

BÖLÜM-V

TEKNOLOJİ VE ULUSAL GÜVENLİK

Doç. Dr. Murat ERDAL

5.1. Ulusal Güvenlik Kavramı

Teknolojinin uluslararası ilişkiler ve kamu yönetiminde oynadığı rol giderek önem kazanmaktadır. Uydu haberleşme sistemlerinden bilgisayarlar mobil telefonlardan yeni malzemelere, modern sağlık hizmetlerinden ileri imalat tekniklerine kadar hemen her alandaki uygulamalar ve gelişmeler insanlığın hizmetine sunulmaktadır. Fakat teknolojinin birçok yararlı tarafları olduğu kadar doğru ve disiplinli bir şekilde kullanılmadığında bu gelişmelerin olumsuz ve sakıncalı tarafları da ortaya çıkmaktadır. Bu sakıncalı taraflar giderek artmakta, kişisel/kurumsal gizlilik ve mahremiyetten ulusal güvenliğe kadar bir çok sahada görünümüleri ortaya çıkmaktadır.

Bir ülkenin demokratik süreçlerinin, bağımsız ve özgür devlet yapısının iç ve dış tehdit altında kalmaması için alınan gerekli önlemlerin toplamı “**ulusal güvenlik**” olarak tanımlanmaktadır¹.

Ulusal güvenlik kavramının temel unsurlarını askeri güvenlik, ekonomi, kaynak/çevre, politik ve kültürel ortam dinamikleri teşkil etmektedir. Tüm bu dinamiklerin günümüzde ulusal-küresel bağlantılar çerçevesinde düşünülmesi gereği açıktır. Teknoloji alanında da yaşanan küresel boyuttaki serbestlik ve yerel boyutlardaki korumanın neticesinde yaşanan gerilim ve çelişkiler yumağı beraberinde “**teknogüvenlik**” kavramını ortaya çıkarmış ve geliştirmiştir. Teknogüvenlik kavramı ise temelde iki boyutludur²:

- 1 – Ülkenin endüstriyel gelişimi ve rekabetçi avantajı
- 2 – Ülkenin güvenlik ve savunması.

¹ Janos Farkas, “New Challenges After the Cold War” , **Military R&D After The Cold War; Conversion and Technology Transfer in Eastern and Western Europe**, Ed.: Philip Gummert, Mikhail Boutoussov, Janos Farkas, Arie Rip, Kluwer Academic Publishers, Netherlands, 1996, s:68.

² Bundo Yamada, Kenji Okumura, “Information Technology, Globalization and the Strategic Management of Technology”, **Techno-Security in an Age of Globalization; Perspectives from the Pacific Rim**, Ed.: Denis Fred Simon, East Gate Book, New York, 1997, s:126.

Tekno-güvenlik boyutunun gelişimi bir zincirin halkaları şeklinde sıralanmaktadır³:

- a - Ülkelerin gücü ve gelişmesi, sahip oldukları sanayinin düzeyi ile doğrudan ve birinci dereceden ilişkilidir.
- b - Ekonomik gelişme endüstriyel gelişmeye bağlı olup, teknoloji üstünlüğü ülkeler arası yarıştaki yeri belirleyen ana parametredir.
- c - Teknoloji üstünlüğünü, tek başına teknoloji ithali ile sağlamak mümkün değildir. Teknoloji üretir duruma gelmek gerekir.
- d - Teknoloji üretiminin temel gereği de bilimsel araştırmadır.

Bu noktada, uluslararası ilişkilerin önemi bir kez daha ortaya çıkmaktadır. Ulusların dünyada meydana gelen değişiklikleri bilinçli bir şekilde izlemeleri, ekonomilerinin hangi sektörlerinde hangi teknolojileri üreterek ve/veya edinerek dünya pazarları için giderek artan rekabetin içine gireceklerine karar vermeleri gerekmektedir. Verilecek kararların akıllıca olabilmesi için bilim ve teknoloji gözlemi yapılması, tüm dünyanın yakından izlenmesi şarttır. Uluslararası ilişkileri bu yönde geliştirmek gerekmektedir⁴.

Ülke güvenlik ve savunmasında devletler ve uluslararası örgütler yeni birtakım unsurlarla karşı karşıya kalmaktadırlar. Soğuk Savaş döneminin sona ermesiyle birlikte savunma sanayi bütçelerinde bir müddet devam eden daralma eğilimi 11 Eylül saldırıları, terörizm eylemleri ve belirsizliklerle birlikte yeniden artma eğilimine bırakmıştır. Günümüzde savunma planlamalarının yapılması son derece zorlaşmıştır. Bunun sonucunda da savunma ile ilgili endüstrilerde doğru ve etkin politikalar uygulanması zorunluluğu önem kazanmıştır.

Bu politikaları dört başlıkta toplamak mümkündür⁵:

A - Ulusal güvenliğin ve stratejik önceliklerin yeniden tanımlanması.

B - Ulusal ve uluslararası savunma kapasitelerinin uygun düzey devamlılığı sağlanırken diğer yandan savunma endüstrisi faaliyetlerinin azaltılması.

Bir yandan asker sayısı azaltılıp hantal organizasyon sistem ve yapıtaşları ortadan kaldırılırken diğer taraftan insan ve sermaye açısından büyük yatırım gerektiren ar-ge yoğun yüksek teknoloji alan ve uygulamalarına öncelik tanınmaktadır.

C - Savunma sanayiindeki kapasitenin sivil sektöre kaydırılması.

³ **I. Bilim Teknoloji Şurası**, 14-16 Mayıs 1990, Tübitak Yayın – Dağıtım Daire Başkanlığı No: 92-0040, 4. Komisyon Raporu, “Endüstriyel Araştırma-Geliştirme Faaliyetleri”, s:110.

⁴ **I. Bilim Teknoloji Şurası**, 14-16 Mayıs 1990, Tübitak Yayın – Dağıtım Daire Başkanlığı No: 92-0040, 3. Komisyon Raporu, “Uluslararası İlişkiler”, s:9.

⁵ Philip Gummett, “West European Defence Industrial Policy After the Cold War”, **Military R&D After The Cold War; Conversion and Technology Transfer in Eastern and Western Europe**, Ed.: Philip Gummett, Mikhail Boutoussov, Janos Farkas, Arie Rip, Kluwer Academic Publishers, Netherlands, 1996, s:34.

Askeri alandaki ar-ge planlarını ve stratejilerini üniversiteler, özel araştırma kurumları, sanayi ile ortak projeler çerçevesinde yürütmek. Yeni fikirlerin yeni perspektiflerin kazanılması yönünde kaynak aktarımıyla birlikte mevcut işbirliklerinin sayısını arttırmaktır.

D - Ticari ve ekonomik gelişmeye zarar vermeden uluslararası askeri know-how ve ekipman akışının kontrol edilmesi.

İngilizleri 2.5 Milyon Kamera İzliyor

11 Eylül sonrasında İngiliz hükümeti, tüm ülkeyi 2.5 milyon akıllı kamera ile donattı. Bu kameralar, suçlu insanları ve aranan taşıtları tanıyıp, güvenlik güçlerini alarma geçirebiliyor. Her İngiliz vatandaşı artık günde ortalama 300 kez bu kameralar tarafından görüntüleniyor.

George Orwell'ın ünlü romanı 'Big Brother' İngiltere'de gerçek oldu. 11 Eylül saldırıları sonrasında, Scotland Yard ülke geneline 2.5 milyon akıllı gizli kamera yerleştirdi. Bu kameralar 24 saat boyunca İngiltere sokaklarını izliyor ve aranan suçluları tanıyarak polisi harekete geçiriyor. Dünyanın en büyük güvenlik yatırımı olarak gösterilen bu sistem ile birlikte her İngiliz vatandaşı günde ortalama 300 kez bu kameralar tarafından görüntüleniyor. İngiliz hükümeti, güvenlik konusunda yapılan bu yatırımın Başbakan Tony Blair'ın koyduğu '2005 yılına kadar e-devlet olma' hedefinin bir adımı olduğunu savunsa da, projenin 11 Eylül sonrasında İngiltere'nin Afganistan'a yapılan harekatta ABD'nin yanında yer alması sonrasında hayata geçirilmesi dikkat çekiyor.

Nasıl Çalışıyor?

Scotland Yard'ın kurduğu ve bir benzeri ABD'de de kullanılan sistem şöyle işliyor.

- *Görüntüleri dijital olarak yakalayan 2.5 milyon CCTV gizli kamera, özellikle insan nüfusunun yoğun olduğu bölgelere yerleştirildi.*
- *Scotland Yard, kötü niyetli kişileri yanıltmak için, görünür yerlere de 'yem kameralar' koydu. Böylece, bu kameralardan kaçmaya çalışanın, gizli kameraların denetimindeki bölgeye yönlendirilmesi hedeflendi.*
- *Kameraların yakaladığı görüntüler, 24 saat boyunca oluşturulan özel izleme merkezlerine aktarılıyor.*
- *İzleme merkezlerinde, kameralardan gelen dijital görüntüler özel bir yazılım ile analiz ediliyor ve bu görüntüler Scotland Yard arşivlerindeki sabıka kayıtları ile karşılaştırılıyor.*

Şüpheliyi Yakalıyor

Akıllı güvenlik sisteminin en önemli özelliği ise, bu sistemin bağlı olduğu bilgi işlem merkezindeki bir yazılım. Bu yazılım, suç işleme eğilimindeki veya suç işleyen insanların

davranışlarını analiz edebiliyor. Böylece, gelen görüntülerde, suç işlemiş insan davranışı sergileyenler de ‘şüpheli’ olarak izleniyor.

Akıllı güvenlik sistemi, sadece insanları izlemekle kalmıyor. Bu kameralar, araçları da takip edebiliyor. Kameralar, emniyet güçlerinin aradığı plakaya veya renk ve modele sahip araçları birkaç saniye içinde tespit edebiliyor.

Tartışma Yarattı

ABD’de de bazı eyaletlerde lokal olarak uygulanan bu güvenlik sistemi, bazı kesimlerden tepki alıyor. İngiliz ve ABD’liler, uygulamanın “özel hayatın gizliliği” ilkesine aykırı olduğunu savunuyorlar.

Kaynak: Mustafa Kutlay, *Hürriyet Gazetesi*, 13 Eylül 2003, s:12.

www.meslekiyeterlilik.com[®]

5.2. Tekno-Güvenlik Kavramı ve Temel Problem Türleri

Ulusal güvenlik alanında teknoloji tabanlı problemi üç ana başlık altında toplamak mümkündür⁶:

- a – Çevre Tabanlı Tekno-Güvenlik Problemleri
- b – Bilgi Tabanlı Tekno-Güvenlik Problemleri
- c – Askeri Tabanlı Tekno-Güvenlik Problemleri.

5.2.1. Çevre Tabanlı Tekno-Güvenlik Problemleri

Teknolojinin yaratmış olduğu problemlerin başında çevre kirliliği, kaynakların zarar görmesi ve kontrolsüz kullanımı gelmektedir. Bu tip tekno- güvenlik problemlerini aşağıdaki gibi sıralayabiliriz⁷ :

- 1- Karbondioksit türevlerinin meydana getirdiği küresel ısınma ve oluşturduğu problemler (iklim değişimleri, düzensizlikleri vb.)
- 2- Ozon tabakasının zarar görmesi
- 3- Atık ve artıkların denetimsizliği
- 4- Nüfus artışının getirdiği problemler

⁶ Murat Erdal, “Tekno-Güvenlik Problemlerinin Uluslararası İlişkilerdeki Yeri ve Türkiye”, **İstanbul Üniversitesi, Siyasal Bilgiler Fakültesi Dergisi**, Sayı:21-22, Ekim 1999- Mart 2000, İstanbul 2000, s.:23-34.

⁷ Kozo Iizuka, “Innovation and Transfer of Industrial Technology – Experience and Problems of Japan”, **Development and Transfer of Industrial Technology**, Ed.: O.C.C. Lin, C. T. Shih, J. C. Yang, Elsevier, Amsterdam, 1994, s:87.

- 5- Asit yağmurları
- 6- Enerji ve kaynak kullanımında yaşanan problemler
- 7- Çeşitli teknolojik kazalar (radyasyon yayılımı, petrol kirliliği vb.)
- 8- Askeri faaliyetlerin sonucunda meydana gelen problemler
- 9- Teknolojinin sağladığı kolaylaştırıcı imkanlarla sınırsız avlanma ve türlerin yok oluşu.

Konuya uluslararası ilişkiler açısından bakıldığında değişik boyutlar ortaya çıkmaktadır. Bu konudaki sorumluluğun tek bir ülke veya tarafa değil bütün dünya ülkelerine ait olması gerekir çünkü kaynaklar sınırlıdır ve tek bir dünya vardır. Çevre tabanlı sorunların çözümü ancak uluslararası alanda ortak mutabakat çerçevesinde çözümlenebilir. Son dönemde yaşanan çevre tabanlı tekno-güvenlik problemlerine örnek olarak Romanya’da altın arama faaliyetlerinde kullanılan kimyasal maddelerin Tuna nehrine karışmasını vermek mümkündür. Nehrin uzunluğu ve geçtiği ülkeler düşünüldüğünde söz konusu kirlenmenin ve çevreye vereceği zararın boyutlarının ne denli büyük olacağı daha iyi anlaşılacaktır.

Türkiye’nin son yıllarda yaşadığı Çernobil Nükleer Santral felaketi ve etkileri, yurt dışı kökenli firmaların Bergama’da altın arama ve çıkarma işlemleri ve bunun sonuçları, Gökova Termik Santrali ve kuruluş yeri seçiminin hatası gibi birçok örnek verilebilir.

Yeni ekonomik düzende, küresel rekabet ortamında ise bunun tam olarak sağlanabilmesi şimdilik pek mümkün gözükmemektedir. Gelişmiş ülkeler açısından avantajlar ve öncelikler ile az gelişmiş ve gelişmekte olan ülkeler açısından durum değerlendirmeleri farklılıklar taşımaktadır.

Az gelişmiş ülkeler uluslararası ekonomik alanda fazla söz sahibi değildirler. Bu düzeydeki ülkelerin öncelikli problemleri arasında gelir dağılımındaki dengesizlikler; yoksulluk, beslenme, sağlık, eğitim gibi temel insan ihtiyaçlarının karşılanamaması gelmektedir.

Kullandıkları teknolojiler ağırlıklı olarak “emek yoğun” teknolojiler olup genelde gelişmiş ülkelerin artık vazgeçtikleri ya da vazgeçmek üzere oldukları “ikinci el teknoloji” ürünü olan makine teçhizat ile imalat yapmaktadırlar. Bu ülkeler açısından ileri teknoloji ürünleri kullanmak son derece maliyetlidir.

Atık yönetimi, çevre dostu ürünlerin üretimi, yeşil yönetim, ISO 14000 çevre standartlarına uygun imalat gibi kavram ve uygulamalar az gelişmiş ülkelerin birincil öncelikleri arasında yer almadığı gibi son derece lüktür.

Gelişmiş ülkeler ise acımasız rekabet ortamının sürükleyicileri olup tekno-küresel problemlerin çözümündeki yansımaların getireceği maliyetlerden dolayı konuya pek sıcak bakmamaktadırlar. Bu ülkelerde satılan her ürün belirli standartlara ve mevzuatlara uymak zorundadır. Az gelişmiş ülkelerin bu mevzuat ve düzenlemeleri aşması ise hiç kolay değildir.

Gelişmiş ülkeler çoğunlukla kendileri için ek maliyet gerektiren, çevreye zarar verebilecek atık oranı fazla olan ürünlerin imalatını az gelişmiş ülkelere transfer etmekte, işlerini bu yolla yürütmektedirler.

Az gelişmiş ve/veya gelişmekte olan ülkeler ise yabancı sermayeden yararlanabilmek uğruna gelecek yatırımların, teknolojilerin doğurabileceği çevre tahribatını gözardı etmektedirler.

Tekno-küresel problemlerin ortadan kaldırılmasında ortak mutabakata varmak her ne kadar zorunluysa da yeter şart olarak görünmemektedir. Buna ilave olarak az gelişmiş ülkelerin aktif şekilde teknoloji transferi ile bilinçlendirilmesi ve desteklenmesi gerekmektedir.

5.2.2. Bilgi Tabanlı Tekno-Güvenlik Problemleri

Çevre tabanlı tekno-güvenlik problemlerin dışında diğer bir güvenlik problem alanı “bilgi tabanlı tekno-güvenlik problemleri”dir. Günümüz toplumu bilgi toplumudur ve bilgi unsurunu en etkin kullanım ortamlarının başında bilgisayarlar ve bilişim teknolojisi gelmektedir.

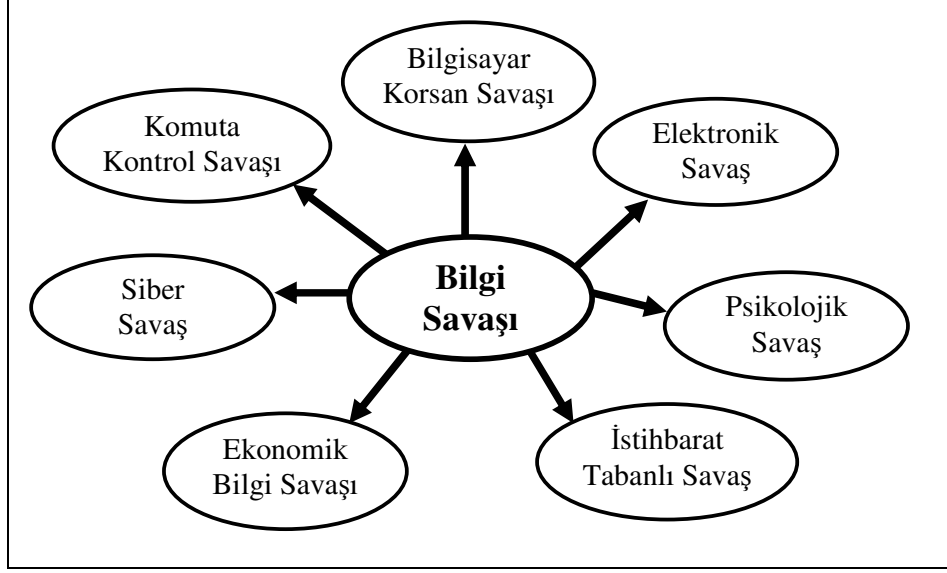
Bilgisayar ortamındaki bu tip problemler “**sanal ortam tehditleri / bombaları**”, “**bilgi / bilişim savaşları**”, “**dijital savaş teknikleri**”, “**siber savaş**” “**bilgi tabanlı problemler**” gibi çeşitli isimlerle adlandırılmaktadır.

Bilgi savaşları teknik ve uygulamaların birçoğu tarihte uygulanmış ve bilinen savaş teknikleridir. Bugün gelinen nokta ise daha hızlı düşünmek ve daha hızlı hareket etme zorunluluğudur.

Bilgi savaşlarını yedi alt başlıkta incelemek mümkündür. Bunlar⁸;

- Komuta Kontrol Savaşı (C2W: Command-and Control Warfare),
- İstihbarat Tabanlı Savaş (IBW: Intelligence-Based Warfare),
- Elektronik Savaş (EW: Electronic Warfare),
- Psikolojik Savaş (PSYW: Psychological Warfare),
- Bilgisayar Korsan Savaşı (Hacker Warfare),
- Ekonomik Bilgi Savaşı (EIW: Economic Information Warfare) ve
- Siber Savaş (Cyber Warfare).

⁸ Martin Libicki, “What is Information Warfare ?”, Institute for National Strategic Studies, <http://www.ndu.edu/inss/actpubs/act003/a003ch02.html>, Erişim Tarihi:30.06.2001, s:1.



Şekil-1 Bilgi Savaşı Türleri.

Kaynak: Martin Libicki, "What is Information Warfare ?", Institute for National Strategic Studies, <http://www.ndu.edu/inss/actpubs/act003/a003ch02.html>, Erişim Tarihi:30.06.2001, s:1.

Komuta Kontrol Savaşı (C2W: Command-and Control Warfare)

Temel amacı komuta kontrol zincirinin kırılmasına dayanan bilinen en eski askeri stratejilerden biridir. Körfez Savaşı ve 2003 yılındaki ABD'nin Irak Operasyonunda görülen elektronik savaş teknikleri uygulamalarında öncelikli savaş alanı yönetim kademeleri yani askeri kurmay düzey (anti head, anti neck) ile operasyonel düzey, uçta savaşan birlikler arasında bağlantıları sağlayan haberleşme ve iletişim sistemlerinin imhası önde gelmiştir.

İstihbarat Tabanlı Savaş (IBW: Intelligence-Based Warfare)

İstihbarat tabanlı savaş, rakibin her hareketini önceden sezebilme ve olası sürprizlere karşı hazırlıklı olma amacına yöneliktir. Operasyon sahasından gelen bilgiler bu açıdan büyük önem taşır. Sahada meydana gelen her türlü gelişmenin karar merkezlerine hızlı ve doğru bir şekilde aktarımında büyük ölçüde yeni teknoloji ürünü araç-gereçlerden yararlanılır. Uzaktan algılama cihazları, uydu takip sistemleri, radarlar ve bilgisayarlar vb. teknolojilerle her türlü bilgi kısa sürede ve net bir şekilde elde edilebilmektedir. Niteliğine göre saldırı ve savunma odaklı olmak üzere iki tür istihbarat tabanlı savaştan bahsetmek mümkündür.

Elektronik Savaş (EW: Electronic Warfare)

Elektronik savaşın temel hedefi anti-radar sistemleri, şifreleme ve anti-iletişim üzerine dayanmaktadır. Rakibin hareketlerini, bilgi akışını ve iletişim sistemini çözmek bunun yanı sıra kendi faaliyetleriyle ilgili ipuçları vermemeyi amaçlayan bu savaş türü elektronik alanındaki teknolojik bilgi birikimi ve yetenekle doğru orantılıdır.

Psikolojik Savaş (PSYW: Psychological Warfare)

Psikolojik savaş, insan beynine odaklaşarak onun duygu ve düşüncelerini etkilemeyi amaçlamaktadır. Psikolojik savaş türlerini temelde dört sınıfta toplamak mümkündür. Bunlar;

- Milli iradeye karşı faaliyetler,
- Rakip komutanlara karşı faaliyetler,
- Rakip birliklere karşı faaliyetler ve
- kültürel anlaşmazlık veya kültürel çatışmalara yönelik faaliyetlerdir.

Bilgisayar Korsan Savaşı (Hacker Warfare)

Bilgisayar korsan savaşı olarak tanımlanan bu türde rakipler coğrafi mekan sınırlaması olmaksızın kilometrelerce öteden birbirlerine zarar verebilmektedir. Üst düzey bilişim teknolojisi bilgisi ve uzmanlık gerekmektedir. Bilgisayar korsanları askeri veya ticari bilgi sistemlerine girebilmekte güvenlik problemlerine yol açabilmektedirler. Rakip olarak hedeflenen ülke, kişi veya kuruma ait sistemlerde zarar meydana getirmek, geçici veya tamamen durmasını sağlamak, stratejik dosya ve bilgileri kendi çıkarları doğrultusunda kullanmak gibi çok çeşitli amaçları olabilmektedir.

İşten Atılan Hackliyor

FBI tarafından yapılan araştırmalara göre ABD’de işten çıkarılan her 100 kişiden 81’i eski şirketlerine dijital saldırıda bulunuyor. Ülkelerin yüzde 21’i diğer ülkelerin sistemlerini çökertiyor. Her 100 firmadan 44’ü rakip şirketin bilgilerine saldırı yoluyla ulaşıyor.

Günümüzün teknolojik devrimi internet kendi kazdığı kuyuya mı düşüyor? 1970’li yılların başında hiçbir güvenlik kaygısı olmadan geliştirilen sistem bugün dijital saldırılara karşı korunmaya çalışıyor. Firmalar sistemlerini çökerterek kendilerini milyonlarca dolarlık zarara uğratan saldırılara çözüm bulunmasını istiyorlar. Sınırsız iletişim ve bilgi özgürlüğünün mekanı internet ‘güvenlik’ savaşı veriyor.

FBI dijital saldırılara karşı savaş açan kurumların başında geliyor. Kurum tarafından yapılan araştırmalara göre ABD’deki kuruluşların %90’ı bugüne kadar en az bir kez dijital saldırıya uğradı. Bu kuruluşların yüzde 70’inin gizli bilgileri çalındı yada zarar gördü.

Araştırmaya göre dijital saldırıların büyük bölümü iç kaynaklı. Örneğin işten çıkarılan her 100 çalışanın 81’i eski şirketine dijital saldırı girişiminde bulunuyor. Bu kişilerin yaptıkları saldırılar verdikleri zararların boyutuna göre değişiyor. Hangi seviyede olursa olsun bir çalışanın bazı şifreleri biliyor olması zarar vermesine yetiyor.

Araştırmaya göre her 100 firmadan 44'ü rakip firmaların sistemlerini çökertiyor. Yalnızca şirketler değil devletler de dijital saldırı yapıyorlar. Buna göre dünyadaki ülkelerin yüzde 21'i diğer devletlere ait bilgi işlem sistemlerine ulaşmak için dijital saldırılar düzenliyorlar.

Türkiye'deki dijital saldırılarla ilgili verilere ulaşmak kolay değil. Çünkü birçok firma dijital saldırıları imaj zedeleyici bir durum olarak niteliyor ve saldırıya uğradığını gizliyor. Hackerların buluşma noktası olarak kabul edilen ancak bir süre sonra yayından kaldırılan www.alldas.de adresli siteye göre Türkiye'de 2001'in ilk beş ayında çökertilen site sayısı 49, ancak e-güvenlik uzmanlarına göre bu rakam çok daha büyük.

Dijital saldırıların boyutu ve sayısı her geçen gün artıyor. Son zamanlarda kamu oyunu en çok meşgul eden 'Nimda', 'I Love You' ve 'Code Red' adlı üç virüs çeşidi dünya genelinde yaklaşık sekiz milyar dolarlık maddi zarara yol açtı.

TÜRKİYE'DE DURUM

FBI'nın 150 şirketin bilgi işlem yöneticileri arasında yaptığı bir başka araştırmaya göre ABD'de 2001 yılında dijital saldırıya uğrayan firma sayısı geçen yıla oranla yüzde 100 arttı ve 40 bine ulaştı. Yöneticilerden 60'ı, şirketlerinin ciddi bir e-güvenlik politikası olmadığını söylüyor.

Firmalara dijital güvenlik hizmeti veren InfoNet'in Genel Müdürü Taner Özdeş, bir firmanın öncelikle doğru bir e-güvenlik politikasına sahip olması gerektiğine dikkat çekiyor: "E-güvenlik profesyonellerin işidir. Düzenli olarak güvenlik değerlendirmesi yapılmalı ve bu doğrultuda önlemler alınmalı. Önlemlerin sürekli güncel tutulması gerekiyor. Fortune 1000 firmalarının geçen yıl 45 milyar dolarlık bilgi hırsızlığına uğramasının arkasında yatan neden bu firmaların e-güvenlik önlemleri almamaları değil, mevcut önlemlerini periyodik olarak güncellememeleri."

Kaynak: Hürriyet İnsan Kaynakları, 10 Mart 2002, Pazar, s:20.

Ekonomik Bilgi Savaşı (EIW: Economic Information Warfare)

Bilgi savaşı ve ekonomik savaş kavramlarının birleşiminden meydana gelen bu türün özünde bilginin bloklanması yani engellenmesi ve bilgi emperyalizmi bulunmaktadır. Dünyada birçok ülke dış ticaretini belirli kalemde malların satışı üzerine dayandırmaktadır. Bazı ülkeler sadece yer altı zenginliklerini bazıları ise sadece gıda, yaş sebze ve meyve gibi ürünleri ihraç edebilmektedir. Bu ülkeler için belirli sektörler için bilgiler hayati önem taşımaktadır. Dünyada o alanda doğru veya yanlış çıkan haberler, dedikodular, istatistikler, sağlığa veya diğer sektörler için etkileri gibi yayınlar ülke dış ticaretini ve dolayısı ile ekonomisini doğrudan etkileyebilmektedir.

Siber Savaş (Cyber Warfare)

“Bilgi terörizmi”, “semantik saldırılar”, “simüle edilmiş savaş stratejileri”, “gelecek senaryoları” ve “sanal karakterlerin kullanımı” siber savaş anlayışının temel referans kaynaklarıdır.

Önceleri sivil ve askeri alandaki önemli bilgilere ulaşma ve izleme şeklinde beliren bu tip uygulamalar zamanla değişim göstermiştir. İlegal olarak bilgisayar sistemlerine girmek, izlemek, verilerin kopyalanması yani çalınması artık neredeyse sıradan hale gelmiştir.

Dünya çapındaki bilgisayar-iletişim ağları bu tip problemlerin uluslararası boyutta yayılmasını ve büyümesini arttırmaktadır. Sanal ortam tehlikelerinin başında yukarıda sözü edilen bilgisayar korsanlığı ve virüsler gelmektedir. Bu tür tehdit ve sorunların meydana getirdiği problemlerin çözümü uygun donanım-yazılım sistemleri, kalifiye insan gücü gerektirmekte ayrıca yüksek para ve zaman maliyetleri oluşturmaktadır

Bu tür tekno-güvenlik problemlerinin yol açacağı sorunlar çok çeşitli tipte olabilir. Barajlar, enerji santralleri, hava alanları, haberleşme ve ulaşım sistemleri, veri bankaları, savunma sistemleri gibi ulaşılabileceği her türlü bilgisayar ortamında ortaya çıkabilir. İstenilen sürelerde kısmi veya tamamen kullanım dışı kalmasına neden olabilir.

Siber Savaş Başladı !

Bush'un, Irak politikası Amerikan sitelerini hedef haline getirdi ve aşırı İslamcı hackerlar sorunu internette savaşa dönüştürdü. AOL Time Warner grubuna ait web sitelerine 8 Eylül tarihinde üç büyük saldırıda bulunuldu. Saldırının ardında kendilerine USG adı veren İslamcı bir hacker grubu çıktı. Sitelerin ön sayfalarına yerleştirilen mesajlarda Irak'ın işgalini eleştiren ifadeler yer aldı.

Online güvenlik kuruluşu mi2g, İslamcı hacker grubunun Eylül ayı içerisinde ABD sitelerine dört önemli saldırı daha gerçekleştirdiğini, grubun kurulduğu Mayıs ayından beri 155 siteye saldırdığını açıkladı. Bu saldırıların hedefleri arasında ABD'deki banka gruplarının da bulunduğu açıklandı.

Diğer bir aşırı İslamcı hacker grubu AIC ise Temmuz ayından bu yana Amerikalı sanal hedeflere 454 saldırı gerçekleştirdi, WFD adı verilen başka bir grup ise geçen Kasım ayından beri faaliyet gösteriyor ve onlar da 400 siteye zarar verdiler.

ALTYAPI SALDIRILARI

Balkanlar'da yaşanan iç savaş ve 1999 yılındaki Çin Tayvan gerginliğinden beri siber terörizm gerçek dünyada yaşanan siyasi gelişmelerden fazlasıyla etkileniyor. Son yıllarda Ortadoğu'da artan gerginlik İsrail web sitelerine ve ağlarına karşı yapılan saldırıların rekor sayıda artmasına neden oldu.

Web sitelerine gerçekleştirilen saldırıların yanı sıra, online bilgisayar ve ödeme

sistemleri de hackerların hedefleri arasında. Bazı hackerların tek hedefi ise rahatsız etmek istedikleri ülkelerin ulusal ve kurumsal altyapılarına zarar vermek.

Bu saldırıların başarıya ulaşması ulaşım, telekomünikasyon ve finansal sistemlerin yıkılmasına yol açabilir. Ancak, ciddi bir şekilde korunan altyapı ağlarının çökertilmesi oldukça güç ve genellikler içerden destek verilmesi gerekiyor.

Kaynak: “Siber Savaş Başladı !”, NTVMSNBC Web Sitesi, Erişim Tarihi: 24.11.2003, <http://www.ntvmsnbc.com/news/175196.asp#BODY>.

Siber-Terörizm Örnekleri

Terörizm bir yönetimi(devlet) veya bir topluluğu, korkutmak veya baskı amaçlı, sosyal ve siyasi amaçlara yönelik olarak insanlara veya mülkiyete karşı kanunsuz güç ve şiddet kullanımınıdır (FBI). Siber terörizm ise klasik terörizm amaç ve hedeflerine ulaşmada bilişim teknolojilerinden faydalanılmasını ifade etmektedir.

Klasik yöntemler olarak bilinen, suikast, rehin alma, adam-uçak kaçırma veya gerilla savaşı yerine terörist neden interneti kullanmayı tercih eder? Bu tür eylemlerde sorunun bir parçası, teröristin bir resmi görevliyi öldürdüğünde onun yerine başka birinin her zaman geçtiği gerçeğini kavramaya başlamasıdır. İnterneti kullanarak terörist birilerini öldürmekten daha fazla zarar verebilir veya amacına ulaşabilmesidir. Bir ülkenin güvenliğini geniş bir coğrafyanın enerjisini keserek devre dışı bırakabilir. Böylelikle daha fazla insanı, daha az risk olarak etkileyebilmekte ve panik yaşatabilmektedir.

Siber terörizm çok çeşitli şekillerde olabilmektedir. En çok duyulan şekli popüler olan bir bankayı bilişim teknolojilerini kullanarak korkutmak veya tehdit etmektir. Siber-terörist bankanın bilgisayar güvenlik altyapısını işe yaramaz hale getirerek yöneticilere amaçlarına uygun bir mesaj bırakırlar. Teröristler, istediklerini belirli bir süre içinde alamadıkları takdirde (ki çoğu zaman bu yüklü miktarda paradır) kuruma ait gizli belgelerin zarar göreceğini, müşteri dosyalarının silineceğini ya da şubelerle olan ağ yapısı bilgi akışının işlevselliğini kaybedeceğini bildirirler. Böyle bir durumda zanlıyı yakalamak çok zordur. Bilişim suçunun niteliği, kim tarafından ne zaman ve nasıl işlendiği, potansiyel suçlunun hangi ülkede olduğunun tespiti, kanıt toplama ve ispat, uluslararası ilişkiler ve anlaşmalar gibi birçok alanda sıkıntı yaşanmaktadır. Bütün bu alanlarda yaşanan sıkıntılar ise siber teröristin işine gelmekte izini kaybettirebilmektedir. Diğer taraftan siberterörist saldırıya uğrayan banka, finansal kurum veya şirket ise bu tür bir saldırıya maruz kaldığını kendi imajı ve güvenilirliği açısından çoğu zaman kamuoyu ile paylaşmamaktadır.

Siber teröristler genellikle terörizm hareketlerini kişisel kazanç sağlamak için işlemektedirler. Bu tür faaliyette bulunan gruplardan biri 1997 yılında kurulan Kaos Bilgisayar Kulübü (Chaos Computer Club)dür. Kulüp üyeleri Quicken muhasebe programı değiştirerek başkalarının banka hesaplarından para çeken bir Active-X yazılım programını

yazdılar. Dünyanın birçok yerinde Active-X yazılım programını bilgisayarına yükleyen insanlar bunun bedelini banka hesaplarından çalınan tasarruflarıyla ödediler.

Çoğu zaman siber teröristler halkın ve kamuoyunu dikkatini çekmeye çalışmaktadırlar. Örneğin **truva atı (trojan horse)** ve **ağ kurtları (network worms)** gibi bilişim savaşı tekniklerinden olan virüsler sadece bilişim altyapılarına zarar vermesi için değil aynı zamanda virüs tasarımcısının kendini ispatlama ve gösterme çabası yüzünden de kullanılır. Bu durum ciddi bir ahlaki problemdir, çünkü bir çok kişi ve kurum bilgisayar virüslerinden etkilenmektedir. Çoğu insan bilgisayar konusunda uzman değildir ve virüslerle mücadele konusunda bilgileri yetersiz kalır. Yaratılan bilgisayar virüs yazılımlarının zaman, emek ve ekonomik maliyeti ise çok büyük kayıplar olarak karşımıza çıkmaktadır.

Siber terörizmin sıra dışı kullanım alanlarından biri de suikasttır. Örneğin hastanede yatan bir hastanın tedavisinde kullanılan ilaçlar bilgisayar sistemine girilerek değiştirip ölümcül ilaçlar almasına sebep olunabilir. Böyle bir olay bir çete liderinin başına gelmiştir. Vurulup hastaneye kaldırılan çete liderinin ilaç listesi, hastane bilgisayar sistemine giren siber-teröristler tarafından değiştirilmiştir. Çete lideri ölümcül bir iğne olarak birkaç saat içinde ölmüştür. Daha sonra suikastçılar bilgisayar kayıtlarında bulunan ilaç listesini eski haline getirmiş, böylece hemşirelerin suçlu görünmelerine sebep olmuşlardır. Hastanenin güvenilirliğini ve prestijini ciddi bir şekilde zedelenmiştir.

Siber terörizmin bir diğer şekli ise yanlış, eksik veya hatalı bilgi (disinformation) üretmek ve/veya internet üzerinde asılsız söylenti yaymaktır. Bu biçim kalabalık bir mekanda örneğin bir tiyatro veya sinema salonunda “yangın var” diye bağırarak gibi etki yaratabilir. Fakat etkilenen insan sayısı sınırlı değildir.

Siber terörizmin bir diğer uygulama alanı da bilgisayar içindeki bilgileri değiştirmek şeklinde gerçekleşmektedir. Sağlık veya finansal kayıtların değiştirilmesi ve şifrelerin çalınması en sık karşılaşılan tipidir. Teröristler bilgisayara giriş yetkileri olan kişilerin bilgisayarlarını kullanmasını engelleyebilir ya da elektronik posta şifresini öğrendiği kullanıcı adına yüzlerce uygunsuz e-postalar gönderebilir. Bu bireysel hak ve özgürlüklere doğrudan saldırıdır ve kişinin gizlilik ve mahremiyetine büyük zarar vermektedir.

İnternette Gizli Mesaj Trafiği Nasıl İşliyor ?

İnternetteki gizli haberleşme olanağından teröristler de yararlanıyor. Dijital iletişime tam denetim mi gerekiyor ?

Dünya Ticaret Merkezi'ne yapılan saldırıdan sadece birkaç saat sonra internette de hummalı bir araştırma başladı. AOL gibi internet şirketleri Amerikan Federal Polisine (FBI) verileri iletirken, Alman üniversiteleri de suçluların e-postalarını aramaya başladılar.

Elektronik ortamda yapılan araştırma ilk başta sadece teröristlerin uçak biletlerini internet üzerinden satın aldıklarını ortaya çıkardı. FBI' a göre teröristler bu iş için Florida'daki Kinko Copyshop İnternet merkezinden yararlanmışlardı. Ayrıca, en azından bazı teröristlerin birbirlerini yalnızca internet aracılığıyla tanıdıkları da anlaşıldı.

Amerika Őu anda da veri akıŐlarındaki Őüpheli kavramları, geliŐmiŐ filtrelerle süzüp toplayan DCS 1000 (eski adı: Carnivore= etobur) adında bir internet izleme sistemi mevcut. Fakat “etobur” veya Echelon gibi dünyaca ünlü dinleme sistemleri de ŐifrelenmiŐ mesajlar karŐısında çaresiz kalıyor. Çünkü internette ücretsiz olarak sunulan Őifreleme programları e-postaları karmaŐık bir veri sahasına dönüŐürtmekte ve dünyanın en geliŐmiŐ bilgisayarları bile esas metni bulamıyor.

“Gönderen ve alıcı, yürürlükte olan bir Őifreleme software programını kullanıyorsa bunu dünyadaki hiçbir güvenlik sistemi kıramıyor” diyor kriptoloji uzmanı Albert Beutelspacher. Çünkü ŐifrelenmiŐ mesajlara ulaşabilmek için Amerikan güvenlik kuruluŐu (NSA) bile henüz olası tüm Őifreleri deneyerek çalıŐıyor.

KuŐkusuz bu geliŐmelerden de en çok ekonomi etkilenecek. Çünkü Őifreler yalnızca sapıkları ve saldırganları deĐil, bankaları ve müŐterileri de koruyor. “Kriptoloji, finans ve internet ekonomisinin temel direĐidir” diyor Bowden (Casper Bowdan (Londra Institute Foundation for Information Policy Research yöneticisi). Őifreleme tekniĐinde yapılacak küçük bir kolaylık bir anda milyarlarca zarar getirebilir. İnternette mektup zarfları bulunmadıĐından dokümanların Őifrelenmesi kaçınılmazdır.

1993 yılında Dünya Ticaret Merkezi'ne yapılan bombalı saldırının ardından Amerikan hükümeti kriptografiyi önlemeye çalıŐmıŐtı. Fakat bu giriŐim pek iŐe yaramadı. Özel bilgiler güvenli bir biçimde korunmadan elektronik ticaret işlemiyordu. Üstelik bugün gizli mesajlar ŐifrelenmiŐ e-postaya göre çok daha Őık yollardan iletilebiliyor. Mesela stenografiden yararlanılarak, fotoĐraf, video yada müzik verilerine yabancılar tarafından fark edilemeyecek ek bilgiler serpiŐtiriliyor. Oysa alıcı, grafikteki bazı piksellerin görüntü içinde bir metni gizlediĐini anlıyor.

Kaynak: Bilim Teknik, Sayı 762, 27 Ekim 2001, Cumartesi,

DiĐer taraftan NATO'nun Yugoslavya Harekatı sırasında Missouri savaŐ gemisinde yaŐanan e-posta problemi ve yurt dıŐında Türkiye aleyhine yayın yapan yazılı ve görsel medya unsurları ilgi çekicidir.

SavaŐ sırasında en önemli unsurlardan biri askerlerin moral gücünün yüksek olmasıdır. Bunun sağlanabilmesi için, görevli askeri personelin ailesi ve yakınlarıyla iletiŐimin anında kurulması amacıyla bir Internet (Web) sayfası tasarlanmıŐ olup hizmete sokulmuŐtur. Üçbin'den fazla kiŐinin görev yaptıĐı bir ortamda her gün yüzlerce e-mail alınıp yollanmaktadır. Üst rütbeli bir görevli Őöyle demektedir. “EĐer insanlar disiplin altına alınmazsa güvenlik problemleri ortaya çıkar. Personelinize güvenmek zorundasınız. HerŐeyi ailenize anlatamazsınız ve biz bütün e-posta'ları kontrol etmek zorundayız.” E-posta kontrolü

için ayrı bir birim oluşturulmuştur. Bu durum üçbin'den fazla insanın görev aldığı bir gemide herkese eşit derecede güven duyulamadığının bir göstergesidir⁹.

Türkiye açısından uluslararası ilişkiler kapsamında bilişim temelli güvenlik problemlerinin başında ülke aleyhinde yayın yapan internet, televizyon, radyo, gazete ve dergiler gelmektedir. Bunlardan en çok bilineni uydu destekli olarak geniş bir yelpazede televizyon yayımlarının yaptırılmasıdır. Konu iki açıdan önem taşımaktadır.

Bunlardan ilki siyasi ve teknolojik destek veren devlet ve Türkiye ilişkileridir. Diğeri ise teknolojinin güvenlik açısından hangi boyutta bir tehdit oluşturduğunun ve bu tür uygulamaların nasıl bir psikolojik savaş enstrümanı olarak kullanıldıklarının gözlemlenmesidir.

Dışışleri'ne Özel Telefon Hattı

Askerden sonra Dışışleri Bakanlığı'da kendi özel haberleşme sistemini kurmaya hazırlanıyor. Başkaları tarafından dinlenmesi mümkün olmayan özel hat, bakanlık ile yurt dışı temsilcilikler arasındaki çok gizli görüşmeler için kullanılacak.

Genel Kurmay Başkanı Orgeneral Hilmi Özkök'ün "Telefonlarımız dinleniyor" açıklaması ile yeniden gündeme gelen "telekulak sorunu" Dışışleri Bakanlığı'nı da harekete geçirdi.

Genel Kurmay Başkanlığı'nın ulusal güvenlik nedeniyle kendi özel haberleşme sistemini oluşturmasının ardından Dışışleri Bakanlığı da kendi özel hattını oluşturmak için düğmeye bastı. Dışışleri Bakanlığı yurt dışı temsilcilikleriyle "Çok gizli" görüşmelerini gerçekleştirmek için Türk Telekom'la "Özel hat" projesi üzerinde çalışmalara başladı.

İnternet Desteği

Bakanlığın ulusal güvenliği tehdit edebilecek dinleme olaylarının önüne geçebilmek için yürüttüğü çalışma ile Dışışleri Bakanlığı'nın Bağdat'taki merkez binası ve Türkiye'nin yurtdışı temsilcilikleri arasında uydu aracılığıyla bir hat oluşturulacak. Türksat'ın kullanılacağı bu hat aynı zamanda, sağlıklı internet erişiminin sağlanamadığı Türk temsilciliklerinin bulunduğu ülkelerde data iletişiminin güçlendirilmesi için de kullanılacak.

Maliyet Azalacak

Henüz proje üzerinde çalışmalar yaptıklarını belirten Türk Telekom Genel Müdürü Mehmet Ekinalan, proje ile servis kalitesini arttırmayı planladıklarını söyledi. Şu an bakanlığa bağlı dış temsilciliklerin merkezle görüşmelerinde verimsiz kanallardan yararlandığını belirten Ekinalan, yeni hatlar sayesinde gizlilik derecesi önem taşıyan

⁹ International Herald Tribune, 27.5.1999, s:8.

bilgilerin deęişiminin daha güvenli yapılacağını vurguladı. Proje ile temsilciliklerin Ankara ile haberleşmesi daha ucuza mal olacak.

Kaynak: Ümit Çetin (Ankara), *Hürriyet*, 8 Kasım 2003 Cumartesi, s:21.

5.2.3. Askeri Tabanlı Tekno-Güvenlik Problemleri

Dünyada bütün askeri organizasyonlarda daima en iyi performansı yakalamak temel amaçtır. Askeri araç-gereç ve sistemlerindeki ilerlemelerin hız kazanması ise teknolojinin çok hızlı seviyede gelişiminden kaynaklanmaktadır. Bütün temel bilimlerde sağlanan ilerlemeler beraberinde yeni birtakım anlayış ve uygulamaları getirmektedir. Bilgisayar ortamında artık bir çok kayıt, bilgi depolama, transfer etme, hesaplama daha kısa sürede ve hatasız bir şekilde yapılabilmekte, çeşitli deneyler ve simülasyonlar gerçek verilerle test edilebilmektedir.

Askeri araç-gereç ve sistemlerinde yüksek teknoloji ve onun ürünlerinin kapsamı bir hayli geniştir. Uzaktan algılamadan radar teknolojisinden tek bir tuş ile füzeyi yüzlerce kilometre uzakta belirlenen koordinatlara isabet ettirmeye, oradan uydu haberleşmesinden uydu gözetleme sistemlerine varıncaya kadar uzanmaktadır. Genetik deneylerden jet uçaklarında yeni malzeme kullanımına, tanklara; nükleer enerji kontrolünden saldırı sistemlerinin bilişim yönetim optimizasyonuna; savunma sistemlerinden muhabere alan koordinasyonlarına kadar her alanda tam bir liderlik hedeflenmektedir. Askeri alanda yaşanmakta olan rekabette belirleyicilik “yüksek teknoloji” ürünü olan silah araç-gereç ve sistemlerden geçmektedir.

Birleşmiş Milletler’in Irak, NATO’nun Yugoslavya Harekatı ve son olarak ABD ve İngiltere’nin Irak Operasyonu günümüz modern savaş cihaz ve teçhizatlarının kullanıldığı en son örneklerdir. Bu kriz ve savaşların sonlandırılmasında yüksek teknolojinin yoğun kullanımının rolü açıktır. Son hareketlerden da görüleceği üzere ülke “savunma odaklı strateji ve anlayışlar” yerini “saldırı odaklı strateji ve anlayışlara” bırakmıştır.

Silah sanayiinde yaşanan rekabetin artmasında “füzyon teknolojileri”nin rolü büyüktür. Yani bir teknolojinin birden fazla alana rahatça uygulanabilir olması, bu alanlarda ve süreçlerde radikal deęişikliklere sebebiyet vermesidir¹⁰.

Teknolojik füzyon kavramının karakteristik özellikleri arasında dięer teknolojilerle işbirliği halinde destekleyici ve tamamlayıcı olabilmesi; buna karşılık yayılışının doğrusal olmaması gibi unsurlar bulunmaktadır¹¹. Örnek vermek gerekirse biyo-teknoloji ve genetik alanındaki gelişmelerle insan geni, şifreleme vb. çalışmalar hız kazanmıştır. Yine bu alanda biyolojik savaş üreticilerine yeni birtakım fırsatlar doğmaktadır. Şarbon, veba ve benzeri virüsleri belirli bir genetik koddaki insan grupları üzerinde aktif hale getirmek veya

¹⁰ David T. Methe, **Technological Competition in Global Industries : Marketing and Planning Strategies for American Industry**, Quorum Books, Westport, 1991, s:210.

¹¹ Fumio Kodama, “Technology Fusion and The New R&D, **Harvard Business Review**, July-August 1992, s:70.

“ABD’nin Ulusal Güvenlik Gereksinimleri” başlıklı 872 sayfalık bir raporda, ABD’ni ziyaret eden Çin vatandaşları; turistler, öğrenciler, iş adamları, akademisyenler, ar-ge kurumlarında çalışanlara kadar incelenmekte ve bilişim akışı konusunda değerlendirmeler yapılmaktadır.

www.meslekiyetlilik.com®

Türkiye ve Sınır Ötesi Harekatlar

Türk Silahlı Kuvvetleri’nin son on yıl içinde BM ve NATO kapsamında Somali, Yugoslavya ve Afganistan’da görev alması, güvenlik problemleri nedeniyle Kuzey Irak’ta sınır ötesi harekatlarda bulunması ordunun uluslararası düzeyde tecrübe kazanmasını sağlamıştır.

Sınır ötesi harekatlarda en önemli unsur “**lojistik yönetimi**”, “**hareket-hız kabiliyeti**” ve “**yüksek vuruş kabiliyeti**”dir. Kuvvetlerin hızlı bir şekilde bir yerden diğer yere aktarılması, birliklerin organizasyonu ve kuvvet bazında yani kara, hava ve deniz birliklerinin koordinasyonu başarı için elzemdir. Lojistik yönetimi, yüksek manevra ve yüksek vuruş kabiliyetinin sağlanmasında yüksek teknoloji ve bilgi kullanımının yoğunluğu artmaktadır.

Örneğin sınır ötesi bir harekata başlamadan önce ihtiyaç duyulan zaruri yedek-hazır parçaların ve yan sanayi ürünlerinin, eğer dışardan geliyorsa, istenilen miktarda ve istenilen zamanda sipariş edilmesi gerekmektedir. Talep olunan parça sayısı ve malzeme miktarının zaman planlamasına uygun olarak gelmesinin gerekli görülen operasyon veya harekatın başarısında önemi büyüktür.

Türkiye karmaşık, özellikli teknolojik silahlar bakımından büyük bir oranda dışa bağımlılığını sürdürmektedir. Türkiye’nin hangi malzemeleri, hangi miktarlarda, hangi takvimde istediği günümüz bilişim sistemleriyle gerek şirket bazında gerekse ülke bazındaki talepleri kolaylıkla izlenebilmektedir.

Bu terminlerdeki sapmalar, yapılması düşünülen operasyon veya harekatların güvenlik derecesinin azalmasına veya gecikmesine, operasyon bölgelerindeki hedeflerin ortadan kalkmasına ve neticede artık gereksiz hale dönüşmesine kadar sürmektedir. Yaşanan birçok siyasi krizde ve askeri anlaşmazlıkta doğrudan veya dolaylı olarak silah ambargosu tehdidi gelmiştir.

5.3. Savunma Sanayii ve Teknolojik Yapı

Dünya silah sanayii pazarı, başta ABD, Almanya, İngiltere ve Fransa olmak üzere teknoloji lideri devletlerin kontrolü altındadır. Japonya teknoloji lideri bir ülke konumunda olmasına rağmen bu pazardan pay alamamaktadır fakat savunma sanayiindeki gelişmeleri yakından takip etmekte, birçok ürünü transfer etmek yerine ilk yatırım maliyeti daha yüksek olan yolu yani kendisinin üretmesini yeğlemektedir. Bundan amaç gerekli teknoloji ve ar-ge yatırım tecrübesinin artırılması, üretim yeteneğinin geliştirilmesi ve insan kaynaklarının bu konuda odaklaştırılmasıdır. Japonya savunma sanayiinde yoğun bir çaba sarf etmekte ve kendi kendine yetebilen bir ülke olma yolunda hızla ilerlemektedir.

Uluslararası pazarlarda, özellikle silah araç-gereç sistem ve donanım pazarlarında rekabet edebilmek hayli zordur. Uluslararası müşteri istek ve ihtiyaçlarına yönelik üretim yapabilmek, küresel ürünlerin ve gereken teknik hizmetlerin zamanında sunulabilmesi uzun vadeli çalışmayı gerektirmektedir. Bu çalışmanın temelinde insan ve sermaye kaynağı, teknoloji alt yapısı ve uluslararası pazarlama birikiminin eş uyum içinde hareket etmesi bulunmaktadır.

Bu sektörde küresel ölçekte başarılı bir şekilde faaliyet gösteren firmalar ve pazarda söz sahibi ihracatçı ülkeler birçok avantaj sağlamaktadırlar. Bu avantajlar şu şekilde sıralanabilir :

Ekonomik açıdan bakıldığında,

- Döviz girdisi,
- Ödemeler dengesine katkı,
- İşsizliğin önlenmesi ve /veya istihdam artışının sağlanması
- Yan sanayinin (KOBİ'lerin) gelişmesi,
- Enflasyona etkisi,
- Toplumsal refahın artırılması,
- Hayat standartlarının yükselmesi.¹³

Siyasi açıdan bakıldığında,

- Kendi bölgesinde lider devlet olabilmek,
- Uluslararası örgütlerde (BM, AB, NATO, vb.) söz sahibi olabilmek.

Askeri açıdan bakıldığında,

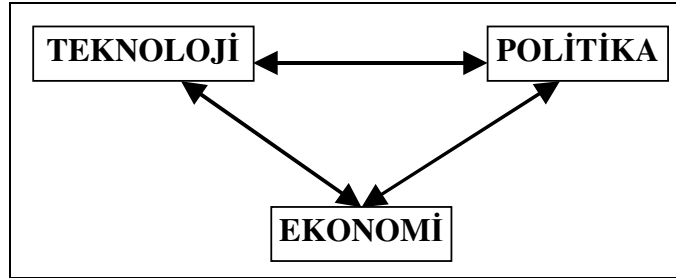
- Askeri açıdan kendi kendine yetebilmek,
- Askeri açıdan stratejik ve taktik kararların alınması ve uygulanmasında etkinliği sağlamak,

¹³ Gülay Günlük Şenesen, "Yerli Silah Sanayiinin Kurulmasının Sanayi Yapısı Üzerindeki Etkileri", **İktisat Dergisi**, Nisan -Mayıs 1997, Sayı:366-367, s:79.

- Askeri anlaşmazlıkların çözümünde caydırıcı rol oynamak,
- Askeri standartlara uygun üretim yapabilmek (ürün ve hizmet bazında kalite, performans, güvenilirlik gibi temel kriterlerin elde edilmesi).

Son dönemde rekabet şiddetinin yoğunluğu nedeniyle uluslararası savunma sanayii pazarına büyük bir oranda hakim olan ABD’de savunma sanayii şirketlerinin sayısında azalmalar ve buna bağlı olarak şirket evlilikleri ortaya çıkmıştır. Avrupa’da ise birleşik proje uygulamaları olmasına rağmen çeşitli güvensizlik kaynakları sonucu tam bir eş uyum sağlanamamaktadır.

Silah sanayii ürünlerinin ar-ge maliyetlerinin çok yükselmesi sonucu bazı savunma sistemi projelerinde iki-üç firma veya devletin işbirliği de yeterli bulunmayıp çok devletli konsorsiyumlar kurulmuş ve devletlerin dahil buldukları askeri ve politik örgütler kontrolü ele almak durumunda kalmışlardır ¹⁴(5 . Komisyon Raporu, s:133).



Şekil – 2 Teknoloji, Ekonomi ve Politika Etkileşimi.

Kaynak : Vicki Golich, “Aviation’s Technology Imperative and the Transformation of the Global Political Economy”, **Technology, Culture and Competitiveness, Change and the World Political Economy**, Ed.: Michael Talalay, Chris Farrands, Roger Tooze, Routledge, London, 1997, s:183.

Bunun sonucu Şekil-2’de de görüldüğü gibi hem ekonomik ve sosyal, hem de askeri ve politik açıdan hükümetleri de yakından ilgilendirdiğinden bu uluslararası ilişkiler hükümetlerin kontrolünde yürütülen devletler arası ilişkilere dönüşmüştür¹⁵.

¹⁴ **I. Bilim Teknoloji Şurası**, 14-16 Mayıs 1990, Tübitak Yayın – Dağıtım Daire Başkanlığı No: 92-0040, 5 . Komisyon Raporu ,“İleri Teknolojiler ve Savunma Araştırma Geliştirme”, s:133.

¹⁵ **I. Bilim Teknoloji Şurası**, 14-16 Mayıs 1990, Tübitak Yayın – Dağıtım Daire Başkanlığı No: 92-0040, 5 . Komisyon Raporu ,“İleri Teknolojiler ve Savunma Araştırma Geliştirme”, s:133.

5.4. İkinci El Teknolojilerin Satışı ve Türkiye Açısından Değerlendirme

İkinci el teknoloji artık güncelliğini yani geçerliliğini kaybetmiş teknolojidir. Onun yerini daha iyi tasarlanmış, daha dayanıklı ve daha işlevsel, amaçlara uygun kısaca daha kaliteli teknolojiler almaktadır.

Türkiye silah araç-gereç ve sistemlerinde büyük ölçüde dışa bağımlıdır. Bu bağımlılıktan kurtulmak için, yeni yeni, mevcut ürünlerin doğrudan ithali yöntemi yerine ortak proje yapımı ve teknoloji transferi yöntemini benimsemektedir.

Türkiye dünyada uzun yıllar ikinci el silah teknolojilerinde önemli bir alıcı konumunda kalmıştır. Stockholm Uluslararası Barış Araştırma Enstitüsü (SIPRI) verilerine göre, 1989-1994 arası 25,2 Milyar Dolar'lık ikinci el silah pazar hacmi içerisindeki ülkelerin aldıkları paylar aşağıda Tablo-1'de görülmektedir.

Tablo-1 Dünya İkinci El Silah Pazar Dağılımı
(1989-1994 arası, 1989 fiyatlarıyla yüzde olarak belirtilmiştir)

İthalatçı Ülkeler		İhracatçı Ülkeler	
Türkiye	17.5	ABD	50.2
Yunanistan	15.9	Almanya	23.7
Endonezya	7.4	İngiltere	4.2
Pakistan	4.7	Rusya	3.8
İsrail	4.4	İspanya	3.5

Kaynak : Bonn International Center for Conversion, Conversion Survey 1996, **Global Disarmament, Demilitarization and Demobilization**, Oxford University Press, Oxford,1996, s:218-9.

İkinci el teknolojinin satışı gönderici ülkeye aşağıdaki temel faydaları sağlamaktadır.

- Ekonomik ve siyasi etki alanını genişletmek,
- Buradan sağlanacak finansmanı yeni ar-ge projelerinde kullanmak,
- Farklı ülke ve doğa şartlarında performans değerlemesi yapmak,
- İkinci el teknolojinin zaten eski olduğunu,yakın bir zaman diliminde diğer ülkeler tarafından da geliştirileceğini bilmek,
- İhraç edilen teknolojinin yedek parça, servis, yenileme maliyeti vb. unsurlarla devamlılığını sağlayarak ek faydalar elde etmek,
- Alıcı ve/veya partner ülke teknolojileri, donanım altyapıları hakkında bilgi sahibi olmak,
- İstihdamı arttırmak, işsizliği önlemek.

Türkiye açısından silah satışları konusunun parasal maliyetinin yanında diğer bir önemli tarafı siyasi baskı amacıyla kullanılmasının giderek ağırlık kazanmasıdır. Bu konuda ihtiyaca yönelik olarak helikopter, tank araç-gereç ve sistemlerinin en son model ve teknolojilerde üretilmesi projeleri örnek verilebilir.

Türkiye son dönemde helikopter ihalesiyle ilgili olarak üç firmaya ait; Bell Textron / AH-1W Super Cobra, Boeing / AH-64 Apache Longbow ve Kamov / Ka-50/2 Black Shark saldırı helikopterleri gündeme gelmişti. Konuyla ilgili çevrelerde ve yayınlarda; Türkiye neden saldırı helikopteri almaktadır ? Bunları nerelerde kullanacaktır ? Kıbrıs, Kuzey Irak ve diğer bölgelerde kullanırsa hangi dengeler değişir ? Ayrıca Türkiye teknoloji transferi istemektedir. Bunun karşılanması durumunda neler olabilir ? gibi detaylı analizler yapılmaktadır.

Tank ortak proje ihalesi ile ilgili olarak ise yine firmalar, örneğin General Dynamics Land System / Abrams M1A2 Tankı (ABD) istekli görünürken ABD Kongresi ve çeşitli çevreler teknoloji transferi kapsamında temkinli yaklaşmaktadırlar. Diğer taraftan Almanya Leopard –II A5 Tankının ortak imalatında ve teknoloji transferinde çelişkili tutumlar sergilemektedir. Almanya bir taraftan pastadan pay almak isterken diğer taraftan “insan hakları ihlalleri” gerekçesiyle konuya sıcak bakmadığını açıklamıştır^{16, 17}.

Türkiye'nin ortak proje ihalelerinde en elverişli model ve ülkeyi seçmesi durumunda dahi bu projenin diğer bütün spesifik projelerde olduğu gibi zamana yayılacağı, gelişmelerin izleneceği, özellikle teknolojik unsurlarda tam bir bilgi akışının sağlanamayacağı açıktır.

ABD'de, özellikle Kongre çalışmalarında, Türkiye adının geçtiği her konuda Rum, Ermeni ve İsrail kökenli lobilerinin etkin olarak çalıştıkları bilinmektedir. Bu çıkar grupları Türkiye'nin bölgesinde lider devlet konumuna yükselmesini istememekte, alınacak her ekonomik ve siyasi kararın aleyhte olabilmesi için yoğun çaba harcamaktadırlar.

Bunların başında Türkiye ile ABD arasındaki askeri araç-gereç ve sistemlerinin satışını mümkün olduğu kadar geciktirmek ve mümkünse engellemek gelmektedir. KKTC'nin 25. kuruluş yıldönümünde ABD'de gerçekleşen gösterilerde Türkiye'ye yapılacak silah satışının mümkünse hemen durdurulması, iki devlet arasında imzalanan anlaşmaların askıya alınarak Türkiye ve KKTC üzerinde baskı kurulması amaçlanmaktadır. Bu baskılar neticesinde ise Kıbrıs'ta yeni kazanımların elde edilmesi planlanmaktadır. Ayrıca askeri silah satışlarının devam etmesinin Rum'ları Kıbrıs konusundaki emellerini her geçen gün zora sokacağı belirtilmektedir.

Türkiye her an dengelerin değiştiği, sürekli yeni stratejik ve taktik planların yapıldığı jeopolitik bir konumda bulunmaktadır. Sovyetler Birliği'nin dağılması ve dağılan birliğin zayıflıklarının her geçen gün farklı bir boyut kazanması ile ABD'nin yeni dünya vizyonu özellikle yeni Avrupa düzeninde, Balkanlar'da, Ortadoğu'da, Kafkaslar'da ve Asya'da birtakım güvenlik sorunlarının ortaya çıkması ve yaşanmasına sebep olmaktadır.

İki kutuplu ve belirli oranda istikrarlı yapının ortadan kalkmasından itibaren dünya bir geçiş süreci yaşamakta olup tarihten kaynaklanan uzun dönemli anlaşmazlıklar ve sorunlar yeniden gündeme gelmiştir. Bölgesel bazlı silah alımları artmaktadır. Türkiye - Yunanistan, Hindistan - Pakistan, Çin – Tayvan ve Ortadoğu ülkeleri arasında yaşanan sorunlar modern silah donanımlarının tedarikine yönelmeyi hızlandırmaktadır.

¹⁶ “Alman Hükümetiyle Leopard Dansı”, **Radikal Gazetesi**, 25 Temmuz 1999, Yıl:3, Sayı:1016, s:11.

¹⁷ “Ankara'nın Tank Projesine ABD'den ‘evet ve hayır’ ”, **Hürriyet Gazetesi**, 3 Haziran 1999, s:22.

Savunma sanayiinde dünya ölçeğinde faaliyet gösteren işletmeler; yüksek teknoloji yatırımları, yüksek ar-ge maliyetleriyle karşı karşıya kalmaktadırlar. Günümüzde şiddetli rekabet ortamının bir gereği olarak işletmeler temel faaliyet alanlarında yoğunlaşma ve uzmanlaşmaya yönelmek durumundadırlar.

Ordu çağımızın modern gereklerine uygun olarak yeniden yapılanmakta olup her türlü koşula uygun görev yapabilecek kapasitede donanıma, çevik organizasyon yapısına ve yüksek vuruş kabiliyetine sahiptir. Teknolojik ihtiyaca yönelik en iyi donanıma sahip olmak birincil, mevcut potansiyelini en etkin ve verimli bir şekilde kullanmak ikincil temel amacı olmalıdır. Bununla birlikte mevcut teknolojik donanımın ortaya çıkarılmasında ve bu donanımın uygun sahada faaliyette bulunmasında birtakım zorluklar ve problemler yaşanmaktadır. Bu zorlukların ve problemlerin başında Savunma Sanayii'nde kullanılmakta olan silah araç-gereç ve sistemlerinin büyük bir oranda yurt-dışı orijinli ve çok sayıda devlet tarafından imal edilmiş olması görülebilir.

Teknoloji transferi ile birlikte üretim becerisinin ülkeye kazandırılmasında; konsorsiyumun şekli, ihale maliyeti, ülkeler arası dağılımı, ortak proje yapılabilirliği gibi konular öne çıkmakta ve çeşitli sıkıntılar yaşanmaktadır. İlerleyen dönemlerdeki yenileme desteği, parça temini, servis-bakım hizmetleri ve bunların maliyetleri ile bağımlılık dereceleri üstünde durulması gereken konulardır.

Doğaldır ki, askeri amaçlı donanımların oluşturulmasında farklı ülkelerin ve firmaların uzmanlık alanlarından yararlanılmış ve Silahlı Kuvvetler için maksimum fayda sağlanması gözetilmiştir. Fakat farklı uzmanlık alanlarından yararlanmanın birtakım sakıncaları da bulunmaktadır.

Bu sakıncaların başında gelen askeri araç-gereç ve sistemlerindeki çeşitliliğin fazla olmasını ve bunun getirdiği problemleri aşağıdaki gibi sıralamak mümkündür¹⁸:

- Alınan stratejik kararların etkin ve verimli bir şekilde hayata geçirilememesi ve/veya gecikmesi,
- Rekabetçi ortamda bu planların gizlilik ve güvenilirlik derecesinin azalması veya zayıflaması,
- Bilgi yoğun teknik araç-gereç ve donanıma uygun olan üst düzey teknik eleman ile ara elemanların yetiştirilmesinde karşılaşılan zorluklar,
- Mevcut teknik donanım parkı arasındaki kullanım ve performans açısından uyumsuzluklar,
 - Malzeme / yedek parça teminindeki yüksek maliyetler ve termin farklılıkları,
 - Malzemenin stoklanması ve ambarlanmasında karşılaşılan güçlükler,
 - İkmal teşekkülleri arasında dağıtım kanalları problemleri,
 - Yurt içi imalatçı uzman firma sayısının azlığı ve yetersizliği.

¹⁸ Murat Erdal, Suat Saraçoğlu, "Küresel Rekabet Ortamında Teknoloji ve Ulusal Güvenlik", **Yöneylem ve Endüstri Mühendisliği XX. Ulusal Kongresi Bildiriler CD'si**, 8-9 Haziran 1999, Ankara, s:9-10.

Kara, deniz ve hava harp silah araç-gereç ve sistemleri tıpkı imalat sektör sınıflaması gibi ayrı sektörler olarak düşünülmektedir. Hepsi bir bütünün parçaları olmasına rağmen günümüzde yüksek teknolojinin yoğunluğunu daha fazla hissettirmesiyle farklılıklar giderek artmaktadır.

Türk Silahlı Kuvvetleri'nin ihtiyacına yönelik olarak faaliyet gösteren yurt içi tedarikçi firmaların askeri kalite standartlarına (A.Q.A.P.) uygun imalat yapması zorunluluğu bulunmaktadır. Savunma sanayii konusunda faaliyet gösteren firma sayısı yetersizdir ve bu işletmeler çoğunlukla kamu kuruluşlarıdır. Arzu edilen ürün kalite ve performansının yakalanmasında yoğun çaba harcanmalıdır.

Askeri amaçlı sistemler bilgi yoğun sektörler konumundadır. Bilgisayar ve sanal ortam tehlikeleri bu endüstrinin ilerlemesiyle birlikte beraberinde birçok belirsizlik ve soru işaretini getirmektedir. Yüksek teknoloji ve bilgi yoğunluğu ar-ge çalışmalarının önemini artırır. Ar-ge çalışmalarının arzu edilen ihtiyaçlara cevap verebilmesi ise büyük miktarda finansal güce ve yetişmiş personele dayanmaktadır. Bugün yaşanmakta olan şiddetli rekabet ortamında ülkelerin başarısı ve başarısızlığı arasındaki fark sadece ar-ge'ye ne kadar kaynak ayırdıklarından değil aynı zamanda onu nasıl tanımladıklarından ileri gelmektedir. Savunma sistemleri için de aynı şeyleri söylemek mümkündür. Güçlü bir savunma sanayii ancak güçlü bir ekonomiyle sağlanabilir. Ancak Türkiye gibi kaynakları sınırlı olduğu ülkelerde savunma harcamaları ayrı bir önem arz etmektedir. Bu konuda azami dikkatin sağlanması, hangi alanlarda derinlemesine uzmanlaşmaya gidilip gidilmeyeceği, ne gibi önceliklere yer verileceği iyi bir şekilde planlanmalıdır.

Araştırma ve geliştirme ise çok boyutludur. Her şeyden önce devletin bilim - sanayi ve ticaret politikalarıyla yakından ilgisi bulunmaktadır. Ülkenin teknoloji bilim altyapısının durum analizi, yani bugünü ve yarını açısından değerlendirmeler elzemdir. Türkiye açısından bilim ve teknoloji konusuna bakıldığında konuya Beş Yıllık Kalkınma Planları'nda özel yer verildiği, özel ihtisas komisyon raporlarının hazırlandığı görülmektedir.

Türkiye'de ar-ge yatırımları ve harcamalarının ağırlıklı olarak kamu kurumlarında yapıldığı ve bunun büyük bölümünün üniversitelerce yürütüldüğü bilinmektedir. Özel araştırma laboratuvarları, özel araştırma kurumları ve enstitülerin sayısı son derece yetersizdir. Özel şirketlerin ise ar-ge için ayırdıkları kaynak ve yıllardan beri gelen tutumları arzu edilen seviyeden çok uzaktır. Üniversite-sanayi işbirliğinin askeri alanda daha fazla uygulamaya geçirilmesi gereklidir. Kuvvet bazında ihtiyaca uygun olarak Kara, Deniz ve Hava harp silah araç-gereç ve sistemlerinin geliştirilmesine ve mevcut donanımın Türkiye koşullarına uygulanabilirliğinin kolaylaştırılması- na yönelik yüksek teknoloji enstitüleri ile firmalarının teşvik edilmesi gereklidir. Yurt içi savunma firmalarının teşviki amacıyla vergi kolaylıkları, ihale mevzuat ve düzenlemelerinde bir Türk firmasının bulunması zorunluluğu, arazi temini, enerji-kaynak kolaylıkları, eğitim olanaklarının artırılması gibi unsurlar sağlanmalıdır.

Silikon Vadisi, Route 128 ve benzerleri gibi temelinde küçük- orta boy ölçekli işletmeler, üniversite, enstitü, ar-ge kurumlarıyla iç içe olan teknoloji geliştirme merkezlerine, "teknopol"lere ihtiyaç vardır. Bunun olabilmesi ise özellikle üniversite-sanayi ve devlet

işbirliği gerektirmektedir. Yeni teknolojileri takip edebilen ve risk alabilen girişimciler, uygun altyapı, yetişmiş kalifiye elemanlar ve sermayenin bir araya gelmesi zaruridir.

Biyolojik, kimyasal ve nükleer silah sistemleri tehditleri günümüzde azalmış ancak Türkiye'nin jeopolitik konumu açısından düşünüldüğünde tamamen de ortadan kalkmamıştır. Bu sebeple alınacak birtakım koruma önlemleri paketinin geliştirilmesi zorunluluğu ortaya çıkmaktadır.

Savunma sanayii alanında, özellikle teknolojinin belirleyici rolü ile bunun getireceği riskler ve belirsizlikler artmaktadır. Stratejik açıdan ulusal ve küresel dengeler düşünüldüğünde, Türkiye kendi kendine yetebilen bir devlet konumuna ulaşabilmek için bütün bu unsurları değerlendirerek uygun çözümler üretmek mecburiyetindedir.