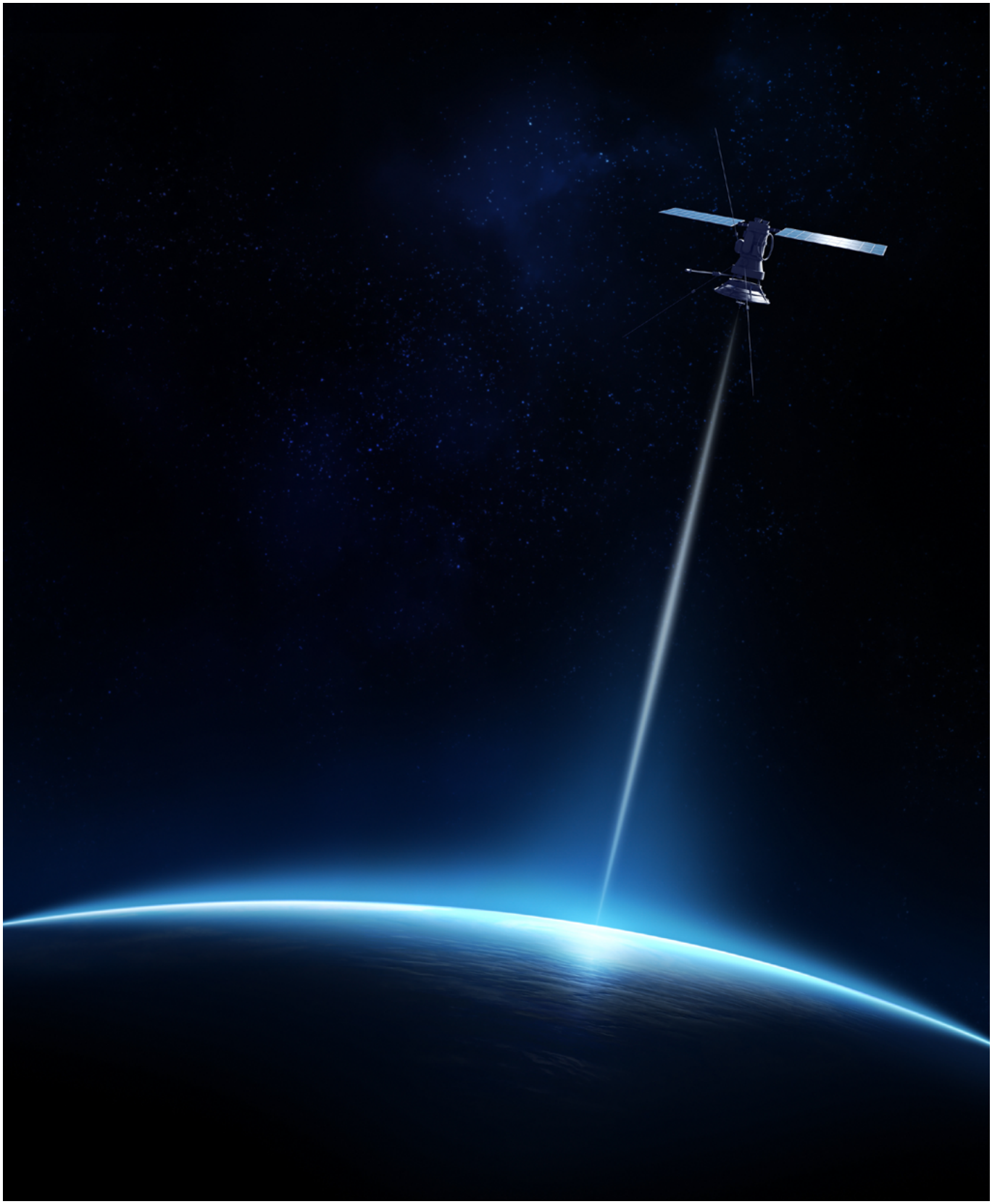
SİNYAL İSTİHBARATI

TREND ANALİZİ HAZİRAN 2018

thinktech
STM Teknolojik Düşünce Merkezi



Mert GÖKDUMAN

1. GİRİŞ

"Denilir ki başkasını ve kendini bilirsen sen, yüz kere savaşsan da tehlikeye düşmezsin; başkasını bilmeyip, kendini bilirsen bir kazanır bir kaybedersin; ne kendini ne de başkasını bilirsen, girdiğin her savaşta tehlikedesin demektir." MÖ 500'de yaşamış ünlü Çinli komutan, filozof ve askeri bilge Sun-Tzu'nun, dünyanın en eski strateji kuramı olarak kabul gören Savaş Sanatı adlı kitabında yer alan bu sözleri askeri istihbarat faaliyetlerinin önemini vurgular.

İstihbarat, "haberler, yeni öğrenilen bilgiler" anlamına gelen Arapça kökenli "istihbar" kelimesinin çoğuludur. Daha özel bir ifade olarak askeri istihbarat ise "Düşman ve düşman olması muhtemel taraf ile harekât bölgesine ait (hava ve arazi dahil) haber ve bilgilerin toplanması, değerlendirilmesi ve yorumlanmasından elde edilen sonuçtur"[1] şeklinde tanımlanır.

İnsanlık tarihi boyunca; devletler, topluluklar, kuruluşlar ve bireyler arası ilişkilerde her zaman önemli bir rol oynamış olan istihbarat, 20'nci yüzyılda bilim ve teknolojideki gelişmelerle farklı bir anlam kazanmıştır.

Günümüzde meydana gelen teknolojik buluş ve gelişmeler, istihbarat faaliyetlerini sürekli bir dönüşüme uğratmaktadır. Bu gelişmeler askeri istihbarat alanında, birçoğunun yanı sıra Sinyal İstihbaratı ve Elektronik İstihbarat gibi uygulama ve kavramları da beraberinde getirmektedir.

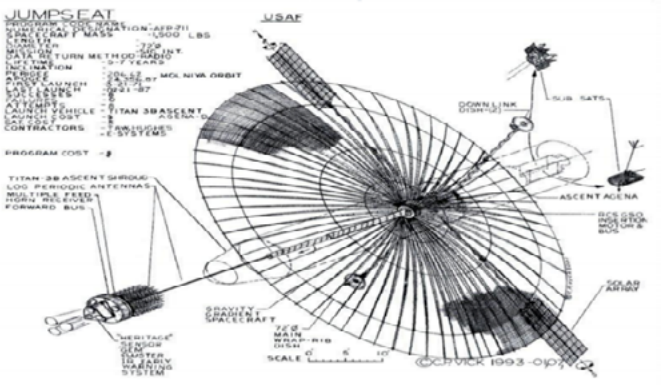
2. SİNYAL İSTİHBARATI NEDİR?

Ülkelerin rakiplerine karşı üstün olabilmek amacıyla büyük yatırımlar yaptıkları istihbarat faaliyetleri ciddi dönüşümler geçirmiş ve insan gücü temelinde inşa edilen istihbaratın yerini daha güvenilir ve süreklilik arz eden yöntemler almıştır.

Sinyal İstihbaratı, potansiyel düşman unsurlarının kullanmakta olduğu haberleşme cihazlarının ve elektronik aygıtların ürettiği sinyallerin (dalgaların) ya da bu cihazların ilettiği verinin belirli teknik yöntemlerle elde edilmesi ve analiz edilerek faydalı bilgiye dönüştürülmesini içeren çalışmalar bütünüdür.

Özellikle İkinci Dünya Savaşı sonrasında önem kazanan sinyal istihbarat faaliyetlerinde temel olarak, karşı tarafın sahip olduğu elektronik ve teknik mimarinin özellikleri, kullandığı cihazların görev ve amaçları, bunların kapasite ve yetenekleri ile karşı tarafın kendi içinde gerçekleştirdiği iletişim içerikleriyle ilgili bilgilerin toplanması ve analiz edilmesi amaçlanır.

Örnek olarak düşman güçlerin savunma mekanizmasında yer alan atış kontrol sisteminin yaydığı sinyallerin elde edilerek değerlendirilmesi sonucu, bu sistemin ne-



Şekil 1: Örnek SIGINT Uydusu

rede bulunduğu ve nasıl bir mühimmatı kontrol ettiği, bu mühimmatın yeteneklerinin neler olduğu gibi değerli bilgilere ulaşılabilir.

Sinyal İstihbaratı kapsamında İletişim İstihbaratı ve Elektronik İstihbarat gibi türlerden bahsedilebilir. Bu yöntemleri, ortak noktaları olan "Sinyal" faaliyetleri altında toplayarak hepsini Sinyal İstihbaratı başlığı altında değerlendirebiliriz.

Sinyal İstihbaratı (Signal Intelligence–SIGINT) iki başlık altında incelenebilir:

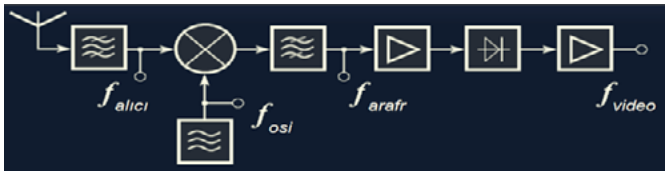
- Elektronik İstihbarat (Electronic Intelligence – ELINT)
- İletişim İstihbaratı (Communications Intelligence – COMINT)

ELINT ve COMINT sistemleri çeşitli yazılım ve donanım teçhizatlarından oluşur. Alınan çoklu sinyallerin analizleri bu faydalı yükler aracılığıyla gerçekleştirilir. Gelen sinyallerden bazıları sistemler tarafından anlık olarak analiz edilirken bazıları kuyruk adı verilen birimlerde geçici olarak saklanır ve işlenmek üzere bekletilir.

2.1. Elektronik İstihbarat

ELINT sistemleri kendilerine gelen sinyalleri alıcılarıyla toplar ve işleyerek sinyal tipi, gelen sinyalin frekansı ve bant genişliği, frekansın tekrarlanma miktarı ve sinyalin yön bilgisi gibi veriler üretir. Bu veriler belleğe alınarak müttefik ve düşman bilgileriyle kıyaslanarak kimlik tespiti yapılır. Sistem; gerçekleştirdiği tüm bu analizler neticesinde hedefin "düşman" olduğu sonucuna ulaşırsa, hedef platformun atış kontrol sistemleri, radar hedefleme sistemleri, gözlem-izleme sistemleri ve füze kılavuz sistemlerinden gelebilecek muhtemel tehditleri tespit ederek bir erken uyarı sistemi gibi çalışır. Tehdit tespiti sonucunda çözüm olarak sinyal bozucu faaliyetleri ya da platformun sahip olduğu teknik yeterlilik çerçevesinde gerekli imha birimlerini harekete geçirebilir.

Hedef platformlardan gelen "bilgi taşıyan sinyaller" yüksek frekansa sahip "taşıyıcı sinyaller" yardımı ile taşınırlar. Elde edilen bu yüksek frekanslı sinyallerden asıl bilgiyi oluşturan düşük frekanslı sinyali elde etmek için sinyalin demodüle edilmesi gerekir. Demodülasyon işleminin yapılabilmesi için bu sinyalin güçlü olması gerekir. Ancak ortam ve görev şartları zorluğu nedeniyle elde edilen bu sinyaller genelde zayıf sinyaller olur. Demodülasyon öncesi bu sinyallerin yükseltilmesi için süperheterodin alıcılar kullanılır. Bu alıcılar sayesinde yükseltilen sinyal, demodüle edilip ilgili bilgi kısmı alınır ve yeniden düşük frekanslı bir sinyale dönüştürülerek "video sinyali" olarak çıkarılır. Superheterodin alıcılar 0,01-40 GHZ aralığında yüksek hassasiyetle çalışır[2]. Bu alıcılar uzak



Şekil 2: Superheterodin Alıcı Tasarımı

menzillerden gelen sinyalleri yakalama ve değerlendirme kabiliyetine de sahiptir.

2.2. İletişim İstihbaratı

İletişim istihbaratı, yakalanan sinyallerin analiz edilerek hedef tarafından gerçekleştirilen iletişimin dinlenmesi ve hedefin mevcut konumunun tespit edilmesi işlemidir. Sinyaller hava dalgaları, fiber optik kablolar veya diğer birçok ortamdan elde edilebilir. Elde edilen bu veriler düşmanın niyet ve misyonu hakkında bilgi sahibi olmayı sağlar. Sinyal toplayıcı cihazlar belirli işleme ve görüntüleme sistemleriyle entegre şekilde çalışarak düşmanın iletişim türü (şekli), sahip olduğu radar sistemi ve hareket yönü gibi bilgilerin elde edilmesini sağlar. Çoklu sinyal analiziyle elde edilen konum verileri veya iletişim içerik verileri anlık olarak haritalandırılabilir.

Örneğin, bir birliğin emri altındaki diğer birliklere gönderdiği mesajların hacminde ciddi bir artış olduğunun tespit edilmesi durumunda, o birliğin görev bölgesinde kısa bir süre içinde bir operasyon başlatılabileceği ihtimali değerlendirilebilir.

Şekil 3: İletişim İstihbarat faaliyetleri için kullanılan sistemlerin örnek görüntüsü

3. ÜLKELERİN SİNYAL İSTİHBARAT TEŞKİLATLARI VE ÇALIŞMALARI

Günümüzde başta sosyal medya platformları olmak üzere her alanda ciddi miktarda veri üretilmekte ve bu veriler çok çeşitli amaçlarla analiz edilip değerlendirilmektedir. 2012 yılında dijital ortamda üretilen veri miktarı 4,4 zetabayt iken bu hızla devam ettiği takdirde 2020 yılında bu miktarın 44 zetabaytı bulacağı öngörülüyor. Veri miktarının yalnızca 8 yıl içinde 10 kat büyüyeceğinin öngörülüyor olması, bizi bekleyen gelecek hakkında net bir fikir veriyor. Teknolojik gelişmelerin gerisinde kalan bireyler, yapılar, şirketler, toplumlar ve hatta devletler yakın gelecekte kendilerine yer bulmak, varlıklarını korumak ve devam ettirmekte bir hayli zorlanacaklar.

Hayatın her alanını sardığını bizzat gözlemlediğimiz dijitalleşme süreçleri hiç şüphesiz ki devletlerarası ilişkilerde, güvenlik mekanizmalarının dizayn edilmesinde ve rakipler karşısında üstünlük sağlama çabalarında ciddi şekilde etkisini göstermektedir. Ülkeler dijital dönüşümlerini başarıyla gerçekleştirerek hem hata paylarını ve

Şekil 4: SIGINT Tesislerinden bir görüntü

maliyetlerini azaltmayı hem de üstün teknolojilere sahip devlet konumuna gelerek ciddi bir "Smart Power"a yani Caydırıcı Güce sahip olmayı hedeflemektedir. Bu güce sahip devletler politikalarını uygulama konusunda daha büyük bir özgüvenle hareket edebilmekte ve etkin oldukları bölgelerde siyasal, ekonomik ve diplomatik alanları kendilerine göre yeniden dizayn edebilmekteler. Özellikle Ukrayna ve Suriye'de senelerdir devam eden askeri gelişmeler, Irak'taki siyasi kargaşalar, senelerdir devam eden Filistin'deki İsrail işgali, hemen yanı başımızdaki Azerbaycan-Ermenistan sorunu, son dönemde gerilen İran-Suudi Arabistan ilişkileri, NATO ile Rusya arasında Ukrayna ve Polonya temelinde yaşanan askeri restleşmeler ve Türkiye'nin kendi iç dinamikleri gibi hususlar göz önüne alındığında, ülkemizin içinde bulunduğu bölge büyük ölçüde kaosun hâkim olduğu bir bölge olarak dikkat çekmektedir. Özellikle son dönemde yabancı devletlerin bölge üzerindeki hedefleri arka planda farklı bir savaşın sahnelenmesine neden oluyor. Ülkeler sahip oldukları teknolojik olanaklarla birbirlerine karşı adeta bir "Enformasyon Savaşı" veriyorlar. Bu bağlamda sinyal istihbaratı faaliyetleri ülkelerin birbirlerine karşı kullandığı yıkıcı bir yöntem halini almış bulunuyor.

Günümüzde önde gelen ülkeler, istihbarat kurumlarına bağlı olarak kurdukları özel birimler ile sinyal istihbaratı alanında ciddi çalışmalar gerçekleştirmektedir. Bu yapıların özellikleri ülkelere göre değişiklik göstermektedir:

3.1. NSA (National Security Agency)

Amerika Birleşik Devletleri'nin (ABD) sinyal istihbarat faaliyetlerini yürüten kurumdur. Yaklaşık 35 bin çalışanı ve yıllık 10 milyar dolar bütçesi olduğu tahmin edilen kurum, Birleşik Devletler'in en fazla istihbarat toplayan kurumu olarak bilinmektedir. Sovyetler Birliği'nin yıkılması sürecinde çok etkili olduğu bilinen NSA özellikle haberleşme ve iletişim ağları üzerinde ciddi bir etkiye sahiptir[3]. Bir dönem bu kurumda çalışmış olan Edward Snowden, NSA'nın her gün 200 milyon mesajı, 5 milyardan fazla konum bilgisini ve sadece Fransa'da 70 milyon görüşmeyi analiz edebildiğini ileri sürmüştü. ABD'nin bu bilgi gücüne sahip olmak için sinyal istihbarat çalışmalarına senede 20 milyar dolar bütçe ayırdığı tahmin edilmektedir[4].

3.2. BND (Bundesnachrichtendienst)

Almanya'nın sinyal istihbarat faaliyetleri doğrudan Başbakanlığa bağlı olarak çalışan Alman Dış İstihbarat Teşkilatı BND tarafından yürütülmektedir[5]. BND, sinyal istihbarat faaliyetleri konusunda NSA ile işbirliği yapmaktadır. Ayrıca bu iki istihbarat teşkilatı arasında SUSLAG (Special US Liaison Activity Germany) adlı ortak bir birim kurulmuştur[6]. ABD, Almanya'nın Wiesbaden şehrinde bir sinyal istihbarat tesisi kurmuş ve bunun karşılığında bu tesiste elde edilen verilere ulaşabilmesi için Alman istihbaratına FTP-Gateway bağlantısı ile NSA sunucularına erişim izni vermiştir. İstihbarat paylaşımının her yıl 700 milyon internet kullanıcısının kimlik verilerin-

Şekil 5: Almanya'nın Bad Aibling şehrinde yer alan BND'ye ait bir Sinyal İstihbarat Analiz Merkezi (sağda) ve Veri Toplama Merkezi (solda) görülmektedir. Sinyal Analiz Merkezinde beyaz çatılı bina ABD'nin Sinyal İstihbarat faaliyetlerini gerçekleştiren NSA'ya tahsis edilen alanı ifade ediyor.

den ve 60 milyon telefon numarası bilgisinden oluştuğu tahmin ediliyor[7].

Almanya'ya ait bazı SIGINT merkezleri şunlardır:

- Bad Aibling, Hof, Langen, Gablingen SIGINT Tesisleri: Öncesinde daha çok ABD'nin kullandığı bu tesisler şimdilerde BND'ye ait SATCOM sistemlerini üzerinde barındıran tesislerden bazılarıdır[8].
- Bramstedtlund, Butzbach, Rheinhausen, Schöningen, Übersee SIGINT Tesisleri: Bu tesislerde BND'ye ait SATCOM Sinyal Tutucu ve Yön Bulucu sistemler bulunmaktadır.

3.3. GCHQ (Government Communications Headquarters)

İngiltere'nin siber ve sinyal istihbarat faaliyetlerini gerçekleştiren kurumdur. 6000'in üzerinde çalışanı olan Government Communications Headquarters (GCHQ), temel amaç ve misyonunu şu şekilde ifade etmektedir: "Teknolojinin gelişmesi hayatın her alanıyla entegre olarak büyük bir fayda sağlarken bir yandan da bilgi güvenliğine yönelik tehditlere, casusluk faaliyetlerine ve terörizme yeni boyutlar katmaktadır. Bilimsel teknolojik gelişmelerin ortaya çıkardığı zafiyetler bireysel alanı tehdit edebildiği gibi zaman zaman milli çıkarlar için de tehdit oluşturmaktadır. Tüm bu nedenlerle Ulusal Güvenlik alanında bilgi sağlamak, bilgi güvenliği alanında karar destek süreçlerine katkıda bulunmak, askeri güçlere bilgi vererek suçların önlenmesini sağlamak başlıca görevimizdir"[9].

GCHQ, Dışişleri Bakanlığına bağlı olarak çalışsa da tüm kurumlara hizmet eder. İletişim ve Elektronik Güvenlik Grubu (CESG) ile Ortak Teknik Dil Servisi (JTLS) olarak iki alt birimi vardır. Bunlara ek olarak 2003'ten beri faaliyet gösteren geniş kapsamlı bir "Terör Analiz Merkezi" (JTAC) bulunmaktadır.

GCHQ'nun CIA ile de işbirliği içinde akıllı televizyonlara sızarak sinyal istihbaratı faaliyetleri kapsamında ses ve görüntü topladığı da ileri sürülmektedir.

3.4. SIGINT (Signal Intelligence)

Asya - Pasifik bölgesinde siber savunma ve sinyal istihbaratı çalışmaları konusunda en büyük organizasyona sahip ülke olan Çin Halk Cumhuriyeti bu alandaki teşkilatına doğrudan SIGINT ismini vermiştir. Yaklaşık 20 bini teknik çalışanı olmakla beraber toplam 130 bin personeli bulunan kurum, Genelkurmay Başkanlığına bağlı olarak çalışmaktadır. Genelkurmay Başkanlığında 3. Daire teknik olarak COMINT faaliyetleri gerçekleştirirken 4. Daire de "Elektronik Önleme ve Radar" alanında ELINT faaliyetleri yürütür. Çin Halk Cumhuriyeti'nin sahip olduğu sinyal istihbarat tesisleri genel itibarıyla bölgesel bir etkiye sahiptir ve Asya-Pasifik bölgesinde konumlandırılmıştır. Çin bu sayede Asya üzerinden geçen her radyo frekansını ve elektronik yayılımı yakalama ve işleme konusunda çok başarılı iken aynı etkiyi diğer bölgelerde gösterememektedir. Ancak son dönemlerde Çin'in Afrika kıtasında ve Hint Okyanusu kıyılarında üs kurma çabaları dikkat çekmektedir[10]. Özellikle Cibuti'ye sinyal yakalama tesisi kurmak için ciddi bir çalışma içerisindedir.

SIGINT tesisleri görüldüğü üzere genel itibarıyla Rusya, Japonya, Tayvan, Moğolistan, Güneydoğu Asya ülkeleri ve Hindistan gibi ülkelerin sınırlarına kurulmuş olmakla beraber bu ülkelerin iç iletişimlerini de hedef almaktadır[11]. Ayrıca Çin'in sinyal yakalama kabiliyetine sahip bazı gemileri ve savaş uçakları sürekli olarak Güney Denizi'nde seyrederek ABD ve Rusya'nın uydularını hedef almaktadır.

3.5 Spetssvyaz

Rusya Federasyonu'nun Özel İletişim ve Bilgi Servisi (STiS) olarak adlandırılan sinyal istihbarat teşkilatıdır. Federal Koruma Servisine (FSO) bağlı olarak çalışan bu kurumda yabancı iletişim sinyallerinin toplanarak analiz edilmesi, kriptoloji/şifreleme içeren sinyallerin çözümlenmesi gibi çalışmalar yürütülmektedir[12]. Soğuk Savaş döneminde KGB'nin 8. ve 16. Müdürlükleri sinyal istihbaratı çalışmalarına ayrılmış durumdaydı. 1960 yılında ABD'ye ait U-2 casus uçağının tespit edilip düşürülmesinin ardından Sovyetler Birliği kendi içinde ve ilişkilerinin iyi olduğu yabancı ülkelerde sinyal istihbarat merkezleri kurmaya başladı[13]. Uydular tarafından iletilen mesaj sin-

Tesis İsmi	Koordinatları	Anten Tipleri
Chanji SIGINT Tesisi	4359N 8729E	3xSATCOM incercept antennas
Cheng-yeng SIGINT Tesisi	3620N 12022E	3xFIX EIGHT CDAA
Ch'ih-Kan HFDF Tesisi	2117N 11017E	THICK EIGHT CDAA
Ching-Yang SIGINT Tesisi	3228N 10849E	THICK EIGHT, 3X FIX EIGHT
Choushan SIGINT Tesisi	3002N 12214E	
Hoshanting ELINT Tesisi	2207N 11248E	
Ho-tien SIGINT Tesisi	3708N 7955E	THICK EIGHT, FIX EIGHT
Hu-ho-hao-te SIGINT Tesisi	4037N 11144E	THICK EIGHT
Ka-ta SIGINT Tesisi	2958N 9548E	THICK EIGHT
Kuangchou SIGINT Tesisi	2307N 11308E	THICK EIGHT
Kunming HFDF Tesisi	2456N 10246E	THICK EIGHT, 3X FIX EIGHT
Lhasa SIGINT Tesisi	2939N 9110E	FIX EIGHT
Lingshui SIGINT Tesisi	1831N 11000E	THICK EIGHT
Nanning SIGINT Tesisi	2249N 10821E	THICK EIGHT
Peng-chia-chang SIGINT Tesisi	3035N 10355E	THICK EIGHT
Pumencheng ELINT Tesisi	2719N 12027E	
Shanghai SIGINT Tesisi	3125N 12125E	THICK EIGHT
Tamaoshan SIGINT Tesisi	2419N 11748E	
Tang-Hsien HFDF Tesisi	3847N 11508E	THICK EIGHT
Tungchingshan ELINT Tesisi	2525N 11938E	
Wangtienting SIGINT Tesisi	2311N 11605E	
Wu-lu-mu-chi SIGINT Tesisi	4343N 8723E	rhombic/FISH BONE

Tablo 1: Çin Halk Cumhuriyeti'nde SIGINT kurumuna bağlı sinyal istihbarat çalışmaları yapan bazı tesislerin isimleri

yallerinin Sovyet servisleri tarafından yakalanmasını sağlayan bu yapıların en büyüğü Küba'da Havana yakınlarındaki Lourdes'de kurulmuştu (2001'de kapatıldı). Tüm bu çalışmalar sonucunda, Rusya'nın 1960-1991 yılları arasından her yıl yaklaşık 100.000 mesajı ele geçirdiği tahmin edilmektedir.

Danimarka, 1950 öncesinde Grönland'dan Bornholm'a kadar konumlanmış olan sekiz ABD tesisi üzerinden veri ve bilgi alabiliyordu. ABD'nin 1950'de bu veri paylaşımını sonlandırması üzerine uzun çalışmaların ardından Danimarka ve Norveç 1992'de kendi ortak uydularını tasarladılar. İlerleyen süreçte bu birliktelik daha da güçlenerek diğer iki İskandinavya ülkesi İsveç ve Finlandiya'yı da içine aldı. Bu ülkeler 2001 yılından itibaren SIGINT faaliyetleri çerçevesinde bir komite oluşturarak tesislerini Rusya ve Batı Avrupa devletlerinin iletişim hatlarını hedef alacak şekilde

Tesis İsmi	Koordinatları	Anten Tipleri
Arsenyev	4410N 13319E	3 NM NE Arsenyev, FIX-24
Artagla	4136N 4454E	THICK EIGHT
Ashkhabad	3758N 5817E	FIX-24
Astrakhan Airfield	4611N 4804E	THICK EIGHT
Baku	4021N 5016E	18 nm east of Baku, FIX-24
Bataysk	4706N 3941E	Unknown CDAA antenna type
Brest	5208N 2342E	THICK EIGHT
Dikson	7333N 8035E	Unknown CDAA antenna type
Kabalovka	6003N 3014E	THICK EIGHT
Kazan	5545N 4915E	FIX FOUR HFDF
Kiev	5022N 3025E	THICK EIGHT
Kiev	5035N 3046E	15 nm NE of Kiev, FIX-24
Krasnoye Selo	5942N 3003E	THICK EIGHT
Krokhalevo	5857N 5525E	nr Tomsk, FIX-24
L'vov	4955N 2404E	THICK EIGHT
Magadan	5937N 14948E	THICK EIGHT
Magadan	5937N 15048E	3 nm north of Magadan, FIX-24
Minsk	5400N 2739E	THICK EIGHT
Moscow/Ostafyevo	5533N 3728E	THICK EIGHT
Murmansk	6851N 3809E	6 nm south of Murmansk, FIX-24
Narva	5920N 2814E	Suspected THICK EIGHT
Nomme	5920N 2437E	THICK EIGHT
Petrozavodsk	6154N 3413E	THICK EIGHT
Petrozavodsk	6152N 3412E	Unknown CDAA type
Riga	5637N 2401E	12 nm south of Riga, FIX-24
Sevastopol	4433N 3333E	4 NM SE Sevastopol, FIX-24
Simperopol	4458N 3402E	THICK EIGHT
Sovetskaya Gavan	4902N 14017E	30 nm NE of Sovetskaya Gavan, FIX-24
Talinn	5929N 2451E	3,5 nm NE Tallinn, FIX-24
Uglovoye	4323N 13158E	FIX EIGHT
Ussuriysk	4357N 13148E	FIX-24
Ventspils	5622N 2134E	1 nm south of Ventspils, FIX-24
Ventspils	5622N 2134E	0,5 nm south of Ventspils, FIX EIGHT
Yuzhno Sakhalinsk	4557N 14241E	THICK EIGHT
Yuzhnyy	4952N 3608E	THICK EIGHT

Tablo 2: Rusya Spetssvyaz kurumuna bağlı sinyal istihbarat çalışmaları yapan bazı tesislerin isimleri

Şekil 6: Spetssvyaz'in kontrolünde çalışan bir tesis Avustralyalı araştırmacılara göre halihazırda Spetssvyaz tarafından yönetilen 130 sinyal istihbarat uydusu, 20 hava aracı ve 60'dan fazla gemi çalışmakta ve havada gezen bilgileri yakalayıp analiz etmektedir[14].

Şekil 7: Almanya Gablingen'de yer alan BND'ye ait bir sinyal kesici ve yön bulucu Wullenweber tesisi

konumlandırdılar ve bu alana ciddi yatırım yaptılar. Bu çalışmalarında ABD ve İngiltere'den zaman zaman ekonomik ve teknik destek alsalar da personel desteğini kabul etmeyerek mahrem alanlarını koruma çabası içinde oldular.

Hindistan, SIGINT faaliyetleri kapsamında İsrail tarafından üretilen Phalcon'ları ve Rusya'nın ürettiği Ilyushin-76 savaş uçaklarını kullanmaktadır.

Japonya'da Savunma İstihbarat Genel Merkezi (Defense Intelligence Headquarters –DIH) bünyesinde çalışan SIGINT birimi DIH organizasyonunun en büyük birimidir. Birimin Kobunato, Oi ve Tachiarai şehirlerinde üç ofisi vardır. Ichigawa şehrinde Kuzey Kore'nin iletişim ve elektronik sinyallerini hedef alan bir yer tesisi bulunmaktadır. Bu tesis iki adet Wullenweber kesici ve yön bulucuya sahiptir[15]. (Wullenweber, geniş alana yayılmış bir dairesel anten dizisidir. Dairesel bir çit görünümündedir. CDAA olarak da adlandırılır ve radyo yön bulma faaliyetlerinde kullanılır.)

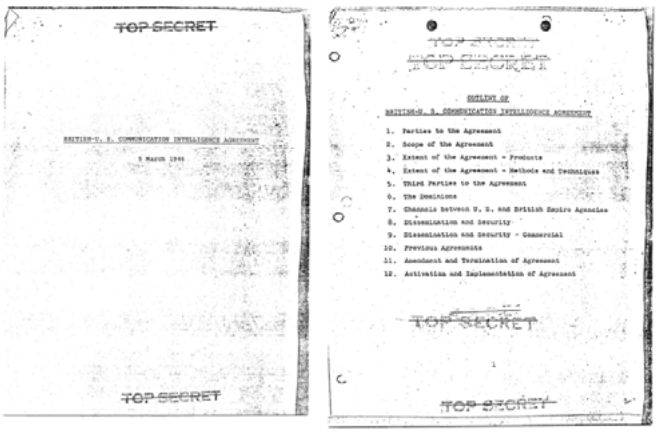
İspanya'da SIGINT faaliyetleri için çalışan bağımsız bir kuruluş yoktur. Bu çalışmalar İstihbarat Teşkilatı CNI çatısı altında ve diğer resmi kurumların desteğiyle yürütülür. SIGINT faaliyetlerinde gemi, uçak ve denizaltı gibi platformlardan yararlanmayı tercih eden İspanya, Boeing 707 Phalcon uçağının İsrail tarafından modifiye edilmiş ve ekipmanları İsrail-İspanyol elektronik sistemleriyle donatılmış farklı bir çeşidini kullanmaktadır. Bu casus uçak Elta EL/L-8300 SIGINT sistemine sahip olmakla beraber Sabitlenmiş Uzun Menzil Gözetleme (SLOS) kabiliyetine de sahiptir. Anlık olarak yüksek çözünürlüklü TV-Kamera görüntüsü sağlamakta ve bu verileri kayıt edebilmektedir. Yaklaşık 100 km menzilde görüntü yakalayabilen bu casus uçaklar Kuzey Afrika'nın batı sınırında, Batı Sahra ve Akdeniz üzerinde İspanya'nın SIGINT birimlerine ciddi veriler toplamaktadır.

4. UKUSA ANLAŞMASI VE ECHELON

UKUSA Anlaşması; İkinci Dünya Savaşı sonrası yaşanan gelişmeler göz önünde bulundurularak, ABD ile Birleşik Krallık arasında 5 Mart 1946 yılında imzalanan ve bu iki ülkenin sinyal istihbarat paylaşımını düzenleyen bir anlaşmadır[16]. İlk başta BRUSA (Britanya-USA) olarak adlandırılan anlaşma 10 Mayıs 1955 tarihinde yenilenerek UKUSA ismini almıştır. Anlaşma çerçevesinde NSA ve GCHQ sinyal istihbarat birimleri ortak çalışma sahaları belirleyecek, birçok alanda etkili olabilecek bir SIGINT yapısı oluşturacak ve bu tesisler aracılığıyla elde edilen istihbaratı ortak bir havuzda toplayarak her iki devletin kullanımına sunacaklardı[17].

UKUSA anlaşmasına daha sonra diğer Commonwealth ülkeleri de (Avusturalya, Kanada ve Yeni Zelanda) dahil edilerek beş ülkeli bir yapı oluşturuldu.

UKUSA anlaşmasının amacı internet üzerinde üretilen her türlü veriyi, uydu ve antenler aracılığıyla iletilen



Şekil 8: 5 Mart 1946 tarihinde imzalanan UKUSA Anlaşmasının içeriği

haberleşme sinyallerini, ülkelerin sahip oldukları askeri altyapıları ve yeni teknolojileri istihbar etmek ve bu bilgileri muhabere sahasında avantaja çevirmektir.

Echelon ise medyada defalarca ifade edilen, hatta bazı ülkelerde hükümet temsilcileri tarafından gündeme getirilen ve birçok kez diplomatik açıklamalara konu olan, UKUSA anlaşması çerçevesinde başlatıldığına inanılan bir "haber alma" projesidir[18]. İlk kez 6 Eylül 1960'da iki eski NSA çalışanının Moskova'da düzenledikleri bir basın açıklamasında dile getirilen bu projede, 40'tan fazla ülkenin kritik birimlerinin UKUSA ülkeleri tarafından sürekli bir dinlemeye tabii tutulduğu belirtilmiştir. Yine bu ülkelerin askeri sistemlerinin radar ve sinyaller üzerinden tespitlerinin yapılarak düzenli olarak raporlamalara konu edildiği iddia edilmiştir[19]. Bu çalışmanın varlığı ABD başta olmak üzere UKUSA üyeleri tarafından ısrarla reddedilmiş, anlaşma çerçevesinde kanundışı herhangi bir dinleme faaliyetinin yapılmadığı ifade edilmiştir. Ancak bu konuda söylentiler ve şüpheler varlığını sürdürmüştür[20].

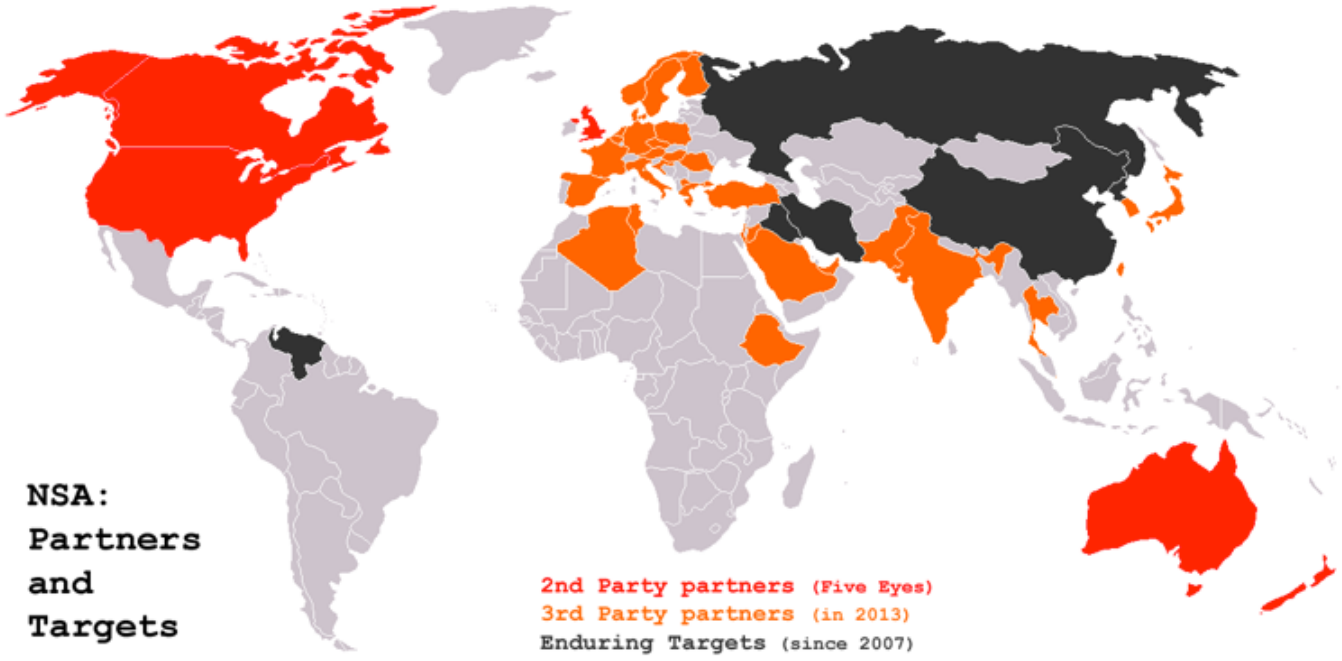
Özellikle son dönemde İngiltere ve ABD'nin Prizma ve Tempora isimli programlar üzerinden Almanya'da her ay yaklaşık 500 milyon telefon ve internet erişimini takip etmesinin Der Spiegel dergisi tarafından resmi belgelerle ispat edilmesi üzerine bu şüpheler artık geri planda konuşulmaktan öte diplomatik krizlere yol açar hale gelmiştir. Yaşanan bu dinleme krizi, Almanya'da dijital ve elektronik izleme konusunda ABD ve İngiltere'ye kıyasla yetersiz kalındığı tartışmalarını gündeme getirmiştir[21].

Ülkeler birbirlerine karşı istihbarat faaliyetleri gerçekleştirirken işbirliği içinde hareket ettiği alanlara da sahip olmuşlardır. BND'ye ait bazı SIGINT tesislerinde NSA tarafından kullanılan bazı bölümlerin yer aldığından bahsetmiştik. UKUSA Anlaşması çerçevesinde buna benzer ortaklıklar, işbirliği alanları oluşturulmuştur. Birleşik Krallık'ın Londra ve Cheltenham bölgelerinde yer alan SIGINT tesislerinde ABD tarafından kontrol edilen Strategic United States Liaison Office (SUSLO) olarak adlandırılan birimler bulunmaktadır. Avusturalya'nın Fort Meade (Canberra) bölgesinde de gene UKASA anlaşması çerçevesinde kurulan NSA'ya ait stratejik ofisler vardır. Bölgesel çalışmalar göz önüne alınarak bu ofislerin benzerleri başka yerlerde de kurulmuştur. Okyanusya ve Asya üzerinde SIGINT çalışmaları için Güney Kore'de ve Afrika bölgesindeki sinyal istihbarat faaliyetleri için de Kenya Mombasa'da stratejik ABD ofisleri oluşturulmuştur[22].

UKUSA anlaşması ilerleyen senelerde daha da genişletilmiş ve Türkiye, Danimarka ve Norveç gibi ülkeler de sisteme dahil edilmiştir. Anlaşma metninde "üçüncü taraflar" olarak nitelendirilen bu ülkelerin sisteme dahil edilmesiyle, ABD ve İngiltere, Avrupa ve Ortadoğu üzerinde SIGINT çalışmaları için yeni tesisler, adeta yeni cepheler açma imkânı bulmuştur. Bununla beraber söz konusu ülkeler de teknik yetersizlikleri olan alanlarda karşılıklı istihbarat paylaşımıyla diğer ülkelerin sistemlerinden gelen verileri kullanma hakkına sahip olmuştur.

4.1. Kıbrıs Ağrotur ve Dikelya Üsleri

Trodos Dağı'nda konumlandığı için Trodos Üssü olarak da isimlendirilen bu sinyal istihbarat tesisleri Birleşik Krallık'ın Ortadoğu-Doğu Akdeniz-Kuzey Afrika üçgeninde adeta gözü kulağı durumundadır[23]. Bulunduğu yer itibarıyla ülkemizi de doğrudan etkileyen bu üs UKUSA Anlaşması çerçevesinde en çok kullanılan ve ciddi miktarda istihbarat üreten tesislerden biridir. Ağrotur ve Dikelya üsleri Güney Kıbrıs Rum Yönetimi ve Kuzey Kıbrıs Türk Cumhuriyeti topraklarının dışında



Şekil 9: UKUSA Anlaşması'na göre NSA'nin birincil ve ikincil partnerleri ile UKUSA Anlaşması çerçevesinden yoğun şekilde hedef alınan ülkeler

Şekil 10: Kıbrıs'ta bulunan Birleşik Krallık topraklarının ve üslerinin yerleri

kalan ve resmen Birleşik Krallık'a ait olan bölgede yer almaktadır. Kıbrıs adasının yüzde 3'üne denk gelen ve 254 kilometrekarelik büyüklüğe sahip olan bu alan Birleşik Krallık'ın AB'den ayrılması sürecinde (Brexit) ciddi tartışma konusu olmuştur. AB tarafı, Birlik dışına çıkacak İngiltere'nin AB üyesi bir ülke olan Kıbrıs'ta bu üsse sahip olamayacağını ileri sürmüştür. Birleşik Krallık ise 1960'da imzalanan anlaşmayla bu topraklar üzerindeki hakkının garanti altında olduğunu ve kendi toprakları sayılan bu alanda gerçekleştirdiği faaliyetlerde özgür olduğunu dile getirmiştir[24].

Bölge üzerindeki tüm radyo frekans dalgalarını ve uydu sinyallerini yakalayarak analiz edebilme kabiliyetine sahip olan bu tesisler, özellikle Rusya'nın Kıtalararası Balistik Füze denemelerini yakından izleyerek raporlamaktadır. İngiltere-ABD ortaklığının yoğun şekilde hissedildiği bu üsler Akdeniz'de görev yapan ABD donanmasına ait 6. Filo'ya ciddi veri akışı sağlarken ayrıca ABD'nin bölge üzerinde bulunan diğer üslerden (Örnek: Türkiye-İncirlik) DTH radarları ile tespit edemediği füze denemelerini erkenden tespit edebildiği bilinmektedir.

5. SİNYAL İSTİHBARAT FAALİYETLERİ VE UYDULAR

Bugün Dünya yörüngesinde farklı ülkelere ait ve farklı görevlere sahip yaklaşık 1.738 adet uydu olduğu düşünülmektedir. Bunların bazıları telekomünikasyon faaliyetlerinin gerçekleşmesine hizmet ederken bazıları da çevresel şartların ve iklim değişikliklerinin izlenmesi amacıyla kullanılmaktadır. Ülkelerin savunma ihtiyaçları bu alanda da yansımalarını göstermiş ve askeri alanda kullanılmak üzere uydu faaliyetlerinden yararlanılmıştır.

Casus Uydu olarak yörüngeye sokulan uydular; elektronik istihbarat ve sinyal istihbaratı yaparak kendilerine biçilen izleme, dinleme, görüntü alma, sinyal yakalama görevlerini yerine getirmektedir.

5.1.Uydu Sahibi Olan Ülkeler, Sayıları ve SIGINT Alanında Kullanımları

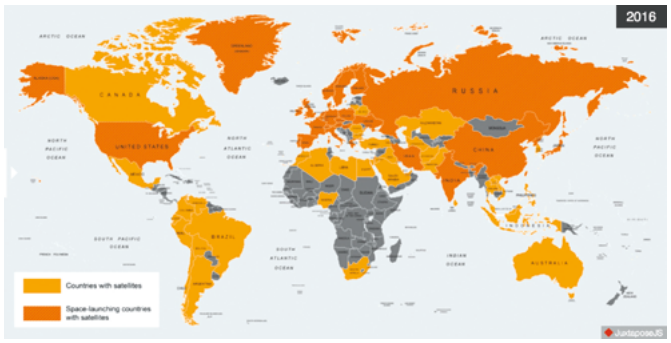
İlk uydu 1957'de SSCB tarafından fırlatıldıktan sonra ülkeler bu alanda çalışmalarına hız vermiş ve bu alanda ciddi yol kat etmişlerdir.

Şekil 12 ve 13'te görülen 1966 ve 2016 yıllarındaki durumu gösteren haritalar bu alandaki büyümeyi bariz şekilde gözler önüne sermektedir. Devletler sınırlarını, güvenliklerini ve vatandaşlarını koruyabilmek için rakiplerine karşı büyük avantaj sağlayan casus uydu faaliyetlerine önem vermekte ve büyük yatırımlar yapmaktadır.

Yüksek çözünürlüklü görüntü alma kabiliyetine sahip uydularla hedefler hızlı ve düşük sapmalarla belirlenebilmekte, hızlı müdahale imkânı elde edilmektedir. Düş-

Şekil 11: Ağrotur (Akrotiri) ve Dikelya (Dhekelia) tesisleri

Şekil 12: 1966 yılında uydusu olan ülkeler turuncu, kendi uydusunu fırlatabilen ülkeler koyu turuncu ile gösterilmiştir. (https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WxZD10iFOUm)



Şekil 13: 2016 yılında uydusu olan ülkeler turuncu, kendi uydusunu fırlatabilen ülkeler koyu turuncu ile gösterilmiştir. (https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WxZD10iFOUm)

man ülkelerin askeri tesisleri, nükleer tesisleri, kritik çalışmaları hakkında veri elde etme kabiliyeti açısından da değerli olan casus uydular; dinleme, radar, erken füze tespiti gibi birçok konuda da hizmet vermektedir.

Bugün Dünya yörüngesinde var olan uyduların yaklaşık yarısı ABD'ye aittir. Bunların kullanım alanları ve sahip oldukları teknik özellikler farklılık göstermektir[25].

Güncel Uydu Unsurları Sayıları ve Amaçları (31 Ağustos 2017 itibarıyla)			
Halihazırda Aktif Çalışan Uydu Sayısı: 1.738			
ABD: 803	Rusya: 142	Çin: 204	Diğer: 589
LEO: 1071	MEO: 97	Elliptical: 39	GEO: 531
Halihazırda ABD'ye Ait Uydular: 803			
Sivil: 18	Ticari: 476	Hükümet: 150	Askeri: 159

LEO (Low Earth Orbit) Alçak Yörünge Uydusu, yeryüzüne daha yakın bir yörüngede görev yapan uydu türüdür. Yüksek teknolojinin kullanıldığı LEO uydular askeri faaliyetler için kullanılan uyduların başında gelir. Yere yakın bir yörüngede çalıştıkları için sinyallerin alınması ve iletilmesinde gecikmeyi minimuma indirerek gerçek zamanda çalışma imkânı sağlar.

GEO (Geostationary) Sabit Yörüngeli Uydular, yerden yaklaşık 35-36 bin km yükseklikte ekvatorun tam üzerinde sabit duran uydulardır. Dünya ile aynı yönde ve aynı hızda hareket ettikleri ve Dünya'ya göre sabit kalabildikleri için bu uydular belirli bir bölge üzerinde işlem yapılan görevler için kullanılır.

Şekil 14: Bir ULA tanıtım afişi

MEO (Medium Earth Orbit) uydular, LEO uydular gibi çalışır; yalnızca bulundukları yörünge ve yükseklik farklıdır. Eliptik Uydular ise Dünya üzerinde eliptik bir yörüngede dönerek görev yaparlar[26].

ABD uydularının yaklaşık beşte biri doğrudan askeri amaçlı olmakla birlikte Hükümet uydusu olarak tanımlanan 150 uydu da askeri uydulara benzer görevler üstlenmektedir.

Birleşik Devletler'de casus uydu faaliyetleri Ulusal İstihbarat Ofisi (NRO) tarafından yürütülür. Bu ofis NSA çatısı altında görev yapmaktadır. Önceki dönemde casus uydu programlarını yalnızca devlet kurumları tarafından yürüten NRO, 2006 yılında aldığı bir karar ile özel şirketlerinde bu çalışmalara katılmasının önünü açmıştır. Bu karar kapsamında Lockheed Martin ve Boeing işbirliğinde United Launch Alliance (ULA) isimli bir şirket kurulması teşvik edilmiş ve ABD Savunma Bakanlığı'ndan aldığı onay ile casus uydu fırlatma yetkisine sahip olan ilk özel kuruluş olma hakkını elde etmiştir. Keza ABD'nin en yeni casus uydusu olan NROL-47 uydusu da yine bu kuruluş tarafından 12 Ocak 2018 tarihinde fırlatılmıştır[27].

2006 yılından itibaren casus uydu programlarında yer alabilen tek, özel kuruluş olan ULA, 2015 yılında ABD Savunma Bakanlığı'nın aldığı bir karar ile bu alandaki tek olma özelliğini kaybetti. SpaceX, ABD Savunma Bakanlığı ile bir işbirliği imzalayarak casus uydu fırlatma yetkisine sahip ikinci özel şirket olma hakkını elde etti. Öyle ki anlaşmadan henüz iki sene sonra geliştirilen NROL-76 casus uydusu SpaceX tarafından fırlatıldı[28]. Bu durum

Şekil 15: GÖKTÜRK 1'in fırlatılmadan hemen önceki görüntüsü

ABD savunma, uzay ve havacılık sektöründe ciddi bir rekabeti beraberinde getirdi. ULA ve SpaceX kendi şirketlerinin bu alanda daha başarılı olduğunu anlatabilmek amacıyla yazılı ve görsel medya üzerinden reklamlar yapmaya başladı.

Kendi casus uydusunu fırlatabilen diğer ülkelerden bir diğeri ise İsrail'dir. 2014 yılında fırlattığı Ofek-10 casus uydusunun zorlu hava koşullarında görev yapma ve alan taraması haricinde, hedeften hedefe atlama kabiliyetine sahip olduğunu öne süren İsrail, bölgede kendisine rakip olan İran'ın nükleer faaliyetlerini her an izleyebileceklerini belirtmiş ve rakiplerine gözdağı vermek istemiştir[29].

Kendi casus uydusunu üretip fırlatma kapasitesine sahip olmadığı için bu hizmeti başka ülkelerden temin ederek uydularını uzaya fırlatan ülkeler de bulunmaktadır. Türkiye bu ülkelerden biridir. Uydu tasarımları maksimum milli imkânlarla oluşturulmasına rağmen fırlatma teknolojisinin yokluğu, yerli uyduların Fransa, İtalya gibi ülkelerin işbirliği ile fırlatılmasını zorunlu kılmıştır.

Gelecek dönemde gelişen teknolojiyle insansız araçların uydulardan verilen komutlarla kontrol edilebileceği, bunlara hareket kabiliyeti kazandırılabileceği ve uyduların bir komuta kontrol merkezi gibi kullanılabileceği öngörülmektedir.

5.2. Türkiye ve Göktürk 1-2 Uyduları

Uzayda uyduya sahip 30 ülkeden biri olan Türkiye, en son 5 Aralık 2016 tarihinde fırlattığı Göktürk-1 askeri gözlem uydusuyla birlikte bugün toplam altı uyduya sahiptir. TÜRKSAT 3A, TÜRKSAT 4A, TÜRKSAT 4B uyduları haberleşme uyduları olarak görev yaparken; GÖKTÜRK 2, RASAT ve GÖKTÜRK 1 uyduları gözlem ve askeri görevleri yerine getiren uydulardır.

GÖKTÜRK 1 uydusu yüzde 20 yerlilik oranıyla üretilmiş olup TAI, ASELSAN, TÜBİTAK, UEKAE, ROKETSAN, TR TECNOLOGY gibi Türk kuruluşları ile İtalyan Telespazio ve Fransız Tales Alenia Space şirketlerinin ortaklığıyla üretilmiş ve fırlatılmıştır.

Şekil 16: Kanada'nin Alberta eyaletindeki Fort McMurray bölgesinde yer alan bir tesisin renkli 50 cm^2 çözünürlüğe sahip görüntüsü (solda) ve İngiltere Longleat bölgesinde yer alan bir tesisin siyah-beyaz 50 cm^2 çözünürlüklü bir görüntüsü (sağda)

Alçak irtifa yörüngeye (LEO) oturan GÖKTÜRK 1, Dünya'nın etrafını 90 dakikada turlamaktadır. Yüksek çözünürlüklü optik kamerasıyla yılda 60 binden fazla görüntü alabilecek teknolojiye sahiptir. Herhangi bir coğrafi kısıtlamaya tabi olmadan Dünya'nın her yerinden görüntü alma kabiliyetine sahip olan uydu; görüntü çözünürlüğü, kapasitesi, veri indirme hızı, manevra kabiliyeti ve gelişmiş yer sistemleri gibi özellikleriyle elektronik istihbarat sağlama konusunda Türkiye'nin elini güçlendirmiş, özellikle terörle mücadele için ciddi farkındalık yaratmıştır[30].

13 Temmuz 2009 tarihinde Savunma Sanayii Müsteşarlığının yaptığı anlaşmayla üretilmeye başlanan GÖKTÜRK 1 uydusunun üretimi ve fırlatılması bazı teknik ve siyasi nedenlerden dolayı gecikmiştir. Bu gecikme 2012 yılında Çin'den fırlatılan GÖKTÜRK 2 uydusunun GÖKTÜRK 1'den erken fırlatılmasına neden olmuştur[31].

Uyduların çektikleri fotoğraflarda her bir piksele yeryüzünden kaç cm^2 alanı sığdırabildiği, o uydunun çözünürlüğünü gösterir. GÖKTÜRK 1 uydusu 50 cm^2 çözünürlükte siyah-beyaz kareler alabilirken, ancak 2 m^2 çözünürlükte renkli görüntüler çekebilmektedir. Bu düzeyde çözünürlük kişilerin ya da küçük unsurların tespiti için yeterli olmazken askeri tesislerin, savaş araçlarının, ordu düzeninin, teknik gücün tespiti açısından ciddi bir destek sağlamaktadır.

Halihazırda ABD'nin sahip olduğu ve istendiği takdirde kiralanabilen bazı sivil uyduların 30 cm^2 çözünürlükte renkli resimler alabildiği bilinmektedir. Ancak GÖKTÜRK 1 uydusuyla elde edilen tecrübe bir sonraki çalışmada daha gelişmiş uyduların milli olarak ortaya konmasına temel olacaktır.

6. SIGINT FAALİYETLERİNDE KULLANILAN UÇAK VE GEMİ PLATFORMLARI

Elektronik istihbarat alanında gerçekleştirilen çalışmalarda uçak ve gemi platformları da yoğun şekilde tercih edilen seçeneklerdir.

6.1. Uçak Platformları

Uçtukları bölge üzerinde yeryüzüne daha yakın oldukları için yüksek çözünürlüklü görüntü alabilen uçaklar IMGINT (Görüntü İstihbaratı) bağlamında etkili olurken dinleme yapma kabiliyetine sahip hava araçları SIGINT amaçları için kullanılabilir. Ayrıca Havadan Erken İhbar Sistemlerine (Airborne Early Warning -AEW) sahip uçaklar, tehditleri erken tespit ederek gerekli tedbirlerin alınması için zaman kazandırabilir. Bu uçaklar 370-420 km menzilde yer alan herhangi bir uçak ya da gemiyi tespit edebilirken, üzerlerinde bulunan güçlü sinyal karıştırıcı unsurlarla düşman unsuru etkileme kabiliyetine sahiptir.

Türkiye'de kullanılan Boeing 737 uçaklarının modernize edilmiş hali olan AEW&C (AWACS) Erken İhbar ve Kontrol Sistemlerine sahip uçakları elektronik istihbarat bağlamında değerlendirebiliriz.

Uçağı	Üretici Ülke	Kategori
Beriev A-50	Rusya	4 Motor
Boeing 707 Phalcon/Condor	İsrail	4 Motor
Boeing 737 AEW&C	ABD	2 Motor
Boeing E-3 Sentry	ABD	4 Motor
Boeing E-767	ABD	2 Motor
DRDO AEW&CS	Hindistan	2 Motor
Embraer R-99/E-99/EMB 145 AEW&C	Brezilya	2 Motor
Grumman E-2 Hawkeye	ABD	2 Motor
Gulfstream G550/IAI Eitam	ABD / İsrail	2 Motor
KJ-200 'Y-8W Balanced Beam	Çin	4 Motor
KJ-2000	Çin	4 Motor
KJ-3000	Çin	4 Motor
Lockheed P-3 AEW&C	ABD	4 Motor
Saab 340 AEW&C (S 100 B/D Argus)	İsviçre	2 Motor
Saab 2000 AEW&C	İsviçre	2 Motor
Shaanxi KJ-500	Çin	4 Motor
Saanxi Y-8W	Çin	4 Motor
Saanxi Y-8 AWACS	Çin	4 Motor
Saanxi ZDK-03 AEW&C	Çin	4 Motor

Tablo 3: Sinyal İstihbaratı (ELINT ve IMGINT dahil olmak üzere) için kullanılabilecek uçaklar

Tablo 3'te görüldüğü gibi çeşitli ülkeler bu alanda farklı uçaklar kullanmaktadır.

Bu uçak platformları haricinde, özel olarak tasarlanan ve sinyal istihbaratı faaliyetlerinde kullanılan uçaklar da bulunmaktadır. Fransa-Almanya ortaklığıyla üretilen C-160 Kargo uçağı daha sonraki yıllarda Fransız havacılık şirketi Thales'in geliştirdiği SIGINT sistemleriyle entegre edilerek C-160G Gabriel adıyla Fransa Hava Kuvvetleri'nde uzun yıllar sinyal istihbarat faaliyetlerinde kullanılmıştır. Bu uçaklar Türk Silahlı Kuvvetleri bünyesinde de kullanılmaktadır.

Almanya, sinyal istihbarat ve elektronik istihbarat faaliyetlerinde NATO üyesi ülkelerin ürettiği uçakların çoğunu kullanmakla beraber ABD tarafından üretilen RQ-4 Block 20 Global Hawk savaş uçağının insansız modeli olan EuroHawk uçaklarını SIGINT faaliyetlerinde yoğun olarak kullanmaktadır.

Şili, Hindistan, Arjantin, Suudi Arabistan gibi ülkeler genel olarak İsrail-ABD üretimi Boeing 707 Phalcon uçaklarını kullanmaktadır. Suudi Arabistan ek olarak Boeing E-3 modellerine de sahiptir.

Rusya sinyal istihbaratı çalışmalarında hava araçlarına ciddi önem vermiş ülkelerden biridir. Bu alanda birçok ürün geliştirmiş ve dünya pazarında önemli bir yer elde etmiştir. Beriev A-50 SIGINT en çok tercih edilen platform olmakla birlikte Tu-214 serisi kapsamında üretilen Tu-214R ve Sovyetler Birliği döneminde üretilen Ilyushin Il-18 sinyal istihbarat faaliyetlerinde ciddi avantaj sağlamıştır.

Şekil 17: ABD tarafından üretilen Boeing E-3 Sentry (solda) ve Rusya tarafından üretilen Beriev A-50 (sağda) modelleri

İspanya, ABD üretimi 707 uçaklarına İspanya-İsrail işbirliği ile geliştirilen Elta EL/L-8300 SIGINT sistemleri entegre ederek bu uçakları sinyal istihbarat faaliyetlerinde kullanmaktadır.

İngiltere, sinyal ve elektronik istihbarat faaliyetlerinde Nimrod Deniz Karakol Uçağı modellerinin bir türü olan ve SIGINT sistemleri Fransız Thales tarafından geliştirilen Nimrod R1 modelini kullanmaktadır.

Görüldüğü üzere ülkeler bu platformları tamamen milli imkânlarla geliştiremeseler de belirli donanım ve modifikasyonları milli ve yerli imkânlarla sağlamaya özen göstermektedir.

6.2. Gemi Platformları

Sinyal yakalama, görüntü alma, radar izi bulma, konum belirleme, sinyal bozma gibi uygulamalar bazı gemi ve denizaltı platformlarıyla da yapılabilmektedir.

Çin bu çalışmalar için özellikle elektronik istihbarat alanında ciddi kabiliyetlere sahip olan dizel motorlu Type 815 casus gemileri kullanırken, Rusya Vishnya ve Balzam sınıfı istihbarat gemilerini kullanmaktadır. Özellikle Balzam sınıfı istihbarat gemileri sahip oldukları orta ve yüksek frekans sonarlar, elektronik dalga bozucu jammer'lar, sinyal yakalayıcı aygıtlar ve kod çözümleme yazılımlarıyla sinyal ve iletişim istihbaratı alanında ciddi kabiliyetlere sahip gemilerdir. Ayrıca üzerlerinde silah ve hava araçları için güdümlü Strela füzeleri bulunmaktadır.

Polonya sinyal istihbaratı faaliyetlerini gemi platformlarına aktarma konusunda başarılı olmuş ülkelerden biridir. Bizzat ürettiği ORP Hydrograf ve ORP Nawigator tipi gemileri bu amaç için kullanmaktadır.

Şekil 18: Ülkelerin SIGINT ve ELINT faaliyetlerinde kullandıkları deniz platformları

Bazı ülkeler ise halihazırda kullandıkları deniz platformlarına SIGINT/ELINT/COMINT sistemlerini entegre ederek istihbarat toplama faaliyetlerini güçlendirmeye çalışmaktadır. Danimarka sınır güvenliği için kullandığı FLYVEFISKEN gemilerine, SIGINT sistemleri ve faydalı yükler ekleyerek bu gemileri sinyal istihbarat faaliyetlerinde kullanmaya başlamıştır. İsveç halihazırda HMS Orion gemilerini SIGINT faaliyetlerinde kullanırken HMS Carlskrona gemilerini de yeniden kullanıma alarak Deniz Kuvvetleri envanterine dahil etmiştir.

Ayrıca bazı ülkeler sinyal istihbaratı faaliyetlerinde kullanmak üzere denizaltı platformlar ve bu platformlara entegre edilerek kullanılan sistemler geliştirmiştir. Mısır, Hollanda, İsveç kendi denizaltı platformlarında ArgoSystems/Condor AR-700 serisi SIGINT sistemlerini kullanmaktadır. Şili, Scorpene tipi denizaltı platformlarında ARGOsystems/Condor AR-900 serisi SIGINT sistemlerini kullanmaktadır. İtalya, eski üretim olan denizaltılarında Elettronica BLD-727 DF sistemlerini kullanırken yeni ürettiği platformlarda Alman SIGINT sistemlerini kullanacaktır. Tayvan ve Çin, İsrail üretimi olan TIMNEX 4 CH ELINT sistemlerini kullanmaktadır.

7. DEĞERLENDİRME VE SONUÇ

Ülkeler; rakipleri karşısında üstünlük sağlamak, bölgelerinde caydırıcı güce sahip ülke konumuna gelmek, düşmanlarının sahip olduğu güç hakkında bilgi sahibi olmak ve bu bilgiler ışığında kendini konumlandırmak, vatandaşlarını ve sınırlarını korumak gibi amaçlarla teknolojinin askeri sistemlerle entegre şekilde kullanılması için ciddi yatırımlar yapıyorlar. Teknolojik gücü elinde bulunduran ülkeler askeri bağlamda daha güçlü olmakla kalmıyor, bu gücü ihraç ederek hem ihtiyaç duydukları ülkeleri yanlarına çekerek yeni müttefikler kazanıyor hem de ciddi ekonomik kazanımlar elde ediyorlar. Öyle ki bu ülkeler teknolojik üstünlüklerini kendi politikalarını dikte etmek amacıyla bir tehdit unsuru olarak da kullanabiliyorlar.

Tüm bu gelişmelerden yola çıkarak 21'inci yüzyıl dünyasında kabuğunuza çekilerek, durağan bir dış politika ve diplomasi izleyerek milli birlik ve bütünlüğünüzü daim kılmanın mümkün olmadığını söyleyebiliriz. Özellikle ülkemizin bulunduğu coğrafyada hüküm süren si-

yasi karmaşa göz önünde bulundurulduğunda sorunları yalnızca bürokrasi ve diplomasiyle çözmeye çalışmak bazen daha karmaşık bir hal alabilmektedir. Bu bağlamda ülkeler bahsettiğimiz güce sahip olmak ve karar alma mekanizmalarını bağımsız işletebilmek için Sinyal İstihbaratı (SIGINT) ana başlığında değerlendirilen Elektronik İstihbarat (ELINT), İletişim İstihbaratı (COMINT) ve Görüntü İstihbaratı (IMGINT) faaliyetlerini yürütmek durumundadır. Düşman kuvvetlerin hamle yapacakları bölgeleri önceden öğrenme, sahip oldukları teknik ekipmanları ve kapasiteyi belirleme, konumlandıkları stratejik bölgeleri ve üsleri tespit etme ve kendi aralarındaki iletişimi analiz edip dinleme gibi kabiliyetler hiç şüphesiz savaş alanında ciddi bir üstünlük sağlayacaktır.

ABD, Çin, Rusya, Almanya, İsrail, Fransa gibi devletlerin büyük destek ve yatırımlarla teşvik ettikleri bu çalışmalar bugün savaş sahasının belirleyici unsuru olarak ön plana çıkmaktadır. Türkiye'de özellikle son dönemde savunma sanayiinde yaşanan sıçrama SIGINT faaliyetlerinde de etkisini göstermektedir. Bazı resmi ve sivil kuruluşlar bu alanda çalışmalarına hız vermiş ve özel olarak bu alanda çalışacak birimler oluşturmuştur.

TÜBİTAK, Elektronik İstihbarat Çözümleri kapsamında IF Dönüştürücü Sistemler, Spektrum Gözetleme Sistemleri, Mikrodalga Frekans Genişletici, Yarı-İletken Tespit Sistemi gibi ürünler geliştirmiş, üretmiş ve bu alanda yeni çalışmalara hız vermiştir[32].

BAYKAR, sinyal istihbarat sistemleri kapsamında gerçek zamanlı istihbarat, keşif ve gözetleme gerçekleştirebilen, geniş frekans aralığında çalışabilen, taşınabilir, yüksek performanslı BS-101 Sinyal İstihbarat Sistemini üretmiş ve hâlihazırda kullanılan Bayraktar TB-2 İHA üzerinden denemelerine başlamıştır. Bu cihazla İHA'lar üzerinden telsiz ve radar tespitine ek olarak dinleme yapma kabiliyeti de kazanılmıştır[33].

ASELSAN, radar ve elektronik harp kapsamında geliştirdiği KORAL ED ve KORAL ET sistemlerini 8x8 askeri araçlar üzerine entegre ederek yerli bir taarruz sistemi üretmiştir. KORAL ED sistemi tespit, teşhis ve yön bulma kapsamında ELINT faaliyetleri gerçekleştirirken; KORAL ET sistemi çoklu hedef karıştırma, tehdit karıştırma ve aldatma yeteneğiyle SIGINT faaliyetleri gerçekleştirmektedir[34].

Bu gelişmeler Türk Silahlı Kuvvetleri'nin harekât kabiliyetini büyük ölçüde artırarak ülkemizin bölgesel çapta rekabet gücünü artırmaktadır. Savunma sektöründe kazanılmış olan bu bilinç artırılarak devam etmeli ve süreç akademik, teknik ve taktik kabiliyetlere sahip öğelerin işbirliğiyle geliştirilerek sürdürülmelidir.

KAYNAKÇA

[1] Dr.Müh.Yb. Turgut KURTTEKİN , «İstihbarat Dersleri Notları ,» 2003,» Milli Savunma Bakanlığı, ANKARA

[2] C. Wolff, «Süperheterodin Alıcılar,» [Çevrimiçi], Available: http://www.radartutorial.eu/09.receivers/rx05.tr.html

[3] NSA, «Frequently Asked Questions,» 3 Mayıs 2016 [Çevrimiçi] Available: https://www.nsa.gov/about/faqs/sigint-faqs.shtml
[4] Amnesty, «Evidence of global opposition to US mass surveillance, » 17 Mart 2016 [Çevrimiçi] Available: https://www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq
[5] BND, «Operational Structure and Historical,» [Çevrimiçi] Available: http://www.bnd.bund.de/EN/About_us/Operational_Structure/Operational_Structure_node.html
[6] Der SPIEGEL Online, «Bad Aibling,» 18 6 2014 [Çevrimiçi] Available: http://www.spiegel.de/netzwelt/netzpolitik/bad-aibling-nsa-standorte-in-deutschland-a-974989.html
[7] M. Lütticke, «BND de dijital casusluk peşinde,» Deutsche Welle, 2 Temmuz 2013 [Çevrimiçi] Available: http://www.dw.com/tr/bnd-de-dijital-casusluk-pe%C5%9Finde/a-16923338
[8] M. Koop, «Report Reveals German BND SIGINT Organization Uses NSA Collection Targeting Tool,» 27 Eylül 2016 [Çevrimiçi] Available: http://www.matthewaid.com/post/151005541146/report-reveals-german-bnd-sigint-organization-uses
[9] British Intelligent Board :GCHQ, «What we do,» [Çevrimiçi]. Available:https://www.gchq.gov.uk/what-we-do
[10] BBC, «Çinli askerler ülkenin yurt dışındaki ilk üssü için yola çıktı,» 12 Temmuz 2017 [Çevrimiçi] Available: http://www.bbc.com/turkce/haberler-dunya-40577764
[11] Matthew M. Aid, «Chinese SIGINT Sites,» 4 Haziran 2012 [Çevrimiçi] Available: http://www.matthewaid.com/post/24424601613/chinese-sigint-sites
[12] Federal Protective Service, «FSO Web Site,» [Çevrimiçi]. Available: http://www.fso.gov.ru/
[13] R. W. Pringle, «Historical Dictionary of Russian and Soviet Intelligence,» 2015,» Rowman & Littlefield Publishers , Lanham/Maryland
[14] Karl de Leeuw ve Jan Bergstra, «The History of Information Security A Comprehensive Handbook,» 2007,» Elsevier Publishers, Amsterdam Univesity / Netherland
[15] United States Naval Communication, «AN/FRD-10 Circularly Disposed Antenna Array (CDAA) Receiving System,» USA Navy, [Çevrimiçi] Available: http://www.navy-radio.com/frd10.htm
[16] Cees Wiebes ve Matthew M. Aid, «Secrets of Signals Intelligence During the Cold War and Beyond,» 2001,» Frank Cass Publishers,London
[17] NSA, «UKUSA Agreement Release 1940 - 1956,» 3 Mayıs 2016 [Çevrimiçi] Available: https://www.nsa.gov/news-features/declassified-documents/ukusa/
[18] U. Keser ve M. D. Sönmez, « Electronic Intelligence, Echelon, and Signal Intelligence at the Eastern Mediterranean,» 2015,» Yayıncı Kıbrıs - Akdeniz Stratejik Araştırmalar Merkezi , Lefkoşa
[19] BBC, «Edward Snowden: Leaks that exposed US spy programme,» 2014 Ocak 2017 [Çevrimiçi] Available: http://www.bbc.com/news/world-us-canada-23123964
[20] L. D. SLOAN, «ECHELON AND THE LEGAL RESTRAINTS ON SIGNALS INTELLIGENCE: A NEED FOR REEVALUATION,» 2001 [Çevrimiçi] Available: https://pdfs.semanticscholar.org/1b44/bf6e150bd3470d4bb98335e832920c221003.pdf
[21] DER SPIEGEL, «How the NSA Targets Germany and Europe,» 1 Haziran 2013 [Çevrimiçi] Available: http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html
[22] Together We Served (TWS), «SUSLO,» [Çevrimiçi] Available: https://navy.togetherweserved.com/usn/servlet/tws.webapp.WebApp?cmd=PublicUnitProfile&type=Unit&ID=12283
[23] Richard J. Aldrich, GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency,» 2011,» Harper Collins Publishers,England
[24] S. Berberakis, «Avrupa Komisyonu: Brexit müzakerelerinde Kıbrıs'taki İngiliz üsleri de masada olsun,» BBC Türkçe, 3 Nisan 2017 [Çevrimiçi] Available: http://www.bbc.com/turkce/haberler-dunya-39481699
[25] Union of Concerned Scientist, «UCS Satellite Database,» 7 Kasım 2017 [Çevrimiçi] Available: https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WoKlOKhl-Um
[26] IOWA State University, «Types of Orbits,» IOWA State University, 2001 [Çevrimiçi] Available: http://www.polaris.iastate.edu/EveningStar/Unit4/unit4_sub3.htm
[27] S. Clark, «SpaceX, ULA win NASA contracts to launch Earth observation satellites,» Space Flight Now, 23 Ekim 2017 [Çevrimiçi] Available: https://spaceflightnow.com/2017/10/23/spacex-ula-win-nasa-contracts-to-launch-earth-observation-satellites/
[28] NTV, «SpaceX ilk kez ABD ordusu için casus uydu fırlattı,» 2 Mayıs 2017 [Çevrimiçi] Available: https://www.ntv.com.tr/galeri/teknoloji/spacex-ilk-kez-abd-ordusu-icin-casus-uydu-firlatti,-SowwfSUFrUi9YriPXY9UWw
[29] Haaretz , «Israel's Most Advanced Satellite, Ofek 10, Enters Orbit,» 10 Nisan 2014 [Çevrimiçi] Available: https://www.haaretz.com/.premium-israel-launches-military-satellite-1.5244635
[30] TAI / TUSAŞ , «GÖKTÜRK-2,» [Çevrimiçi]. Available: https://www.tai.com.tr/urun/gokturk-2
[31] Aljazeera Türk, «Casus uydu yörüngede,» Agence France-Presse, 10 Nisan 2014. [Çevrimiçi] Available: http://www.aljazeera.com.tr/haber/casus-uydu-yorungede

thinktech

STM Teknolojik Düşünce Merkezi

http://thinktech.stm.com.tr