thinktech
STM Teknolojik Düşünce Merkezi

Uydudan Elektronik Harp Uygulamaları: Gelişmeler ve Gelecek Öngörüleri

Soğuk Savaş'ın sona ermesinin ardından yeterince ilgi bulamayan Elektronik Harp Sistemleri (EH), günümüzde gelişen teknolojilerin de katkısıyla yeniden önem kazanmaya başlıyor. 21'inci yüzyılın teknolojilerinin hızlandırdığı savunma teknolojilerindeki değişim, artan uluslararası gerginlikler ve çatışmalar, çok kutuplu güç siyaseti ve buna bağlı olarak hızlanan silahlanma, Elektronik Harbi kara, hava, deniz, uzay ve siber uzay ile birlikte asli operasyon alanlarından biri hâline getiriyor. Aralarında Türkiye'nin de bulunduğu belli başlı ülkelerin savunma sanayileri, Elektronik Harp Sistem ve çözümleri geliştirmeye devam ediyor. Bu sistemler gün geçtikçe kabiliyetlerini artırırken aynı zamanda çoklu işlev kabiliyeti ve bilişsel yeteneklerini de güçlendiriyor[1].

Giderek karmaşıklaşan modern Elektronik Harp, bu tür sistemlere sahip silahlı kuvvetlere stratejik avantaj sağlarken, yüksek kabiliyetli Elektronik Harp sistemlere sahip olmayan silahlı kuvvetleri zor durumda bırakabiliyor. Dördüncü nesil savaş olarak adlandırılan Elektronik Harp, savaş veya çatışmalarda gelişen bilişim teknolojilerinin önemini artırıyor. Bu noktada Elektronik Harp sistemleri savaş veya çatışmalardaki destek, savunma ve saldırı yeteneklerini büyük ölçüde değiştiriyor[2].

Uydudan Elektronik Harp Uygulamaları

Uzay son yıllarda, insanların günlük hayatlarını idame ettirmelerinde, ülkelerin ekonomik gelişimlerinde, stratejik gözlem ve iletişim uygulamalarında ve daha birçok savunma sanayii uygulamalarında büyük öneme sahip uyduların bulunduğu bir alan olarak yeniden ilgi odağı hâline geliyor[3].

Uzay, Elektronik Harp açısından istihbarat ve keşiflerin yeni sınırı olarak düşünülüyor. Uzay aynı zamanda dünyanın geniş açıyla görülebileceği bir yer. Bu yaklaşım, askeri yetkililerin ülkelerini koruma ve sınırları izleme konusunda daha iyi kararlar almasına yardımcı olabilir[4].

Günümüz dünyasında yörüngede gezen uydular, savunma ve havacılık sanayiine iletişim, navigasyon ve gözetleme hizmetlerinin sağlanmasında kritik bir rol oynuyor. Ancak Elektronik Harp ve siber saldırıların karmaşıklığının artmasıyla birlikte bu uydular çok çeşitli tehditlere karşı savunmasız hâle gelmeye başlıyor. Bu nedenle uydu sistemlerinin bütünlüğünü ve etkinliğini sağlamak için etkili Elektronik Harp ve siber savunma stratejilerinin geliştirilmesi ve uygulanması gerekiyor[5].

1 https://thinktech.stm.com.tr/tr/bilissel-elektronik-harp-ve-radar-sistemleri
2 https://thinktech.stm.com.tr/tr/insansiz-hava-araclarinda-elektronik-harp-uygulamalari
3 https://www.emsopedia.org/entries/space-ew/
4 https://kstatelibraries.pressbooks.pub/spacesystems/chapter/soace-electronic-warfare-jamming-spoofing-and-ecd-nichols-mai/
5 https://incompliancemag.com/electronic-warfare-and-cyber-defense-of-satellites/

Uydudan Elektronik Harp uygulamaları ülkelerin çıkarlarının korunmasının yanı sıra, düşmanların uzay varlıklarını kullanmasını engelleme yeteneği sağlayan operasyonel sistemleri de içeriyor. Operasyonel sistemler, bağımsız tek görevli sistemlerden, dinamik komuta ve kontrolün yanı sıra uzaktan operasyon yeteneklerine sahip çok görevli platformlara doğru ilerliyor. Elektromanyetik spektrum hâkimiyeti, uzay alanı operatörlerinin savaş için gerekli olan kritik işlevleri yerine getirmesine olanak tanıyor. Bunlar, tehditleri bulma, düzeltme, izleme, hedefleme, müdahale etme ve değerlendirme olarak biliniyor. Elektromanyetik spektrum içinde hareket etme özgürlüğü ve düşmanların erişimini engelleme yeteneği olmayan sistemlerin uzayda hâkimiyet kurması beklenmiyor[6].

Uzaya gönderilen uydular günümüzde Elektronik Harp Sistemleriyle donatılarak savunma veya savaş hâlinde saldırı amacıyla da kullanılabiliyor. Geçmişte ağırlık olarak iletişim veya gözlem amacıyla kullanılan uyduların yeni kullanım alanı olan elektronik harp uygulamaları için çok çeşitli seçenekler bulunuyor[7].

Uydudan Elektronik Harp; Elektronik Destek (ED), Elektronik Taarruz (ET) ve Elektronik Koruma (EK) olarak üç başlıkta değerlendirilebiliyor. Elektronik Taarruz doğrudan yapılan müdahaleleri, engellemeleri, aldatma faaliyetlerini içerebiliyor[8].

Elektronik Taarruz kapsamında değerlendirilebilen uyduların yörüngede engellenmesi veya doğrudan uydunun yakın mesafeden engellenmeye çalışılması yapısal özellikler nedeniyle oldukça zor bir durum oluşturuyor. İrtifa veya boyuta bakılmaksızın bir iletişim uydusu çok fazla güce ihtiyaç duyuyor. İletişim uydularına gönderilecek yüksek kapasiteli veri bombardımanı ise uydunun veri alma veya iletme yeteneğini bozmayı amaçlıyor. Uydunun yakın mesafeden engellenebilmesi için ise çok yakınına başka bir uydu gönderilmesi gerekiyor. Bu durum jeopolitik olarak oldukça riskli bir strateji olmasının yanı sıra pek çok uluslararası kriz ihtimalini de bünyesinde taşıyor.

Skynet gibi askeri uydular ise engelleyici sinyallerin üstesinden gelmek için iletim gücünü artıran ve güvenilir iletişim sağlayan uyarlanabilir güç kontrolünün kullanımı da dahil olmak üzere çok sayıda anti-parazit tekniği kullanıyor. Bir diğer açıdan da normal çalışma sırasında enerji tasarrufu sağlamak ve uydunun tespit edilmeye karşı hassasiyetini en aza indirmek için çalışma gücünü azaltabiliyor. Askeri uydular ayrıca, antenlerin her biri boş değerler veya zayıf sinyal alanları oluşturmak ve diğer alanlarda sinyal gücünü artırmak için kullanılabilen bir dizi anten elemanından oluşan sistemleri de kullanıyor. Kullanılan bu dizili anten teknolojisi ile, jammer yönünü sıfırlama veya ilgilendikleri sinyal yönüne hüzme yönlendirme teknikleri uygulanabiliyor.

Bir uydu ağını engellemenin basit bir yolu daha var. Bu yöntem karasal engelleme olarak da biliniyor. İletişim uydularından farklı olarak navigasyon uyduları, sinyalleri iletmek için çok daha az güç kullanıyor ve engellenmesi çok daha kolay hedefler hâline geliyor. Çoğu ordunun, radyo frekans sinyallerini doğrudan kapsamak istedikleri alana iletebilen, karada veya uçakta bulunan büyük mobil birimleri bulunuyor. Bu sinyaller uyduların kapsama alanına yayınladığı sinyallerden daha güçlüyse, bu durum GPS iletimini ve alımını etkileyebiliyor[7].

Karasal engelleme, bir dizi normal GPS sinyaline benzeyecek şekilde yapılandırılmış sahte GPS sinyalleri yayınlayarak bir GPS alıcısını aldatma girişimi olarak kullanılıyor. Bu sinyal bozucu sahte sinyaller alıcının konumunun gerçekte bulunduğu yerden başka bir yerde olduğunu gösterebiliyor. Bu sahte sinyaller ayrıca hareketli hedeflerin varacakları yere, düşman tarafından belirlenen farklı bir zamanda varacağına yönelik yanlış tahminde bulunulmasına da neden olabiliyor[9].

6 https://www.l3harris.com/all-capabilities/space-electronic-warfare
7 https://www.linkedin.com/pulse/how-electronic-warfare-driving-design-satellite-systems-julian-hewson-se9lc
8 https://www.savunmasanayiidergilik.com/tr/HaberDergilik/Elektronik-destek-sistemlerinde-veri-analizi
9 https://capec.mitre.org/data/definitions/599.html

GPS artık dünya çapında çeşitli askeri uygulamalar için vazgeçilmez bir araç olarak hizmet veriyor. Muharebe senaryolarında GPS, hava saldırılarının ve topçuların doğru hedeflenmesine olanak tanıyarak operasyonel verimliliği artırırken ikincil hasarı en aza indirebiliyor. Birlik ve varlık hareketleri, gerçek zamanlı konumlandırma ile kolaylaştırılarak durumsal farkındalık ve koordinasyon artırılıyor. Uydu iletişimi açısından GPS, yer istasyonları ve uydular arasındaki sinyallerin doğru senkronizasyonunu sağlamak için hassas zamanlama ve konumlandırma verileri sağlayarak çok önemli bir rol oynuyor[7].

GPS engelleme ve yanıltma tehdidi, ulusal savunma ve ticari ulaşım sistemleri için önemli riskler oluşturuyor. Bu kötü niyetli eylemler, özellikle çekişmeli veya dar coğrafyalarda navigasyon hatalarına ve operasyonel güvenliğin tehlikeye atılmasına yol açabiliyor[10].

Uydu Elektronik Harp uygulamalarının parçası olarak düşünülen ve Elektronik Destek alanının en önemli yapıtaşı olan bir diğer uygulama da sinyal ve iletişimle ilgili bilgilerin toplanması ve manipülasyonunu içeriyor. Sinyal İstihbaratı (Signal Intelligence -SIGINT) olarak da bilinen bu uygulama bir düşmanın veya hedefin işleyişi hakkında bilgi edinmek için kullanılan sinyallerin ve iletişimle ilgili bilgilerin toplanmasını tanımlıyor. SIGINT, radyo dalgalarının dinlenmesi, uydu iletişimlerinin izlenmesi, şifreli mesajların çözümü, telefon konuşmalarına sızma ve açık kaynak verilerinin analizi gibi çeşitli metotlar kullanıyor. SIGINT, İletişim İstihbaratı (Communications Intelligence -COMINT), Elektronik İstihbarat (Electronic Intelligence -ELINT), Yabancı Enstrümantasyon Sinyalleri İstihbaratı (Foreign Instrumentation Signals Intelligence -FISINT) olarak üç alt başlıkta incelenebiliyor. İstihbarat teşkilatları COMINT aracılığıyla iletişimleri keserek görevlerinde yardımcı olabilecek değerli bilgilere erişim sağlayabiliyor. ELINT, çeşitli elektronik sistemlerden kaynaklanan iletişim dışı emisyonların toplanmasına ve analiz edilmesine odaklanıyor. FISINT de elektronik gözetim operasyonlarında kullanılabilecek destekleyici kanıtları güçlendirmek için ek bilgiler sağlayarak SIGINT'te hayati bir rol oynuyor. SIGINT'in yardımıyla dünya çapındaki ordular, düşmanları hakkında daha iyi kararları daha hızlı almalarına yardımcı olan değerli bilgilere hızlı bir şekilde erişebiliyor[11].

Elektronik Harp uygulamalarının iki önemli kolu olan Elektronik Harp ve Elektronik Destek (SIGINT) ayrı amaçlar için ortaya çıkmış olsa da sıklıkla birbirlerini destekler şekilde benzer sonuçlar için faaliyet gösteriyor ve günümüzde birbirinden bağımsız düşünülemeyecek şekilde iç içe çalışıyor. İki uygulamanın toplama, işleme ve raporlama yöntemleri ve prosedürleri farklı bir şekilde ilerliyor ancak toplanan sinyal verileri benzerlik gösteriyor. SIGINT verileri Elektronik Harp uygulamalarını destekleyebiliyor. Bu şekilde elde edilen veriler savunma ve düşman kuvvetlerine karşı Elektronik Taarruz aşamasında saldırı imkânı sağlıyor[12].

İtalyan Elettronica firması SIGINT alt kollarından ELINT uygulamaları için geliştirdiği uydusu ile Elektronik Harp uydularının kullanımlarına bir örnek oluşturuyor. 2023'ün Nisan ayında yörüngeye gönderilen Scorpio uydusu bilgi işleme ve sınıflandırma için yapay zekâ algoritmalarından yararlanarak karasal Radyo Frekans sinyallerinin uzaydan alınmasına, tanımlanmasına ve yerelleştirilmesine olanak tanıyor. Elettronica, hâlihazırda araştırma ve geliştirme çalışmalarına devam ettikleri Elektronik Harp ve siber güvenlik uygulamalarını da uydu sistemlerine entegre ederek uzay hâkimiyetinde söz sahibi olmayı hedefliyor[13].

Rusya-Ukrayna Savaşı'nda da Elektronik Harp sistemlerinin varlığı belirgin bir şekilde ortaya çıkmıştı. 2022'nin Mart ayında Ukrayna askeri birlikleri tarafından ele geçirilen Rus Krasukha-4 bunun kanıtlarından biri olarak biliniyor. Krasukha-4, öncelikle E-8 Müşterek Gözetleme Hedef Saldırı Radarı Sistemi (Joint Surveillance Target Attack Radar System -JSTAR) ve Havadan Uyarı ve Kontrol Sistemi (Airborne Warning

10 http://bit.ly/3xB5xqG
11 https://www.magaero.com/what-is-sigint-and-how-its-maximizing-military-capabilities/
12 https://mipb.army.mil/documents/12618257/15543935/EW.pdf/18a57fdd-3e72-454c-90a0-41f0d5598cb8
13 https://www.shephardmedia.com/news/digital-battlespace/elettronica-joins-space-race-with-first-electronic-warfare-satellite-payload/

And Control System -AWACS) uçakları gibi ABD keşif platformlarında kullanılan X ve Ku bantlarındaki havadan veya uydu tabanlı atış kontrol radarlarını karıştırmak için tasarlanmış bir sistem olarak öne çıkıyor[14].

Türkiye'nin önde gelen savunma sanayii firmalarından olan STM Savunma Teknolojileri Mühendislik A.Ş. (STM) sivil ve askeri uygulamalar kapsamında kaçak ve şüpheli yayınların tespitine ve izlenmesine yönelik milli algoritmalar ile entegre konum kestirim sistemleri geliştiriyor[15].

Türkiye'de faaliyet gösteren bir diğer firma olan SDT Uzay ve Savunma Teknolojileri firması Elektronik Harp sistemlerinin Elektronik İstihbarat (ELINT), Sinyal İstihbaratı (SIGINT), Haberleşme İstihbaratı (COMINT) alt başlıklarının tamamında alt sistem ve sistem seviyesinde ürünler ortaya koyuyor. SDT tarafından geliştirilen EH ürünleri saha ve muharebe tecrübesini kazanmış, Türk Silahlı Kuvvetleri ve güvenlik birimleri tarafından başarıyla kullanılan sistemler. Bu alanda Elektronik Harp Kayıt Birimleri, Analog/Sayısal Almaçlar gibi donanımlar yanında, Offline Sinyal İşleme Yazılımları, Yayın Kaynağı Tespit Yazılımları, Gürültü Altı Yayın Tespit Yazılımı gibi yazılım birimleri geliştiriliyor[16].

Meteksan Savunma tarafından geliştirilen KEMENT Taktik Datalink (TDL) Sistemi ile Anti-Jam GNSS Sistemi ve ASELSAN tarafından geliştirilen İşlemsel EHF Uydu Aktarıcısı, Türk savunma sanayii tarafından geliştirilen Anti-Jam ürünlerinin bir kısmını temsil ediyor. KARA SOJ projesi kapsamında ASELSAN tarafından geliştirilen KORAL Mobil Elektronik Destek ve Taarruz Sistemi, her biri 8×8 askeri araç üzerine entegre edilmiş bir adet Radar Elektronik Destek (KORAL ED) Sistemi ve dört adet Radar Elektronik Taarruz (KORAL ET) Sisteminden oluşuyor. KORAL ED/ET Sistemi; hava, kara ve deniz platformlarında mevcut radar sistemlerine köreltme ve aldatma uygulamak için ASELSAN tarafından geliştirilmiş bir proje olarak öne çıkıyor.

ASELSAN tarafından geliştirilen MİLKAR-3A3 Mobil V/UHF Elektronik Taarruz Sistemi de farklı platformlarda V/UHF frekans bandında haberleşme yapan hedef muhabere sistemlerine Elektronik Taarruz uygulanması amacıyla geliştirilmiş bir sistem olarak dikkat çekiyor. Bu sistem hedef V/UHF bandı haberleşmesinin engellenmesi, geciktirilmesi veya yanlış bilgi iletimine sebep olunarak dost birliklere taktik sahada avantaj sağlanması amacıyla kullanılıyor.

TÜBİTAK-BİLGEM tarafından geliştirilen F-16 Tatik Elektronik Destek Podu (EDPOD) ise tehdit radarlarını tespit ve teşhis etmek, tehdit radarlarının konum bilgilerini kullanarak Elektronik Muharebe Düzenine (EMD) katkıda bulunmak üzere geliştirilmiş bir sistem olarak biliniyor. EDPOD Sistemi, alınan kayıtların Yer Destek Sistemindeki yazılımlarla analiz edilmesini sağlıyor. Analizler sonunda Elektronik Harp bilgi bankasının güncellenmesine katkıda bulunuyor[17].

Birleşmiş Milletler Dış Uzay İlişkileri Ofisi (United Nations Office for Outer Space Affairs -UNOOSA) verilerine göre 2018 yılı itibarıyla yörüngede 4.856 obje bulunuyordu. Ancak Union of Concerned Scientists (UCS) verilerine göre, yörüngedeki uyduların sayısı şaşırtıcı derecede azdı. Uzaydaki uyduların yüzde 37,5'i, yani 1.738 tanesi çalışmaya devam ediyordu[18].

2024'ün Mayıs ayında "Orbiting Now" adlı web sitesinden elde edilen verilere göre de Dünya yörüngesinde 9.900 aktif uydu bulunuyor. Uydular toplamda 105 ülke kontrolünde kullanılıyor. Günümüzde uzayda bulunan bütün uydulardan toplam 554 adeti askeri uydu olarak faaliyet gösteriyor[19].

14 https://thinktech.stm.com.tr/tr/savunma-sanayii-ve-teknoloji-perspektifinden-rusya-ukrayna-savasi-rusya-ukrayna-savasi-baglaminda-elektronik-harp-ve-otonom-sistemler
15 https://www.stm.com.tr/tr/cozumlerimiz/komuta-kontrol/radar-ve-elektronik-harp
16 https://www.sdt.com.tr/tr/cozumlerimiz/radar-elektronik-harp-ve-haberlesme
17 https://www.savunmasanayist.com/elektronik-harp-nedir/
18 https://thinktech.stm.com.tr/tr/uydu-savaslari
19 https://worldpopulationreview.com/country-rankings/military-satellite-by-country

Uyduların günlük hayatın vazgeçilmezi olduğu günümüzde Elektronik Harp uygulamalarının uydular üzerinden kullanım olasılığı savunma sanayii firmalarının yatırım yapabileceği bir alan olarak öne çıkıyor. Uzayda hâkimiyet sağlayan güçler Elektronik Harp uygulamalarıyla tüm savaş cephelerinde üstünlük sağlayarak ülkelerin savunmasında avantaj elde ediyor. Ayrıca “Uydudan Desteklenen Elektronik Harp” uygulamalarıyla savaş alanında sağlanan üstünlük karşıt güçlerin zayıflatılması ve hatta savaşın kazanılmasında kritik bir rol oynama potansiyeli taşıyor.

Elektronik Harp uygulamaları geliştikçe uzayda bulunan uyduların sayısının artması mümkün. Bu sistemlerin gelişen teknolojilerin de desteğiyle savaş alanlarında sağlayacağı üstünlük geleceğin savaşlarının sonucunda etkili bir rol oynayabilir. Elektronik Harp teknolojilerine yatırım yapan ve bunların uydu entegrasyonunu sağlayan ülkelerin, geleceğin uzay çağında söz sahibi olma ihtimali yüksek görünüyor.