ISSN: 3108-7248
Yıl: 2026, **Cilt:** 1, **Sayı:** 1, **Haziran** 2026 s. 83-100 **Makale Türü:** Araştırma
Makalenin Geliş Tarihi: 02.04.2026 **Makalenin Kabul Tarihi:** 25.06.2026

İç Güvenlik Tehdidi Olarak Ticari Dronelar

Cansu Ulu[1]

Öz

Ticari droneların sivil kullanımı son yıllarda artış göstermiştir. Ticari dronelar tarımdan lojistiğe, haritalandırmadan medyaya birbirinden farklı alanlarda sivil hayatın içinde yer almaktadır. Ancak bu teknolojinin kolay erişilebilir olması, düşük maliyeti ve modifiye edilebilir olması güvenlik alanında riskleri beraberinde getirmektedir. Özellikle küçük boyutlu ticari dronelar üzerindeki sensörler sayesinde devlet dışı aktörler tarafından gözetim ve istihbarat operasyonlarında ve silahlandırılarak bireysel saldırılarda kullanıldığında iç güvenlik açısından asimetrik tehdit unsuru yaratmaktadır. Bu çalışma ticari drone teknolojisinin iç güvenlik üzerindeki etkilerini incelemeyi amaçlamaktadır. Çalışmada öncelikle drone teknolojisinin yaygınlaşma süreci ve çift kullanım niteliği ele alınmakta, ardından droneların terörizm, organize suç faaliyetleri ve kritik alt yapılara yönelik saldırılar gibi farklı güvenlik riskleri bağlamında nasıl kullanıldığı örneklerle analiz edilmektedir. Son olarak iç güvenlik kurumlarının bu yeni tehdit türüne karşı geliştirebileceği düzenleyici ve teknolojik politika seçenekleri tartışılmaktadır. Çalışma, ticari drone teknolojisinin iç güvenlik alanında giderek artan bir asimetrik tehdit oluşturduğunu ve buna yönelik bütüncül politikalara ihtiyaç duyulduğunu ortaya koymaktadır.

Anahtar kelimeler: *Ticari Drone, İç Güvenlik, Asimetrik Tehdit, Çift Kullanım*

[1] Cansu Ulu, İzmir Rüştü Ünsal PMYO, Öğr. Gör. Dr., 0000- 0002- 3976- 218x

Journal of Faculty of Homeland Security

ISSN: 3108-7248
Year: 2026, **Volume:** 1, **Issue:** 1, **June** 2026 p. 183-100 **Article Type:** Research
Received: 02.04.2026 **Accepted:** 25.06.2026

Commercial Drones as a Threat to Homeland Security

Abstract
The civilian use of commercial drones has witnessed a significant surge in recent years, finding applications in diverse sectors ranging from agriculture and logistics to mapping and media. However, the accessibility, low cost, and modifiable nature of this technology introduce substantial security risks. Particularly when equipped with advanced sensors and utilized by non-state actors for surveillance, intelligence, or weaponized individual attacks, small-scale commercial drones constitute an asymmetric threat to homeland security. This study aims to examine the implications of commercial drone technology on homeland security. The research first addresses the proliferation of drone technology and its dual-use characteristics, followed by an analysis of how drones are employed in various security contexts, such as terrorism, organized crime, and attacks against critical infrastructure. Finally, regulatory and technological policy options that homeland security institutions can develop against this emerging threat are discussed. The study concludes that commercial drone technology increasingly poses an asymmetric threat in the realm of homeland security, necessitating the implementation of holistic policy frameworks.

Keywords: *Commercial Drones*, *Homeland Security*, *Asymmetric Threat*, *Dual-Use Technology*

Giriş

Ticari dronelar son yıllarda teknolojik gelişmelerin etkisi ile hızla yaygınlaşmış ve sivil kullanım alanında hayatımızın bir parçası haline gelmiştir. Başlangıçta fotoğrafçılık, tarım ve lojistik gibi alanlarda kullanılan bu araçlar, düşük maliyetli, kolay erişilebilir ve kullanıcı dostu yapıları sayesinde hem bireysel hem de kurumsal kullanımda geniş kitleler tarafından benimsenmiştir. Ticari droneların temel olarak iki işlevi bulunmaktadır. Üzerlerindeki sensörler sayesinde veri toplama ve gözetim için kullanıma uygundurlar. Diğer bir işlevi ise çeşitli yükler ile insanların yaptıkları görevleri daha kısa bir sürede yerine getirmeleridir. Örneğin tarım alanında ticari dronelar ilaçlama, gübreleme, sulama, tohumların ekimi gibi faaliyetlerde kullanılmaktadır. Bu faaliyetler insanın yerine getirebileceği ancak verimin drone aracılığı ile arttırıldığı faaliyetlerdir. Aynı zamanda tarım alanında dronelar veri toplama ve mahsüllerin durumunun takibi için de kullanılır. Bunun için dronedan elde edilen verilerin uygun şekilde işlenmesi gerekmektedir.

Ticari dronelar; çok rotorlu dronelar, sabit kanatlı dronelar, tek rotorlu dronelar ve sabit kanatlı hibrit dronelar olarak ayrılırlar. Çok rotorlu sistemler, dikey iniş-kalkış (VTOL) yapabilme ve havada asılı kalabilme yetenekleriyle dar alanlardaki gözlem ve medya faaliyetlerinde öne çıkarken; sabit kanatlı modeller, aerodinamik yapıları sayesinde uzun menzilli haritalandırma ve tarımsal analiz süreçlerinde yüksek verimlilik sunmaktadır. Tek rotorlu dronelar, helikopter benzeri tasarımlarıyla ağır yük taşıma kapasitesi gerektiren endüstriyel lojistik operasyonlarında tercih edilmektedir. Sabit kanatlı hibrit dronelar ise, pist gereksinimini ortadan kaldıran dikey kalkış avantajı ile uzun süreli uçuş performansını birleştirerek zorlu arazi koşullarında stratejik bir esneklik sağlamaktadır (Varnalı, 2026). Bu yapısal farklılıklar, droneların sadece sivil sektörlerdeki verimliliğini değil, aynı zamanda güvenlik birimlerinin karşı karşıya kaldığı tehditlerin spektrumunu da genişletmektedir.

Dünya Ekonomik Forumu'nun 2021 yılında yayınladığı raporda pandemi sonrası drone kullanımının arttığı belirtilmiştir. Özellikle lojistik sektöründe ağır yük taşımacılığı arayışlarına gidilmiştir (Abusalem et al., 2021). Grand View Research (2026) pazar araştırması küresel drone pazar hacminin 2026-2033 yılları arasında %9,5 artacağını öngörmektedir. Pazar araştırmaları, drone teknolojisinin sadece bir donanım satışı olmaktan çıkıp 'Hizmet Olarak Drone' (DaaS) modeline evrildiğini ve kentsel hava hareketliliği projeleriyle lojistik sektöründe yeni pencereler açtığını göstermektedir (Research and Markets, 2025). Ancak bu ticari büyüme, otonom uçuş ve yapay zeka tabanlı hedef tanıma gibi ileri seviye özelliklerin sivil kullanıma girmesini de beraberinde getirmektedir. Sivil alanda kullanılan araçların ileri düzeyde sensör donanımları barındırması ve veri işleme depolama teknolojilerinin kullanılması yeni fırsatlar kadar risklerde yaratmaktadır. Bu durum, iç güvenlik perspektifinden bakıldığında, hava sahasının denetlenmesini zorlaştırmakta ve yeni savunma açıklarını tetiklemektedir.

Ticari drone teknolojisinin iç güvenlik üzerindeki etkilerini analiz ederken temel alınması gereken kavramsal çerçeve, bu araçların çift kullanım (dual-use) niteliğidir. Çift kullanım, en genel tanımıyla bir teknolojinin hem meşru sivil amaçlara hizmet edebilme hem de askeri veya yıkıcı operasyonlarda kullanılabilme potansiyelini ifade eder. Sivil amaçlar ile kullanılabilen araçlar uluslararası ticari arenada kolaylıkla ticareti yapılabilen unsurlardır. (Fuhrmann, 2008). Fuhrmann, çift kullanım teknolojilerinin sadece drone ile hayatımıza girmediğini nükleer teknolojilerin de benzer güvenlik sorununu barındırdıklarını vurgulamıştır. Nükleer araştırmaların sivil ve bilimsel gerekliliklerle başlayarak uluslararası güvenlik ortamında silah üretimine yönelebileceğini vurgulamıştır (Fuhrmann, 2012).

Bu teknolojik "esneklik", güvenlik bürokrasisi için ciddi bir ikilem yaratmaktadır. Zira ticari droneların düşük maliyetli ve modifiye edilebilir yapısı, gelişmiş devletlerin sahip olduğu sofistike hava kabiliyetlerini, devlet dışı aktörlerin ve suç örgütlerinin erişebileceği bir seviyeye indirgemiştir (Sandvik ve Jumbert, 2016). Dolayısıyla, droneların sivil pazardaki demokratikleşmesi ve hızla yayılması, aynı zamanda asimetrik tehdit unsurlarının "hava sahası hakimiyetini" ucuzlatarak iç güvenlik kurumlarının savunma maliyetlerini ve risk projeksiyonlarını yukarı çekmektedir.

Ticari droneların yarattığı risk, Lupovici (2021) tarafından geliştirilen çift kullanım güvenlik ikilemi (dual-use security dilemma) kavramı üzerinden derinleştirilebilir. Çift kullanım güvenlik ikilemi, bir aktörün çift kullanım teknolojilerine sahip bir aktörün niyetinden ve kabiliyetlerinden tam olarak emin olamayacağını vurgular. Bu nedenle teknolojiye sahip olmayan taraf için sivil de kullanılsa çift kullanım teknolojileri bir güvenlik tehdidi olarak algılanacaktır ve güvenlik politikalarında sert tedbirlere neden olacaktır. Geleneksel güvenlik perspektifinden bakıldığında, politika yapıcılar karşı tarafın gerçek niyetinden (savunma mı yoksa saldırı mı?) emin olamadıkları için, sivil karakterli bu teknolojileri potansiyel birer tehdit olarak kodlama eğilimi gösterirler. Bu belirsizlik hali, güvenlik birimlerini proaktif önlemler almaya zorlamakta; ancak alınan bu savunmacı tedbirler (yasal kısıtlamalar, anti-drone sistemleri vb.), karşı tarafı da kendi sivil projelerini silahlandırmaya veya daha sofistike askeri araçlara yönelmeye iterek her iki tarafın da güvenliğini azaltan bir güvenlik sarmalına yol açmaktadır.

Drone teknolojisinin yaygınlaşmasıyla birlikte bu araçların kötüye kullanımına yönelik örneklerin artması, özellikle iç güvenlik alanında çok boyutlu bir sorun haline gelmiştir. Küçük boyutları, radar kesit alanlarının düşüklüğü sebebiyle tespit edilmelerinin zor olması ve uzaktan kontrol edilebilmeleri, bu araçları suç faaliyetleri ve terörist eylemler için asimetrik birer enstrüman olarak cazip kılmaktadır. Saha uygulamalarındaki vakalar, bu tehdidin sadece teorik değil, operasyonel bir gerçeklik olduğunu kanıtlamaktadır.

Enerji güvenliği bağlamında, 2019'da Suudi Arabistan'daki Aramco tesislerine düzenlenen saldırılar, kritik ekonomik altyapıların ne denli kırılgan olduğunu

belgelemiştir. Ayrıca, Orta Doğu'da çatışan devlet dışı aktörlerin ticari sistemleri silahlandırarak taktiksel hava desteği sağlaması ve organize suç örgütlerinin Meksika-ABD sınırı gibi bölgelerde uyuşturucu sevkiyatı ile cezaevlerine yasaklı madde sokma faaliyetleri, tehdidin spektrumunu genişletmektedir. Bu tür vakalar, iç güvenlik kurumlarının geleneksel savunma paradigmalarının ötesine geçerek teknoloji odaklı, bütüncül ve proaktif güvenlik politikaları geliştirmesini zorunlu kılmaktadır.

Kavramsal Çerçeve

Savaş tarih boyunca gerçekliğini sürdüren bir kavramdır. Ancak savaşın enstrümanları teknolojinin gelişmesi ile değişim göstermektedir. Drone teknolojileri savaşın biçimini değiştiren teknolojiler arasında yer almaktadır. Bu durum Clausewitz'in iktisadi ve teknolojik imkânların savaşın yürütülüş biçimini belirlediği yönündeki öngörüsünü doğrular niteliktedir (Clausewitz, 2003). Zira düşük maliyetli dronelar, geleneksel güç dengelerini sarsan yeni bir stratejik araç seti sunmaktadır. Creveld 4000 yıllık araştırmasında tarih boyunca teknoloji ve savaş arasındaki ilişkiyi incelemiştir. Creveld teknolojinin sadece operasyonel destek unsurlarının modernleşmesi olarak görülmemesi gerektiğini, savaşın organizasyonel ve stratejik mantığını dönüştürdüğünü vurgulamıştır (Creveld, 1989).

McFate, modern çatışma ortamını dayanıklı düzensizlik (durable disorder) olarak tanımlamıştır. Günümüzde küresel sistem, düzensizliklerin çözümüne değil; sürdürülmesine odaklanmıştır. Bu durumda Batı'nın 1945 sonrası konvansiyonel silahları önceleyen stratejisinin kaybetmeye mahkûm olduğunu vurgulamaktadır. ABD penceresinden yaptığı değerlendirmede; günümüzde sadece Rusya ve Çin gibi revizyonist devlet aktörlerinin değil; terörist gruplar gibi devlet dışı aktörlerin de savaş arenasında varlık gösterdiğini belirterek konvansiyonel silahlar dışında bilgi, ideoloji, zaman gibi kavramların da silah olarak kullanılabileceğini ifade etmiştir (McFate, 2019). Ticari droneların sadece silah donanımları ile modifiye edilmesi dışında istihbarat sağlayan araçlar olarak kullanılması bilginin silahlandırılmasına örnektir. Dronelar doğruda fiziki zarar vermek amacıyla doğrudan vuruş yapacak şekilde kullanılabilmektedir. Bu doğrudan vuruş yapma stratejisi ticari droneların kullanılabileceği yöntemlerden sadece biridir. Diğer yandan hibrit savaşlarda olduğu gibi konvansiyonel silahların yanı sıra psikolojik savaş unsuru olarak da kullanılabilmektedir. Hoffman (2007), hibrit savaşların sadece fiziksel yıkımı değil, konvansiyonel güçlerin teknolojik ve psikolojik araçlarla harmanlanarak rakibin karar alma mekanizmalarında kaos yaratmayı hedeflediğini belirtmektedir.

Mary Kaldor'un yeni savaş kuramı, ticari droneların yarattığı iç güvenlik tehditlerini anlamlandırmak için temel görüşlerden birini sunar. Kaldor'a (1999)

göre modern çatışmalar, artık iki düzenli ordunun cephede karşılaştığı eski savaşlar formundan çıkarak, devlet içi ve devlet dışı aktörlerin, paramiliter grupların ve suç şebekelerinin dâhil olduğu karmaşık bir yapıya bürünmüştür. Bu yeni savaşlar paradigmasında, şiddetin tekeli devletin elinden alınması ve teknolojiye erişimin kolaylaşması, ticari dronelar gibi raftan satın alınabilen sivil araçları asimetrik birer stratejik silaha dönüştürmüştür. Castells'in (2005) 'Ağ Toplumu' perspektifinden bakıldığında, ticari dronelar sadece birer uçan aygıt değil, hiyerarşik devlet yapısına karşı ağ tipi örgütlenen asimetrik aktörlerin kullandığı yatay güç enstrümanlarıdır. Bu süreçte dikey (devletler arası) hiyerarşiler yerini yatay (hücresel ve ağ tipi) örgütlenmelere bırakırken; ticari dronelar, devletin geleneksel hava sahası kontrolü ve şiddet tekeline karşı devlet dışı aktörlerin asimetrik kabiliyetleri haline gelmiştir. Friedman (2007), küreselleşme 3.0 kavramı ile bilgi iletişim teknolojilerinin dünyayı hiç olmadığı kadar düzleştirdiğini ve bireylerin devletlerle yarışacak şekilde güç unsularına erişimine imkân verdiğini ifade etmiştir.

Teknolojik demokratikleşme ve hiyerarşilerin düzleşmesi süreci, modern güvenlik literatüründe asimetrik savaş kavramının yeniden tanımlanmasına yol açmıştır. Geleneksel anlamda asimetri, taraflar arasındaki askeri ve ekonomik kapasite uçurumunu ifade etse de; günümüzde asimetri, bu kapasitenin kullanım biçimindeki farklılaşmaya evrilmiştir (Arreguín-Toft, 2001). Ticari dronelar, bu noktada düşük maliyetli bir teknolojik kaldıraç görevi görerek, sınırlı kaynaklara sahip devlet dışı aktörlerin, devletlerin çok katmanlı ve pahalı hava savunma doktrinlerini baypas etmesine imkân tanımaktadır. McFate asimetriyi Davut ve Goliath alegorisi üzerinden anlatmıştır. Büyük orduların konvansiyonel taktikler ile yavaş hareket ettiğini ve operasyonların maliyetlerinin yüksek olduğunu belirtmiştir. Buna karşılık zayıf devletler hayatta kalma mücadelesi verirken daha düşük maliyetli esnek organizasyon yapısı ile hızlı hareket edebilen gerilla taktikleri ile hareket etmektedir. Dolayısıyla McFate (2019) uzun vadede savaşın maliyetinin büyük devletleri yıpratacağını ve zayıf devletin eninde sonunda başarı elde edeceğini iddia etmektedir. Konvansiyonel orduların hantal yapısına karşı, küçük ve esnek hücreler halinde örgütlenen bu aktörler, raftan satın aldıkları teknolojileri modifiye ederek stratejik hedeflere yönelik yüksek etkili tacizler gerçekleştirebilmektedir. Devletler arası çatışmalarda da maliyet ve teknoloji avantajının farkı göze çarpmaktadır. İran yapımı kamikaze dronelarının maliyetinin güdümlü balistik füzelerden daha ucuz olması hava savunma sistemlerini yıpratmaya ve aşırı yüklemeye yönelik stratejilerin uygulanmasına neden olmuştur.

Savaş alanının demokratikleşmesi, tarihsel olarak devletlerin tekelinde bulunan gelişmiş gözetleme, istihbarat ve hassas vuruş kabiliyetlerinin, ticari drone teknolojisi aracılığıyla sivil aktörlerin erişimine açılmasını ifade etmektedir. Geleneksel güvenlik paradigmasında hava sahası hâkimiyeti, devasa savunma bütçeleri ve karmaşık askeri endüstriyel yapılar gerektiren dikey bir güç unsuru iken; günümüzde raftan satın alınabilen teknolojiler bu gücü yatay düzleme indirmiştir.

Bu süreç, sadece teknik bir yayılımı değil, aynı zamanda Weber'in (2006) tanımladığı devletin "meşru fiziksel şiddet kullanma tekeli" üzerinde ciddi bir aşınmayı beraberinde getirmektedir. Artık bireysel kullanıcılar veya küçük ölçekli gruplar, küresel pazar üzerinden edindikleri ucuz araçlarla, devletlerin stratejik derinliklerine sızma ve operasyonel etki yaratma kapasitesine sahip hale gelmiştir (Hammes, 2016).

Bu demokratikleşme süreci, savaş alanını sadece coğrafi bir mekân olmaktan çıkararak hibrit ve dijital bir alana dönüştürmektedir. Singer'ın (2009) vurguladığı üzere, robotik ve insansız sistemlerin yaygınlaşması, savaşın sadece profesyonel askerlerin bulunduğu kapalı bir devre olmaktan çıkıp, sivillerin teknoloji aracılığıyla dâhil olduğu şeffaf ve katılımcı bir platforma dönüşmesine neden olmuştur. Ticari droneların sağladığı yüksek çözünürlüklü görüntüleme ve canlı yayın imkânları, taktiksel bir eylemi saniyeler içinde küresel bir bilgi savaşı unsuru haline getirebilmektedir. Cronin (2018), yeni teknolojilerin devlet dışı aktörler tarafından asimetrik unsurlar olarak kullanılabileceğine vurgu yaparak tarihsel örneklerle bu iddiasını analiz etmektedir. Cronin, ticari droneların sadece saldırı için değil istihbarat için de tehdit oluşturduğunu ifade etmiştir. Ticari drone pazarını domine eden Çin markası Da-Jiang Innovations (DJI) her kullanımda firmaya veri geribildiriminde bulunduğu için Cronin'e göre bir istihbarat açığı yaratmaktadır.

Ticari droneların sivil pazardaki yayılımı, uluslararası ilişkiler literatüründe güvenlikleştirme teorisi bağlamında yeni bir tartışma alanı açmıştır. Kopenhag Okulu'nun kavramsallaştırdığı güvenlikleştirme süreci, bir meselenin teknik veya siyasi bir konu olmaktan çıkarılarak "varoluşsal bir tehdit" olarak tanımlanması ve bu yolla olağanüstü önlemlerin meşrulaştırılmasıdır (Buzan, Waever ve de Wilde, 1998). Ticari dronelar özelinde bu süreç, daha önce vurgulanan Lupovici'nin (2021) çift kullanım güvenlik ikilemi ile derinleşmektedir. Hansen ve Nissenbaum (2009), siber teknolojilerin tamamı üzerinde geliştirilen güvenlikleştirme söylemini incelemiştir. Siber uzay teknolojilerinin insanlığa dair yok edici ve yıkıcı bir kıyamet getireceği fikrinin güvenlikleştirme söylemine yerleştirilmesini hiper güvenlikleştirme olarak tanımlamaktadırlar. Hiper güvenlikleştirme, ticari dronaların ekipmanlarına yönelik olmaktan ziyade veri teknolojilerine yönelmiş bir söylem olarak karşımıza çıkmaktadır.

Bu güvenlik ikilemini daha karmaşık hale getiren temel unsur, drone teknolojisinin donanım ve yazılım katmanları arasındaki geçişkenliktir. Donanım düzeyinde ticari bir drone, tarımsal ilaçlama veya paket taşımacılığı gibi meşru sivil faaliyetler için optimize edilmiş görünse de; yazılım düzeyinde yapılan otonom uçuş algoritmaları, yapay zeka tabanlı hedef tanıma sistemleri ve şifrelenmiş iletişim protokolleri bu araçları sofistike birer istihbarat veya saldırı platformuna dönüştürebilmektedir (Giscard, 2020). Güvenlik birimleri için asıl ikilem, donanımı tamamen yasal olan bir aracın, yazılımsal bir müdahale veya modifikasyonla dakikalar içinde stratejik bir tehdide dönüşebilme potansiyelidir. Dolayısıyla, do-

nanımsal şeffaflık (sivil görünüm) ile yazılımsal opaklık (askeri potansiyel) arasındaki bu gerilim, geleneksel silah kontrol rejimlerini yetersiz kılmaktadır. Bu duruma örnek Haziran 2017'de Karadeniz'de yaklaşık 20 geminin Küresel Navigasyon Uydu Sistemleri (GNSS) sinyallerini bozan sahtecilik vakasıdır (Goward, 2017). 2026 yılında benzer bir saldırı Hürmüz Boğazı'nda 1000'den fazla geminin rotasının sapmasına neden olmuştur (GZT, 2026).

Ticari Droneların Kullanıldığı Operasyonlar ve Oluşturduğu Güvenlik Tehditleri

Ticari droneların hobi amaçlı araçlar olmaktan çıkıp asimetrik savaşın çok yönlü enstrümanlarına dönüşümü, modern çatışma sahasının dönüşümünü yansıtmaktadır. Bu araçların güncel kullanımı; hedef alınan unsurun niteliğine, teknik modifikasyonun türüne ve beklenen stratejik çıktıya göre temelde dört ana eksende sınıflandırılabilir. İlk olarak, hava gücünün "demokratikleşmesi" olarak adlandırılan süreçte, devlet dışı aktörlerin ve düzenli orduların ticari sistemleri doğrudan kinetik saldırı amaçlı kullandığı görülmektedir. Bu kapsamda, basit mühimmat bırakma sistemlerinden stratejik tesisleri vuran uzun menzilli platformlara, hatta tank imha eden düşük maliyetli Birinci Şahıs Görüşü (FPV) dronelara kadar uzanan bir spektrum, konvansiyonel hava hâkimiyeti doktrinlerini kökten sarsmaktadır.

İkinci bir kategori olarak, fiziksel imha gerçekleşmese dahi kritik altyapılar üzerinde gerçekleştirilen uçuşlar, güvenlik protokollerinin kırılganlığını ifşa ederek karar vericiler üzerinde bir «psikolojik felç» hali yaratmakta ve hibrit savaşın belirsizlik yaratma amacına hizmet etmektedir. Bu süreçle eş zamanlı olarak dronelar, sadece fiziksel bir tehdit değil, aynı zamanda siber sızma araçları olarak da karşımıza çıkmaktadır. Wi-Fi Pineapple veya Raspberry Pi gibi donanımlarla entegre edilen cihazlar, fiziksel bariyerleri aşarak yüksek güvenlikli alanlara dijital bir koridor açmakta ve istihbarat operasyonlarını siber uzama taşımaktadır. Son olarak, radara yakalanmama ve düşük irtifa avantajları, bu araçları sınır güvenliği ihlalleri ve yasa dışı lojistik faaliyetler için ideal birer asimetrik unsura dönüştürmektedir. Bu operasyonel çeşitlilik, aşağıda detaylandırılacak olan saha örneklerinde ticari teknolojinin nasıl birer stratejik silaha dönüştüğünü ve iç güvenliği tehdit ettiğini açıkça göstermektedir.

Hava Gücünün Demokratikleşmesi: Doğrudan Kinetik Saldırılar

Hava gücü, yirminci yüzyıl boyunca yüksek maliyetli platformlar ve pilot eğitimleri ile nitelikli insan sermayesi gerektirmesi nedeniyle ancak devlet aktörü tarafından sahip olunabilecek bir kapasite olmuştur. Ancak ticari droneların si-

lahlandırılması, bu hiyerarşiyi temelden sarsarak hava hakimiyetini "demokratikleştirmiş" ve devlet dışı aktörlerin dahi hava operasyonları yapabilmesine olanak tanımıştır. Doğrudan vuruş saldırılarında ticari drone kullanımı devlet dışı aktörler örneğinde terör örgütleri ve organize suç örgütleri örnekleri ile incelenmiştir, diğer yandan devletler arası çatışmalarda asimetrik savaş unsuru olarak kullanım örneğine de yer verilmiştir.

Hava gücünün devlet dışı aktörler tarafından ticari imkânlar ile kullanılmasının ilk büyük ölçekli saha uygulaması, 2016-2017 Musul operasyonları sırasında DEAŞ tarafından gerçekleştirilmiştir. Örgüt, basit hobi dronelarını mühimmat bırakacak şekilde modifiye ederek konvansiyonel ordular üzerinde beklenmedik bir taktik baskı kurmuştur. DEAŞ ticari ürünler ile kendisine hem bir insansız hava aracı filosu hem de yer ünitesinde verileri toplayıp değerlendirme imkânı sağlamıştır. Bu ürünler ticari dronelar dışında GoPro kameralar, hafıza kartları, GPS cihazları ve bunları işleyecek bilgisayar ekipmanları gibi raflarda bulunabilecek ürünlerdir (Rassler et al., 2017). DEAŞ, DJI Phantoms ticari dronelarını 40 milimetre mühimmat taşıyacak ve hedefe bırakacak şekilde modifiye ettiği kayda geçmiştir. Bu donanımların yanı sıra DEAŞ yazılım olarak açık kaynak ticari yazılımları ve Google Maps verilerini kullanmıştır (Balkan, 2017: 17-18).

Bu taktiksel evrim, terör örgütleri dışında organize suç örgütlerinin faaliyetlerinde de gözlemlenebilmektedir. Latin Amerika'da CJNG (Jalisco Yeni Nesil Karteli) gibi suç örgütlerinin, üzerine C4 patlayıcı yerleştirilmiş droneları rakip gruplara ve emniyet güçlerine karşı kullanmışlardır. C4 patlayıcılar ve şarapnel etkisi yaratan bilyelerle modifiye ederek rakip kartel üyelerinin toplandığı alanlara veya polis konvoylarına karşı 'hassas güdümlü' olmayan ancak yüksek tahrip gücüne sahip hava saldırıları düzenlemektedir (Ziemer, 2025). Meksika'nın Michoacán eyaletinde gözlemlenen vakalar, bu droneların sadece birer taciz aracı değil, rakip bölgeleri ele geçirmek için kullanılan birer 'öncü hava birliği' gibi işlev gördüğünü kanıtlamaktadır (Felbab-Brown, 2026). Sonuç olarak, ticari droneların doğrudan vuruş kapasitesi, organize suç gruplarının operasyonel menzilini genişletirken, devletin yerel düzeydeki güvenlik mimarisini tehlikeye sokmaktadır.

Devletler arası çatışmalarda ticari droneların asimetrik savaş unsuru olarak Ukrayna Rusya Savaşında kullanılmıştır. Yaklaşık 500 dolarlık FPV (First Person View) droneların, RPG-7 mühimmatları ile Leopard 2 veya Abrams tanklarını saf dışı bırakması, modern harp tarihinin en çarpıcı maliyet/etkinlik devrimlerinden biridir (Chaari, 2025). Benzer şekilde, başlangıçta tarım amaçlı üretilen çok rotorlü ve yüksek yük taşıma kapasitesi ile güdümlü mühimmat taşıyabilen "Baba Yaga" droneları gece görüş kabliyeti ile donatılarak ağır bombardıman araçlarına dönüştürülmüştür (CSIS, 2025).

Doğrudan vuruş stratejisi, suç örgütlerine iki temel asimetrik avantaj sağlamaktadır: Birincisi, fiziksel bariyerlerin (duvarlar, zırhlı araçlar, kontrol noktaları) üzerinden aşarak hedefi dikey düzlemde vurabilme kabiliyeti; ikincisi ise saldır-

ganın kimliğini ve konumunu gizleyerek karşı saldırı riskini minimize etmesidir. Tüm bunların yanı sıra düşük maliyet ile yüksek hasar verebilmektedir.

Stratejik Hedefleme ve Psikolojik Harp: Kritik Altyapılara Yönelik Operasyonlar

Hibrit savaşın en ayırt edici özelliklerinden biri, hedefin sadece fiziksel imhasına değil, rakibin karar alma mekanizmalarının aksamasına ve toplumsal güven algısının sarsılmasına odaklanmasıdır. Ticari dronelar, düşük maliyetleri ve tespit edilme zorluklarıyla, devletlerin en hassas noktaları olan kritik altyapılara yönelik asimetrik bir tehdit unsuru olarak bu stratejinin merkezinde yer almaktadır. Bu operasyonlar çoğu zaman doğrudan bir yıkım yaratmak yerine, güvenlik protokollerinin kırılganlığını ifşa ederek stratejik belirsizlik ve psikolojik yıpratma süreci başlatmayı hedeflemektedir.

Bir devlet dışı aktörün kısıtlı imkânlar ile ve ambargo altında küresel ölçekte tehdit yaratabilecek hava kabiliyetine sahip olmasının çarpıcı örneklerinden biri Husi Hareketi'nin geliştirdiği drone programıdır. Bu sürecin çalışmanın önemi için en önemli özelliği, Husilerin başlangıçta tamamen sivil amaçlı üretilen parçaları (hobi motorları, açık kaynaklı uçuş kontrol kartları ve GPS modülleri) parçalanmış bir tedarik zinciri üzerinden temin ederek sofistike insansız hava araçlarına dönüştürmesidir. Conflict Armament Research (CAR) Husiler tarafından kullanılan ve düşürülmüş olan dronlar üzerinde yaptığı araştırmada bu ekipmanların nasıl oluşturulduğunu tespit etmeye çalışmıştır. Çalışmanın sonucunda Husilerin yasadışı yollarla çeşitli kaynaklardan ticari teknik donanımları ülkeye sokarak kendi ürettiği parçalarla birleştirmesi sonucu hem gözetim hem de vuruş kabiliyeti olan dronelar elde ettiği tespit edilmiştir. Yurt dışından getirilen teknik parçaların bir kısmı Çin menşeli Mile Hao Xiang Technology Co., Ltd firmasından temin edilse de firma alıcı kayıtlarını tutmadıklarını belirtmiştir, firmaya ait DLE motorları Amazon, E-bay gibi uygulamalar üzerinden satın alınmıştır. Diğer bir tedarik firması ise Tayvan merkezli MINMAX Technology Co. Ltd. şirketidir. Bu şirket araştırmaya konu olan parçaların seri numarasından bu ürünleri İran'a ait bir firmaya sattığını belirtmiştir. Ek olarak bazı parçaların İran yapımı droneların parçaları ile benzerlik gösterdiği tespit edilmiştir (Conflict Armament Research, 2020). Buradan da Yemen'e giren parçaların bir kısmının İran üzerinden getirildiği gözlemlenebilmektedir.

Bu teknik kapasitenin en sarsıcı stratejik uygulaması, 2019 yılında Suudi Arabistan'ın Abqaiq ve Khurais petrol tesislerine (Aramco) düzenlenen saldırılardır. Sadece birkaç bin dolarlık ticari parçalarla modifiye edilen bu dronelar, milyar dolarlık Patriot hava savunma sistemlerini baypas ederek dünyanın en büyük petrol işleme tesislerini hedef almıştır. Bu saldırı ile dünya petrol arzının %5'i

zarar görmüştür (Aljazeera, 2019). Armed Conflict Location & Event Data Project (ACLED) raporuna göre 2018-2022 yılları arasında Husiler tarafından Suudi Arabistan'a yönelik gerçekleştirilen drone saldırılarının ana hedefi hidrokarbon tesisleri olmuştur (Nevola & d'Hauthuille, 2024). Bu vaka, ticari droneların sadece yerel bir vuruş gücü olmadığını, aynı zamanda küresel ekonomik altyapıları hedef alarak devletler üzerinde stratejik bir baskı yaratarak psikolojik etki yaratabildiğini göstermektedir. Husilerin bu eylemleri, düşük maliyetli asimetrik araçların, yüksek maliyetli konvansiyonel savunma mimarilerini geçersiz kılmasına örnektir.

Vuruş kabiliyetine başvurmadan psikolojik olarak güvenliksizlik ortamı yaratan operasyon örneği Fransa ve Almanya'daki nükleer santraller üzerinde uçuş gerçekleştiren dronelardır. Kritik altyapıların korunmasında kullanılan geleneksel yöntemlerin, sivil teknolojiden devşirilen asimetrik tehditler karşısında ne kadar işlevsiz kalabileceği 2014 ve 2015 yıllarında Avrupa'nın kalbinde test edilmiştir. Ayrıca 2017 yılında Greenpeace aktivistleri Fransa'nın nükleer tesislerinde uçuşa yasak bölgede drone uçuşu gerçekleştirmiş ve radyoaktif materyal bulunduran duvara bu dronu çarparak eylem gerçekleştirmiştir (Gliadkovskaya, 2018). Fransa genelinde, aralarında dünyanın en büyük nükleer tesislerinin de bulunduğu 13'ten fazla santralin üzerinde kimliği belirlenemeyen ticari droneların eş zamanlı ve sistematik uçuşlar gerçekleştirmesi (Guardian, 2014), güvenliksizlik hissi yaratmaktadır. Bu dronelar, reaktör binaları ve yakıt havuzları gibi en hassas noktalar üzerinde uçarak herhangi bir kinetik saldırı gerçekleştirmemiştir; ancak devletin en sıkı korunan bölgelerinin sivil bir teknolojiyle kolayca delinebileceğini kanıtlamışlardır.

Kritik altyapılara yönelik drone tehdidinin bir diğer boyutu, 2018 yılının Aralık ayında Londra Gatwick Havalimanı'nda küresel sivil havacılık güvenliğinde yaşanan krizdir. Kimliği belirlenemeyen ticari bir dronenun havalimanı sahası içinde görülmesi üzerine başlatılan güvenlik protokolleri, yaklaşık 33 saat süren bir operasyonel duraksamaya neden olmuştur. Bu süreçte 1.000'den fazla uçuş iptal edilmiş, 140.000 yolcu mağdur olmuş ve havacılık sektöründe milyonlarca sterlinlik doğrudan ekonomik kayıp meydana gelmiştir (BBC, 2018).

Gatwick vakası, hibrit savaşın asimetrik maliyet ilkesini en yalın haliyle ortaya koymaktadır. Piyasa değeri birkaç bin doları geçmeyen tek bir ticari cihazın, dünyanın en gelişmiş ve yoğun ulaşım ağlarından birini günlerce kilitleyebilmesi, konvansiyonel güvenlik sistemlerinin yetersizliğini ifşa etmiştir. Olayın en dikkat çekici yönü, herhangi bir fiziksel saldırı veya patlama gerçekleşmemesine rağmen, sadece drone varlığının yarattığı potansiyel riskin tüm sistemi kapatmaya yetmesidir. Bu olay çift kullanım güvenlik ikilemini en net gösteren örneklerden biridir.

Elektronik Savaş ve Siber Saldırıların Yeni Boyutu: Uçan Dijital Tehditler

Ticari droneların hibrit çatışmalardaki rolü, kinetik saldırıların ötesine geçerek siber uzam ile elektromanyetik spektrumun kesiştiği tehdit sahasına evrilmiştir. Bu araçlar, siber güvenliğin en temel varsayımı olan fiziksel izolasyon ve mesafe güvenliğini, dikey hareket kabiliyetleri sayesinde anlamsız kılmaktadır.

Elektronik savaş kapsamında ticari donanımlar ile güçlendirilmiş ticari dronelar ticari merkezlerin, kritik alt yapıların ve devlet kurumlarının yakınlarında uçurularak hassas verilere yönelik saldırılar yapılabilmektedir. Droneların elektronik savaş kapsamında kullanılmasının yaratacağı potansiyel tehditleri analiz edebilmek amacıyla Westerlund ve Asif (2019) geliştirdikleri similasyon ile düşük maliyetli donanımları kullanarak yapılabilecek saldırıları tespit etmiştir. Bu saldırılarda ticari dronelara Wifi Pineapple ve Raspberry Pi donanımları monte edilmektedir.

Wifi Pineapple, günümüzde kullanılan Wifi teknolojisi temeline dayanan bir nevi sahte sunucu görevi görür hem etik hem de etik dışı kullanımları mevcuttur. Oldukça hafif ve küçük bir donanım olmasının yanı sıra güncel fiyatı 250 USD civarındadır ve internetten rahatlıkla temin edilebilir. Normalde Wifi adresinin bir servis seti tanımlayıcısı bulunur. Wifi Pineapple servis seti tanımlayıcısını taklit ederek sunucu ile cihaz arasında bir ara ajan olarak çalışır. Bu durumda Wifi üzerinden aktarılan tüm veriler Wifi Pineapple kullanıcısı tarafından ele geçirilebilir (Kuntz, 2024).

Raspberry Pi ile kabaca kredi kartı büyüklüğündeki bir cep bilgisayarıdır. Wifi Pineapple gibi internetten kolayca temin edilebilir, güncel fiyatı kapasitesine göre değişim göstermekle birlikte 45 USD bandındadır. Tıpkı Wifi Pineapple da olduğu gibi hem etik hem de etik dışı kullanımları mevcuttur. Günümüzde teknik anlamda yapay zeka çalışmalarında kullanılmaktadır. Etik dışı kullanımlarında veri sızıntılarına sebebiyet verebilir. Raspberry Pi, ethernet cihazı gibi davranarak internet trafiğini takip edebilir, HTTP çerezlerini çalabilir, arka kapı saldırıları gerçekleştirebilir, P4wnP1 hizmeti ile klavye ve fare gibi çalışarak zararlı komutlar verebilir, cihazların ağ erişim kontrollerini taklit ederek ağlarına sızabilir, uzun süreli ve fark edilmesi güç gelişmiş sürekli tehditler (APT) saldırısı yapabilir (Sepio, 2020).

Saldırganlar, bu donanımlar ile güçlendirilmiş ticari dronelar ile hedef kurumların kablosuz ağ trafiğini manipüle ederek Araya Giren Adam (Man-in-the-Middle - MitM) saldırıları gerçekleştirebilmekte, ağ paketlerini koklayarak (sniffing) hassas verileri sızdırabilmektedir (Westerlund & Asif, 2019). Siber saldırıların bu fiziksel boyutu, droneların sinyal istihbaratı (SIGINT) kabiliyetleriyle birleştiğinde daha da sofistike bir hal almaktadır. Ticari dronelar; iletişimi kesme (jamming),

sahte baz istasyonu kurma veya telsiz sinyallerini taklit etme gibi elektronik savaş taktiklerini asimetrik bir düzleme taşımaktadır. Sonuç olarak dronelar, dijital sızma ile spektrum manipülasyonunu birleştirerek, fiziksel bariyerlerin arkasına saklanan kritik sistemleri siber ve elektronik birer hedef haline getirmektedir.

Elektronik ve siber operasyonlar kapsamında ticari droneların kullanımı, teorik bir tehdit olmaktan çıkıp devletlerin stratejik güvenlik açıklarını ifşa eden somut vakalara dönüşmüştür. Örneğin, 2017 yılında Güney Kore topraklarında ele geçirilen bir Kuzey Kore dronunun, ABD'ye ait THAAD füze savunma sistemlerini fotoğraflayarak bölgedeki dijital izleri takip etmesi, bu araçların düşük maliyetli birer SIGINT aracına dönüştüğünü kanıtlamıştır (Reuters, 2017). Benzer bir fiziksel sızma vakası 2019 yılında NASA'nın Jet İtki Laboratuvarı'nda (JPL) yaşanmış; ağa gizlice bağlanan bir Raspberry Pi cihazı üzerinden yaklaşık 500 MB'lık kritik verinin dışarı sızdırılması, en üst düzey teknoloji kurumlarının bile ne kadar savunmasız kalabileceğini göstermiştir (BBC, 2019).

Dijital casusluk faaliyetleri, kritik altyapılara yönelik doğrudan müdahalelerle de birleşmektedir. Temmuz 2020'de Pensilvanya'daki bir elektrik trafo merkezinin üzerinde yakalanan modifiye edilmiş drone, altına yerleştirilen özel donanım düzeneğiyle şebeke sistemine siber saldırı gerçekleştirmeyi amaçlayan ilk resmi vaka olarak kayıtlara geçmiştir (Lyngaas, 2021). 2021-2022 yıllarında Norveç'teki petrol ve doğalgaz platformları çevresinde gözlemlenen yoğun drone hareketliliği saptanmıştır (Euronews, 2022). Yakalanan cihazların üzerinden çıkan veri depolama birimleri, bu uçuşların sadece görüntüleme değil, sistemlerin siber dayanıklılığını test etme ve sinyal verilerini toplama amacı taşıdığını doğrulamıştır.

Asimetrik Lojistik ve Devlet Otoritesinin Baypas Edilmesi

Ticari dronelar, sınır güvenliği ve organize suç örgütlerinin tedarik zinciri konularında devlet egemenliğine yönelik tehdit oluşturmaktadır. Asimetrik lojistik olarak tanımlanabilecek bu yeni fenomen, devletin gümrük kapıları, cezaevi duvarları ve sınır hatları gibi fiziksel bariyerlerle tesis ettiği otoriteyi, dikey düzlemde anlamsız kılmaktadır. Reilly (2025) asimetrik lojistiği büyük askeri lojistik sistemleri yerine parçalanmış tedarik ağları ile sağlanan geniş bir ağ ile olası saldırılara karşı ve acil durumlara karşı uyum sağlama yöntemi olarak tanımlamıştır. Daniel (2010) ise asimetrik lojistik uygulamalarının devlet dışı aktörler tarafından kullanımını Hizbullah örneği üzerinden analiz etmiştir. Koyuncu vd. (2015) silah, mühimmat, propaganda malzemeleri, kamp malzemeleri ve diğer araç gereçlerin terör sempatizanları, destekleyici devletler, kuryeler gibi sistemler ile terör gruplarına ulaştırılmasının modelini incelemiştir. Özellikle Meksika-ABD sınırında uyuşturucu kartelleri tarafından kullanılan ağır yük kapasiteli modifiye dronelar,

devletin konvansiyonel sınır güvenliği mimarisini baypas etmektedir. Benzer şekilde, cezaevlerine yönelik gerçekleştirilen yasaklı madde sevkiyatları, devletin mutlak kontrolü altında kabul edilen en korunaklı alanların dahi ticari teknoloji karşısında geçirgen hale geldiğini kanıtlamaktadır. Bu durum, lojistik süreçlerin merkezileşmiş devlet kontrolünden çıkarak asimetrik aktörlerin elinde birer stratejik araca dönüşmesine neden olmaktadır.

Meksika-ABD sınırında faaliyet gösteren Jalisco Yeni Nesil Karteli (CJNG) gibi organize suç örgütlerinin modifiye edilmiş ticari droneları kullanması geleneksel duvarların, sismik sensörlerin ve sınır devriyelerinin üzerinden dikey düzlemde, yüksek miktarda uyuşturucu ve silah sevkiyatını radarlara yakalanmadan gerçekleştirerek devletin gümrük ve sınır denetim mekanizmalarını işlevsiz kılmaktadır (Felbab-Brown, 2026). Benzer bir geçirgenlik hali, cezaevi güvenliğinde de gözlemlenmektedir. Örneğin, İngiltere ve Galler'deki cezaevlerine yönelik gerçekleştirilen drone uçuşları 2019-2023 arası verilerde %770'in üzerinde bir artış kaydedilmiştir (Ministry of Justice, 2026), devletin en izole ve mutlak kontrollü alanlarına dahi dışarıdan uyuşturucu, cep telefonu ve hatta ateşli silah sokulabildiğini göstermiştir. Bu durum, fiziksel bariyerlerin ticari teknoloji karşısındaki yetersizliğini kanıtlamaktadır.

Lojistiğin bu asimetrik dönüşümü sadece suç dünyasıyla sınırlı kalmamış, modern çatışma alanlarında da stratejik bir boyut kazanmıştır. Ukrayna-Rusya Savaşı'nda sivil gönüllü ağları tarafından yönetilen ticari drone filoları, büyük orduların hantal lojistik kuyruklarına ihtiyaç duymadan cephe hattına ilaç, kritik bataryalar ve mühimmat ulaştırarak geleneksel askeri ikmal doktrinlerini sarsmıştır. Reilly'nin (2025) vurguladığı parçalanmış tedarik ağları burada somut bir karşılık bulmuş; merkezi bir komuta yapısı olmaksızın, sivil pazardan temin edilen araçlarla kurulan bu lojistik ağ, devlet dışı veya zayıf aktörlerin operasyonel sürekliliğini sağlamıştır. Sonuç olarak, asimetrik lojistik uygulamaları, devletin fiziksel egemenlik iddia ettiği her noktada (sınırda, hapishanede veya cephede) otoriteyi dikey bir meydan okuma ile karşı karşıya bırakmaktadır.

Sonuç ve Öneriler

Bu çalışmada incelenen teknik veriler ve saha örnekleri, ticari droneların modern hibrit savaş literatüründe stratejik birer asimetrik güç çarpanına dönüştüğünü ortaya koymaktadır. Bu araçların en temel özelliği, teknolojinin savaş alanını demokratikleşmesi neticesinde devlet dışı aktörlere ve küçük gruplara, normal şartlarda sadece düzenli orduların sahip olabileceği hava kabiliyeti ve elektronik savaş yeteneklerini çok düşük maliyetlerle sunmasıdır. Eskiden yüksek bütçeli savunma sanayii yatırımı gerektiren SIGINT veya operasyonel lojistik gibi kabiliyetlerin, bugün internetten kolayca temin edilebilen WiFi Pineapple ve Raspberry

Pi gibi donanımlarla sivil bir platforma entegre edilebilmesi, geleneksel güvenlik hiyerarşisini sarsmaktadır.

İç güvenlik perspektifinden bakıldığında bu durum, devletin kendi egemenlik alanı içerisindeki mutlak denetim kapasitesine yönelik çok katmanlı bir meydan okumadır. Dronelar; Gatwick Havalimanı vakasındaki gibi ulaşım ağlarını felç edebilme, nükleer tesisler üzerinde uçarak psikolojik harp yürütebilme ve siber-fiziksel sızma girişimleriyle kritik altyapıları hedef alabilme yeteneğine sahiptir. Devletin fiziksel engeller üzerinden tesis ettiği koruma kalkanı, bu araçların dikey hareket kabiliyeti ve dijital sızma kapasitesi karşısında geçirgen hale gelmektedir.

Nihayetinde, ticari droneların yarattığı bu tehdit profili sadece kinetik bir asayiş sorunu değil; siber, elektronik, hukuki ve lojistik boyutları olan bütüncül bir hibrit meydan okumadır. Devlet dışı aktörlerin, devasa savunma bütçelerine sahip devlet mekanizmalarına karşı erişilebilir ve ucuz teknolojilerle stratejik etki yaratabiliyor oluşu, modern güvenlik mimarilerinin yeniden tasarlanmasını zorunlu kılmaktadır. Geleceğin iç güvenlik stratejileri, fiziksel bariyerlerin ötesine geçerek; elektromanyetik spektrumun savunulmasını, otonom tespit sistemlerinin entegrasyonunu ve bu asimetrik araçlara karşı proaktif bir egemenlik tanımını kapsayan dinamik bir çerçeve benimsemelidir. Ayrıca devletlerin güvenlik algısında yaratabileceği güvenlik ikilemi ticari unsurları da içine alarak güvenliksizlik ortamını tetiklemektedir.

Bu çok boyutlu tehditler karşısında devletler, geleneksel hava savunma doktrinlerini küçük ve yavaş hedefleri de kapsayacak şekilde revize ederek yeni nesil karşı koyma stratejileri geliştirmektedir. ABD İç Güvenlik Bakanlığı'nın 2026 başında kurduğu özel drone ofisi (Homeland Security, 2026), Avrupa Komisyonu'nun yayınladığı "Drone ve Karşı-Drone Güvenlik Eylem Planı» (European Commision, 2026) ve ASELSAN tarafından geliştirilen İHTAR sistemi (Aselsan, 2026) sivil hava sahasının korunmasını bir ulusal egemenlik meselesi olarak yeniden tanımlamaktadır. Bu kapsamda, sadece kinetik imha yöntemleri değil; 5G ağlarının birer radar gibi kullanılması, yapay zeka destekli otomatik tespit sistemleri ve güvenilir drone etiketleme mekanizmaları gibi siber-elektronik savunma katmanları oluşturulmaktadır. Devletler, teknolojinin demokratikleşmesinin yarattığı bu güvenlik açığını, savunma sanayii ve sivil teknoloji firmalarıyla kurdukları stratejik iş birlikleriyle kapatmaya çalışırken; elektromanyetik spektrumun savunulmasını iç güvenliğin yeni ve kaçınılmaz bir cephesi olarak kabul edilmelidir.

Kaynakça

Abusalem, K., Alsaleh, M., Reuter, T., Alsedairy, T. (2021, Temmuz 21). Why the future is bright for drone technology. World Economic Forum. https://www.weforum.org/stories/2021/07/the-bright-future-for-drones/?gad_source=1&gad_campaignid=22228224717&gbraid=0AAAAAoVy5F7f1eXQEd4WUqNcPI5E_dmUE

Aljazeera. (2019). Saudi oil attack: All the latest updates. https://www.aljazeera.com/news/2019/9/30/saudi-oil-attack-all-the-latest-updates

Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International Security, 26*(1), ss. 93–128.

Aselsan. (2026). İHTAR 100. https://www.aselsan.com/tr/savunma/urun/2654/ihtar-100

Balkan, S. (2017). daesh's drone strategy technology and the rise of innovative terrorism. SETA Publications. https://media.setav.org/en/file/2017/08/daeshs-drone-strategy-technology-and-the-rise-of-innovative-terrorism.pdf

BBC. (2018, Aralık 22). Gatwick drones: Two arrested over flight disruption. https://www.bbc.com/news/uk-england-46657505

BBC. (2019, Haziran 24). Raspberry Pi used to steal data from Nasa lab. https://www.bbc.com/news/technology-48743043

Buzan, B., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Castells, M. (2005). The network society: From knowledge to policy. M. Castells ve G. Cardoso (Ed.), The network society: From knowledge to policy içinde (ss. 3–22). Johns Hopkins University Center for Transatlantic Relations.

Clausewitz, C. V. (2011). Savaş üzerine (H. Akbulut, Çev.). Eriş Yayınları.

Conflict Armament Research. (2020). Evolution of UAVs employed by Houthi forces in Yemen. https://www.conflictarm.com/reports/evolution-of-uavs-employed-by-houthi-forces-in-yemen/

Creveld, M. V. (1989). Technology and war: From 2000 B.C. to the present. Free Press.

Cronin, A. K. (2018). Power to the people: How open technological innovation is arming tomorrow's terrorists. Oxford University Press.

CSIS. (2015, Mayıs 28). The Russia-Ukraine drone war: Innovation on the frontlines and beyond. https://www.csis.org/analysis/russia-ukraine-drone-war-innovation-frontlines-and-beyond

Daniel, J. M. (2010). Hizbullogistics: The asymmetrical application of logistics in war. Joint Military Operations Department Naval War College. https://apps.dtic.mil/sti/pdfs/ADA525226.pdf

Euronews. (2022, Ekim 20). Norway on alert after drone sightings near key infrastructure. https://www.euronews.com/2022/10/20/norway-on-alert-after-drone-sightings-near-key-infrastructure

European Commision. (2026). Action plan on drone and counter drone security. https://digital-strategy.ec.europa.eu/en/policies/drone-security

Felbab-Brown, V. (2026, Şubat 18). How Mexican cartels are using drones, now and in the future. Brookings. https://www.brookings.edu/articles/how-mexican-cartels-are-using-drones-now-and-in-the-future/#:~:text=Like%20other%20non%2Dstate%20actors,an%20area%20unusable%20for%20civilians.

Friedman, T. L. (2007). The world is flat: A brief history of the twenty-first century (3. baskı). Picador; Farrar, Straus and Giroux.

Fuhrmann, M. (2008). Exporting mass destruction? The determinants of dual-use trade. *Journal of Peace Research*, *45*(5), ss. 633-652.

Fuhrmann, M. (2012). Splitting atoms: Why do countries build nuclear power plants?. *International Interactions*, *38*(1), ss. 29-57.

Giscard, S. (2020). The dual-use dilemma in unmanned aerial systems. *Journal of Strategic Security*, *13*(4), ss. 1–15.

Gliadkovskaya, A. (2018, Haziran 3). Greenpeace activists pilot and crash drone into French nuclear plant's no-fly zone. Euronews. https://www.euronews.com/2018/07/03/greenpeace-activists-pilot-and-crash-drone-into-french-nuclear-plant-s-no-fly-zone

Goward, D. (2017). GPS spoofing incident points to fragility of navigation satellites. National Defense, 102(766), ss. 18-19. https://www.jstor.org/stable/pdf/27021938.pdf?refreqid=fastly-default%3A599504d8dc1182aa6679551f6b99bdab&ab_segments=&initiator=&acceptTC=1

Grand View Research (2026). Drone market (2026 - 2033). https://www.grandviewresearch.com/industry-analysis/drone-market-report

GZT. (2026, Mart 3). Hürmüz Boğazı'nda hayalet gemiler: Binden fazla gemi rotasını şaşırdı, GPS sinyalleri felç oldu. https://www.gzt.com/dunya/hurmuz-bogazinda-elektronik-savas-1100-gemi-kayboldu-gps-spoofing-ve-jamming-krizi-gemiler-neden-karada-gorunuyor-4022136

Hammes, T. X. (2016). The technologies converge. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2016/01/The_Technologies_Converge_web_0126.pdf

Hansen, L., ve Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), ss. 1155–1175.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.

Homeland Security, (2026, Ocak 12). Department of Homeland Security launches new office to advance drone and counter-drone technologies. https://www.dhs.gov/news/2026/01/12/department-homeland-security-launches-new-office-advance-drone-and-counter-drone

Kaldor, M. (2012). New and old wars: Organized violence in a global era (3. baskı). Polity Press.

Koyuncu, T.Z, Aplak, H.S., Gerdan, O. (2015). Asimetrik lojistik faaliyetlerin engellenmesi: Doğrusal programlama modeli uygulaması. *Güvenlik Bilimleri Dergisi*, *4*(1), ss. 87-109. https://dergipark.org.tr/en/download/article-file/208217

Kuntz, G. (2024). Infiltrating Wi-Fi networks: Wi-Fi Pineapple Mark VII [Yüksek lisans tezi, Iowa State University]. https://dr.lib.iastate.edu/entities/publication/5243167e-406c-48be-806b-35719992f7f2

Lupovici, A. (2021). The dual-use security dilemma and the social construction of insecurity. *Contemporary Security Policy*, *42*(3), ss. 322–347.

Lyngaas, S. (2021, Kasım 4). Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure,' according to federal law enforcement bulletin. CNN. https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation

McFate, S. (2019). The new rules of war: Victory in the age of durable disorder. William Morrow.

Ministry of Justice. (2026). Battlefield tactics to inspire UK fight against prison drones. Press Release. https://www.gov.uk/government/news/battlefield-tactics-to-inspire-uk-fight-against-prison-drones

Nevola, L. & d'Hauthuille, V. (2024). Six Houthi drone warfare strategies: How innovation is shifting the regional balance of power. ACLED. https://acleddata.com/report/six-houthi-drone-warfare-strategies-how-innovation-shifting-regional-balance-power#:~:text=The%20Houthis%20have%20used%20drone%20warfare%20strategies,*%20**Identifying%20and%20exploiting%20the%20enemy's%20weaknesses**

Rassler, D., Gunaratna, R., ve Amarasingam, A. (2017). The Islamic State's evolving drone threat. Combating Terrorism Center at West Point. https://ctc.westpoint.edu/the-islamic-states-evolving-drone-threat/

Reilly, A. (2025). Beans before bullets: Asymmetric logistics as deterrence and offense in near-peer competition. Project Muse. Marine Corps University Press https://muse.jhu.edu/pub/419/article/949596/pdf

Research and Markets. (2025). Drones as a service market by applications and leading industries with global, regional and country forecasts 2025 – 2030. https://www.researchandmarkets.com/report/drone-as-a-service?srsltid=AfmBOopsvS2og7QNWGCKnUzJSraL7W_zjBc1rKmrnqdASh4twTaaevuC

Reuters. (2017, Haziran 13). Suspected North Korea drone spied on U.S. anti-missile system: South Korea officials. https://www.reuters.com/article/world/suspected-north-korea-drone-spied-on-us-anti-missile-system-south-korea-offic-idUSKBN1940J8/

Sandvik, K. B., & Jumbert, M. G. (Eds.). (2016). The good drone. Routledge.

Sepio. (2020). Raspberry Pi – A friend or foe? Cyber physical security challenges https://sepiocyber.com/wp-content/uploads/2020/08/Raspberry-Pi-Risks-Article-E-Book-new-logo.pdf

Singer, P. W. (2009). Wired for war: The robotics revolution and conflict in the twenty-first century. Penguin Press.

The Guardian. (2014, Eylül 30). French investigate drones spotted over nuclear plants. https://www.theguardian.com/world/2014/oct/30/french-investigate-drones-spotted-over-nuclear-plants

Varnalı, T. (2026). The transformation of the global drone ecosystem: A systematic assessment of autonomy, artificial intelligence and market strategies. *Journal of Sivas Cumhuriyet University Social Sciences Institute, 2*(1), ss. 56-73. https://dergipark.org.tr/tr/download/article-file/5465786

Weber, M. (2006). Siyaset mesleği (M. Uzun, Çev.). Say Yayınları.

Westerlund, O., & Asif, R. (2019). Drone hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and privacy threats for the Internet-of-Things. 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS). IEEE. https://ieeexplore.ieee.org/document/8658279/

Ziemer, H. (2025, Haziran 11). Illicit innovation: Latin america is not prepared to fight criminal drones. CSIS. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones