SAVUNMA BİLİMLERİ DERGİSİ
The Journal of Defense Sciences

https://dergipark.org.tr/tr/pub/khosbd

Uzaktan Komutalı El Yapımı Patlayıcıların Doğaçlama Ev Yapımından Tüketici Elektroniği Bileşenleri ile Tasarımına Evrimi: Tehdit Şebekelerince Tüketici Elektroniği Pazarının Kullanımına Yönelik Bir Araştırma

Evolution Of Radio Controlled Improvised Explosive Devices From Improvised Homemade To Consumer Electronics Components: A Research On Potential Use Of Mass Market Consumer Electronics By Threat Networks

Serkan KOÇ[1,*]

[1] *NATO CIED Center Of Excellence*

Makale Bilgisi
Derleme
Başvuru: 23.05.2022
Düzeltme: 01.07.2022
Kabul: 06.11.2022

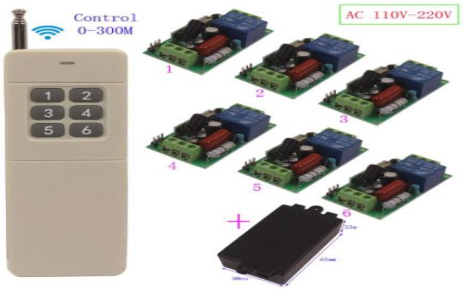
Keywords
Improvised explosive devices
Electronic counter measures,
Consumer electronics
Technological trends
Threat networks

Anahtar Kelimeler
El yapımı patlayıcı
Elektronik karşı tedbirleri
Elektronik karşı tedbirleri
Teknolojik trendler
Tehdit şebekeleri

Önemli Noktalar / Highlights

El Yapımı Patlayıcılar genellikle basit malzemelerden yapılabilir ve düşük maliyetle üretilebilirler. El yapımı patlayıcıların çoğu, patlatıcılar, zamanlayıcılar veya uzaktan kumanda sistemleri gibi elektronik cihazlarla tetiklenir. Bu cihazlar tüketici elektroniği malzemelerinin hazır alınarak kullanılmaktadır.

Grafiksel Özet / Graphical Abstract



Özet

El Yapımı Patlayıcı (EYP)'lar, yıkıcı, öldürücü, zarar verici etkileri olan, piroteknik veya yangın çıkarıcı kimyasallar içerebilen, doğaçlama bir şekilde yerleştirilen veya imal edilen ve yok etmek, etkisiz hale getirmek, taciz etmek veya dikkatini dağıtmak maksadıyla tasarlanan cihazlardır. EYP'ler askerî açıdan taktik silahlar olmakla birlikte stratejik etkiler yaratabilirler. Bu çalışmanın amacı, EYP yapımında terörist unsurlar ve tehdit şebekeleri tarafından sıklıkla kullanılan tüketici elektroniği ürünleri ve bu pazardaki mevcut eğilimlerin yanı sıra tehdit şebekeleri tarafından uzaktan komutalı EYP'lerde ticari kullanıma hazır (COTS) ürünlerin artan kullanımını incelemektir. Çalışmanın alana temel katkısı, elektronik bileşenlerin pazardaki yüksek bulunabilirliği ve düşük fiyatının etkileri göz önüne alındığında, terör örgütleri ve tehdit şebekeleri tarafından kullanılan taktik, teknik ve prosedürler kapsamında, uzaktan komutalı EYP'lerin tercih edilmesinin nedenleri, yeni teknolojilerin tehdide muhtemel etkileri ve tehdit şebekelerinin tüketici elektroniği malzemelerinin hazır alınarak kullanılmasına yönelik mevcut girişimlerinin ortaya konulmasıdır.

Abstract

Improvised Explosive Devices (IEDs) are devices that have destructive, lethal, damaging effects, that may contain pyrotechnic or incendiary chemicals, that are placed or manufactured in an impromptu manner and that are designed to destroy, neutralize, harass or distract. Although IEDs are tactical weapons from a military point of view, they can create strategic effects. The aim of this study is to reveal the current trends in the consumer electronics market, which is frequently used by terrorist organizations and threat networks in the construction of IEDs, as well as the increasing use of off-the-shelf (COTS) products in remote-controlled IEDs by threat networks. The main contribution of the study to the field is to reveal the reasons for the preference of remote-controlled IEDs within the scope of the tactics, techniques and procedures used by terrorist organizations and threat networks, the possible effects of new technologies on the threat, and the current attempts of threat networks to use readily available consumer electronics materials in the marketplace.

*Corresponding author, e-mail: serkankoc1982@gmail.com

DOI: 10.17134/khosbd.1120073

Elektronik/Online ISSN: 2148-1776
Basılı/Printed ISSN: 1303-6831

1. GİRİŞ (INTRODUCTION)

Elektronik endüstrisi 20. yüzyılda ortaya çıkmış ve sıradan insanların hayatına tüketici elektroniği olarak girmesinden bu yana her sene artan bir ivme ile büyüyerek trilyon dolarlık bir piyasa haline gelmiştir. Tüketici elektroniği pazarının baskın özelliği, elektronik ürünlerin sürekli artan bulunabilirliğidir. Moore Yasasına göre, yarı iletken bileşenlerin performansları her iki yılda bir iki katına çıkmaktadır. Bu eğilim, tüketici elektroniği pazarında ürün fiyatlarında bir düşüş eğilimine yol açmıştır. Genel olarak, bu durum elektronik endüstrisinde görülen üretim verimliliği artışı ve otomasyonda meydana gelen iyileşmelerin yanı sıra düşen işçilik maliyetleri ve genel tasarım iyileştirmelerindeki kazanımlar sonucu ortaya çıkmıştır. Omdia Tüketici Elektroniği Raporu'na göre tüketici elektroniği endüstrisi bugün 1,3 trilyon doların üzerinde bir değere sahiptir ve önümüzdeki yıllarda söz konusu endüstrinin piyasa değerinin daha da artması beklenmektedir. İkinci bir piyasa olarak göz önünde bulundurulabilecek küresel tüketici elektroniği onarım ve bakım pazarı ise, 2020'de tahmini 16,52 milyar ABD Doları artışla büyümeye devam etmektedir.

Uzaktan komutalı (Radyo Kontrollü) EYP'lerin yaygınlaşması, EYP'ler ile mücadele eden birimlere karşı, düşük maliyetli, oldukça esnek ve öngörülemeyen bir tehdit oluşturmuştur. Tüketici elektroniğinin pazarda yüksek mevcudiyeti ve hazır elektronik bileşenler, terör örgütleri ve tehdit şebekeleri tarafından uzaktan komutalı EYP yapımını kolaylaştırmaktadır. EYP'lerde ana imla hakkı adı verilen ve patlayıcının yapımında kullanılan bileşenler genellikle amonyum nitrat gübresi, ağartıcı (peroksit), oje çıkarıcı, fren hidroliği, herbisitler, dezenfektanlar ve temizleme çözücüleri gibi kolayca elde edilebilen ticari malzemelerdir. Bu ürünlerin ticareti, nakliyesi ve depolanması, tipik olarak, geleneksel mühimmatın nakliyesi ve depolanmasından daha az derecede inceleme ve düzenlemeye tabidir. EYP'ler üzerine yapılan araştırmalara göre, EYP yapımında kullanılan ticari mallar yasal üreticilerden terör örgütlerine doğrudan ulaşmamaktadır. Aksine, bölgesel dağıtım şirketlerinden birden fazla kullanım alanı olan malzemeler satın alan küçük yerel ticaret kuruluşları, gözetim zincirinin en zayıf halkası gibi görünmektedir. Söz konusu küçük kuruluşların istihbari açıdan gözetim altında tutulması da oldukça güçtür. Küçük işletmelerden kolaylıkla temin edilebilen elektronik malzemeler EYP yapımında kullanılan temel malzemelerdendir. Uzaktan komutalı EYP'lerde kullanılan en önemli elektronik bileşenlerden biri ise yarı iletkenlerdir. Tüketici elektroniği endüstrisinin arkasındaki merkezi itici güç, kendi başına 500 milyar dolara yakın yıllık satış rakamına sahip olan yarı iletken endüstrisi sektörüdür.

The International Criminal Police Organization (INTERPOL) 'a göre, organize bir biçimde milyarlarca dolarlık finansal kaynakları yöneten küresel suç örgütleri, sahte mal ticaretinden para kazanmaktan çekinmemektedirler. Uluslararası, bölgesel ve ulusal kanun uygulayıcı makamlar dünyanın birçok yerinde yürüttükleri soruşturmalarda, bu suç örgütleri

ile yasadışı uyuşturucu ticareti, kara para aklama ve yolsuzluk dahil olmak üzere diğer ciddi suçları işleyen örgütler arasındaki karmaşık bağlantıları ortaya çıkarmıştır. Bazı tahminlere göre, yasa dışı sahte ürün (fason elektronik malzemeler) işinin yılda 250 milyar doları fazlasıyla aştığını ortaya koymaktadır [1].

Bu sahte ürünlerin bir kısmı da, uzaktan komutalı EYP'lerin bileşenleri olarak kullanılabilmektedir. Yapılan araştırmalarda bu sahte elektronik ürünler arasında güç dağıtım bileşenleri, transformatörler, şalt cihazları, röleler, kontaklar, zamanlayıcılar, devre kesiciler, sigortalar, dağıtım panoları ve kablolama aksesuarları, piller gibi kullanımı kolay birçok bileşen bulunmaktadır.

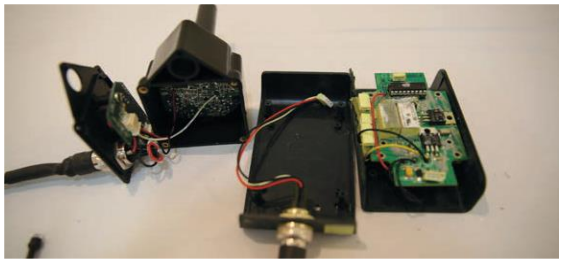
Bu çalışmanın amacı, EYP yapımında terörist unsurlar ve tehdit şebekeleri tarafından sıklıkla kullanılan tüketici elektroniği pazarındaki mevcut eğilimlerin yanı sıra tehdit şebekeleri tarafından uzaktan komutalı EYP'lerde ticari kullanıma hazır (COTS) ürünlerin artan kullanımını araştırmaktır. Çalışmanın alana temel katkısı, elektronik bileşenlerin pazardaki yüksek bulunabilirliği ve düşük fiyatının etkileri göz önüne alındığında, tehdit şebekelerinin tüketici elektroniği malzemelerini hazır bir biçimde alarak kullanmaya yönelik mevcut girişimlerinin ortaya konulmasıdır. Ayrıca terör örgütlerince hazırlanan EYP'lerin tespit ve imhasına yönelik yakın gelecekte daha sık kullanılabilecek karşı tedbir sistemleri hakkında bilgiler verilecektir.

2. UZAKTAN KOMUTALI EYP TEHDİDİ (REMOTE CONTROLLED IED THREAT)

Uzaktan komutalı EYP'ler dünyadaki en yaygın EYP başlatma sistemidir. Tetikçi, ateşleme zincirini başlatmak veya ana şalteri devreye almak için elektromanyetik bir darbe göndererek cihazı çalıştırır. Elektromanyetik radyasyon yoluyla sinyal gönderip alabilen herhangi bir elektronik cihaz, Uzaktan komutalı EYP'lerin tetik anahtarı olarak kullanılabilir. Türlerine ve niteliklerine göre bu anahtarların bireysel avantajları ve sınırlamaları vardır. Örneğin son raporlara göre; Bahreyn'de uzaktan komutalı EYP yapımında kullanılabilecek elektronik kitleri ve kurban tarafından aktif edilen pasif kızılötesi (Passive Infrared-PIR) tetikleme bileşenleri bir arada kullanılmaktadır. Bu senaryoda, radyo kontrollü birimler, EYP'ye sadece devreye monte edilen PIR sensörü hedef tarafından ihlal edildiğinde aktif olabilecek şekilde bir sinyal gönderir. Çeşitli EYP olaylarında görüldüğü gibi, bir uzaktan komutalı EYP'nin yapımı, amaçlanan hedefe ve dost kuvvet karşı tedbirlerine ve terörist taktik, teknik ve prosedürlerine göre değişir [2].

EYP'lerin kullanımındaki son trendlere göre, terör örgütleri amaçlanan hedefe ve mevcut malzemelere göre cihaz tasarım ilkelerini belirlemektedir. Hedef bertaraf edilmesi vazgeçilmez derecede önemli olduğunda ve EYP saldırısının özellikle konvoyda gerçekleştirilmesi gerektiğinde, EYP'ler pasif bir kızılötesi sensör kullanılarak mobil telsizler tarafından tetiklenebilir. Cihazın güvenliği ve tetikleyicinin yanlışlıkla kendi kendini imha etmesine karşı korunması maksadıyla ikincil ve üçüncül başlatma düzenekleri EYP'ye dahil

edilmektedir. EYP'lerin emniyetli biçimde etkisiz hale getirilmesi prosedürleriyle ilgili olarak, bu karmaşık tasarım, Patlayıcı Madde İmha (Explosive Ordnance Disposal/EOD) operatörünün görevini ciddi şekilde karmaşıklaştırmaktadır. Raporlara göre, son yirmi yılda tüm EOD operatör ölümlerinin yaklaşık yüzde 36'sı, komutla başlatılan cihazların etkisiz hale getirilmesi esnasında meydana gelmiştir.



Şekil 1: Bahreyn Hizbullah militan hücrelerinde 2017-2018 yıllarında ele geçirilen bir Pasif Kızılötesi Alıcı (PIR) devresi [2].

Uzaktan komutalı EYP'ler, kablosuz başlatma sinyalini değişken mesafelerden göndermek için yapılarında çok çeşitli ticari ve ev yapımı almaç-göndermeç setleri içerirler. Hâlihazırda piyasada kolaylıkla temin edilebilen, çeşitli çıkış güçlerinde ve farklı frekanslarda haberleşme sağlayabilen elektronik cihazlar bulunmaktadır. Son yirmi yılda, terör örgütleri tarafından; Çift Tonlu Çoklu Frekans (DTMF), Uzun Menzilli Telsiz Telefonlar (LRCT), Kişisel Mobil Telsizler (PMR), Araba Alarmları, Oyuncaklar için RC Kontrol Cihazı, telemetri cihazları, çeşitli kablosuz iletişim cihazları ve cep telefonları gibi Tablo 1'de sunulan birçok uzaktan komutalı EYP anahtar varyasyonu kullanılmıştır. Tüketici elektroniğinin çalışma frekansları, farklı yasal gereklilikler nedeniyle bölgeden bölgeye büyük farklılıklar gösterebilmektedir. Örneğin Asya'da aynı dış görünüş ve tasarıma sahip uzaktan komutalı oyuncağın çalışma frekans aralıkları Afrika, Avrupa veya Amerika'dan önemli ölçüde farklılık gösterebilmektedir. Tüketici elektroniği artık her geçen gün çok daha kolay erişilebilir olması ve internet üzerinden herhangi bir kısıtlama olmaksızın satın alınabilmesi nedeniyle, söz konusu tehdide karşı başarılı bir savunma için ele geçirilen EYP'lerin teknik kıymetlendirilmesi (Technical Exploitation) ve bunun sonucunda üretilen değerlendirme raporu büyük önem taşımaktadır.

Tarihsel olarak incelendiğinde, bir terör örgütü tarafından EYP yapımında kullanılan malzemelerin diğer terör örgütleri tarafından da kullanıldığı açıkça görülebilmektedir. Örneğin, Bahreyn'de faaliyet gösteren bir terör örgütünün militanlarından, Husi isyancılarından ya da Yemen'deki Arap Yarımadası'ndaki El Kaide (AQAP) militanlarından ele geçirilen uzaktan komutalı EYP bileşenlerinin, toplu miktarlarda sipariş edilerek internetten temin edilebilecek çok yaygın kullanılan elektronik bileşenlere sahip olduğu tespit edilmiştir. Yüksek güçlü bir elektronik cihazı açıp kapatmak ve kontrol etmek için kullanılan basit bir röle, büyük miktarlarda temin edilebilmekte ve çoğu uzaktan komutalı EYP tipinde kullanılabilmektedir. Bu eğilim mikro denetleyicilerde de görülmektedir.

Tablo 1: Irak ve Arap yarımadasında karşılaşılan EYP'lerde bulunan elektronik bileşenler 2016-2018.

Elektronik Devre Elemanı	Bahreyn'de Kullanılan U/K'lı Kit ve PIR Sistemi	Yemen'de Husiler Tarafından Kullanılan U/K'lı Kit ve PIR Sistemi	Yemen'de Husiler Tarafından Kullanılan Mini/mikro İHA'lar	Yemen'de Kullanılan EYP'ler	Irak'ta DAEŞ Tarafından Kullanılan EYP'ler
HKE Sinyal Rölesi	X	X	X	X	X
Mikroçip Mikroişlemciler	X				X
Mikroçip Atmel Mikroişlemcileri	X		X		
Mikrosemi MT8770DE DTMF Almaç	X			X	
Nais AGN2004H Güç Geciktirici	X	X			
Omron GS6K-2-H PCB Güç Rölesi	X	X	X		
Panasonic Sinyal Rölesi	X				
Princeton Technology Corp PT2262 Uzaktan Komutalı Kodlayıcı	X				
ST Microelectronics Voltaj Düzenleyici	X	X	X	X	X
Woe Heat-Shrink Wrap	X	X	X		
Gri Kablo	X	X	X		

Birleşmiş Milletler'in (BM) en son raporlarına göre, silahlı grupların giderek daha karmaşık cihazları çeşitlendirme, tasarlama ve dağıtma konusundaki teknik kapasitesi artmaktadır. Tablo 2'de karşılaşılan EYP türlerine yönelik, tasarım ilkeleri ve farklı bölgelerde kullanılan malzemeler hakkında bilgiler sunulmuştur.

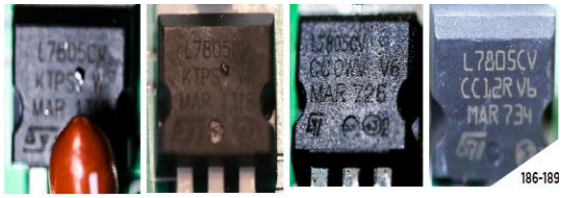
Tablo 2: EYP türlerine yönelik, tasarım ilkeleri ve farklı bölgelerde kullanılan malzemeler [3].

Ülke İsmi	Son Dönemde Karşılaşılan EYP'lerde Teröristlerce Kullanılan Tasarım Prensipleri	Terör Örgütlerince Kullanılan EYP Türleri	EYP Yapımında Kullanılan Materyal	Terör Örgütüne Yönelik Özel Bilgiler
Kongo Demokratik Cumhuriyeti	Askerî ve çift kullanım alanı bulunan ticari elektronik bileşenlerle yapılan basit tasarımlar	Kablo komutalı EYP	Ele geçirilen askerî ya da ticari patlayıcı ve fünyeler	Silahlı grupların giderek daha karmaşık cihazları geliştirmek, tasarlamak ve yerleştirmek için teknik kapasitelerinde bir artış gözlemlendi.
Nijerya	Askerî ve çift kullanım alanı bulunan ticari elektronik bileşenlerle yapılan basit tasarımlar	Kurban tarafından tetiklenen EYP İnsan üzerine yerleştirilmiş intihar saldırısı niteliğinde EYP		
Somalia	Çift kullanım alanı bulunan ticari elektronik bileşenler ve kimyasallar	Araçlı EYP saldırısı	Savaş sonucu ele geçirilen askerî patlayıcılar	El-Şebab Terör Örgütü (Al-Shabaab), ev yapımı patlayıcılar kullanarak, EYP yapım yöntemlerinin çeşitlendiğini göstermektedir.
Kolombiya	Hedefi seçmek maksadıyla tasarlanmış kompleks EYP saldırısı	Kablo komutalı EYP		Kullanılan EYP'lerde görülen çeşitlilik, silahlı gruplar arasında teknik kapasitede bir artışa işaret etmektedir.
Yemen	EYP ana imla hakkı olarak anti personel mayınların kullanımı	Basma düzenekli EYP'ler	EYP'lerin çok sayıda fabrikasyon seviyede üretimi	Kurban tarafından tetiklenen EYP'lerin kullanımında görülen yeni taktikler mevcuttur. Örnek; EYP'lere müdahale eden personelin fark edememesi maksadıyla EYP'lerin kayaların içine gizlenmesi

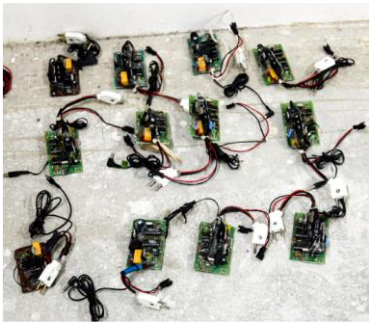
Son yıllarda, Bahreyn'de ele geçirilen uzaktan komutalı EYP'ler ve Yemen'deki Husilerden ele geçirilen uzaktan komutalı EYP'ler ile dronlar incelendiğinde, mikrodenetleyiciler, güç röleleri ve voltaj regülatörleri gibi birçok elektronik bileşen söz konusu örgütlerce aynı marka ve modelde temin edilerek kullanılmıştır.

Şekil 2: PIC16F628A mikrodenetleyici.

Şekil 3: Omron, NAIS ve HKE markalı güç röleleri.



Şekil 4: STM markalı voltaj düzenleyiciler.



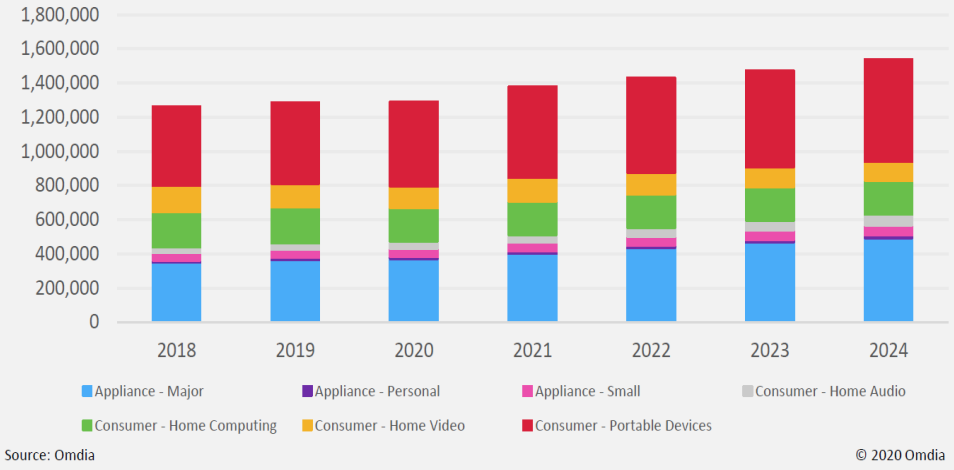
Şekil 5: DTMF alıcı devreleri.

2.1. Tüketici Elektroniği Pazarında Eğilimler

Tüketici elektroniği pazarındaki eğilimlerin EYP'ler üzerindeki etkilerini analiz etmeden önce, tüketici elektroniğinin neleri içerdiğinin net bir tanımını yapmakta fayda bulunmaktadır. "El Yapımı Patlayıcı Teknik Kıymetlendirme Sözlüğü"ne göre,

- Pazarda yaygın olarak bulunabilen tüketici elektroniği malzemeleri:
  - Uzaktan Komutalı Oyuncaklar
  - Beyaz Eşya/Küçük Ev Aleti Kumandası
  - Garaj Kapısı Kumandası
  - Kapı Zili
- Elde Kullanılabilen Telsizler
  - Kişisel Mobil Telsizler (PMR)
  - Radyo Almaç Göndermeçler
- Elde Kullanılamayan Telsizler
  - Taksi Radyosu
  - Herhangi Araç Gövdesine Monte Radyolar
- Kablosuz Telefonlar
  - Uzun Mesafe Kablosuz Telefon (LRCT)
  - Yüksek Güçlü Kablosuz Telefon (HPCP)
- Cep Telefonu
  - Mobil Haberleşme Amaçlı Küresel Sistem (GSM)
  - Kod Bölmeli Çoklu Giriş (CDMA) Telefonu
- Diğer radyo haberleşme cihazları
  - Kablosuz Almaç (WICR)
  - Çift Tonlu Çok Frekanslı (DTMF) MOD 1-5 Cihazlar
  - Frekans Atlamalı Kablosuz Sensör Haberleşmesi (Multi-hop RF)
  - Havai Fişek Uzaktan Komutası
- Telemetri Sistemleri
  - Linx (DECT Telefonlar)
  - Maxstream (Radyo Modemler)
- Diğerleri.

Tüketici elektroniğine en geniş açıdan bakıldığında, günümüzde yapılan son araştırmalara göre, tüketici elektroniği endüstrisi 1,3 trilyon doların üzerinde bir değere sahiptir ve söz konusu endüstrinin önümüzdeki yıllarda istikrarlı bir şekilde büyümesi beklenmektedir. Gelişen ve yıkıcı teknolojiler ve mevcut teknolojilerde görülen yenilikler, pazarı yönlendirmeye devam etmektedir. Ayrıca, pazara sürülen her yeni ürünün sahip olduğu yetenekler müşteri beklentilerini beslemekte ve sonuç olarak insanların gerekirse başka harcama kalemlerinden kısıntı yapmak pahasına bu yeni teknolojilere yönelik harcama iştahlarını büyütmeleri yol açmaktadır.

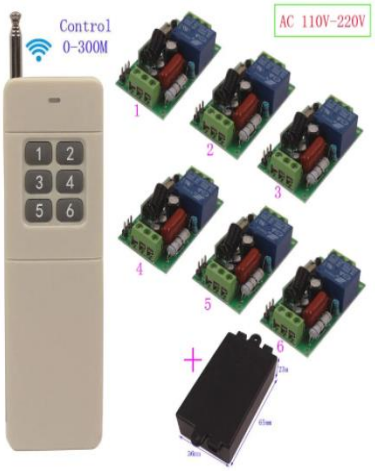


Şekil 6:Tüketici elektroniği gelirleri (ABD Doları) [4].

Terör örgütleri ve EYP tehdit şebekeleri, hazırladıkları EYP'lerde seri üretim ticari kullanıma hazır bileşenleri (COTS) her geçen gün daha fazla olacak şekilde kullanmaya devam etmektedirler. Özellikle radyo kontrol almaç-göndermeç kitlerinin kolay erişilebilirliği, terör örgütlerinin kullanımı açısından güvenilir ve emniyetli bir EYP yapımını kolaylaştırmaktadır. Pazarda mevcut ve tedariki kolay mikro denetleyicilerin internet vasıtasıyla verilen kendin yap tipi eğitimlerle (do it yourself) kolaylıkla programlanabilirliği ve söz konusu hazırlanan EYP'lerin çalıştırılabileceği çok geniş bir frekans aralığının mevcudiyeti, uzaktan komutalı EYP'yi dost güçlere karşı kullanılabilecek etkili bir silah haline getirmektedir. Haberleşme elektroniği pazarının genişlemesi ve bunlara kolay erişim sayesinde, uzaktan komutalı EYP'lerin hazırlığı aşamasında kullanılan kitler çok az değişiklik gerektirmekte veya hiçbir tasarıma gerek kalmaksızın hazır olarak ana imla hakkına bağlanarak EYP olarak kullanılabilmektedir. Mobil telsizler veya RF verici modülleri günümüzde artık her zamankinden daha yeteneklidir ve herhangi bir uzaktan komutalı EYP içinde ateşleme anahtarı olarak kolayca kullanılabilmektedir. Genel olarak, piyasada bulunan tüketici elektroniği malzemeleri, yüksek kalitede, güvenilir ve seri üretilmeleri nedeniyle düşük maliyetlidir. Ayrıca terör örgütünce başvurulacak saldırı taktiğine göre programlanabilmekte ve günümüzün karmaşık ve yoğun elektromanyetik spektrumunda çalışmak üzere tasarlanmaktadırlar. Geçmişte terör örgütleri, saldırı esnasında kullanacakları frekansı belirlerken, piyasada mevcut olan RF cihaz veya almaç göndermeç modülü için önceden belirlenmiş frekanslar arasından seçim yapmaktaydılar. Ancak günümüzde çok daha geniş seçeneğe sahip olmanın özgürlüğünü kullanarak taktik ve tekniklerini belirleyebilmektedirler.

Şekil 7: Geçmişin basit PMR telsizleri 446 MHz.

Şekil 8: Çin üretimi Baofeng (20 Euro)136-174, 400-480, 430-450 MHz.



Şekil 9: Hazır kablosuz uzaktan komutalı algılayıcı anahtarlar (25 Euro).

Şekil 10: Pasif kızılötesi (0.44 Euro).

Bu cihazların kolay erişilebilirliği ve terör örgütlerince çokça kullanılabilirliği, tüketici elektroniği pazarındaki son dönemde görülen eğilimlerden kaynaklanmaktadır. Dünyada orta sınıf ekonomik statüdeki nüfus, son birkaç yıldır hızla artmaktadır. Ayrıca, kentlerde yaşayan tüketicilerin yaşam tarzında bir değişim görülmektedir. Artan internet penetrasyonu ve artan gelir, tüketicilerin birden fazla elektronik cihaz kullanmasına imkân tanımaktadır. Bu süreç, önümüzdeki birkaç yıl içinde de tüketici elektroniği pazarının büyümesini hızlandırmaya devam edecektir [5].

Geleneksel olarak, terör örgütleri tarafından planlanan EYP saldırısına yönelik en önemli tasarım ilkelerinden biri, EYP'yi güvenli bir mesafeden tetikleyebilmektir. Bu ihtiyacı karşılamaya yönelik en önemli cihazlar RF kontrollü elektronik devrelerdir. Ancak RF haberleşmede kullanılan radyo dalgaları atmosferik koşullardan önemli ölçüde etkilenir; özellikle radyo dalgaları atmosferik etkiler nedeniyle değişen miktarlarda yansıyabilir, kırılabilir, emilebilir veya saçılabilir. Bu sınırlamalar nedeniyle, teröristler sinyali alıcıya göndermek için yeterince açık ve verimli iletişim kanallarını seçme eğilimindedirler. Söz konusu tehdide yönelik elektronik karşı tedbir geliştirmekten sorumlu mühendisler ve EYP uzmanları son döneme kadar esas olarak uzaktan komutalı EYP'lerin frekans çalışma aralığına odaklanmışlardır. Geçmişte mevcut RF cihazlarının sağlıklı iletişim kanallarının dar bantlara sahip olması, terör örgütlerince uzaktan komutalı EYP yapımında daha az sayıda frekans seçilmesine bunun sonucunda da karşı tedbir olarak kullanılan karıştırma sistemlerinin (jammer) de nispeten dar frekans bantlarında çalışacak şekilde tasarlanmasına yol açmıştır. Bugün piyasada farklı elektronik bileşenlerin bolluğu göz önüne alındığında, terör şebekelerinin uzaktan komutalı EYP'yi

tetiklemek için tercih edebileceği çok geniş bir frekans aralığı bulunmaktadır.

Bugünün tüketici elektroniği pazarı radyo frekans haberleşme alanında çok verimli ve etkili cihazları geçmişten çok ucuz fiyatlarla sunmaktadır. MHz'den GHz'e kadar elektromanyetik spektrumun değişik frekans bantlarında ticari olarak temin edilebilen RF cihazların kullanılabildiği EYP'lere karşı geliştirilen karşı tedbirler de çalışma frekans bantları açısından artık Khz ve Ghz bant aralığındaki tüm RF spektrumunu kapsamaktadır. Öte yandan, akıllı bir elektronik karşı tedbir uzmanı, dost güçlerin elektronik karşı önlemlerine karşı haberleşme frekanslarının karıştırılmasını önlemek maksadıyla (frequency de-confliction) daha karmaşık ve gelişmiş tasarımlara gitmek zorundadırlar. Söz konusu tasarım kriterleri ve gerekli olan yazılım ve donanımlar, elektronik karşı tedbir sistemlerinin üretim maliyetlerini artırmaktadır.

Diğer yandan günümüzde yeni teknolojiler, terör örgütleri ve EYP tehdit şebekelerinin, kendi uzaktan komutalı EYP tasarımlarını tek seferde çok sayıda seri bir biçimde üretmesine imkân tanımaktadır. Eklemeli imalat veya 3D baskı ile, bilgisayarlı bir tasarım süreci sonunda malzemeler katmanlanarak üç boyutlu ürünler (EYP dış kapları için yeni tasarımlar vb.) oluşturulabilmektedir. Kısa işlem süresi, düşük maliyet ve daha yüksek kalitede nihai ürüne imkân tanıyan bu teknolojiler artık terör örgütlerinin de sıkça kullandığı imkânlar halini almıştır. Söz konusu teknolojiler sadece EYP dış kabı vb. materyal tasarımında faydalar sağlamamıştır. Uzaktan komutalı EYP'ler kullanılabilecek yeni, hızlı ve yüksek bant genişliğine imkân tanıyan bir teknoloji olan 5G'nin ortaya çıkmasıyla birlikte, terör örgütleri daha yüksek doğrulukta ve kesintisiz iletişim yapmakla kalmayacak, nesnelerin interneti (internet of things) ile yeni imkânlar kazanacaktır. Bu şekilde bir elektronik cihaz ekosistemi aynı ağa bağlanarak (burada 5G), uzaktan erişilebilir sensör teknolojileri ile aynı ağa bağlı cihazlar kullanılarak uzaktan sürü EYP saldırıları gerçekleştirilebilmektedir.

Ayrıca 5G teknolojisi, yıkıcı yapısıyla sadece bu teknolojiyi daha etkili EYP saldırıları için kullanmayı hedefleyen düşmanları değil, bu teknolojiye karşı önlem geliştirmeye çalışan dost güçleri de etkileyecek gibi görünmektedir. Dost kuvvetler açısından bakıldığında, 5G teknolojisi, istihbarat, gözetleme ve keşif (ISR) sistemleri, komuta-kontrol uygulamaları, insanlı ve otonom araçlar alanında yeni yeteneklere sahip yeni ekipmanların ortaya çıkmasına yol açacaktır. Bununla birlikte, 5G teknolojisinin kullanılabildiği frekans bandı yalnızca kısa bir mesafe kat edebileceğinden, 5G bağlantı aralığının büyük olmaması gibi bazı kısıtlamalarla birlikte gelir. 5G kapsama alanı sağlanabilmesi maksadıyla yeni 5G baz istasyonlarında kullanılacak antenler kurulmalıdır. Bu hem pahalı hem de zaman alıcı bir iştir. Son olarak, söz konusu teknolojiye kırsal kesimden erişim problemli olacağından bu durum terör örgütleri ve tehdit şebekeleri için bir sınırlama anlamına gelmektedir.

3. TERÖR ÖRGÜTLERİ VE EYP TEHDİT ŞEBEKELERİ TARAFINDAN TÜKETİCİ ELEKTRONİĞİ MALZEMELERİNİN EYP OLARAK KULLANIMINDAKİ EĞİLİMLER (TRENDS IN THE USE OF CONSUMER ELECTRONICS MATERIALS AS IEDS BY TERRORIST ORGANIZATIONS AND IED THREAT NETWORKS)

3.1. Afrika

3.1.1. Mali/Burkina-Faso/Niger

Önemli Tehdit Şebekeleri: Cemaat Nusrat al İslam vel Müslimin (JNIM) / Büyük Sahra'da Daesh (ISGS) / İslami Mağrip'te El Kaide (AQIM)

Modifiye edilmiş (tristörlü veya transistörlü) kişisel mobil telsiz (PMR) ve cep telefonları kullanımından, uzaktan komutalı EYP'lerin anahtar devrelerinde, tüketici elektroniğinin yoğun kullanımına doğru açık bir evrim gözlemlenmektedir.

- Garaj Kapısı Kumandaları / Uzun Mesafeli (LoRa) spektrum modülasyon cihazları:
  - CX9-2C
  - TAD-T80
  - KL-BT serisi
  - KL-K120 serisi
  - KL-K400 serisi
  - KL-3000 serisi
  - KL-5000 serisi
- Araç Alarmları:
  - KFZ serisi

3.1.2. Nijerya/Çad/Kamerun

Önemli Tehdit Şebekeleri: Batı Afrika'da IŞİD (ISWAP) / Boko Haram

Mali/Burkina-Faso/Nijer'de kullanılan bazı modellerin yanı sıra diğer bazı farklı modeller de dahil olmak üzere garaj kapısı kumandaları ve ev eşyası kumandalarının kullanımının yoğun olduğu bildirilmektedir.

3.1.3. Cezayir/Tunus/Libya/Mısır

Önemli Tehdit Şebekeleri: İslami Mağrip El Kaidesi (AQIM) / Ensar al-Sharia / Anasr al-Islam / Cund al-Islam/Daeş'in yan kolları

Libya'da uzaktan komutalı EYP'lerin anahtar devrelerinde tüketici elektroniğinin (araç alarmları) bazı kullanımları tespit edilmiş olsa da, söz konusu gruplar tarafından çoğunlukla uzaktan komutalı EYP'lerin anahtar devrelerinde ev yapımı veya modifiye elektronik cihazlar kullanılmaktadır:

- Doğrudan cep telefonuna veya kişisel mobil telsize (PMR) bağlı Çift Tonlu Çoklu Frekans (DTMF)
- Tristör veya transistör ilavesi ile modifiye edilmiş cep telefonları
- Çift çıkışlı özel uzaktan komutalı elektronik anahtarlar

3.1.4. Somali/Mozambik/Demokratik Kongo Cumhuriyeti

Önemli Tehdit Şebekeleri: El Şebab/Orta Afrika'da DAEŞ (IS-CAP)/Şebab

Modifiye edilmiş cep telefonlarının uzaktan komutalı EYP'lerin anahtar devrelerinde göreceli bir kullanımı vardır, ancak doğrudan piyasadan temin edilen tüketici elektroniği malzemelerinin kullanımı giderek artmaktadır:

- Ev aleti uzaktan kumandası:
  - GV-DCKZ
  - TY-RS-L011
  - KL-K103X
  - KL-CW11

- Motorsiklet Alarmları:
  - CL-A006
  - BM-338

3.2. Asya

3.2.1. Kuzey Kafkasya

Önemli Tehdit Şebekeleri: Kafkaslar ve Ceyş el-Mücahirin vel-Ensar'da Faaliyet Gösteren DAEŞ

Bu gruplar tarafından, ele geçirilen askeri cihazlarla birlikte çoğunlukla ev yapımı uzaktan komutalı EYP'lerin anahtar devreleri, modifiye cep telefonları veya modifiye Kişisel Mobil Telsiz (PMR) anahtarları kullanılmaktadır.

3.2.2. Afganistan

Önemli Tehdit Şebekeleri: Afganistan İslam Emirliği / Horasan Vilayeti'nde DAEŞ Afganistan ve Pakistan'daki eğilimler, piyasadan doğrudan temin edilip hazır olarak kullanılabilen tüketici elektroniği malzemelerinin yerine, elektronik olarak modifiye edilmiş Kişisel Mobil Telsiz (PMR) cihazlarının, modifiye edilmiş cep telefonlarının, Çift tonlu Çok Frekanslı (DTMF) alıcılara dayalı ev yapımı uzaktan komutalı EYP anahtar devrelerinin kullanımını ortaya koymaktadır.

3.2.3. Güneydoğu Asya

Önemli Tehdit Şebekeleri: Arakan Ordusu/Dawlah Islamiya/Ebu Seyyaf Grubu/Yeni Halk Ordusu/Bangsamoro İslami Özgürlük Savaşçıları

Elektronik olarak modifiye edilmiş Kişisel Mobil Telsiz (PMR) kullanımının zaman zaman bildirilmiş olmasına rağmen, bölgede uzaktan komutalı EYP'lerin anahtar devreleri olarak modifiye edilmiş cep telefonlarının baskın bir kullanımı gözlemlenmektedir.

3.2.4. Güney Asya

Önemli Tehdit Şebekeleri: Naksalit/Ceyş-i Muhammed/Assam/Maoist grupların Birleşik Kurtuluş Cephesi

Uzaktan komutalı EYP'lerin anahtar devrelerinde piyasadan doğrudan temin edilip hazır olarak kullanılabilen tüketici elektroniği malzemelerinin kullanımı tespit edilmemiştir.

3.2.5. Pakistan

Önemli Tehdit Şebekeleri: Tehreek-e-Taliban Pakistan/Jammu ve Keşmir Ulusal Kurtuluş Ordusu/Belucistan Kurtuluş Cephesi/Lashkar-e-Taiba/Lashkar-e-Jhangvi

Bölgede az sayıda karşılaşılan motosiklet alarmı devreleri dışında uzaktan komutalı EYP'lerin anahtar devrelerinde piyasadan doğrudan temin edilip hazır olarak kullanılabilen tüketici elektroniği malzemelerinin yaygın kullanımı tespit edilmemiştir.

3.2.6. Suriye

Önemli Tehdit Şebekeleri: Şam'da DAEŞ/Hay'at Tahrir al-Sham/Şii milisleri

Suriye'de son aylarda, bulunan/ele geçirilen uzaktan komutalı EYP'lerin anahtar devreleri çoğunlukla modifiye edilmiş cep telefonlarına ve Çift Tonlu Çoklu frekans (DTMF) veya Uzun Menzilli Telsiz Telefona (LRCT) dayalı ev yapımı uzaktan komutalı cihazlara dayanmaktadır.

3.2.7. Irak

Önemli Tehdit Şebekeleri: Irak'ta DEAŞ ve Levant/Şii milisleri

Irak'ta DEAŞ tarafından kullanılan (daha çok ev yapımı veya modifiye edilmiş elektronik cihazlara dayanan) uzaktan komutalı EYP'lerin anahtar devreleri ile İran tarafından sağlanan elektronik bileşenler/cihazların bir karışımından ve bazı tüketici elektroniğinden oluşan Şii milisler tarafından kullanılanlar arasında büyük bir fark bulunmaktadır. Farklı terör örgütleri ve gruplar tarafından, araç alarmları, ev eşyası uzaktan kumandası ve Wi-Fi tabanlı cihazlar kullanılabilmektedir.

3.2.8. Arap Yarımadası

Önemli Tehdit Şebekeleri: Arap Yarımadası'ndaki El Kaide (AQAP)/Ensar Allah/DAEŞ

Bölgedeki en aktif tehdit şebekesi, doğrudan İran tarafından desteklenen Ensar Allah'tır (Husi isyancıları olarak da bilinir). İran'ın hedefleri mali destek, askerî eğitim ve Tahran'daki liderlik için "güvenli bir sığınak" sağlamak olarak görünmektedir [6].

Alınan bu destek sayesinde uzaktan komutalı EYP'lerin anahtar devreleri olarak İran tarafından sağlanan ev yapımı cihazlara rastlanmaktadır. Çok fazla olmamakla birlikte Husiler tarafından uzaktan komutalı EYP'lerin anahtar devrelerinde piyasadan doğrudan temin edilip hazır olarak kullanılabilen tüketici elektroniği malzemelerinin kullanımı da tespit edilmiştir.

3.2.9. Lübnan/Filistin/İsrail

Önemli Tehdit Şebekeleri: Hizbullah/El Kassam Tugayları/İslami Filistin Cihadı

Uzaktan komutalı EYP'lerin anahtar devreleri olarak, ev yapımı veya değiştirilmiş elektronik cihazların (örneğin uzaktan parmakla çalıştırılan düğme tetikleyicileri, RFT, modifiye cep telefonları, RF modüllerine dayalı ev yapımı elektronik cihazlar) kullanımı yaygındır ancak doğrudan piyasadan temin edilebilen araç alarmlarının sınırlı kullanımı da bildirilmektedir.

3.3. Amerika

3.3.1. Kolombiya

Önemli Tehdit Şebekeleri: Ulusal Kurtuluş Ordusu (ELN)/ Kolombiya Devrimci Silahlı Kuvvetleri (FARC)

Uzaktan komutalı EYP'lerin anahtar devreleri olarak söz konusu gruplar tarafından, ev yapımı modifiye edilmiş elektronik cihazlar kullanılmaktadır.

3.3.2. Meksika

Önemli Tehdit Şebekeleri: Jalisco Yeni Nesil Kartel/Birleşik Karteller/Sinaloa Karteli

Uzaktan komutalı EYP'lerin anahtar devreleri olarak Meksika'da faaliyet gösteren gruplar tarafından ev yapımı elektronik anahtar devreleri ile modifiye edilmiş elektronik cihazların kullanımının baskın olduğu bildirilmektedir.

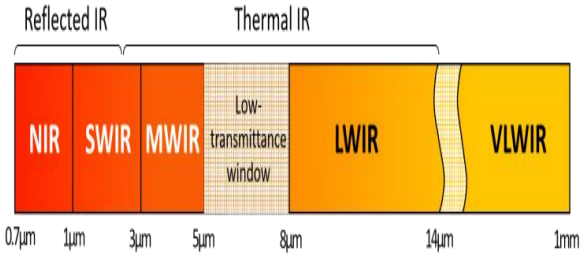
4. GELECEK ÖNGÖRÜLERİ (FUTURE PREDICTIONS)

Uzaktan komutalı EYP'ler, terör örgütleri açısından oldukça esnek kullanım alanlarına

sahip, etkili ve düşük maliyetli bir tehdittir. Tehdit ağları, piyasada kullanıma hazır ve elektromanyetik spektrumun çok çeşitli bölgelerinde farklı frekanslarda çalışan elektronik cihazları EYP yapımında kullanabilmektedir. Söz konusu tehdide yönelik elektronik karşı tedbirlerin geliştirilmesi açısından, tehdidi doğru bir şekilde tanımlamak tüketici elektroniği pazarının genişlemesi ve erişiminin kolaylaşması nedeniyle, karşı tedbir geliştiricilere büyük zorluklar çıkarmaktadır.

Teknolojik karşı tedbirler açısından, EYP'nin tespit edilmesi, etkisiz hale getirilmesi ve EYP'nin tetiklenmesinin önlenmesi alanlarında çeşitli teknolojiler mevcuttur. Bu teknolojilerin farklı teknolojik hazırlık seviyeleri bulunmakta ve bazıları için harekât alanda kullanım için yeterli olgunluğa ulaşmasının 10-20 yıl sürebileceği değerlendirilmektedir.

Uzaktan tespit teknolojilerinden birisi olan Hiperspektral Görüntüleme (HS), hiperspektral sensör ve kamera teknolojilerinin gelişimi ile giderek daha fazla dikkat çekmektedir. Sensör teknolojisi ve sistemlerindeki önemli gelişmeler, dost kuvvetlere, hedeflerin tespitini ve sınıflandırılmasını sağlamak maksadıyla gelişmiş imkânlar sağlamaktadır. Özellikle havadan tespitte kullanılan HS kameralar son on yılda hem gittikçe daha etkili hem de maliyet açısından etkin hale gelmiştir. Optik tabanlı herhangi bir uzaklık algılama tekniği için, üç ana operasyonel bileşen gereklidir: söz konusu hedefi aydınlatmak için aşağı doğru yönlendirilebilen önemli ölçüde parlak bir kaynak, hedeften optik sinyali toplama yeteneğine sahip optikler ve ilgilenilen bir hedefin varlığı veya yokluğunu tanımlayan araçlar [7]. HS görüntüleme, bitki hastalıklarının, böcek zararlılarının ve istilacı bitki türlerinin izlenmesi, ürün verimi tahmini ve tarımsal ürünlerin sınıflandırılması gibi çeşitli uygulamalarda kullanılmıştır. Hiperspektral uzaktan algılamada 4 tip hiperspektral veri kullanılır: Görünür (VIS) bölge, kısa dalga kızılötesi (SWIR), orta dalga kızılötesi (MWIR) ve uzun dalga kızılötesi (LWIR). Hem yansıma hem de emisyonun spektral imzalarının kullanılması, uzaktan algılama uygulamalarında önemli olabilmektedir [8].



Şekil 11: Hiperspektral uzaktan algılamada kullanılan dalga boyları.

Bu teknolojilerden bir diğeri olan Doğrusal Olmayan Bağlantı Algılama Teknolojisi (Non-Linear Junction Detection), açık veya kapalı olmalarına bakılmaksızın cihazlarda bulunan elektronik bileşenlerin varlığını tespit etme ve doğrulama yeteneğine sahiptir. Yeterli olgunluğa ulaşabilmesi durumunda söz konusu teknolojinin kullanıldığı sistemlerle, uzaktan komutalı EYP'lerle mücadelede, güzergâhın EYP'den temizlenmesi operasyonları sırasında EYP'lerdeki yarı iletkenlerin tespit edilmesi amaçlanmaktadır. Çünkü tüketici elektroniği pazarındaki eğilimin ana itici gücü olan yarı iletkenler, doğrusal olmayan özelliklere sahiptir. Tespit sistemleri ile alınan sinyalin 2.

ve 3. harmoniklerini kullanarak bu bileşenleri ayırt etmek mümkündür. Harmonik radar ismi verilen bu tespit sistemi f_0 frekansında (desimetre dalga boylarında) elektromanyetik dalgalar yayar ve doğrusal olmayan elektronik bileşenler veya IED'deki farklı metallerin oksitlenmiş bağlantıları tarafından üretilen harmonik frekanslarda (2 f_0, 3 f_0) dalgaları alır [9]. Bu teknolojide bu harmonik frekansları almak için çok hassas alıcılar kullanılır ve yarı iletkenin EYP'deki yerini belirlemek için yönlendirilmiş bir anten kullanılır.

Diğer bir gelecek teknolojisi olan THz frekanslarındaki elektromanyetik radyasyon, diğer birçok frekansa kıyasla güçlü nüfuz etme yeteneklerine sahiptir. Terahertz tekniklerinde kullanılan çok kısa darbeler (femtosaniye), nesnelerin 3 boyutlu görüntülenmesini sağlar. Bu, toprak ve diğer kaplama malzemelerinin altında görüntülemeye yardımcı olur. İletken olmayan birçok malzemenin içini görmemizi sağlar ve farklı kaplara ve diğer EYP malzemelerine nüfuz etme avantajlarına sahiptir. THz spektral bölgesindeki birçok elektronik bileşenin benzersiz spektral izleri bulunmaktadır. Orijinal ve sahte malzeme bile THz frekanslarında görüntülenmesiyle ayırt edilebilmektedir. THz radyasyonu iyonize edici radyasyon değildir ve bu özellik, bu teknolojinin mikrowatt aralıklarında çok düşük güç seviyelerinde çalışmasını mümkün kılar. Öte yandan, X-ışını sinyallerinin aksine zararlı değildirler. Havalimanı giriş kontrollerinde gizli malzemeleri bulmak için uzun yıllardır başarıyla kullanılmaktadır. Ancak yarı iletkenler gibi elektronik bileşenlerin tespiti için kullanılabilmesi için halen teknoloji hazırlık düzeyi düşüktür. Bir cisim üzerinde THz radyasyonunun tespiti, bolometre veya piroelektrik dedektörlerle yapılabilmektedir. Tutarlı bir algılama için THz radyasyonuna benzer fotoiletken anten veya elektro-optik kristal femtosaniye lazer darbeleri birlikte kullanılır [10]. Bu teknolojiden gelecekte yüksek potansiyel beklenmekte, güzergâhın EYP'lerden temizlenmesi operasyonlarında sıklıkla kullanılacağı öngörülmektedir.

Uzaktan komutalı EYP'lerden gelen tehdit karşısında sıklıkla modern ordularca kullanılan karıştırma teknolojisi son yirmi yıldır gelişim göstermektedir. Temel olarak geleneksel karıştırma sistemleri, herhangi bir EYP'nin radyo sinyali gönderme ve alma yeteneğini bozan bir elektromanyetik balon oluşturur. Son yıllarda reaktif karıştırma, aktif karıştırmaya göre daha az güç gerektirdiğinden, giderek daha popüler hale gelmiştir. Reaktif karıştırma yönteminde, EYP'de bulunan uzaktan komutalı cihazın aktivasyon sinyalinin gönderilmiş olması gerekmektedir. Söz konusu aktivasyon sinyalinin ve bu sinyalin frekansının tespitinden sonra karıştırma sinyali üretilmekte ve sadece bu kanal için gönderilmektedir [11]. Yazılım tanımlı karıştırma sistemleri, tüm tehdit bandını kapsayan "DDS tabanlı FPGA kontrollü Süpürme Karıştırma" adı verilen teknikten yararlanmaktadır. Bu tür sistemler programlanabilmekte ve farklı tehditlere göre özel operasyonel ve taktik gereksinimler için özelleştirilebilirler. Tüketici elektroniği pazarındaki son eğilimlerin bir sonucu olarak ve farklı frekanslarda çalışabilen geniş ürün yelpazesi ile reaktif karıştırma teknolojisinin kullanılması ile tüm frekans spektrumunu çok

kısa bir sürede (milisaniye) incelenebilmekte ve tehdit sinyallerine hızla tepki verilebilmektedir. Reaktif bozucularla oluşturulan baloncuk ve etkin koruma aralığı, aynı çıkış gücüne sahip aktif bir karıştırıcıdan çok daha fazladır. Bugün birçok modern ordu, uzaktan komutalı EYP'lere karşı bu karmaşık tasarımlı reaktif karıştırma teknolojisini kullanmaktadır. Gelecekte bu teknolojinin kullanımının giderek yaygınlaşacağı öngörülmektedir.

5. SONUÇ VE DEĞERLENDİRME (CONCLUSIONS AND EVALUATION)

Terör örgütleri ve tehdit ağları tarafından, tüketici elektroniği pazarından kolaylıkla temin edilebilen elektronik bileşenler, uzaktan komutalı EYP'lerin üretiminde kullanılmaktadır. Dost unsurlara yönelik gerçekleştirilen EYP saldırılarında görülen son eğilimler ile terörist taktik ve tekniklerine göre terör örgütleri EYP tasarım ilkelerini belirlerken, hedeflerinin ne kadar kritik olduğuna ve ellerinde mevcut malzemelere göre seçmektedir. Piyasada bulunan tüketici elektroniği malzemeleri, seri üretimleri nedeniyle yüksek kaliteli ve ucuzdur, ayrıca karmaşık ve sıkışık bir elektromanyetik ortamda çalışabilecek şekilde tasarlanmıştır. Uzaktan komutalı (Radyo Kontrollü) EYP'lerin yaygınlaşması, EYP'ler ile mücadele eden birimlere karşı, düşük maliyetli, oldukça esnek ve öngörülemeyen bir tehdit oluşturmuştur. Söz konusu EYP'lerin yapımında kullanılan ticari mallar yasal üreticilerden terör örgütlerine doğrudan ulaşmamakla birlikte genellikle küçük bölgesel dağıtım şirketleri ve acentalarca bu transfer gerçekleşmektedir. Bu anlamda istihbarat birimlerince bölgesel dağıtım şirketlerinden birden fazla kullanım alanı olan malzemeler satın alan küçük yerel ticaret kuruluşları, gözetim zincirinin en zayıf halkası olmaları nedeniyle çok sıkı gözetim altında tutulması gerekmektedir.

EYP'lerin tespiti sonrası her ne kadar tehdit bertaraf edilmiş görünse de, karşı tedbir geliştiriciler ve silahlı kuvvetler açısından söz konusu tehdide karşı başarılı bir savunma için ele geçirilen EYP'lerin teknik kıymetlendirilmesinin büyük bir titizlikle yapılması gerekmektedir. Bu anlamda tespit edilen EYP'ler ve diğer malzemeler adlî delil niteliği taşıdıkları için söz konusu teknik kıymetlendirme ancak kolluk kuvvetlerince yerine getirilebilmektedir. Ülkemizde silahlı kuvvetlerin karşı tedbir geliştirmekle görevli birimleri, kolluk kuvvetlerince üretilen değerlendirme raporlarını incelemeyi talep etmeli ve buradan elde edilen bilgiler doğrultusunda tedbir geliştirmelidir.

Terör örgütleri ve tehdit şebekelerinin EYP yapımında giderek daha karmaşık cihazları kullanma, tasarlama ve dağıtma konusundaki teknik kapasitesi her geçen gün artmaktadır. Bu kapsamda teknik kıymetlendirme raporları hazırlayan kolluk kuvvetleri bünyesindeki analistler yakın gelecekte, ele geçirilen EYP'lerden elde ettikleri büyük miktarda veriyi işleyerek ve verilerdeki kalıpları tanıyarak belirli görevleri yerine getirecek şekilde eğitilebilir yapay zekalı yazılımları kullanabilecek, geriye dönük analizler yapabilecek, gelecekteki olası EYP saldırılarının yerini ve türünü tahmin etmeye

çalışacaktır. Bu tür bir analiz, silahlı kuvvetler ve diğer güvenlik birimlerinin yeni tehditlere odaklanmasını ve karşı önlemler veya yeni tespit teknikleri geliştirmesine de imkân tanıyacaktır.

YAZAR KATKILARI (AUTHORSHIP CONTRIBUTION STATEMENT)

Serkan KOÇ: Kavramsal tasarım, araştırma, metodoloji, kaynaklar, görselleştirme, yazma-taslak, yazma-gözden geçirme ve düzenleme.

ÇIKAR ÇATIŞMALARI (CONFLICTS OF INTEREST)

Yazar, herhangi bir çıkar çatışması olmadığını beyan eder.

KAYNAKLAR (REFERENCES)

[1] United Nations "Focus On: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime." *https://www.unodc.org/unodc/en/enewsunodc/2014/February/unodc-enews---4-february-2014.html* (05.05.2022).

[2] Conflict Armament Research, "THE IED THREAT IN BAHRAIN", London, 2019.

[3] United Nations General Assembly, "Countering the threat posed by improvised explosive devices", Report of the Secretary General, 2020.

[4] OMDIA, "Consumer Electronics Market Tracker - Q2 2020" *https://omdia.tech.informa.com/om012080/consumer-electronics-market-tracker---q2-2020.* (05.05.2022).

[5] Persistent Market Research, "Consumer Electronics Market Revenues to Rake in at a CAGR of 15.4%, Smartphones to Continue Dominance over 2016-2020" 23 Aralık 2016.

[6] J. Freeman,"The al Houthi insurgency in the North of Yemen: An analysis of the Shabab al Moumineen." Studies in Conflict & Terrorism, 2009.

[7] Major, K.J., Shaw, L.B., Busse, L., Gattass, R., Arnone, D., Lopez, E., Pushkarsky, M., Kane, J., Clewes, R.J., Lee, L. and Howle, C.R., "Fiber optic coupled quantum cascade infrared laser system for detection of explosive materials on surfaces. Optics & Laser Technology," 119, sf.105635, 2009.

[8] Sakarya, U., Teke, M., Demirkesen, C., Haliloğlu, O., Kozal, A.Ö., Deveci, H.S., Öztoprak, A.F., Töreyin, B.U. and Gürbüz, S.Z., "June. A short survey of hyperspectral remote sensing and hyperspectral remote sensing research at TÜBITAK Uzay", In 2015 7th International Conference on Recent Advances in Space Technologies (RAST), sf. 187-192, 2015.

[9] Bajic, Milan, and Tamara Ivelja. "The rationale and concept of collecting IED, UXO and landmines signatures." www. mine. vlada. Hr, 2018.

[10] Châteauneuf, Marc, et al. "Detection of explosives using THz time domain spectroscopy." International Society for Optics and Photonics, 2007, Vol. 6796, 2007.

[11] Mileusnić, Mladen, et al. "Analysis of jamming successfulness against RCIED activation with the emphasis on sweep

jamming." Facta Universitatis, Series: Electronics and Energetics 32.2, 211-229, 2019.