Özet

11 Eylül 2001 tarihi birçok açıdan dönüm noktası sayılmaktadır. Bu denli az kişiyle bu denli etki yaratacak bir olayın daha önce sahnelenmemiş olduğunu söylemek sanırım yanlış olmaz. Dünya Ticaret Merkezi'nin (DTM) ikiz kulelerine ve Pentagon'a yapılan intihar saldırılarının ardından yaşananlar, ABD ve İngiltere'nin Afganistan'a yönelik harekatları, dünya ülkelerinin ve medyalarının tutumları, vb. irdelendiğinde farklı analizlerin ortaya çıkabileceği açıktır. Saldırının neden küresel ekonomik güç (DTM) ve küresel askeri güç (Pentagon) sembollerine yapıldığı ve neden, örneğin, Özgürlük Anıtı'na yapılmadığı, nasıl olup ta bu saldırının ardında ABD tarafından yetiştirilen ve uzun süre desteklenen Suudi milyarder Usame Bin Laden'in çıktığı gibi soruları da uzun süre tartışılacak konulardan sadece birkaçıdır. Bu yazının amacı bu ve benzeri konuları irdelemek değildir. Yazının amacı, bu nedenlerle gündeme gelen elektronik savaşlar, sanal ortamda haberleşme ve saldırı, akıllı füzeler benzeri konulara, teknik açıdan değinmek, bu kapsamda ulusal savunma sistemimizi ele almak ve gelişmekte olan teknolojileri tartışmaktır.

Giriş

11 Eylül 2001 DTM ve Pentagon intihar saldırıları (bkz. Şekil 1) hiç kuşkusuz tarihte bir şeylerin değiştiği ancak bunların neler olduğunun anlaşılmasının uzun yıllar alacağı süreç olarak yerini alacaktır. Saldırı, henüz haftalar olmasına karşın, yeni bin yılın ilk savaşını tetiklemiştir. Terörü beslediğini öne sürerek ABD ve İngiltere, bölge ülkelerinin de desteğini(!) alarak Afganistan'daki Taliban yönetimine karşı bir savaş başlatmıştır. Terörün tanımının dahi yapılamadığı, birinin teröristinin diğeri tarafından kurtuluş savaşçısı olarak görülebildiği, dünün Sovyetler rejimine karşı Yeşil Kuşak Teorisi kapsamında bugünün terörizminin tohumlarının atıldığı bir ortamda sonuçların ne olacağı uluslararası kamuoyunda merak ve kaygıyla izlenmekte, sağduyulu sesler ve eleştiriler savaş ve intikam çığlıkları arasında (en azından şimdilik) duyulmamaktadır. Bu yazının amacı bu saldırının ardındaki nedenleri ele almak, bireysel ya da örgütlü terör ve terör olaylarının hukuksal, sosyopolitik, ekonomik ve kültürel nedenlerinin tahlilini yapmak değildir. Amaç, bu saldırı ile gündeme gelen sanal savaşlar, elektronik savaşlar, akıllı füzeler gibi bilgi ve teknoloji yoğun sistemleri ve geleceğin ulusal savunmasında bilgi güvenliği ve elektronik gözetlemenin yerini Elektrik Mühendisleri Odası (EMO) üyelerine aktarmaktır.

11 Eylül 2001 tarihinden bu yana görsel ve yazılı basında konuyla ilgili doğru/yanlış bir çok soru yer almakta, yorumlar yapılmaktadır. Örneğin,

- İlk günlerde küçük bir elektronik vericiyle uçakların yerden kontrol edilerek saldırının gerçekleşmiş olabileceği söylendi.
- Kaçırılan uçakların hiçbir radara yakalanmamış olmasının nedeni olarak saldırının içeriden planlanması yanında elektronik karıştırma kullanılması gösterilebildi.
- ABD Federal Soruşturma Bürosu (FBI) teröristlerin

INTERNET üzerinde porno sitelerinden haberleştiklerini açıkladı.

- ABD ve İngiltere'nin Körfez ve Bosna harekatlarından sonra Afganistan'da da Tomahawk füzelerini kullandığı ve çok akıllı olan bu füzelerin hedefini hiç şaşmadığı belirtilmekte.
- Artık ABD'nin son yıllarda üzerinde çalıştığı Füze Kalkanı Savunma projesinin bir anlamının kalmayacağı iddia edilmekte.

Bu ve benzeri teknik soruların/konuların doğruluk payı nedir? Bunlar olabilir mi? Fiziksel olarak mümkün mü? Bu yazıda bu soruların yanıtları ele alınmaktadır. Önce bilgi ve haberleşme güvenliği ele alınmıştır, ardından elektronik savaşlar ve akıllı füzeler üzerinde durulmuştur. Bunlara bağlı olarak ulusal savunma ve elektronik gözetleme kavramları, yeni tip algılayıcılarla birlikte tartışılmış ve sonuçlar değerlendirilmiştir.

Bilgi ve Haberleşme Güvenliği

Teknolojinin baş döndürücü gelişimi elektronik ortamda bilgi ve haber iletimini dünyanın en ücra köşelerine dek yaymayı başarmıştır. Evler ve arabalar tam donanımlı birer ofise, tek kişilik bir atölye küresel bir işletmeye dönüşebilmiş, firmalar dünyanın değişik bölgelerinde küçük fakat etkin ofisler kullanarak, 24saat sürekli proje üretecek etkinliğe ulaşabilmiş, uzaktan eğitim (distant education), elektronik ticaret (Ebusiness) gibi kavramlar uygulanmaya başlamışlardır. Hatta, teknolojik gelişime bağlı olarak, bir ülkenin hastanesindeki bir uzmanın bir başka ülkenin hastanesindeki bir hastaya, bilgi ve haber kanalları üzerinden akıllı robotlar yardımıyla, ciddi ameliyatlar yapabilmesi düzeyine gelinmiştir. Doğal olarak bu gelişmeler sorunlarını da beraberinde getirmektedir. Sosyal, psikolojik, vb. sorunlar bir tarafa teknik olarak en önemli sorun bilgi ve haber güvenliği sorunudur.

Haberleşme ve bilişimde temel sorun bilgi güvenliğidir [1]. INTERNET gibi dünyanın hemen her noktasına açık erişimin sağlandığı bir ortamda bilgi güvenliği can alıcı bir öneme sahiptir. Teknoloji geliştikçe bilgi çoğalmakta, bilgiye erişim, paylaşma, koruma, eleme, vb. önem kazanmakta. Tüm bunların güvenli bir ortamda ve biçimde gerçeklenmesi için parola sorma, şifreleme gibi teknikler kullanılmakta.

Bilgi teknolojilerine giderek artan bağımlılık, yönetimleri değişik güvenlik önlemleri almaya yöneltmekte. INTERNET üzerinden banka fon transferleri, bireysel bankacılık işlemleri, uçak rezervasyonları, sanal ortamda alış veriş gibi ekonomik ve toplumsal yaşamın her alanında olduğu kadar, ulusal savunma ve ulusal güvenlik konularında da güvenlik bir numaraları sorun haline gelmiştir. Şu unutulmamalıdır; köprünün başını tutan, kimin geçeceğine de karar verecektir. Yani INTERNET alt yapısında ve haberleşme araç gereçlerinde teknolojiyi belirleyenler haberleşme ve güvenlik konusunda da en avantajlı ülkelerdir. INTERNET üzerinde tam güvenliğin sağlanması olanaksızdır. O halde sorun,

bilgi ve haberleşme güvenliğinin yüksek oranda sağlanmasının nasıl gerçekleneceğinde düğümlenmekte.

INTERNET üzerinde porno sitelerinden nasıl gizli mesaj gönderilebilir? Bu sorunun yanıtını görüntü işleme uzmanları "watermarking" diyerek açıklıyor. "Watermarking" (suya yazmak) bir belgeye, bir ses kaydına ya da bir resme, görünürde kaliteyi bozmadan ve fark edilmeyecek şekilde bir şifrenin, bir mesajın hatta diğer bir görüntünün eklenmesi olarak açıklanabilir. INTERNET üzerinde veri akışını kontrol etmek belli filtre mekanizmaları yardımıyla içinde belli sözcüklerin geçtiği bilgiyi izlemek, kopyasını çıkarmak olası. Ancak, aranan sözcük bilgi içinde şifrelenmiş biçimde bulunuyorsa uzmanlar bilgiye bu şekilde erişimin hemen hemen olanaksız olduğunu belirtmekte. Örneğin, Şekil 2'deki iki resim arasında fark yokmuş gibi görünmekte. Oysa sağdaki resim, soldaki resmin içine "IDDN.CH.010.0077853. 000.R.P.2000.030.40100" kodu gizlenerek oluşturulmuştur [2].

INTERNET üzerinde bilgi, haber gizliliğini sağlamanın başlıca yolları olarak [3];

- Kriptografi: Bilginin/haberin gönderen tarafında özel bir programla şifrelenmesi. Alıcının da aynı programı kullanarak şifreyi çözmesi
- Stenografi: Gönderilecek bilginin/haberin bir ses ya da görüntü kaydının içine şifrelenerek yerleştirilmesi ve alcı tarafta şifrenin çözülerek bilgiye/habere ulaşılması

sayılabilir. Bunların yanında, bilginin/haberin aktarmalı olarak birden fazla eposta adresinden gönderilmesi, ya da pek duyulmamış, kullanılmayan siteler aracılığı ile iletişimin sağlanması gibi yöntemler de kullanılmaktadır.

Bilgi ve haberleşme güvenliğine karşı tehditler kabaca üç başlık altında toplanabilir [1]:

- Sisteme yetkisiz giriş, gizlice dinleme, bilgi çalma, casusluk ve TEMPEST (yayılan elektromanyetik dalgalardan bilgiyi oluşturma) gibi kasıtlı eylemler,
- Bilgi ağı ve haberleşme sisteminin doğal afetler sonucu kısmen ya da tamamen çökmesi,
- Teknolojinin ve malzemenin kötü kullanımı ya da işletme hataları.

Bu ve benzeri tehditlere karşı alınacak önlemler de değişik başlıklar altında toplanabilir:

- Haberleşme güvenliği (COMSEC: Communication Security): Bilgi ve haberin iletişim kanallarından güvenli iletimiyle ilgilenir ve bilgisayar sistemlerine ağ girişleri ve dış dünyaya bağlantı sağlayan noktalarda güvenlik

teknolojileri ile ilgilidir.

- Bilgisayar güvenliği (COMPUSEC: Computer Security): Bilgi ve haberin bilgisayar ortamında oluşturulması ve depolanması sırasında yetkisiz kişilerce erişimin engellenmesine yönelik olup daha çok işletim sistemleri ve yazılım güvenlikleri ile ilgilidir.
- Bilgi Güvenliği (INFOSEC: Information Security): İşlenen, depolanan ve gönderilen bilgi ve haber yanında diğer tüm elektronik sistemlerin de güvenliği ile ilgilidir (bilgi teknolojilerindeki gelişmelere paralel olarak haberleşme, donanım ve yazılımların iç içe geçmesi sonucu COMSEC ve COMPUSEC disiplinlerinin birleştirilmesine verilen ad).

Son zamanlarda bilgi güvenliği (INFOSEC) yerine bir adım daha öteye gidilerek, gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability) alt başlıklarını bir arada toplayan, bilgi güvencesi (Information assurance) deyimi kullanılmaya başlanmıştır. Bilgi güvencesi için;

- Donanım güvenliği
- Yazılım güvenliği
- Kripto güvenliği
- Emisyon güvenliği (TEMPEST)
- Ağ güvenliği
- İletişim güvenliği
- Personel güvenliği
- Fiziki güvenlik
- Doküman güvenliği
- Yöntem güvenlig

gibi unsurların bir arada gözönünde tutulması kaçınılmazdır. Örneğin, pahalı yatırımlarla, yazılım ve donanım güvenliğini sağlamanıza karşın personel gizlilik konusunda yeterli eğitim ve bilinçle donatılamazsa bilgi ve haberleşme güvenliğinin sağlanması hayalden öte gidemez. Keza, her türlü önlemi almanıza ve hatta kripto kullanmanıza karşın, örneğin gönderilen kriptolu mesajların sonuna klasik "arz/rica ederim", "emirlerinizi beklerim" gibi klasik tümceler koymak tüm güvenliği bir anda sıfırlamak anlamına gelebilir.

11 Eylül 2001 Değişen Dünya'da Elektronik Savaşlar, Bilgi Güvencesi ve Ulusal Savunma

Doç. Dr. Levent

Roket, Füze ve Elektronik Savaşlar

Günümüzde etkili silahlarının başında roket, füze ve insansız hava araçları (UnAttended Vehicle, UAV) gelmekte. İnsansız hava araçları daha çok operasyon yapılacak bir bölgede ve alçaktan uçmak gerektiğinde keşif amacıyla kullanılırken, roket ve füzeler adeta adrese teslim etkili tahrip silahları olarak ürkütücü yeteneklerle donatılmakta.

Roket ya da füze sözcükleri çoğu kez birbiri yerine kullanılabilmektedir. Oysa genel olarak roket (Ballistic Missile, BM) denince bir platformdan fırlatılan ve itme kuvveti ile belirlenen bir yörünge üzerinde hedefe ulaşan araç akla gelmelidir.

SEVGİ

1958 yılında Akhisar'da doğdu. İlk öğrenimini 1969 yılında Altı Eylül İlkokulunda, orta öğrenimini 1976 yılında Eskişehir Anadolu Lisesinde tamamladı. Lisans öğrenimini 1982'de İTÜ, İstanbul Teknik Üniversitesi, Elektrik Fakültesi'nde, Yüksek lisans ve doktora öğrenimlerini ise, sırasıyla 1984 ve 1990 yıllarında İTÜ Fen Bilimleri Enstitüsü, Elektronik ve Haberleşme Anabilim dalında tamamladı. 1991'de Yardımcı Doçent, 1995'te Doçent ünvanı aldı. İTÜ ElektrikElektronik Fakültesi, Elektronik ve Haberleşme Mühendisliği, Elektromanyetik Alanlar ve Mikrodalga Tekniği Anabilim dalında 19821990 yılları arasında araştırma görevlisi, 19911994 yılları arasında yardımcı doçent ve 19951998 yılları arasında doçent olarak çalıştı. 19971998 arasında Bölüm Başkan yardımcılığı görevini üstlendi. 19881990 yılları arasında Amerika Birleşik Devletleri'nde New York Polytechnic Üniversitesi'nde Weber Araştırma Merkezinde doktora araştırmalarında

Füze ise (Cruise Missile, CM) yine itme kuvvetiyle bir platformdan fırlatılmasına karşın bir seyir planı doğrultusunda hedefi arayan araç olarak algılanmalıdır (İngilizce'de "Missile" sözcüğü genelde hem roket hem de füze anlamında kullanılmaktadır). Roketlerde kılavuz (guidence) sistem hedefe ilerlerken ani rüzgar değişimi gibi nedenlerle oluşacak sapmaları gidermek amacıyla kullanılır. Ayrıca, belli bir noktaya kadar radyo dalgalarıyla kontrol yetenekleri de olabilen roketlerde son yıllarda GPS (Global Positioning System) alıcıları da kullanılabilmektedir. Bütün bunlara karşın, kabaca söylemek gerekirse, roket önceden verilen ve fırlatmadan sonra değiştirilemeyen yörünge üzerinde hedefe ilerler. Taktik amaçlı (yaklaşık 50 km menzile sahip), kısa (1000 km), orta (1000300km), uzun (3000 6000 km) ve kıtalararası (6000 km'den büyük) menzilli diye gruplandırılmaktadırlar. Roket, takılan savaş başlığına göre etkisi farklı olan bir silah olup nükleer, biyolojik, kimyasal başlıklar kullanılabilmektedir. İçlerinde Mısır, İran, Irak ve İsrail'in de bulunduğu yaklaşık 15 ülkede üretilmekte ve satılmakta olup 40'a yakın ülkenin bir çeşit rokete sahip olduğu bilinmektedir [4].

Oysa füze her an için kontrol edilebilen, görev değişimine açık ve bir uçak gibi seyredebilme yetenekleri olan bir araçtır. Ayrıca, füze rokete göre daha ucuz, küçük boyutlu ama aynı oranda etkiye sahip olabilen, savunma radarlarınca yakalanması çok zor olan ve karar verme mekanizmaları yüklenmiş akıllı araçlardır. Bugün için yaklaşık 20 ülkede üretimi yapılmakta ve 60'a yakın ülkenin ise en az bir çeşit füzeye sahip olduğu bilinmektedir [4]. Yaygın olarak bilinen füze, son on yılda Irak, Bosna, Sudan ve şimdi de Afganistan'da kullanılmakta olan Tomahawk füzesidir (bkz. Şekil 3). Tomahawk füzeleri de kısa, orta ve uzun menzilli olarak farklılık göstermektedir. Bunun yanında karadan havaya, denizden ya da denizaltından karaya fırlatılan farklı tipleri de bulunmaktadır. Tomahawk füzesi ortalama 6m boyunda ve 50 cm çapında, kanat açıklığı 2.5 m'yi geçmeyen 9001000 km/saat hızına erişebilen bir silahtır. Savaş başlığının ağırlığı 500 kg'a kadar çıkabilmektedir. Maliyetleri 500,000 ile 2,000,000 ABD doları arasındadır. Hava savunma sistemleri, haberleşme tesisleri, ana karargahlar gibi hedeflere etkili olarak kullanılmaktadır.

Füzeler, belirtilen hedefe oldukça yüksek doğrulukla vurabilmekte. Doğruluk (hedeften sapma), neredeyse 12m'nin altına düşürülebilmekte. Bu, güçlü haberleşme, elektronik algılayıcı ve akıllı yazılımlarla sağlanmakta. Örneğin, Tomahawk'larda şu dört sistem bir arada bulunmakta [4] :

- GPS alıcısı: bu sayede füze, atıldıktan sonra uydular aracılığı ile sürekli konumunu kontrol edebilmekte.
- TERCOM (Terrain Contour Matching) sistemi: Füze, hedefe doğru yol alırken, üzerindeki bir radar ile sürekli yükseklik bilgisi ölçmekte ve kendisine önceden yüklenen sayısal harita bilgisi ile karşılaştırabilmekte. Bu sayede adeta yüzeyi yalayarak ve araziye uyarak (30 50 m'ye dek alçalarak) kendini savunma radarlarında gizleyebilmekte (bkz. Şekil 4).

bulundu. 19931997 yılları arasında Savunma Sanayi Projelerinde uzman araştırıcı olarak yer aldı. Propagasyon, Radar sistemleri, RCS Modelleme ve Sistem geliştirme üzerinde araştırmalara katıldı. 19981999 yılları arasında Kanada'da Raytheon Canada Limited firmasının Bilimsel Araştırma Grubu'nda yer aldı. Geliştirilmekte olan Çok Algılayıcılı Deniz Gözetleme Sistemi üzerinde çalışmalar yaptı. Aynı dönemde Waterloo Üniversitesi Mühendislik Fakültesinde ortak çalışmalarda bulundu. 19992000 yılları arasında TÜBİTAKMAM, Marmara Araştırma Merkezi Bilişim Teknolojileri Araştırma Enstitüsü'nde Elektronik Sistemler Grup Başkanlığı yaptı. Bu dönemde NATO SAS Panelinde TÜBİTAKMAM, Milli Savunma Bakanlığı Ulusal Sensörler ve Elektronik Sistemler Panelinde TÜBİTAK üyesi olarak görev aldı. İTÜ Fen Bilimleri Enstitüsü, Hava Harp Okulu, Uludağ ve Doğuş Üniversitelerinde Lisans, Yüksek Lisans ve doktora dersleri vermekte ve tezler yönetmektedir. Halen

- TOA (Time of Arrival) Sistemi: Füze hedefe yaklaşık ne kadar süre sonra ulaşacağını knotrol edebilmekte. Böylece hızlı erişimden hassas arama moduna geçerek hedefe kilitlenebilmekte.
- DSMAC (Digital Scene Matching Area Correlation) sistemi: Füze üzerinde hedefe ait yüksek çözünürlüklü uydu fotoğrafı bulunmakta (örneğin, bkz. Şekil 5). Hedef yakınına geldiğinde füze, kendi kamerasından gördüğü resim ile daha önce yüklenen uydu resmini karşılaştırmakta ve bu iki resim üst üste çakışıncaya kadar hedefi aramakta.

Bu kadar akıllı sistemlerle donatılmış füzelerin hedefi vurma yüzdeleri ve doğruluklarının oldukça yüksek olacağı aşikardır. Roket ve füze gibi sistemlerde bile tüm elektronik yeniliklerin kullanıldığı günümüzde elektronik savaşlar önem kazanmakta. Elektronik savaşlar, Elektronik Harp (EH), Elektronik Destek Tedbirleri (EDT), Elektronik Karşı Tedbirler (EKT), Elektronik Karşı Karşı Tedbirler (EKKT) gibi isimlerle sınıflandırılmakta. Tüm bunlar modern elektronik donanım yanında akıllı yazılımlar ve yetenekli operatörler gerektirmekte. Tüm bu unsurların yer aldığı tipik iki senaryo Şekil 6 ve 7'de resmedilmiştir [58]. Şekil 6'da günümüz operasyonlarından birisi resmedilmişken, Şekil 7'de önemli hava tehditleri gösterilmiştir. Her iki senaryodan da görüleceği üzere tüm operasyonlar erken uyarı, haberleşme, atış kontrol ve koordinasyon üzerine kurulu elektronik ortamda gerçeklenmektedir. Yani, günümüz savunma sistemlerinde elektronik haberleşme, radar ve erken uyarı sistemleri vazgeçilmez unsurlar haline gelmiştir.

Bulunduğu coğrafi bölgede Türkiye, bu ve benzeri roket ve füzelere sahip ya da geliştirme çabası içerisinde olan komşularla çevrilidir. Stratejik konumu nedeniyle uluslararası gözler de sürekli üzerinde olduğu için, Türkiye sağlam bir ulusal ekonomi ve ulusal savunmaya sahip olmak zorunda. Sağlam bir ekonomi ve bugünkü durum bu yazının konusu dışında tutulmuştur. Ancak, elektronik savaşlar ve tüm ülkenin 24saat, kesintisiz gözetlenmesi kapsamında "Nasıl bir Ulusal Savunma?" sorusunun yanıtı ele alınmıştır.

Ulusal Savunma ve Elektronik Gözetleme

Teknolojinin gelişimine bağlı olarak savunma stratejileri de günden güne değişmektedir. Yüzyılın başında karada uzun savunma hatları oluşturmak ve olası düşman hareketlerine karşı mevzi almak belirleyiciyken, ikinci dünya savaşıyla beraber tank ve uçakların etkinliği ön plana çıkmıştır. Son on yıllarda ise (özellikle körfez ve Bosna savaşlarından sonra) her biri akıllı bilgisayarlarla donatılmış taktik, balistik ve nükleer füzeler gündeme gelmiştir [8].

Ulusal savunma stratejileri ülkelerin bulundukları coğrafi bölgelere, komşu ülkelerin siyasi, ekonomik ve kültürel yapılarına ve uluslararası konjektüre bağlıdır. Örneğin, iki tarafı okyanusla

İTÜ Vakfı, Savunma Araştırmaları Merkezinde yarı zamanlı çalışmaktadır. İlgi ve uzmanlık alanları arasında Elektromanyetik Uyumluluk ve Kirlilik, Biyoelektromanyetik, Sayısal Modelleme, Radarlar, Anten ve Propagasyon, RCS modelleme ve Çok algılayıcılı Tümleşik Sistemler sayılabilir.

(doğal güvenli sınır) kaplı olan ABD ya da Kanada gibi ülkelerin savunma anlayışları ve stratejileri, Türkiye yada İsrail gibi dört bir yanı sorunlu ülkelerle çevrili ülkelerden çok farklıdır. Bununla birlikte bütün ulusal savunma stratejilerinde elektronik harp ve elektronik savunma belirleyici duruma gelmiştir. Artık ülkeler tüm savunmalarını belli merkezlerden 24saat, kesintisiz kontrol edebilecek gözetleme, izleme, kontrol etme, karar verme, savunma silahlarını uzaktan kumanda edebilme gibi kavramlar üzerine oturtmaktadırlar [7-9].

Günümüzde amaca uygun seçilecek olan algılayıcılar gözetleme, kontrol, erken uyarı gibi elektronik sistemlerinin temel taşını oluşturur. Kullandığı dalga cinsi, frekansı yada diğer parametreleri ne olursa olsun her algılayıcı değişik fiziksel temellere sahiptir. Örneğin, toprak altında yüzeyden birkaç cm derinliğe gömülen nesneleri algılamak için kullanılan sistem ile, yerin onlarca metre altında gömülü taktikbalistik füzeleri, nükleer silahları yada binaları saptamak, tünelleri bulmak için kullanılacak sistem çok farklı olacaktır. Benzer şekilde, iki vadi arasındaki sınır boyunu gündüz yada gece sürekli gözetlemek için düşünülen sistem ile karasularımızı ve 200 deniz miline dek uzanan uluslararası sulardaki haklarımızı gözetmek için kullanılacak sistem birbirine hiç benzemeyebilecektir. Uzun menzilli taktikbalistik füzeler ve normal hava tehditleri için bugün kullanılan mikrodalga radarları genelde yeterli olurken, çok alçaktan (100m'nin altında) uçan ve akıllı sensörler ve sayısal haritalarla araziyi adeta yalayarak izleyen ve radarlara görünmeden hedefe kadar yaklaşabilen CM füzeleri ve UAV'ler hava savunmasında büyük bir tehlikedir. Yine radar yakalanmayacak şekilde tasarlanan hayalet "stealth" uçakların tipik mikrodalga radarları ile yakalanması çok zordur (aslında radara yakalanmayan hayalet uçak diye bir şey yoktur, belli bir konumda ve özellikteki radara yakalanmayan hayalet hedefler bir diğer radar tipi ile yakalanabilmektedir). Bu nedenle, savunma sistemlerinde, gözetleme ve erken uyarı amacıyla genelde kullanılabilecek algılayıcı bulunamadığından değişik algılayıcıların bir arada kullanılacağı tümleşik sistemler ön plana çıkmakta ve yeni algılayıcı geliştirme çabaları hızlanmaktadır. Yeni algılayıcılar içerisinde HF ve VHF radarlarının geliştirilmesi çalışmaları hızla sürdürülmektedir.

1970'li yıllara gelindiğinde HF (330MHz) ve VHF (30300MHz) frekanslarını kullanan elektronik sistemlere "eski teknolojiler" ve mikrodalga frekanslarını (yaklaşık 1GHz ve üstü) kullanan sistemlere "yeni teknolojiler" denmekteydi. Mikrodalga haberleşme sistemleri, mikrodalga radarları, uydu verici ve terminallerinin yaygınlaşmaya başlaması teknolojinin buna ayak uydurmasını zorlamaktaydı. Aradan geçen otuz yıla yakın sürede mikrodalga teknolojisi gelişti, oturdu ve elektronik sistemlerin vazgeçilmezleri arasında yerini aldı. Son on yılda, özellikle radar sistemleri açısından "eski ve yeni teknolojiler" deyimleri yer değiştirir gibi oldu. Bunun en önemli nedeni yüksek kapasite ve hızlı bilgisayarların kullanımı ve radar işaret işleme tekniklerindeki gelişmeler sonucu HF ve VHF radarlarının önem kazanmaya

başlamaları olarak gösterilebilir.

Mikrodalga radarlarının kullanımı ufuk hattıyla sınırlıdır. Bu nedenle, örneğin zeminden 4050m yukarıdaki bir platformda bile görüş alanı 40km'yi geçmez. Daha geniş bölgeleri kapsayabilmek için mikrodalga radarları ya hava platformlarına (uçaklara) ya da yüksek tepelere konuşlandırılır.

HF/VHF frekanslarını kullanan radarlar uzak mesafeleri ve geniş bölgeleri kapsayabilen algılayıcılardır. Özellikle HF frekanslı dalgalar ufuk hattının ötesine ulaşabildiklerinden deniz gözetleme sistemlerinde yaygın olarak kullanılmaya başlanmışlardır. Yer dalgalarıyla 500km'ye gök dalgalarıyla ise binlerce km'ye ulaşabilmeleri olasıdır. VHF frekanslı algılayıcılarla daha dar bölgelerde gözetleme ve algılama yapılabilir. Ayrıca VHF radarları yüzeyde bitki örtüsü altında örtülmüş yada gizlenmiş nesnelerin havadan (uçak yada uydudan) saptanmasında kullanılmaktadır.

Mayın, sığınak gibi gömülü nesnelerin saptanmasında değişik algılayıcılar kullanılmaktadır. Örneğin, yüzeye yakın gömülü nesnelerin saptanmasında mikrodalga algılayıcıları kullanılır. Daha derinlerde gömülü (cephane, sığınak, vb) nesnelerin algılanması için HF yada VHF frekanslı algılayıcılar kullanılmak zorundadır. Frekans arttıkça kayıplı zemine elektromanyetik enerjinin nüfuz etmesi zorlaşır ve nüfuz derinliği azalır. Bu nedenle, hangi zeminde ne kadar derinlikteki nesnelerin algılanacağına bağlı olarak algılayıcı tipi değişir.

HF radarları yer ve gök dalgalı HF radarları olmak üzere ikiye ayrılır. Özellikle ABD ve Çin gibi okyanusa kıyı ülkeler yukarı HF frekanslarını (1530 MHz) kullanan gök dalgalı HF radarlarını 1950'lerden bu yana kullanmaktadır. Örneğin, ABD Atlas okyanusunu Avrupa, Pasifik okyanusunu ise Çin kıyılarına kadar kapsayabilmektedir. Gök dalgalı HF radarları hem kurulmaları hem de işletimleri çok pahalı olduğundan, günümüzde tüm dünyayı değişik yörüngelere yerleştirdiği yüzlerce uydu ile kapsayabilen ABD bu sistemlerden vazgeçmeye başlamıştır. Öte yandan, alt HF frekanslarını (310 MHz) kullanan yer dalgalı HF radarları değişik amaçlarla yaygın olarak kullanılmaya başlanmıştır. Gök dalgalı HF radarlarına göre hem kurulumu hem de işletimi son derece ucuz olan yer dalgalı HF radarları ile hem gözetleme, hem kontrol hem de oşinografik bilgi elde etmek olasıdır. Örneğin, Kanada Donanması Kanada hükümeti ve Raytheon Kanada firmasının yaklaşık on yıldır ortaklaşa sürdürdükleri çalışmalar sonucu geliştirilen ve denenen iki radarlı sistemi yakın zaman önce ulusal sistemine katmış ve kullanmaya başlamıştır [1012]. Avrupa Birliği üye ülkelerinden Almanya, Norveç, İngiltere ve İspanya'nın birlikte yürüttüğü önemli bir çalışma olan EuroROSE (European Radar Ocean Sensing) projesinde ise yine yer dalgalı HF radarlarından küçük ve orta ölçekte kapsamalar için kullanılan Codar ve Wera sistemleri başarıyla denenmektedir [13]. Bu sistemlerle, örneğin Kanada hükümeti hem Atlas okyanusunda

zengin petrol yataklarının bulunduğu Terra Nova bölgesindeki dev petrol platformları için tehdit oluşturan kuzey buzullarını gözetlemekte hem de savunmasını güçlendirmektedir. Norveç hükümeti benzer amaçlarla batı kıyılarında bir HF radarı kullanmaktadır. İspanya oşinografik amaçlı bir HF radarını yine EuroROSE projesi çerçevesinde denemektedir. Almanya, deniz ticaretinin önemli bir yükünü taşıyan Hamburg limanı çevresinde hem oşinografik hem de deniz trafiğinin kontrolü amaçlarıyla HF radarları kullanmaktadır. ABD'de Teksas A&M Üniversitesi öncülüğünde Teksas kıyıları ve körfezi, fırtına, dalga yüksekliği, akıntı yönleri, vb. açılarından orta düzeyde mobil HF radarlarıyla sürekli denetlenmektedir. Avustralya, Yeni Zelanda, Hong Kong ve Singapur'da da benzer çalışmalar yer almaktadır. Mikrodalga ve HF radarlarının birlikte kullanıldığı ve Türkiye genelinde kullanılabilecek bir gözetleme sistemi örneği Şekil 8'de resmedilmiştir. Bu senaryoda ikişer adet HF radarı ile tüm Karadeniz ve Akdeniz'in (Kıbrıs'ın ardına dek) kapsanabildiği gösterilmektedir. Benzer şekilde EgeAkdeniz giriş/çıkışı da bir adet HF radarı ile kapsanmaktadır. Bunlar ilave olarak kritik bölgelerde kullanılacak karada konuşlu mikrodalga radarları ve istenirse sürekli ya da zaman zaman kaldırılacak bir uçakta konuşlu bir mikrodalga radarı ile tüm Türkiye'nin sürekli, kesintisiz kapsanması olasıdır. Böyle amaç için gerçek senaryonun çıkarılması çok önemlidir ve bunun için ciddi altyapı çalışması veya kapsama analizleri yapılmalıdır.

Sonuçlar ve Öneriler

Değişen dünyada elektrikelektronik ve bilgisayar mühendislerinin ilgi ve sorumluluk alanları günlük yaşamdan ulusal savunmaya, ticaretten eğitime dek genişlemektedir. Modern elektronik cihazlar, güçlü bilgisayar donanımları ve akıllı yazılımlarla oluşturulan sistemler hemen her alanda kullanılmaktadır. Bu durumda da bilgi ve haberleşme güvenliği önemli sorunların başında gelmekte. Hemen her sisteme bir giriş ya da çıkışı olan INTERNET ağının ekonomik, ticari, savunma ve benzeri alanlarda yaratacağı iletişim güvenliği sorunu ulusal düzeyde ele alınması gereken önemli bir olgudur. Bugünlerde INTERNET üzerinde bazı kısıtlamalara gidilmesi, güvenlik birimlerince izinsiz izleme yapılması gibi girişimler başta ABD olmak üzere birçok ülkenin gündemindedir. Ancak, şifreleme ve bilgi/haber güvenliği sadece savunma alanında kullanılmamaktadır. Çok daha fazlası elektronik ticaret, bankacılık gibi alanlarda da vazgeçilmez unsur olduğundan yakın bir gelecekte bu girişimlerin kabul göreceğini söylemek zordur. O nedenle, bilgi/haber güvenliğinin elektronik ortamda bir numaralı sorun olmayı sürdüreceği ve şifreleme benzeri tekniklerinin vazgeçilmez araçlar olarak kalacağını söylemek yanlış olmayacaktır.

Ayrıca, Türkiye gibi üç tarafı denizlerle çevrili bir ülkenin kıyıları dahil sınırlarının kesintisiz gözetlenmesi güvenlik ve ulusal savunma açısından önemlidir. Bunun yanında terör, kaçakçılık, yasak avlanma, çevre koruma, balıkçılık, oşinografi, kaçak göçmen sorunu gibi birçok nedenle de kesintisiz gözetleme gereklidir.

Özellikle bilgisayar teknolojilerindeki gelişmelere paralel olarak güçlü sayısal işaret işleme tekniklerinin uygulanabilir olmasıyla HF ve VHF radarları gibi yeni algılayıcı tipleri kullanılır olmuştur. Bu radarlar geliştirme ve deneme aşamalarından kullanım aşamasına geçmeye başlamışlardır. Önceleri mikrodalga radarlarını tamamlayıcı algılayıcılar olarak düşünülürken artık ana algılayıcı olarak da kullanılabilecek seviyeye gelmeye başlamışlardır. Türkiye için bugün gelinen noktada, özellikle yüksek teknolojiye mahkum olmadan bu yeni tip HF ve VHF radarlarına kolay ve ucuz yollardan sahip olma olanağı vardır. Konuyla ilgili birikime sahip olma yanında bu sistemi istenirse tamamen yerli ya da uluslararası konsorsiyum şeklinde ama büyük bir oranda yerli katkıyla üretebilecek ulusal deneyim de bulunmaktadır [6].

Son olarak, 11 Eylül saldırılarının hemen her alanda düşüncelerin, planların ve stratejilerin sil baştan gözden geçirilmesi sürecini başlatacağını söylemek sanırım falcılık olmayacaktır. Teknolojiye, pahalı sistemlere yapılan yatırımlar kadar (belki daha fazlasının) insana, eğitime, barışa ve hakça bölüşüme yatırım yapma zamanı geldi ve geçmekte.

Kaynaklar

1. O Salcan, "Bilgi Güvenliği", Silahlı Kuvvetler Dergisi, Sayı 370, sf: 5467, Ekim 2001
2. Bkz. Http://www.alpvision.com , (resimdeki şifreleme bu siteden ücretsiz alınan Signit DEMO programı ile gerçeklenmiştir)
3. Cumhuriyet Bilim Teknik, sayı 762, 27 Ekim 2001 sayısı
4. Bkz. Http://www.fas.org, ve Http://www.chinfo.nayv.mil siteleri
5. L. Sevgi, "Ulusal Savunma Sistemleri Ulusal ARGE Kuruluşları", MSB Araştırma Teknoloji ve Faaliyetleri Bülteni, Sayı 11, sayfa 2230, Kasım 1999,
6. L. Sevgi, "Uzun Menzilli Füzeler ve Erken Uyarı Sistemleri", KKK Hava Savunma Okulu ve Eğitim Merkez Komutanlığı Hava Savunma Dergisi, Eylül 1999, İstanbul
7. L. Sevgi, "Gömülü, Örtülü ve Gizlenmiş cisimlerin Saptanması ve Algılayıcı Tipleri", KKK 21inci Yüzyıl Harekatı ve Modern İstihkam Techizatı Sempozyumu, 78 Ekim 1999, İzmir
8. L. Sevgi, "HFVHF Radarları ve Ulusal Savunma Ağındaki Yeri",Silahlı Kuvvetler Dergisi, Sayı 370, sf: 68,74, Ekim 2001
9. L. Sevgi, "Integrated Maritime Surveillance Systems Based on HF Radars", SIU99, Proc. Of Turkish Signal Processing and Its Applications Symposium, June 1619, 1999 , Ankara
10. L. Sevgi, A. M. Ponsford & H.C. Chan, "An Integrated Maritime Surveillance System Based on Surface Wave HF Radars, Part I Theoretical Background and Numerical Simulations", IEEE Antennas and Propagation Magazine, Vol. 43, No:4, pp.2843, Aug. 2001
11. L. Sevgi, A. M. Ponsford & H.C. Chan, "An Integrated

Maritime Surveillance System Based on Surface Wave HF Radars, Part II Operational Status and System Performance", IEEE Antennas and Propagation Magazine, Vol. 43, No:4 (basılmakta), Oct. 2001

12. L. Sevgi, "Target Reflectivity and RCS Interaction in Integrated Maritime Surveillance Systems Based on Surface Wave HF Radar Radars", IEEE Antennas and Propagation Magazine, Vol. 43, No.1, pp.3651, Feb. 2001
13. H. Gunther, et all, "The EuroROSE Project", Proceedings of the 16th International Conference of the American Meteorological Society on "Interactive Information and Processng Systems (IIPS) for Metereology, Oceanography and Hydrology", California, USA, pp 214...217, 9.14. January 2000