanyasıyla müdahale*	*Almanya: APT28 ve GRU*	*Rus büyükelçisinin çağrılması, "karşı tedbir" açıklaması*

> ***Bu olayların ortak özelliği, hedeflerin askerî tesisler değil, gündelik hayatın altyapısı olmasıdır: Süpermarketteki dondurucu, havalimanındaki check-in bankosu, kan bankasının soğuk odası, banliyö treni. İtalya Başbakanı Giorgia Meloni'nin Kasım 2026'da vurguladığı gibi saldırılan şey sivil altyapıdır. Atlantik Konseyi'nden Elisabeth Braw'ın deyişiyle, bir ülkenin ordusuna saldırıldığında karşılık verilir; ancak sivil altyapı hedef alındığında demokratik devletlerin elinde askerî bir yanıt seçeneği kalmamaktadır (Schneid, 2026). Hukuki sorumluluk mekanizmaları tam da bu boşlukta önem kazanmaktadır.***

1.4. Rakamlarla Tehdit ve Avrupa Birliği'nin Hukuki Yanıtı

ENISA'nın Temmuz 2024-Haziran 2025 dönemini kapsayan raporu 4.875 olayı incelemiştir. Bu olayların yaklaşık yüzde 77'si hizmet engelleme (DDoS) saldırılarıdır ve büyük kısmı ideolojik motivasyonlu hacktivist gruplardan kaynaklanmaktadır. Olayların yüzde 7,2'si ise devletle bağlantılı aktörlere aittir; bunlar arasında Rusya bağlantılı yapılar en aktif olanlar olduğu iddia edilmektedir (ENISA, 2025). ENISA'nın vurguladığı en önemli eğilim, siber suçlular, hacktivistler ve devletle bağlantılı aktörlerin giderek aynı araç ve yöntemleri kullanmasıdır. **Bu yakınsama, kimin kim adına hareket ettiğini tespit etmeyi, yani devlete yapılacak atıfı, her geçen gün zorlaştırmaktadır.**

AB'nin hukuki yanıtı üç düzlemde gelişmiştir.

- **Birinci düzlem yaptırımlardır.** AB 2019'da siber saldırılara karşı bir **yaptırım rejimi kurmuş** (Konsey Kararı (CFSP) 2019/797), 8 Ekim 2024'te ise Rusya'nın istikrarsızlaştırıcı faaliyetlerine karşı ayrı bir **hibrit tehdit rejimi** oluşturmuştur (Konsey Kararı (CFSP) 2024/2643). Bu rejim kapsamında Mart 2026 itibarıyla 80 kişi ve 20 kuruluş listelenmiştir (Council of the European Union, 2026).
- **İkinci düzlem düzenlemedir.** NIS2 Direktifi (2022/2555), Siber Dayanıklılık Yasası (Tüzük 2024/2847), Siber Dayanışma Yasası (Tüzük 2025/38) ve Yapay Zekâ Yasası (Tüzük 2024/1689) **kritik altyapı işletmecilerine ve teknoloji üreticilerine özen ve bildirim yükümlülükleri getirmektedir.** Ancak Komisyon'un Temmuz 2026'da NIS2'yi iç hukuka aktarmayan dört üye devleti Adalet Divanı'na sevk etmesi, uygulamadaki gecikmeyi göstermektedir.
- **Üçüncü düzlem uluslararası hukuk beyanıdır.** AB Konseyi, 18 Kasım 2024'te siber alanda uluslararası hukukun uygulanmasına ilişkin ortak bir anlayış beyanı kabul etmiştir. Bu beyan egemenlik, müdahale yasağı, özen yükümlülüğü ve devlet sorumluluğuna açıkça yer vermekte ve kritik altyapıyı zaruret hâlinde korunabilecek "esaslı menfaat"[4] olarak nitelendirmektedir (Council of the European Union, 2024).

> ***Bu üç düzlem arasındaki dikkat çekici ayrışma şudur: AB yaptırımları kişileri ve kuruluşları hedef almakta, bir devleti uluslararası haksız fiilden sorumlu ilan etmemektedir. Başka bir deyişle Avrupa, saldırıların arkasında bir devlet gördüğünü söylemekte, fakat bu tespiti devletler arası sorumluluk hukukunun diline çevirmekten kaçınmaktadır.***

Bu durumun nedenlerini anlamak için önce saldırıların asıl failleri olan devlet dışı aktörlerin uluslararası hukuktaki yerini incelemek gerekmektedir.

2. Uluslararası Hukukta Devlet Dışı Aktörler

2.1. Devlet Dışı Aktör Kimdir? Olumsuz Bir Tanımın Sorunları

"Devlet dışı aktör" kavramı, uluslararası hukukun en sık kullanılan ama en az tanımlanan kavramlarından biridir.[5] Kavram, olumlu bir içerikten çok bir dışlama üzerine kuruludur: **Devlet olmayan ve uluslararası ilişkilerde etki doğurabilen her varlık bu kategoriye girmektedir.** Bu nedenle kavram; silahlı muhalif gruplardan terör örgütlerine, çok uluslu şirketlerden sivil toplum kuruluşlarına, özel askerî şirketlerden tek başına hareket eden bilgisayar korsanlarına kadar birbirinden çok farklı varlıkları aynı çatı altında toplamaktadır.

---

[4] **"Esaslı menfaat" (essential interest),** ARSIWA m. 25'te düzenlenen **zaruret hâlinin** temel kavramıdır. Bir devlet, kendisi veya uluslararası toplum için hayati önemdeki bir çıkarı ağır ve yakın bir tehlikeye karşı korumak zorunda kaldığında, başka bir uluslararası yükümlülüğüne aykırı davranabilir. Bu durumda davranışın hukuka aykırılığı ortadan kalkar. Korunan bu hayati çıkara "esaslı menfaat" denir. Uluslararası Hukuk Komisyonunun ve içtihadın verdiği örnekler şunlardır:

- Devletin varlığı ve güvenliği,
- Nüfusun hayatta kalması ve temel ihtiyaçları,
- Çevrenin korunması
- Uluslararası toplumun ortak çıkarları.

[5] Kavramı genel olarak tanımlayan bağlayıcı bir uluslararası belge bulunmamaktadır; mevcut tanımlar, ait oldukları belgenin amacıyla sınırlıdır. Örneğin BM Güvenlik Konseyi'nin kitle imha silahlarının yayılmasının önlenmesine ilişkin 1540 sayılı kararı, devlet dışı aktörü yalnızca o kararın amaçları bakımından ve karar kapsamındaki faaliyetleri yürütürken herhangi bir devletin hukuka uygun yetkisi altında hareket etmeyen kişi veya kuruluş olarak tanımlamaktadır (UN Security Council, 2004). AB ile Afrika, Karayip ve Pasifik ülkeleri arasında imzalanan Cotonou Anlaşması ise aynı kavramı kalkınma iş birliği bağlamında özel sektör, ekonomik ve sosyal ortaklar ve sivil toplum olarak belirlemektedir (Cotonou Partnership Agreement, 2000, m. 6). Böylece aynı kavram, bir belgede silah kaçakçılığı yapabilecek bir aktörü, diğerinde ise kalkınmanın ortağını ifade edebilmektedir.

Philip Alston, bu tanımlama biçimini "kedi-olmayan sendromu" (not-a-cat syndrome) olarak adlandırır. Benzetme şudur: Bir köpeği yalnızca "kedi olmayan hayvan" diye tanımlarsak, köpeğin ne olduğu, nasıl davrandığı ve neye ihtiyaç duyduğu hakkında hiçbir şey söylemiş olmayız. Aynı şekilde bir aktörü yalnızca "devlet değildir" diye tanımlamak da onun ne olduğunu ve hangi kurallara tabi olması gerektiğini açıklamaz. Üstelik bu tanım, devleti ölçüt alıp diğer bütün aktörleri onun eksik bir türevi gibi gösterir; böylece uluslararası hukukun yalnızca devletler etrafında kurulduğu yönündeki geleneksel anlayışı farkında olmadan sürdürür (Alston, 2005).
Bu eleştiri çalışmanın konusu açısından özellikle önemlidir. Bir teknoloji şirketi ile bir terör örgütü, ikisi de devlet olmadığı için aynı başlık altında toplanabilir; ancak amaçları, yapıları ve tabi oldukları kurallar birbirinden tamamen farklıdır. Hepsini "devlet dışı aktör" diye tek bir kategoriye koymak bu farkları görünmez kılar ve her biri için doğru sorumluluk kuralını bulmayı zorlaştırır.

Bu yaklaşımın sakıncası iki yönlüdür.

- **Birincisi,** devlet dışı aktörün fiili uluslararası hukuka ancak bir devlet üzerinden ulaşabildiğinden, fiil bir devlete atfedilemediğinde ve özen yükümlülüğü ihlali de ispatlanamadığında zarar uluslararası düzlemde karşılıksız kalmaktadır.
- **İkincisi,** atıf için aranan yüksek eşik, devletleri doğrudan hareket etmek yerine vekil kullanmaya teşvik etmekte ve "makul inkâr edilebilirlik" stratejisine fiilen hukuki koruma sağlamaktadır (Cassese, 2007).

Bununla birlikte devlet merkezli yaklaşımın hukuki belirlilik sağlaması ve devlet dışı aktörlerin meşrulaştırılmasını önlemesi gibi savunulabilir yönleri de bulunmaktadır. Cenevre Sözleşmeleri ortak 3. maddesinin, hükümlerinin uygulanmasının çatışmanın taraflarının hukuki statüsünü etkilemeyeceğini açıkça belirtmesi bu kaygının ifadesidir (Geneva Convention I, 1949, ortak m. 3). Bu nedenle asıl sorun devlet merkezli yapının kendisi değil, bu yapının bıraktığı boşlukların nasıl kapatılacağıdır.

Uluslararası Hukuk Derneği (ILA), 2010-2016 yılları arasında çalışan Devlet Dışı Aktörler Komitesi aracılığıyla kavramı sistematik biçimde ele almıştır. Komite çalışmalarının ortaya koyduğu temel sonuç, devlet dışı aktörlerin uluslararası hukukun yapımına, uygulanmasına ve denetlenmesine fiilen katıldığı, ancak bu katılımın hukuki statüye her zaman yansımadığıdır (Noortmann vd., 2015).

> ***Noortmann makalesinde devlet dışı aktör, "devletin organı olmayan, kendi iradesiyle hareket edebilen ve uluslararası alanda hukuken anlamlı sonuçlar doğurabilecek fiiller gerçekleştirme kapasitesine sahip gerçek veya tüzel kişi ya da örgütlü yapı" olarak tanımlanmaktadır. Bu tanım bilinçli olarak işlevseldir: Belirleyici olan aktörün biçimsel statüsü değil, uluslararası hukukça korunan bir menfaate zarar verme kapasitesidir.***

2.2. Süje mi, Katılımcı mı? Literatürdeki Yeri

Klasik uluslararası hukuk doktrini, uzun süre devletleri hukuk düzeninin tek süjesi olarak kabul etmiştir. Uluslararası Adalet Divanı'nın (UAD) 1949 tarihli Reparation for Injuries danışma görüşü bu yaklaşımı ilk kez esaslı biçimde sarsmıştır. Divan, herhangi bir hukuk sistemindeki süjelerin nitelik ve hakların kapsamı bakımından birbirinin aynı olmak zorunda olmadığını belirterek Birleşmiş Milletler'in uluslararası kişiliğini kabul etmiştir (*Reparation for Injuries*, 1949, s. 178). Bu görüş, uluslararası kişiliğin dereceli ve işlevsel bir kavram olabileceğinin kapısını aralamıştır.

Doktrinde bu tartışma iki ana yaklaşım etrafında şekillenmiştir. "Süje" yaklaşımı, bir varlığın uluslararası hak ve yükümlülüklerin doğrudan taşıyıcısı olup olmadığını sorar ve devlet dışı aktörlerin çoğunu bu kategorinin dışında bırakır. Rosalyn Higgins'in öncülük ettiği "katılımcı" yaklaşımı ise süje-nesne ikiliğinin entelektüel bir hapishane olduğunu, uluslararası hukukun bir karar alma süreci olarak anlaşılması gerektiğini ve bu sürece katılan herkesin hukuki analizde yer alması gerektiğini savunur (Higgins, 1994). Andrew Clapham, insan hakları yükümlülükleri bakımından bu ikinci yaklaşımı geliştirmiş ve devlet dışı aktörlerin, uluslararası hukuk kişiliği tartışmasından bağımsız olarak doğrudan yükümlülük taşıyabileceğini savunmuştur (Clapham, 2006). Jean d'Aspremont ise "katılımcılar" kavramının hukuki belirliliği zayıflatma riskine dikkat çekerek, hangi aktörün hangi kuralın muhatabı olduğunun her somut norm bakımından ayrıca belirlenmesi gerektiğini vurgulamaktadır (d'Aspremont, 2011).

Bu tartışmanın pratik sonucu şudur: Devlet dışı aktörlerin bir kısmı (örneğin silahlı gruplar insancıl hukuk bakımından, bireyler uluslararası ceza hukuku bakımından) bazı uluslararası yükümlülüklerin doğrudan muhatabıdır. Ancak bu aktörlerin uluslararası haksız fiil sorumluluğunu doğrudan üstlenebileceği genel bir sorumluluk rejimi bulunmamaktadır. Şirketler bakımından durum daha da belirgindir:

BM İş Dünyası ve İnsan Hakları Rehber İlkeleri şirketlere insan haklarına "saygı gösterme" sorumluluğu yüklemekle birlikte bu sorumluluk bağlayıcı bir uluslararası yükümlülük niteliği taşımamaktadır (UN Human Rights Council, 2011). Sonuç olarak devlet dışı aktörün verdiği zarar, uluslararası düzlemde ancak bir devletin sorumluluğuna bağlanabildiği ölçüde hukuki karşılık bulmaktadır.

2.3. Bir Tipoloji Denemesi

Devlet dışı aktörleri devlet sorumluluğu bakımından anlamlı biçimde sınıflandırmak için iki ölçüt birlikte kullanılabilir: Aktörün kendisine doğrudan uygulanan uluslararası normlar ve aktörün davranışının bir devlete bağlanabileceği hukuki yollar.

Aktör türü	Örnek	Doğrudan bağlayıcı uluslararası norm	Devlete bağlanma yolu
Örgütlü silahlı gruplar	Kontralar, Bosnalı Sırp güçleri	Ortak m. 3, II No.lu Ek Protokol, örf ve âdet insancıl hukuku	ARSIWA m. 4 (fiilî organ), m. 8, m. 10
Terör örgütleri	El Kaide, IŞİD	BM Güvenlik Konseyi kararları (ör. 1373), uluslararası ceza hukuku	m. 8, m. 11; barınak devletinin özen yükümlülüğü
Özel askerî ve güvenlik şirketleri	Wagner Grubu	Montrö Belgesi (bağlayıcı değil), ulusal hukuk	m. 5, m. 8; sözleşme yapan, toprak ve ev sahibi devletin yükümlülükleri
Teknoloji şirketleri	Bulut, uydu, yapay zekâ ve gözetleme yazılımı sağlayıcıları	BM Rehber İlkeleri (bağlayıcı değil), AB mevzuatı	m. 5, m. 8, m. 16; ev sahibi devletin özen yükümlülüğü
Siber vekiller ve hacktivist gruplar	APT28 (GRU birimi), Rusya yanlısı hacktivistler	Ulusal ceza hukuku, Budapeşte Sözleşmesi	m. 4 (devlet birimi ise), m. 8, m. 11; toprak devletinin özen yükümlülüğü
Bireyler ve "tek kullanımlık ajanlar"	Sabotaj için çevrim içi işe alınan kişiler	Uluslararası ceza hukuku, ulusal ceza hukuku	m. 8 (talimat)

Siber alan bakımından Tim Maurer'in sınıflandırması ayrıca yol göstericidir.

Maurer, devletler ile siber vekiller arasındaki ilişkiyi üç modele ayırır:

- Devletin vekile belirli bir görev verdiği "yetki devri" (delegation),
- Devletin vekili doğrudan yönetmeden finansman, araç ya da bilgiyle desteklediği "orkestrasyon" (orchestration)
- Devletin vekilin faaliyetlerine göz yumduğu "onaylama" (sanctioning) (Maurer, 2018).

Bu üç model, ileride görüleceği üzere, ARSIWA'nın üç farklı sorumluluk yoluna kabaca karşılık gelmektedir: Yetki devri m. 8'deki talimata, orkestrasyon m. 8'deki yönlendirme ve kontrol ile m. 16'ya, onaylama ise özen yükümlülüğü ihlaline.

2.4. Kuvvet Kullanımı ve Silahlı Çatışmalar Hukukunda Devlet Dışı Aktörler

Devlet dışı aktörlerin uluslararası hukuktaki görünürlüğü 11 Eylül 2001 saldırılarıyla birlikte köklü biçimde artmıştır. BM Güvenlik Konseyi'nin 1368 ve 1373 sayılı kararları, terör örgütlerinin saldırıları karşısında meşru müdafaa hakkını hatırlatarak devlet dışı aktörlerin de "silahlı saldırı" gerçekleştirebileceği tartışmasını başlatmıştır. UAD ise İşgal Altındaki Filistin Topraklarında Duvar danışma görüşünde Şart m. 51'in devletlerarası bir silahlı saldırıyı öngördüğünü belirtmiş (*Legal Consequences of the Construction of a Wall*, 2004, par. 139), Kongo-Uganda davasında da bu soruyu açık bırakmıştır (*Armed Activities on the Territory of the Congo*, 2005, par. 147).

Bu tartışmanın devlet sorumluluğu bakımından önemi şudur: Bir devlet dışı aktörün saldırısı ile ev sahibi devlet arasındaki ilişkinin niteliği, hem saldırıya uğrayan devletin karşı tedbir ve meşru müdafaa gibi tepki araçlarını hem de ev sahibi devletin sorumluluğunu belirlemektedir. Literatürde "isteksiz ya da yetersiz" (unwilling or unable) devlet doktrini olarak bilinen yaklaşım da özünde, devlet dışı aktörü kontrol etmeyen devletin özen yükümlülüğü ihlali ile sorumluluk hukukunun kesiştiği bir alandır.

2.5. Siber Alanda Devlet Dışı Aktörün Özgüllüğü

Siber alan, devlet dışı aktörlerin etkisini benzersiz biçimde büyütmektedir. Birincisi, saldırı maliyeti son derece düşüktür. Kasım 2026'daki süpermarket saldırıları, birkaç kişinin internete bağlı soğutma sistemlerindeki zayıf kimlik doğrulamasından yararlanarak on ülkede on milyonlarca avroluk zarara yol açabildiğini göstermiştir. İkincisi, anonimlik ve sahte bayrak operasyonları atıfı teknik olarak zorlaştırmaktadır. Üçüncüsü, siber araçlar yayılmaya elverişlidir; bir devlet için geliştirilen bir saldırı aracı suç örgütlerinin eline geçebilmektedir.

Uluslararası toplum bu riski erken fark etmiştir. 2015 tarihli BM Hükümet Uzmanları Grubu (GGE) raporu, devletlerin bilgi ve iletişim teknolojileri aracılığıyla uluslararası haksız fiiller işlemek için vekil kullanmaması ve topraklarının devlet dışı aktörlerce bu tür fiiller için kullanılmamasını sağlamaya çalışması gerektiğini öngörmüştür (UN General Assembly, 2015, par. 28(e)). Bu ifade, sorumluluk hukukunun iki temel kanalını, yani vekil fiillerinin atfı ile toprak devletinin özen yükümlülüğünü, siber alana özgü bir dille yeniden ifade etmektedir.

2.6. Devlet Dışı Aktörden Devletin Sorumluluğuna

Buraya kadar ortaya konan tablo bir "hesap verebilirlik boşluğuna" işaret etmektedir. Devlet dışı aktörler uluslararası düzlemde ciddi zararlar doğurabilmekte, ancak kendileri genellikle uluslararası haksız fiil sorumluluğunun muhatabı olamamaktadır. Bu boşluk uluslararası hukukta iki yoldan doldurulmaktadır.

- **Birinci yol,** devlet dışı aktörün fiilinin belirli koşullarda devletin fiili sayılmasıdır **(atıf).**
- **İkinci yol,** devletin, devlet dışı aktörün fiilini önlemek veya bastırmak için gerekeni yapmaması nedeniyle kendi ihmalinden sorumlu tutulmasıdır **(özen yükümlülüğü).**

Uluslararası Hukuk Komisyonu bu iki yolu açıkça birbirinden ayırmaktadır. ARSIWA şerhine göre genel kural, özel kişilerin davranışının devlete atfedilmemesidir; atıf yalnızca kişinin devletle olgusal ya da hukuki bir bağ içinde hareket ettiği istisnai durumlarda mümkündür (International Law Commission [ILC], 2001, Bölüm II'ye giriş şerhi, par. 3). Ancak atfın bulunmaması, devletin sorumluluktan kurtulduğu anlamına gelmez; devlet, özel kişilerin fiillerine ilişkin kendi davranışı nedeniyle sorumlu olabilir. Tahran Rehineleri davası bu ayrımın klasik örneğidir: UAD, öğrencilerin büyükelçiliği işgalini başlangıçta İran'a atfetmemiş, ancak İran'ın büyükelçiliği korumak için gereken önlemleri almamasını doğrudan bir yükümlülük ihlali olarak kabul etmiştir (*United States Diplomatic and Consular Staff in Tehran*, 1980, par. 61-68).

Bir siber operasyonun ya da yapay zekâ destekli bir hedefleme kararının "askerî fiil" niteliği taşıyıp taşımadığı, uygulanacak birincil kuralları (insancıl hukuk, kuvvet kullanma yasağı, müdahale yasağı) belirler; atıf ve özen yükümlülüğü ise bu kuralların ihlalinin hangi devlete yükleneceğini belirleyen ikincil ve birincil mekanizmalardır. Bir sonraki bölüm bu mekanizmaları ayrıntılı biçimde incelemektedir.

3. Devlet Dışı Aktörlerin Fiillerinden Doğan Devlet Sorumluluğu

3.1. Uluslararası Haksız Fiilin Unsurları ve Siber Alana Uygulanabilirlik

ARSIWA m. 1 ve 2'ye göre bir devletin uluslararası haksız fiili, uluslararası hukuka göre o devlete atfedilebilen ve devletin uluslararası bir yükümlülüğünü ihlal eden bir davranıştan (fiil veya ihmal) oluşur. Kusur ve zarar, birincil kural aksini öngörmedikçe sorumluluğun genel unsurları arasında yer almaz (ILC, 2001, m. 2 şerhi, par. 9-10). Bu yaklaşım, otonom ve yapay zekâ destekli sistemler bakımından ileride önem kazanacaktır; zira devletin sorumluluğu için bir yetkilinin kastını ispat etmek gerekmemektedir.

Bu yaklaşım, otonom ve yapay zekâ destekli sistemler bakımından ileride önem kazanacaktır. Devletin sorumluluğu için, ihlal edilen birincil kural özel bir zihinsel unsur aramadıkça, sistemi onaylayan ya da kullanan yetkilinin kastını ispat etmek gerekmez; değerlendirme bireyin zihni yerine devletin kurumsal davranışına, yani sistemin test edilmesi, hukuki incelemesi ve insan denetimi gibi önlemlere odaklanır.

Uluslararası hukukun siber alana uygulanabilirliği bugün tartışma konusu değildir. BM GGE'nin 2013, 2015 ve 2021 raporları ile BM Genel Kurulu tarafından onaylanan normlar çerçevesi, BM Şartı'nın ve devlet sorumluluğuna ilişkin kuralların siber alanda geçerli olduğunu teyit etmektedir (UN General Assembly, 2015, 2021). 2021-2025 Açık Uçlu Çalışma Grubu (OEWG) ise Temmuz 2025'te oybirliğiyle kabul ettiği nihai raporla bu alanda kalıcı bir "Küresel Mekanizma" kurulmasının yolunu açmıştır. Asıl tartışma, genel kuralların siber alanın kendine özgü koşullarına nasıl uygulanacağı üzerinedir.

3.2. Devlet Organları ve Fiilî Organlar (m. 4)

ARSIWA m. 4'e göre iç hukukta devlet organı statüsüne sahip her kişi veya birimin davranışı devlete atfedilir. Bir ordunun siber birimi ya da bir askerî istihbarat servisinin alt birimi bu kategoriye girer. Almanya ve AB'nin değerlendirmelerinde APT28 grubu, Rus askerî istihbarat servisi GRU'nun 26165 numaralı birimi olarak tanımlanmaktadır. Bu nitelendirme doğruysa APT28'in fiilleri herhangi bir "kontrol" testine gerek kalmaksızın doğrudan Rusya'ya atfedilir; sorun hukuki değil, olgusal ispat sorunudur.

UAD, Bosna Soykırımı kararında iç hukukta organ statüsü bulunmayan kişi veya grupların da devlete "tam bağımlılık" içinde olmaları hâlinde fiilî organ (de facto organ) sayılabileceğini kabul etmiştir. Ancak bu ölçüt son derece yüksektir: Grubun devletin basit bir aracı olması ve hiçbir gerçek özerkliğe sahip olmaması gerekir (*Bosnia and Herzegovina v. Serbia and Montenegro*, 2007, par. 392-393). Siber alanda kendini "gönüllü" olarak sunan hacktivist grupların bu eşiğe ulaştığını ispat etmek pratikte neredeyse imkânsızdır.

3.3. Kamu Yetkisi Kullanan Kişiler ve Kuruluşlar (m. 5)

ARSIWA m. 5, devlet organı olmamakla birlikte iç hukukla kamu yetkisinin unsurlarını kullanmaya yetkilendirilmiş kişi veya kuruluşların, bu sıfatla hareket ettikleri ölçüde davranışlarının devlete atfedileceğini öngörür. Komisyon şerhine göre belirleyici olan, kuruluşun mülkiyet yapısı değil, kendisine devredilen yetkinin "kamusal" niteliğidir; özel güvenlik şirketlerine cezaevi işletme yetkisi verilmesi buna örnek gösterilmektedir (ILC, 2001, m. 5 şerhi, par. 2).

Bu hüküm teknoloji şirketleri bakımından henüz yeterince işletilmemiş bir potansiyele sahiptir. Bir devletin, ulusal siber savunma merkezinin işletilmesini, kritik altyapı ağlarının izlenmesini, istihbarat verisinin analizini veya askerî hedefleme altyapısını yasal bir düzenleme ya da idari bir yetkilendirme yoluyla özel bir şirkete devretmesi hâlinde, şirketin bu faaliyet kapsamındaki davranışları m. 5 uyarınca devlete atfedilebilir. Buna karşılık bir bulut sağlayıcısının devlete sıradan ticari veri depolama hizmeti sunması kamu yetkisi kullanımı değildir. Ayrım çizgisi, şirketin devlet adına bir egemenlik işlevi yerine getirip getirmediğidir.

3.4. Talimat, Yönlendirme veya Kontrol (m. 8): Doktrinin Düğüm Noktası

ARSIWA m. 8'e göre bir kişi veya kişi grubunun davranışı, bu kişiler fiilen devletin talimatıyla ya da devletin yönlendirmesi veya kontrolü altında hareket ediyorsa devlete atfedilir. Siber ve hibrit operasyonlarda en sık başvurulan ve en çok tartışılan hüküm budur.

UAD, Nikaragua davasında ABD'nin kontraları finanse etmesi, örgütlemesi, eğitmesi ve donatmasının, kontraların fiillerini ABD'ye atfetmek için yeterli olmadığına karar vermiştir. Divan'a göre atıf için ABD'nin ihlallerin gerçekleştiği **"belirli operasyonlar üzerinde etkin kontrol"** sahibi olduğunun ispatı gerekmektedir (*Nicaragua v. United States*, 1986, par. 115). Eski Yugoslavya Uluslararası Ceza Mahkemesi (ICTY) Temyiz Dairesi ise Tadić kararında, örgütlü silahlı gruplar bakımından devletin grubu örgütlemesi, koordine etmesi ve planlamasına katılmasını yeterli sayan daha esnek bir **"genel kontrol"** ölçütü önermiştir (*Prosecutor v. Tadić*, 1999, par. 131-137). **UAD, Bosna Soykırımı kararında Tadić yaklaşımını devlet sorumluluğu bakımından açıkça reddetmiş; genel kontrol ölçütünün bir silahlı çatışmanın uluslararası nitelik taşıyıp taşımadığının belirlenmesinde uygun olabileceğini, ancak atıf için etkin kontrolün aranması gerektiğini teyit etmiştir (*Bosnia and Herzegovina v. Serbia and Montenegro*, 2007, par. 400-406).** Antonio Cassese bu tercihi, devletlerin vekiller aracılığıyla sorumluluktan kaçmasına imkân tanıdığı gerekçesiyle sert biçimde eleştirmiştir (Cassese, 2007).

Siber alanda etkin kontrol ölçütü kendine özgü zorluklar doğurmaktadır. Tallinn Kılavuzu 2.0'ı hazırlayan uluslararası uzmanlar grubu etkin kontrol ölçütünü benimsemiş (Schmitt, 2017, Kural 17); Almanya (2021) ve Fransa (2019) gibi devletler de ulusal pozisyon belgelerinde aynı ölçütü kabul etmiştir. **Ancak siber vekillerle kurulan ilişkiler çoğunlukla operasyon bazında talimat izi bırakmamaktadır.** Kâmil Mačák bu sorunu aşmak için m. 8'in üç unsurunun, yani "talimat", "yönlendirme" ve "kontrol"ün birbirinden ayrı ve bağımsız atıf temelleri olarak okunması gerektiğini savunmaktadır (Mačák, 2016). **Bu okuma özellikle "talimat" unsurunu öne çıkarır: Devletin belirli bir hedefe yönelik bir operasyonu sipariş ettiğinin ispatı, operasyonun her aşaması üzerinde kontrol bulunduğunun ispatından çok daha kolaydır.**

Avrupa'daki son olaylar bu ayrımın pratik önemini göstermektedir. Polonya'nın Kasım 2025 demiryolu sabotajında failleri "Rus istihbaratı adına hareket eden" kişiler olarak tanımlaması ve Polonya İç Güvenlik Ajansı'nın Rusya'nın "tek kullanımlık ajanlar" kullandığını açıklaması, m. 8'deki talimat unsurunun örneğidir. Çevrim içi olarak işe alınan, belirli bir görev için ödeme vaat edilen ve görevi yerine getiren bir kişinin fiili, talimatın ispatı hâlinde doğrudan devlete atfedilebilir.

Buna karşılık Kasım 2026'daki süpermarket saldırılarını üstlenen hacktivist grupların bir devletin talimatıyla hareket ettiğini ispat etmek çok daha güçtür; bu grupların devletin finansmanı ve teşvikiyle ama kendi inisiyatifleriyle hareket ettiği durumlar, Nikaragua ölçütüne göre atıf için yeterli değildir.

3.5. Benimseme (m. 11) ve Yardım ile Destek (m. 16)

ARSIWA m. 11'e göre başlangıçta devlete atfedilemeyen bir davranış, devletin bu davranışı kendi davranışı olarak tanıması ve benimsemesi hâlinde ve ölçüsünde devletin fiili sayılır. UAD, Tahran Rehineleri davasında İran makamlarının büyükelçilik işgalini onaylayan ve sürdürülmesine karar veren açıklamalarının, işgali İran devletinin fiiline dönüştürdüğüne hükmetmiştir (*United States Diplomatic and Consular Staff in Tehran*, 1980, par. 74). **Siber alanda bir devletin vekil saldırıyı açıkça övmesi, failleri ödüllendirmesi ya da iade taleplerine karşı onları koruma altına alması, benimseme tartışmasını gündeme getirebilir.** Ancak Komisyon şerhi, basit onay veya destek beyanlarının benimseme için yeterli olmadığını, davranışın açıkça **"kendi davranışı olarak" kabul edilmesi gerektiğini vurgulamaktadır** (ILC, 2001, m. 11 şerhi, par. 6).

ARSIWA m. 16 ise türev sorumluluğu düzenler: Başka bir devlete uluslararası haksız fiil işlemesinde yardım veya destek sağlayan devlet, durumu bilerek hareket etmişse ve fiil kendisi tarafından işlenseydi de haksız olacaksa sorumludur. UAD, Bosna Soykırımı kararında bu hükmü örf ve âdet hukukunun bir parçası olarak kabul etmiştir (*Bosnia and Herzegovina v. Serbia and Montenegro*, 2007, par. 420). **Hüküm, bir devletin başka bir devlete saldırı**

amaçlı siber araç, gözetleme yazılımı ya da hedefleme algoritması sağladığı durumlar bakımından doğrudan uygulanabilir niteliktedir.

3.6. Özen Yükümlülüğü: Korfu Kanalı'ndan Siber Alana

Atfın kurulamadığı durumlarda devletin sorumluluğu, kendi topraklarındaki veya kendi yetki alanındaki faaliyetler bakımından özen yükümlülüğünü ihlal etmesine dayanabilir. UAD, Korfu Kanalı davasında her devletin kendi topraklarının bilerek başka devletlerin haklarına aykırı fiiller için kullanılmasına izin vermeme yükümlülüğü altında olduğunu ilan etmiştir (*Corfu Channel*, 1949, s. 22). Pulp Mills kararında Divan, özen yükümlülüğünün bir sonuç yükümlülüğü değil, bir davranış yükümlülüğü olduğunu ve devletin elindeki tüm makul araçları kullanmasını gerektirdiğini belirtmiştir (*Pulp Mills on the River Uruguay*, 2010, par. 197). Bosna Soykırımı kararında ise önleme yükümlülüğünün kapsamının, devletin olayları etkileme kapasitesine göre belirleneceği vurgulanmıştır (*Bosnia and Herzegovina v. Serbia and Montenegro*, 2007, par. 430).

Tallinn Kılavuzu 2.0, bir devletin kendi topraklarındaki veya hükümet kontrolündeki siber altyapının, başka devletlerin haklarını etkileyen ve ciddi olumsuz sonuçlar doğuran siber operasyonlar için kullanılmasına izin vermeme yükümlülüğünü kabul etmektedir (Schmitt, 2017, Kural 6-7). Ancak devletler bu konuda ikiye ayrılmıştır. Fransa ve Hollanda özen yükümlülüğünü bağlayıcı bir uluslararası hukuk kuralı olarak kabul ederken, Birleşik Krallık ve Amerika Birleşik Devletleri bunu bağlayıcı olmayan bir davranış normu olarak görmektedir. AB'nin 2024 tarihli beyanı ise özen yükümlülüğüne açıkça yer vererek Avrupa'nın ortak tutumunu bağlayıcılık yönünde güçlendirmiştir (Council of the European Union, 2024). Eric Talbot Jensen ve Sean Watts, özen yükümlülüğünün siber alanda kapsamı belirsiz kaldığı sürece istikrar sağlamak yerine gerilimi artırabileceği uyarısında bulunmuştur (Jensen ve Watts, 2017).

Özen yükümlülüğünün içeriği bakımından kritik soru, devletin "bilgisinin" nasıl ölçüleceğidir. Korfu Kanalı kararı fiilî bilgiyi esas almakla birlikte, bu bilginin dolaylı delillerle ve olgusal karinelerle ispat edilebileceğini kabul etmiştir. **Siber alanda devletlerin kendi topraklarından kaynaklanan saldırılar hakkında başka devletlerden, uluslararası CERT ağlarından ve teknoloji şirketlerinden sürekli bildirim aldığı dikkate alındığında, "bilmesi gereken" (constructive knowledge) standardının uygulanması hem Korfu Kanalı içtihadıyla hem de UAD'nin 2025 tarihli İklim Değişikliği danışma görüşünde benimsediği risk temelli ve gerekli özen anlayışıyla uyumludur.**

3.7. Atıf Sorununun Teknik, Siyasi ve Hukuki Boyutları

Atıf sorunu yalnızca hukuki bir ölçüt sorunu değil, aynı zamanda bir ispat sorunudur. UAD, devlet sorumluluğunu doğuracak ağır iddiaların "tamamen ikna edici" delillerle ispatlanması gerektiğini belirtmiştir (*Bosnia and Herzegovina v. Serbia and Montenegro*, 2007, par. 209). Siber operasyonlarda bu deliller çoğunlukla istihbarat servislerinin elindedir ve kaynakları ifşa etmeden paylaşılamamaktadır. Thomas Rid ve Ben Buchanan, siber atfın ikili bir "var/yok" meselesi değil, teknik, operasyonel ve stratejik katmanlardan oluşan ve nihayetinde siyasi bir yargıya dayanan bir süreç olduğunu vurgulamaktadır (Rid ve Buchanan, 2015).

Almanya'nın 12 Aralık 2025 tarihli açıklaması bu gerilimi açıkça yansıtmaktadır. Almanya, DFS saldırısını APT28 ve GRU'ya kesin delillere dayanarak atfettiğini açıklamış, ancak bu delilleri istihbarat gerekçesiyle kamuoyuyla paylaşmamıştır. BM GGE'nin 2015 raporu devletlere yöneltilen suçlamaların temellendirilmesi gerektiğini öngörse de bu norm bağlayıcı değildir (UN General Assembly, 2015, par. 28(f)). **Sonuç olarak Avrupa'da sıkça rastlanan durum, güçlü bir siyasi atfın hukuki bir sorumluluk talebine, yani tazminat talebine, uluslararası yargıya başvuruya ya da ARSIWA anlamında karşı tedbire dönüştürülmemesidir.**

3.8. Mağdur Devletin Tepki Araçları

Sorumluluk hukuku mağdur devlete çeşitli tepki araçları sunmaktadır. Birincisi karşı tedbirlerdir: ARSIWA m. 49-54, mağdur devletin sorumlu devleti yükümlülüklerine uymaya zorlamak amacıyla kendi yükümlülüklerinden geçici olarak ayrılabileceğini öngörür. Ancak karşı tedbirler; önceden bildirim, orantılılık, geri döndürülebilirlik ve kuvvet kullanmama koşullarına tabidir ve yalnızca sorumlu devlete yöneltilebilir. Estonya Cumhurbaşkanı Kersti Kaljulaid'in 2019'da savunduğu "kolektif karşı tedbir" fikri, yani doğrudan zarar görmeyen devletlerin mağdur devlet adına karşı tedbir alabilmesi, Fransa tarafından reddedilmiş ve henüz genel kabul görmemiştir.

İkincisi zarurettir: ARSIWA m. 25, esaslı bir menfaati ağır ve yakın bir tehlikeye karşı korumanın tek yolu olan bir davranışın hukuka aykırılığını, katı koşullar altında ortadan kaldırır (*Gabčíkovo-Nagymaros Project*, 1997, par. 51-52). Zaruretin özelliği, saldırganın kimliğinin tespit edilmesini gerektirmemesidir. AB'nin 2024 beyanında kritik altyapının esaslı menfaat sayılabileceğinin kabul edilmesi, atıfın yapılamadığı hibrit saldırılara karşı zaruretin önemli bir hukuki dayanak olabileceğini göstermektedir.

Üçüncüsü retorsiyondur: Büyükelçi çağırma, diplomat sınır dışı etme veya ekonomik ilişkileri kısıtlama gibi, kendisi hukuka aykırı olmayan "dostane olmayan" tedbirler. Avrupa devletlerinin şimdiye kadarki tepkilerinin büyük kısmı bu kategoriye girmektedir. AB'nin kişi ve kuruluşlara yönelik kısıtlayıcı tedbirlerinin hukuki niteliği ise tartışmalıdır;

bu tedbirler devlete yöneltilmediği için klasik anlamda karşı tedbir sayılmamakta, daha çok AB hukukuna dayanan bağımsız bir dış politika aracı olarak işlemektedir.

4. Yeni Devlet Dışı Aktörler Olarak Teknoloji Şirketleri

4.1. Neden "Yeni" Aktörler?

Teknoloji şirketleri uluslararası hukuk açısından yeni değildir; ancak modern çatışmalardaki rolleri niteliksel olarak değişmiştir. Geleneksel özel askerî şirketler devlete insan gücü ve hizmet sağlarken, teknoloji şirketleri devletin savaşma ve savunma kapasitesinin altyapısını kontrol etmektedir. Bir orduya bulut depolama, uydu iletişimi ya da yapay zekâ destekli veri analizi sağlayan şirket, bu hizmeti tek taraflı olarak kesebilir; başka bir deyişle elinde bir tür "kapatma anahtarı" bulunur. Bu güç, devlet ile şirket arasındaki klasik ilişkiyi tersine çevirebilmektedir. Bu çalışmada teknoloji şirketleri çatışmalardaki işlevlerine göre üç tipe ayrılmaktadır:

(a) Saldırıya uğrayan devletin yanında yer alan "savunma ortağı" şirketler,

(b) bir devletin askerî veya istihbarat faaliyetlerine altyapı ve yapay zekâ hizmeti sağlayan "altyapı sağlayıcı" şirketler

(c) saldırı kabiliyeti üreten, satan veya kullanan "saldırı aracı" şirketler. Her tip, devlet sorumluluğu bakımından farklı sorular doğurmaktadır.

4.2. Savunma Ortağı Şirketler: Ukrayna Deneyimi

Rusya'nın Şubat 2022'de Ukrayna'ya yönelik tam ölçekli işgali, teknoloji şirketlerinin savunma ortağı rolünü görünür kılmıştır. Microsoft, işgalin ilk saatlerinden itibaren Ukrayna kamu kurumlarına yönelik yıkıcı yazılım saldırılarını tespit ettiğini ve Ukrayna hükümetinin verilerinin yurt dışındaki veri merkezlerine taşınmasına destek verdiğini açıklamıştır (Microsoft, 2022). Google ve bağlı şirketi Mandiant tehdit istihbaratı paylaşmış, SpaceX'in Starlink uydu ağı ise Ukrayna ordusunun ve sivil altyapısının iletişiminde kritik bir rol üstlenmiştir.

Bu tablo iki hukuki soruyu gündeme getirmektedir. Birincisi, bu şirketlerin faaliyetlerinin ev sahibi devlete (çoğunlukla ABD'ye) atfedilip atfedilemeyeceğidir. **Kural olarak bir şirketin kendi inisiyatifiyle yürüttüğü ticari veya gönüllü faaliyetler devlete atfedilmez.** Ancak şirketin devletle sözleşme ilişkisi içinde ve devletin talimatıyla belirli bir askerî destek faaliyeti yürüttüğü durumlarda m. 8 kapsamında atıf tartışmaya açılır. İkincisi, şirketin bir hizmeti kısıtlama veya kesme kararının, örneğin belirli bir bölgede uydu kapsama alanını sınırlamasının, bir askerî operasyonu fiilen engelleyebilmesidir. Bu durum, özel bir aktörün çatışmanın seyrini etkileyebildiği ancak bu etkinin hiçbir devletin sorumluluk rejimine doğrudan bağlanamadığı yeni bir "hesap verebilirlik boşluğu" yaratmaktadır.

4.3. Altyapı Sağlayıcı Şirketler: Microsoft ve Birim 8200 Vakası

Altyapı sağlayıcı şirketlere ilişkin en çarpıcı güncel örnek, Microsoft'un İsrail askerî istihbaratına sunduğu bulut hizmetleridir. The Guardian, +972 Magazine ve Local Call'un Ağustos 2025'te yayımladığı ortak araştırmaya göre İsrail'in askerî istihbarat birimi Birim 8200, Gazze ve Batı Şeria'daki Filistinlilere ait milyonlarca telefon görüşmesinin kayıtlarını Microsoft'un Azure bulut platformunda, kısmen Hollanda'daki veri merkezlerinde saklamaktaydı. Microsoft bir iç inceleme başlatmış ve 25 Eylül 2025'te Başkan Brad Smith, İsrail Savunma Bakanlığı'na bağlı bir birimin belirli bulut depolama ve yapay zekâ hizmetlerine erişiminin durdurulduğunu açıklamıştır (CNN, 2025). İddialar yargısal olarak doğrulanmamış olup iddia olarak değerlendirilmektedir.

Vaka, sorumluluk hukuku bakımından çok katmanlı bir analiz gerektirir.

Birinci katmanda, bulut altyapısını kullanarak gözetleme yapan askerî birimin fiilleri m. 4 uyarınca doğrudan İsrail'e atfedilir; şirketin rolü bu atfı değiştirmez.

İkinci katmanda, verilerin Hollanda'da barındırılması, toprak devleti olarak Hollanda'nın özen yükümlülüğünü gündeme getirir: Bir devlet, kendi topraklarındaki altyapının başka bir devletin uluslararası hukuka aykırı faaliyetleri için kullanıldığını bildiği veya bilmesi gerektiği hâlde makul önlemleri almaktan kaçınırsa sorumlu olabilir.

Üçüncü katmanda, şirketin merkezinin bulunduğu ev sahibi devlet olarak ABD'nin, kendi yetki alanındaki şirketlerin yurt dışı faaliyetlerini düzenleme yükümlülüğü tartışılabilir.

Dördüncü katmanda ise şirketin kendisinin, BM Rehber İlkeleri uyarınca çatışmadan etkilenen bölgelerde "artırılmış" insan hakları özen yükümlülüğü bulunmaktadır (UN Human Rights Council, 2011, İlke 7 ve 17-19).

Microsoft'un hizmeti kesme kararı, hukuken bağlayıcı bir yükümlülüğün değil, şirketin kendi kullanım koşulları ve itibar kaygılarının ürünüdür. Bu durum, şirketlerin fiilen bir tür denetim işlevi üstlendiğini, ancak bu işlevin hiçbir uluslararası hukuki çerçeveye bağlı olmadığını göstermektedir.

Altyapı sağlayıcı şirketler, saldırının hedefi olduklarında da devlet sorumluluğu tartışmasına dahil olmaktadır. Eylül 2025'teki Collins Aerospace saldırısı, tek bir yazılım tedarikçisinin birden fazla AB havalimanını aynı anda felç edebildiğini göstermiştir. Bu vaka devlete atfedilen bir saldırı değildir; ancak NIS2 Direktifi'nin temel hizmet sağlayıcılara yüklediği tedarik zinciri güvenliği yükümlülükleri ile devletin kritik altyapıyı koruma yönündeki özen yükümlülüğü arasındaki bağlantıyı somutlaştırmaktadır.

4.4. Saldırı Aracı Şirketler: Pegasus ve Siber Paralı Askerler

Üçüncü tip, saldırı kabiliyeti üreten ve satan şirketlerdir. İsrail merkezli NSO Group'un geliştirdiği Pegasus casus yazılımı, gazetecilerin, insan hakları savunucularının ve muhalif politikacıların telefonlarının birçok ülkede gizlice ele geçirilmesinde kullanılmıştır. Avrupa Parlamentosu'nun PEGA Soruşturma Komitesi, 2023 tarihli raporunda bazı AB üye devletlerinin de bu yazılımı kullandığını tespit etmiştir. ABD'de WhatsApp'ın NSO Group aleyhine açtığı davada Mayıs 2025'te jüri şirketi yaklaşık 167 milyon dolar cezai tazminata mahkûm etmiş, ancak Kaliforniya Kuzey Bölge Mahkemesi Ekim 2025'te bu tutarı yaklaşık 4 milyon dolara indirmiştir.

Devlet sorumluluğu bakımından bu tablo üç ayrı sorumluluk ilişkisi doğurur.
Casus yazılımı kullanan devletin fiili, kullananlar devlet organı olduğu için m. 4 uyarınca o devlete atfedilir ve devlet, örneğin özel hayatın gizliliği hakkını ihlal etmekten sorumludur. Yazılımın ihracatına izin veren ev sahibi devlet ise, yazılımın insan hakları ihlallerinde kullanılacağını bildiği veya bilmesi gerektiği hâlde ihracat izni vermişse, m. 16 kapsamında yardım ve destek sorumluluğu ya da kendi özen yükümlülüğü bakımından sorumluluk ile karşı karşıya kalabilir. Şirketin kendisi ise ancak ulusal hukuk önünde sorumlu tutulabilmektedir.

Uluslararası toplum bu alanı düzenlemeye yönelik ilk adımları atmıştır. Birleşik Krallık ve Fransa'nın Şubat 2024'te başlattığı Pall Mall Süreci, ticari siber saldırı kabiliyetlerinin yayılmasını sınırlamayı amaçlamakta ve 2025'te devletler için bir Uygulama Kuralları belgesi ortaya koymuştur. Ancak süreç bağlayıcı değildir. Özel askerî ve güvenlik şirketlerine ilişkin 2008 tarihli Montrö Belgesi'nin sözleşme yapan devlet, toprak devleti ve ev sahibi devlet ayrımı, siber paralı askerler bakımından da analojik bir çerçeve sunabilir.

4.5. İnsancıl Hukuk Açısından Teknoloji Şirketleri

Silahlı çatışma sırasında askerî operasyonlara destek veren teknoloji şirketleri, uluslararası insancıl hukuk bakımından da yeni sorular doğurmaktadır. Uluslararası Kızılhaç Komitesi'nin (ICRC) Düşmanlıklara Doğrudan Katılım Kavramına İlişkin Yorumlayıcı Rehberi, bir sivilin korunmuş statüsünü kaybetmesi için zarar eşiği, doğrudan nedensellik ve muharip bağlantı koşullarının birlikte gerçekleşmesini aramaktadır (Melzer, 2009). Bir şirket çalışanının yapay zekâ destekli hedefleme sistemini anlık olarak işletmesi bu koşulları karşılayabilirken, genel bulut altyapısının bakımını yapması genellikle karşılamaz.

Şirket altyapısının kendisi de askerî hedef hâline gelebilir. I No.lu Ek Protokol m. 52(2), niteliği, konumu, amacı veya kullanımı itibarıyla askerî harekâta etkin katkıda bulunan ve tahribi kesin bir askerî avantaj sağlayan nesneleri askerî hedef olarak tanımlamaktadır. Askerî verilerin sivil bulut altyapısında barındırılması, bu altyapıyı "çift kullanımlı" bir nesneye dönüştürerek sivil kullanıcıları da risk altına sokmaktadır. Bu nedenle I No.lu Ek Protokol m. 58'deki savunan tarafın önlem alma yükümlülüğü, devletlerin askerî verilerini sivil altyapıdan ayırma yükümlülüğü olarak yorumlanabilir. ICRC, Ekim 2023'te çatışmalara katılan sivil bilgisayar korsanları için sekiz temel kural yayımlamış, Ekim 2024'te toplanan 34. Uluslararası Kızılhaç ve Kızılay Konferansı ise sivillerin bilgi ve iletişim teknolojisi faaliyetlerinin insani maliyetine karşı korunmasına ilişkin bir karar kabul etmiştir.

4.6. Şirket Sorumluluğu ile Devlet Sorumluluğunun Kesişimi

Teknoloji şirketlerinin uluslararası hukukta doğrudan sorumluluğu bulunmadığından, bu alandaki hesap verebilirlik büyük ölçüde devletler üzerinden kurulmaktadır. BM Ekonomik, Sosyal ve Kültürel Haklar Komitesi'nin 24 No.lu Genel Yorumu, devletlerin kendi yetki alanındaki şirketlerin yurt dışındaki faaliyetlerinin insan haklarına zarar vermesini önlemek için makul önlemler alması gerektiğini belirtmektedir (Committee on Economic, Social and Cultural Rights, 2017). AB'nin Kurumsal Sürdürülebilirlik Özen Yükümlülüğü Direktifi (2024/1760) ise şirketlere değer zincirlerinde insan hakları risklerini belirleme ve önleme yükümlülüğü getirmektedir.

Bu düzenlemeler, devletin özen yükümlülüğü ile şirketin özen yükümlülüğü arasında bir köprü kurmaktadır. Devlet, şirketlerine bu tür yükümlülükler getirdiği ve bunları denetlediği ölçüde kendi uluslararası özen yükümlülüğünü yerine getirmiş sayılabilir. Tersine, şirketlerinin askerî veya gözetleme amaçlı hizmetlerinin uluslararası hukuka aykırı faaliyetlerde kullanıldığını bildiği hâlde hiçbir düzenleyici önlem almayan devlet, kendi ihmali nedeniyle sorumluluk riskiyle karşı karşıya kalır.

5. Stratejik Bir Silah Olarak Yapay Zekâ ve Devletin Sorumluluğu

5.1. Kavramsal Ayrımlar

Yapay zekânın askerî kullanımı tek bir olgu değildir ve hukuki analiz bakımından en az dört kategoriye ayrılmalıdır. Birincisi, insan müdahalesi olmaksızın hedef seçebilen ve angaje edebilen ölümcül otonom silah sistemleridir (LAWS). İkincisi, hedef önerisi üreten ancak nihai kararı bir insana bırakan yapay zekâ destekli karar destek sistemleridir. Üçüncüsü, zafiyet tespiti, oltalama ve kötü amaçlı yazılım geliştirme gibi siber saldırı zincirinin aşamalarını hızlandıran yapay zekâ araçlarıdır. Dördüncüsü ise sahte ses ve görüntüler (deepfake) ile otomatik içerik üretimine dayanan dezenformasyon kampanyalarıdır.

Bu ayrım önemlidir; çünkü her kategori farklı birincil kurallarla ilişkilidir. Otonom silahlar ve hedefleme sistemleri ağırlıklı olarak insancıl hukukun ayrım, orantılılık ve önlem ilkeleriyle; yapay zekâ destekli siber operasyonlar egemenlik ve müdahale yasağıyla; dezenformasyon kampanyaları ise özellikle seçimlere müdahale bağlamında müdahale yasağı ve insan haklarıyla ilişkilidir.

5.2. Çok Taraflı Süreçler: Bağlayıcı Bir Rejim Hâlâ Yok

Otonom silahlar konusundaki uluslararası tartışma, 2014'ten bu yana Belirli Konvansiyonel Silahlar Sözleşmesi (CCW) çerçevesinde yürütülmektedir. 2017'de kurulan Hükümet Uzmanları Grubu (GGE), 2023'te üç yıllık yeni bir yetki almış ve Eylül 2026'da bağlayıcı olmayan bir nihai raporu oybirliğiyle kabul etmiştir. Bağlayıcı bir belge müzakere edilip edilmeyeceği kararı, 16-20 Kasım 2026'da toplanacak Yedinci Gözden Geçirme Konferansı'na bırakılmıştır.

BM Genel Kurulu da konuya giderek daha fazla ilgi göstermektedir. Genel Kurul'un ölümcül otonom silah sistemlerine ilişkin 2024 tarihli kararı (A/RES/79/62) 166 lehte, 3 aleyhte ve 15 çekimser oyla kabul edilmiştir. 1 Aralık 2025 tarihli karar (A/RES/80/57) ise 164 lehte, 6 aleyhte ve 7 çekimser oyla kabul edilmiş; ABD önceki yıllardaki olumlu oyunun aksine bu kez aleyhte oy kullanmıştır. Bu değişiklik, devlet uygulaması bakımından dikkate alınması gereken önemli bir gelişmedir.

Yumuşak hukuk düzleminde Hollanda ve Güney Kore'nin öncülüğünde başlatılan Askerî Alanda Sorumlu Yapay Zekâ (REAIM) zirveleri 2023'te Lahey'de, 2024'te Seul'de ve Şubat 2026'da İspanya'nın A Coruña kentinde toplanmıştır. A Coruña'da kabul edilen belge 85 katılımcı devletten yalnızca 35'i tarafından imzalanmış, ABD ve Çin imzalamamıştır.

Avrupa düzleminde ise dikkat çekici bir boşluk bulunmaktadır. AB Yapay Zekâ Yasası, münhasıran askerî, savunma veya ulusal güvenlik amaçlarıyla piyasaya sürülen ya da kullanılan yapay zekâ sistemlerini kapsam dışında bırakmaktadır (Regulation (EU) 2024/1689, 2024, m. 2(3)). Avrupa Konseyi'nin 2024 tarihli Yapay Zekâ ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi de ulusal savunmaya ilişkin konuları kapsamına almamaktadır (Council of Europe, 2024, m. 3(4)). Dolayısıyla askerî yapay zekânın hukuki çerçevesi, Avrupa'da da genel uluslararası hukuka, yani insancıl hukuka, insan hakları hukukuna ve devlet sorumluluğu kurallarına geri dönmektedir.

5.3. Gazze ve Ukrayna'da Yapay Zekâ Destekli Hedefleme

Yapay zekânın askerî kullanımına ilişkin tartışma, iki güncel çatışmayla somutlaşmıştır. +972 Magazine ve Local Call'un Kasım 2023 ve Nisan 2024 tarihli araştırmaları, İsrail ordusunun Gazze'de "Gospel" (Habsora) ve "Lavender" adlı yapay zekâ destekli sistemlerle çok büyük ölçekte hedef ürettiğini, insan doğrulamasının ise bazen yalnızca birkaç saniye sürdüğünü ileri sürmüştür. İsrail ordusu bu iddiaları reddetmiş ve söz konusu sistemlerin yalnızca analistlere yardımcı araçlar olduğunu belirtmiştir. Ukrayna'da ise her iki taraf da yapay zekâ destekli drone ve hedef tanıma sistemlerini yoğun biçimde kullanmaktadır.

Hukuki açıdan bu vakaların sonucu açıktır: Bir yapay zekâ sisteminin önerdiği hedefi onaylayan ve saldırıyı gerçekleştiren askerin fiili, ARSIWA m. 4 uyarınca devlete atfedilir. Sistemin hatalı bir öneride bulunması, devletin sorumluluğunu ortadan kaldırmaz. ARSIWA m. 23'teki mücbir sebep, devletin kontrolü dışındaki karşı konulamaz olayları kapsar; devletin kendi tercihiyle konuşlandırdığı bir sistemin hatası ise bu kapsamda değildir. Ayrıca I No.lu Ek Protokol m. 36, devletlere yeni silah, araç veya yöntemlerin insancıl hukuka uygunluğunu önceden inceleme yükümlülüğü getirmektedir; yapay zekâ destekli bir hedefleme sisteminin bu incelemeden geçirilmeden kullanılması başlı başına bir yükümlülük ihlali oluşturabilir.

5.4. "Sorumluluk Boşluğu" Tartışması

Felsefe ve etik literatüründe Andreas Matthias ve Robert Sparrow, öğrenen sistemlerin davranışlarının önceden öngörülemeyebileceğini ve bu nedenle hiç kimsenin bu davranışlardan ahlaken sorumlu tutulamayacağı bir "sorumluluk boşluğu" doğabileceğini ileri sürmüştür (Matthias, 2004; Sparrow, 2007). Bu argüman, otonom silahların yasaklanması yönündeki kampanyaların temel dayanaklarından biri hâline gelmiştir.

Ancak devlet sorumluluğu açısından bu boşluk büyük ölçüde mevcut değildir. Devlet sorumluluğu kusur gerektirmediğinden, bir otonom sistemi konuşlandırma kararı devlet organının fiilidir ve sistemin sonradan ortaya çıkan davranışlarından doğan ihlaller devlete atfedilir. Rebecca Crootof, bu nedenle otonom silahlar için devletlerin kusursuz sorumluluğuna dayanan bir "savaş haksız fiilleri" (war torts) rejimi önermiştir (Crootof, 2016). Berenice Boutin de askerî yapay zekâ uygulamalarında devlet sorumluluğunun, bireysel ceza sorumluluğundaki boşlukları telafi edebilecek temel mekanizma olduğunu savunmaktadır (Boutin, 2023).

Bu nedenle çalışmada üç katmanlı bir sorumluluk modeli önerilmektedir. Birinci katman devletin sorumluluğudur: Atıf ve insancıl hukuk ihlali üzerinden kurulur ve kusur gerektirmez. İkinci katman bireysel ceza sorumluluğudur:

Roma Statüsü m. 30'daki kast şartı ve m. 28'deki komutan sorumluluğu nedeniyle sorumluluk boşluğunun gerçekten ortaya çıktığı katman budur. Üçüncü katman şirket sorumluluğudur: Sistemi geliştiren veya işleten şirketin ulusal hukuk ve insan hakları özen yükümlülüğü çerçevesindeki sorumluluğudur. Sorumluluk boşluğu söylemi, bu üç katmanı birbirinden ayırmadığı için devlet sorumluluğunun mevcut kapasitesini olduğundan zayıf göstermektedir.

5.5. Yapay Zekâ Destekli Siber Operasyonlar ve Dezenformasyon

Yapay zekâ, siber saldırıların ölçeğini ve inandırıcılığını artırmaktadır. ENISA'nın 2025 raporuna göre yapay zekâ destekli oltalama, küresel sosyal mühendislik faaliyetinin büyük bölümünü oluşturmaktadır (ENISA, 2025). Almanya'nın Aralık 2025'te Rusya'ya atfettiği "Storm-1516" kampanyası ise Şubat 2025 federal seçimleri öncesinde sahte haber siteleri ve manipüle edilmiş videolar aracılığıyla yürütülmüştür.

Bu tür kampanyaların hukuki nitelendirmesinde müdahale yasağı ön plana çıkmaktadır. UAD, Nikaragua kararında yasak müdahalenin iki unsurunu, yani devletin serbestçe karar verme hakkına sahip olduğu bir alanı hedef alması ve "zorlama" (coercion) unsuru içermesini aramıştır (*Nicaragua v. United States*, 1986, par. 205). Dezenformasyon kampanyalarının zorlama unsuru taşıyıp taşımadığı doktrinde tartışmalıdır. Ancak bir devletin seçim altyapısına yönelik siber saldırılar ya da seçmenlerin karar verme sürecini çarpıtmaya yönelik sistematik ve gizli kampanyalar, Almanya ve Fransa gibi devletlerin ulusal pozisyonlarında müdahale yasağının ihlali olarak kabul edilmektedir.

Yapay zekânın atıf bakımından getirdiği asıl yenilik, saldırıların daha az insan emeğiyle, daha hızlı ve daha fazla kaynaktan yürütülebilmesidir. Bu durum, bir devletin az sayıda vekil aracılığıyla çok büyük ölçekte etki yaratmasını mümkün kılmakta ve m. 8'deki talimat ile kontrol ilişkisinin ispatını daha da zorlaştırmaktadır. Ancak hukuki ölçüt değişmemektedir: Yapay zekâ bir aktör değil, araçtır. Belirleyici olan, aracı kullanan kişi veya grubun devletle olan ilişkisidir.

6. Değerlendirme ve Öneriler

6.1. Mevcut Hukukun Yeterli Olduğu Alanlar

İncelenen vakaların önemli bir kısmında mevcut sorumluluk hukuku açık ve uygulanabilir yanıtlar sunmaktadır. Askerî siber birimlerin ve istihbarat servislerinin fiilleri m. 4 uyarınca doğrudan devlete atfedilir. Yapay zekâ destekli hedefleme sistemlerini kullanan orduların fiilleri de aynı kapsamdadır ve devlet sorumluluğunun kusur gerektirmemesi, otonom sistemlerin öngörülemezliğinden doğan sorunların önemli bir kısmını çözmektedir. Saldırı amaçlı siber araçların veya gözetleme yazılımlarının başka devletlere transferi m. 16 ile, kamu yetkisinin teknoloji şirketlerine devri ise m. 5 ile karşılanabilmektedir.

6.2. Yetersiz Kalan Alanlar

Buna karşılık dört alanda ciddi güçlükler bulunmaktadır. Birincisi, m. 8'deki etkin kontrol eşiğinin siber vekiller bakımından ispatı pratikte neredeyse imkânsızdır. İkincisi, UAD'nin tamamen ikna edici delil standardı, istihbarat kaynaklarına dayanan siber atıflarla bağdaşmamaktadır. Üçüncüsü, özen yükümlülüğünün siber alandaki bağlayıcılığı ve içeriği devletler arasında hâlâ tartışmalıdır. Dördüncüsü, teknoloji şirketlerinin uluslararası hukuki kişiliğinin bulunmaması, şirketin "kapatma anahtarı" gücünü hiçbir uluslararası hesap verebilirlik mekanizmasına bağlamamaktadır.

6.3. Uygulama Açığı: Siyasi Atıftan Hukuki Sorumluluğa

En önemli bulgu, sorunun büyük ölçüde kurallardan değil, uygulamadan kaynaklandığıdır. Avrupa devletleri 2024-2026 döneminde Rusya ve Çin'e yönelik çok sayıda kamuya açık atıf yapmış, büyükelçiler çağırmış ve AB düzeyinde yaptırımlar uygulamıştır. Ancak bugüne kadar hiçbir Avrupa devleti, bir siber operasyon nedeniyle başka bir devlete karşı uluslararası yargıya başvurmamış, ARSIWA anlamında resmî bir tazminat talebinde bulunmamış ya da açıkça karşı tedbir olarak nitelendirdiği bir tedbir almamıştır. Bu tercih; delillerin gizliliği, tırmanma korkusu ve karşı tarafın uluslararası yargı yetkisini kabul etmemesi gibi gerekçelerle açıklanabilir. Ancak sonuçta sorumluluk hukuku siber alanda fiilen "askıya alınmış" görünmektedir.

6.4. De Lege Ferenda Öneriler

Bu tespitler ışığında beş öneri ileri sürülmektedir.

1. **Yorumsal öneriler:** ARSIWA m. 8'deki "talimat" unsuru, devletin vekile verdiği teknik şartnameleri, hedef listelerini ve görev tanımlarını da kapsayacak biçimde yorumlanmalıdır. m. 5, teknoloji şirketlerine yapılan egemenlik yetkisi devrini açıkça kapsayacak biçimde işlevsel olarak okunmalıdır. Özen yükümlülüğü, devletin kendi topraklarından kaynaklanan saldırılar hakkında aldığı bildirimler dikkate alınarak "bilmesi gereken" standardıyla somutlaştırılmalıdır.
2. **Kurumsal öneriler:** BM'nin yeni Küresel Mekanizması bünyesinde, devletlerin istihbarat kaynaklarını ifşa etmeden teknik atıf delillerini paylaşabileceği bağımsız bir uzmanlar paneli kurulmalıdır. AB düzeyinde ise üye devletlerin atıf metodolojilerini uyumlaştıran ortak bir çerçeve geliştirilmelidir.

3. **Hukuki sorumluluğun işletilmesi:** Avrupa devletleri, siyasi atıfı en azından bazı vakalarda resmî bir sorumluluk bildirimine dönüştürmeli ve ARSIWA m. 43 anlamında sorumlu devletten tazminat talep etmelidir. Bu adım, devlet uygulamasının oluşması ve sorumluluk hukukunun siber alanda işlerlik kazanması açısından gereklidir.
4. **Askerî yapay zekâ:** CCW Gözden Geçirme Konferansı'nda yasaklar ve düzenlemelerden oluşan iki katmanlı bağlayıcı bir belgenin müzakere edilmesi için yetki verilmelidir. I No.lu Ek Protokol m. 36 kapsamındaki silah incelemelerinin yapay zekâ sistemleri için ortak standartlara kavuşturulması ve AB Yapay Zekâ Yasası m. 2(3)'teki askerî istisnanın çift kullanımlı sistemler bakımından sınırlarının netleştirilmesi gerekmektedir.
5. **Teknoloji şirketleri:** Çatışmadan etkilenen bölgelerde askerî veya istihbarat müşterilerine hizmet veren teknoloji şirketleri için zorunlu ve artırılmış bir insan hakları özen yükümlülüğü getirilmelidir. Pall Mall Süreci bağlayıcı ihracat kontrol kurallarına dönüştürülmeli; Uluslararası Hukuk Komisyonu ise ev sahibi devletin kendi şirketlerinin yurt dışı faaliyetleri bakımından özen yükümlülüğünü açıklığa kavuşturan bir çalışma başlatmalıdır.

Türkiye bakımından da bu tartışmanın önemli bir boyutu bulunmaktadır. Hem NATO üyeliği hem de AB ile ilişkileri dikkate alındığında, Türkiye'nin atıf ölçütleri, özen yükümlülüğü ve karşı tedbirler konusundaki tutumunu açıklayan bir belge hazırlaması, uluslararası hukukun bu alandaki gelişimine katkı sağlayacaktır.

Sonuç

Avrupa, Kasım 2026'da gıda zincirinden kan bankalarına ve sivil havacılığa kadar gündelik hayatın altyapısını hedef alan bir hibrit saldırı dalgasıyla bir kez daha sarsılmıştır. Bu olaylar, son iki yılda hanelere dağıtılan kriz rehberlerinin ve güvenlik yetkililerinin kamuoyuna yönelik uyarılarının boş bir alarm olmadığını göstermiştir. Ancak bu saldırıların ortak özelliği, failin büyük ölçüde görünmez kalmasıdır: **Saldırıyı üstlenen hacktivist grup, sabotajı gerçekleştiren tek kullanımlık ajan ya da hizmeti sağlayan teknoloji şirketi, hepsi devlet dışı aktörlerdir.**

Vardığımız temel sonuç, uluslararası sorumluluk hukukunun bu yeni tabloya karşı kural düzeyinde büyük ölçüde hazırlıklı olduğudur. Devlet organlarının siber ve yapay zekâ destekli fiilleri doğrudan devlete atfedilmekte; kamu yetkisi devri, talimat ve benimseme kuralları devlet dışı aktörlerin fiillerini devlete bağlayacak araçları sunmakta; özen yükümlülüğü ise atfın kurulamadığı durumlarda devletin kendi ihmalinden sorumlu tutulmasını sağlamaktadır. **Yapay zekâ, "sorumluluk boşluğu" yaratan bağımsız bir aktör değil, devletin sorumluluğunu ortadan kaldırmayan, yalnızca sorumluluk zincirini uzatan bir araçtır.**

Asıl boşluk, kurallarda değil ispat ve irade düzlemindedir. Etkin kontrol eşiği siber vekiller bakımından neredeyse aşılamaz; özen yükümlülüğünün içeriği belirsizdir ve Avrupa devletleri güçlü siyasi atıfları hukuki sorumluluk taleplerine dönüştürmekten kaçınmaktadır. **Teknoloji şirketlerinin çatışmanın seyrini etkileyebilen gücü ise hiçbir uluslararası hesap verebilirlik mekanizmasına bağlı değildir.**

Bu nedenle çözüm yeni bir antlaşmadan çok, mevcut kuralların cesaretle işletilmesinde aranmalıdır. **Atıf delillerinin paylaşımını kolaylaştıran kurumsal mekanizmalar, özen yükümlülüğünün somutlaştırılması, teknoloji şirketlerine yönelik artırılmış özen yükümlülükleri ve askerî yapay zekâda anlamlı insan denetimini güvence altına alan bağlayıcı kurallar, bu alandaki en acil adımlardır.** Devlet dışı aktörlerin askerî ve askerî nitelikli fiillerinden doğan devlet sorumluluğu, önümüzdeki dönemde uluslararası hukukun en dinamik alanlarından biri olmaya devam edecektir. Gelecek araştırmalar bakımından CCW Gözden Geçirme Konferansı'nın sonucu, Tallinn Kılavuzu'nun üçüncü sürümü ve BM Küresel Mekanizması'nın ilk çıktıları yakından izlenmelidir.

Kaynakça

Kitaplar, Makaleler ve Kitap Bölümleri

- Alston, P. (2005). The "not-a-cat" syndrome: Can the international human rights regime accommodate non-state actors? P. Alston (Ed.), *Non-state actors and human rights* içinde (s. 3–36). Oxford University Press.
- Boutin, B. (2023). State responsibility in relation to military applications of artificial intelligence. *Leiden Journal of International Law, 36*(1), 133–150.
- Cassese, A. (2007). The Nicaragua and Tadić tests revisited in light of the ICJ judgment on genocide in Bosnia. *European Journal of International Law, 18*(4), 649–668.
- Clapham, A. (2006). *Human rights obligations of non-state actors*. Oxford University Press.
- Crootof, R. (2016). War torts: Accountability for autonomous weapons. *University of Pennsylvania Law Review, 164*(6), 1347–1402.
- d'Aspremont, J. (Ed.). (2011). *Participants in the international legal system: Multiple perspectives on non-state actors in international law*. Routledge.
- Higgins, R. (1994). *Problems and process: International law and how we use it*. Clarendon Press.
- Jensen, E. T. ve Watts, S. (2017). A cyber duty of due diligence: Gentle civilizer or crude destabilizer? *Texas Law Review, 95*(7), 1555–1577.
- 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 and Security Law, 21*(3), 405–428.
- Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology, 6*(3), 175–183.
- Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.
- Melzer, N. (2009). *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*. International Committee of the Red Cross.
- Noortmann, M., Reinisch, A. ve Ryngaert, C. (Ed.). (2015). *Non-state actors in international law*. Hart Publishing.
- Rid, T. ve Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.

- Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Sparrow, R. (2007). Killer robots. *Journal of Applied Philosophy, 24*(1), 62–77.

Mahkeme Kararları ve Danışma Görüşleri

- *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, 2007 I.C.J. 43 (Feb. 26).
- *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, 2005 I.C.J. 168 (Dec. 19).
- *Corfu Channel (United Kingdom v. Albania)*, Merits, Judgment, 1949 I.C.J. 4 (Apr. 9).
- *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, 1997 I.C.J. 7 (Sept. 25).
- *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. 136 (July 9).
- *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, 1986 I.C.J. 14 (June 27).
- *Prosecutor v. Duško Tadić*, Case No. IT-94-1-A, Judgment (Int'l Crim. Trib. for the Former Yugoslavia, Appeals Chamber, July 15, 1999).
- *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, 2010 I.C.J. 14 (Apr. 20).
- *Reparation for Injuries Suffered in the Service of the United Nations*, Advisory Opinion, 1949 I.C.J. 174 (Apr. 11).
- *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment, 1980 I.C.J. 3 (May 24).

Uluslararası Belgeler ve Mevzuat

- Committee on Economic, Social and Cultural Rights. (2017). *General comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities* (E/C.12/GC/24).
- Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225).
- Council of the European Union. (2024). *Declaration by the High Representative on behalf of the European Union on a common understanding of the application of international law to cyberspace*.
- Council of the European Union. (2026). *Sanctions against Russia's destabilising activities (hybrid threats)*. https://www.consilium.europa.eu/en/policies/sanctions-against-russia-hybrid-threats/
- European Commission. (2025, 26 Mart). *EU Preparedness Union Strategy to prevent and react to emerging threats and crises* [Basın bülteni].
- 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.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). OJ L, 2024/1689.
- UN General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174).
- UN General Assembly. (2021). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (A/76/135).
- UN Human Rights Council. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework* (A/HRC/17/31).

Kurum Raporları ve Resmî Açıklamalar

- Direktoratet for samfunnssikkerhet og beredskap. (t.y.). *Self-preparedness*. Erişim adresi: https://www.dsb.no/en/egenberedskapsuka/Self-preparedness/
- European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. ENISA. https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups
- MI5. (2025, 16 Ekim). *Director General Ken McCallum gives threat update*. https://www.globalsecurity.org/intell/library/news/2025/intell-251016-mi501.htm
- Microsoft. (2022). *Defending Ukraine: Early lessons from the cyber war*. Microsoft Corporation.
- National Cyber Security Centre. (2025). *NCSC annual review 2025*. https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025

Basın Kaynakları

- Associated Press. (2024, 8 Ekim). Sweden updates Cold War-era preparedness booklet. *The Washington Times*. https://m.washingtontimes.com/news/2024/oct/8/sweden-updates-cold-war-era-preparedness-booklet/
- CNN. (2025, 25 Eylül). [Microsoft'un İsrail Savunma Bakanlığı'na bağlı bir birime sunduğu bulut hizmetlerini durdurmasına ilişkin haber]. https://www.cnn.com/2025/09/25/tech/microsoft-israel-surveillance
- Notes from Poland. (2026, 12 Ocak). Government sends safety handbook to every household in Poland. https://notesfrompoland.com/2026/01/12/government-sends-safety-handbook-to-every-household-in-poland/
- Reuters. (2025, 11 Aralık). NATO's Rutte warns allies they are Russia's next target. *The Star*. https://www.thestar.com.my/news/world/2025/12/11/nato039s-rutte-warns-allies-they-are-russia039s-next-target
- Reynolds, J. C. ve Croft, A. (2026, 7 Kasım). All the "hybrid attacks" across UK and Europe as supermarkets targeted. *The Independent*. https://www.independent.co.uk/news/world/europe/uk-europe-cyber-attacks-b3079159.html
- Schneid, R. (2026, 7 Kasım). Europe's bomb threats raise fears of hybrid warfare. *TIME*. https://time.com/article/2026/11/07/europe-bomb-threats-raise-fear-new-warfare/
- The Local France. (2025, 20 Kasım). "World in crisis": France publishes new emergency survival guide. https://www.thelocal.fr/20251120/world-in-crisis-france-publishes-new-emergency-survival-guide

Prof. Dr. Murat KOÇ / Çağ Üniversitesi Bölgesel Güvenlik Çalışmaları Uygulama ve Araştırma Merkezi