TEŞEKKÜR

Yüksek Lisans Eğitimime başladığımdan bu yana, anlayış ve hoşgörüsüyle yardımlarını esirgemeyen hocalarım Prof.Dr. Abdulkadir AKÇİN, Doç. Dr. Ali Akgün ve Doç.Dr. Halit KESKİN ‘e,

Yüksek Lisans yapmam için beni teşvik eden, dedem Kazım PINAR’a, hiçbir fedakarlıktan kaçınmadan beni yetiştiren annem Gülsüm KESKİN’e, babam Mustafa Sami KESKİN’e ve bana desteği ve anlayışıyla güç veren sevgili eşim Zeliha KESKİN'e

Yüksek Lisans Eğitimimin özellikle tez aşamasında, gösterdiği hoşgörüyle bana destek olan müdürüm Sayın Hanefi Kalın’a teşekkürlerimi sunarım.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

KISALTMALAR

3DES .....Üçlü Veri Şifreleme Standardı (Triple Data Encryption
AAA ..... Açık Anahtar Altyapısı
AAA .....Authentication, Authorization ve Accounting
AB .....Avrupa Birliği
ABD ..... Amerika Birleşik Devletleri
ADSL ..... Asymmetric Digital Subscriber Line
AES ..... Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)
AM ..... Amplitude Modulation (Genlik modülasyonu)
ARPA ..... Advanced Research Projects Agency
ARGE.....Araştırma Geliştirme
ATM ..... Asenkron Transfer Modu
BRA .....Basic Rate Access
C2..... Command and Control (Komuta Kontrol)
C4ISR ..... Komuta, Kontrol, Muhabere, Bilgisayar, Gözetleme ve Keşif
CDM.....Kod Bölmeli Çoklama
COMSEC..... İletişim Güvenliği
CW .....(Siber Savaş) Cyber War
DES ..... Veri Şifreleme Standardı (Data Encryption Standard)
DPT ..... Devlet Planlama Teşkilatı
DSA ..... Sayısal İmza Algoritması (Digital Signature Algorithm)
E1 .....2.048 Mbps data hızı
ECCM ..... Elektronik Karşı-Karşı Önlemler
ECM ..... Elektronik Karşı Önlemler
EDT ..... Elektronik Destek Tedbirleri
EHF ..... Çok yüksek frekans
EKT ..... Elektronik Korunma Tedbirleri
ELINT ..... Elektronik istihbarat
EMP ..... Elektromanyetik Dalga
ESA ..... Avrupa Uzay Ajansı (European Space Agency)
EUTELSAT ..... Avrupa Uydu Haberleşme Örgütü
EW ..... Elektronik Savaş (Electronic Warfare)

FDM ..... Frekans Bölmeli Çoklama
FDMA ..... Frekans Bölmeli Çoklu Erişim
FM ..... Frekans Modülasyonu
FR.....Frame Relay
FSS ..... Sabit Uydu Sistemi
GAA ..... Geniş Alan Ağı
GEO .....Geostationary Orbit
GPS ..... Küresel Yer Bulma Sistemi
HDSL ..... High-bit-rate DSL
HEO ..... Yüksek Yörünge
HF ..... Yüksek Frekans
HTTP..... Hipermetin Aktarma İletişim Kuralı (Hypertext Transfer Protocol)
IDEA .....Uluslararası Veri Şifreleme Algoritması (International Data Encryption Algorithm)
IGMP..... Internet Group Multicast Protocol
INMARSAT ..... Uluslararası Deniz Uydu Haberlesme Sistemi
INTELSAT ..... Uluslararası Uydu Haberlesmesi Örgütü
IP ..... İnternet Protokolü
IPSec .....İnternet Protokolü Güvenliği (Internet Protocol Security)
ISDN ..... Entegre Sistemler Sayısal Ağı
ISDN ..... Integrated Services Digital NetworkInverse
ISDN ..... Integrated Services Digital Network
IT ..... Bilgi Teknolojileri
ITU ..... Uluslar arası Telekomünikasyon Birliği
KKBS ..... Komuta Kontrol Bilgi Sistemi
LAN .....Yerel Alan Ağı (Local Area Network)
LEO ..... Düşük Yörünge
LF ..... Alçak Frekans
MEO ..... Orta Yörünge
MF ..... Orta Frekans
MGK .....Milli Güvenlik Kurulu
MSAT ..... Mobil Uydu
NATO.....Nortrh Atlantic Treaty Organization
NSA .....ABD Ulusal Güvenlik Kurumu (National Security Agency)

OSPF ..... Open Shortest Path First
PAM ..... Darbe Genlik Modülasyonu (Pulse Amplitude Modulation)
PCM ..... Darbe Kod Modülasyonu (Pulse Code Modulation)
PM ..... Açı modülasyonu(Phase Modulation)
PRI ..... Primary Rate Interface
PSK ..... Evre Kayma Anahtarlaması
RF ..... Radyo Frekansı
RSA ..... Rivest-Shamir-Adleman
S/MIME Güvenli / Çok Amaçlı Genel Ağ Posta Eklentileri (Secure / Multipurpose Internet Mail Extensions)
SDMA ..... Uzay Bölmeli Çoklu Erisim
SFTP ..... Güvenli Dosya Transfer Protokolü (Secure File Transfer Protocol)
SHA-1 ..... Güvenli Özetleme Algoritması-1 (Secure Hash Algorithm-1)
SNMP ..... Standart Şebeke Yönetim Protokolü
SSH ..... Güvenli Kabuk (Secure Shell)
SSL ..... Soket Düzeyi Güvenlik (Secure Sockets Layer)
SSMA ..... Geniş Spektrum Çoklu Erişim
TAFICS ..... Turkish Armed Forces Integrated Communication System
TASMUS ..... Taktik Saha Muhabere Sistemi
TCP/IP .....Transfer Kontrol Protokolü / İnternet Protokolü (Transmission Control Protocol / Internet Protocol)
TDM ..... Time Division Multiplex(Zaman Bölünmeli Çoğullama)
TSK ..... Türk Silahlı Kuvvetleri
TSL .....Ulaşım Güvenlik Katmanı (Transport Security Layer)
UDP ..... User Datagram Protocol
UHF ..... Ultra Yüksek Frekans(Ultra High Frequency)
VHF ..... Çok Yüksek Frekans(Very High Frequency)
VLF ..... Çok Düsük Frekans(Very Low Frequency)
VPN ..... Sanal Özel Ağ (Virtual Private Network)

Dünya'da istihbarat alanında faaliyet gösteren kurumlar;

ACSS: Assistant Chief of M16 - İngiliz Gizli Entelijans Servisinin Baş Yardımcısı

AFOSI: Air Force Office Of Special Investigations - ABD Hava Kuvvetleri Özel Araştırmalar Ofisi (OSI) olarak da tanınır.

AMAN: İsrail Askeri İstihbaratı

ASIO (ASIS): Australian Security and Intelligence Service - Avustralya İstihbarat Teşkilatı

AVB: Allami Vedelmi Batosag - Macar İstihbarat Servisi

BCA: Bo Cong An-Vietnam İstihbarat Servisi.

BCRA: Bureau Central de Renseignements et d' Action -Fransız Merkezi ve Harekât Bürosu.

BFV: Bundesamt für Verfassungsschutz - Batı Alman Güvenlik Servisi.

BND: Bundesnachrichtendienst - Batı Alman Entelijans Servisi

BSC: British Security Coordination - İngiliz Güvenlik Koordinasyonu.

Bundes Polizei: İsviçre Güvenlik Servisi.

CIA: Central Intelligence Agency - ABD Merkezi Haberalma Teşkilatı

CID: Connittee of Imperial Defeance - İngiliz Kraliyet Savunma Komitesi.

CIFE: Combined Intelligence Far East - İngiliz Uzak Doğu Birleşik Entelijansı

CIS: Combined Intelligence Service - İngiliz Birleşik Entelijans Servisi.

COI: Coordinator of Information - İngiliz Enformasyon Koordinatörü.

CRO: Cabinet Research - Japonya İstihbarat Teşkilatı

CSIS: Kanada İstihbarat Servisi

CSS: Chief Of M16 - İngiliz Gizli Entelijans Servisinin Başkanı.

D Branch: Counterespionage Branch ofM15 -İngiliz Güvenlik Servisi Kontrespiyonaj Bölümü

DCI: Director Of Central Intelligence -CIA Direktörü.

DCSS: Deputy Chief Of M16 - İngiliz Gizli Entelijans Servisinin Başkan Yardımcısı

DDCI: Deputy Director Of Central Intellige nce–CIA Direktör Operasyonlar Yardımcısı Teşkilat'ın 2'nci adamı.

DDO: Deputy Director for Operations–CIA direktör Operasyonlar Yardımcısı Operasyonlar Direktörlüğünün (DO-Directorate for Operations) Başı

DGI: Direccion General de Inteligencia - Küba İstihbarat Teşkilatı.

DGSE: Direction Generale de Securite Exterieur - Fransız Dış Güvenlik Servisi.

DIA: Defense Intelligence Agency - ABD Savunma İstihbarat Teşkilatı.

DIE: Departmentul de Informatii Externe - Romen Dış İstihbarat Başkanlığı.

DMI: Director Of Military Intelligence - İngiliz Askeri Entelijans Direktörü.

DNI: Director Of Naval Intelligence - İngiliz Deniz Kuvvetleri Entelijans Direktörü.

DST: Direction de la Surveillance du Territoire - Fransız Güvenlik ve Kontrespiyonaj Servisi. İngiliz M15 ve A merikan FBI Teşkilatlarına muadildir.

DS: Drzaven Sigurnost - Bulgar İstihbarat Teşkilatı

FBI: Federal Bureau Of Investigation -ABD Federal Soruşturma Bürosu

FOE: Forsvarvarsftaben Operativ Enhat - İsveç Güvenlik Teşkilatı.

GCHO: Goverment Communications H eadquartes - İngiliz Hükümet Haberleşme Merkezi.

GCR: Groupement de Controles Radio-Electrique-Fransız İstihbarat Servisi Kripto Bölümü.

GRI: Çin İstihbarat Teşkilatı

GRU: Glavnoye razvedyvatelnoye Upravleniye - Sovyet Askeri İstihbaratı. Sovyet Genel Kurmayına bağlı bir direktörlük

HVA: Hauptvewaltung für Auklarung - Doğu Alman İstihbarat Servisi

IIC: Industrila Intelligence Center - İngiliz Endüstri Entelijansı Merkezi.

ISIC: International Services Intelligence Committee – Uluslararası İstihbarat Servisleri Komitesi MI5 ve MI6'yı kontrol eden komite

ISLD: Inter Services Liasion Department - İngiliz Servisler Arası Liyezon Bölümü

JIC: Joint Intelligence Committee - İngiliz Birleşik Entelijans Komitesi.

KGB: Komitet Gosudarstvennoy Bezopasnostri - Sovyet Devlet Güvenlik Komitesi.

KYP: Yunan İstihbarat Servisi.

MEIC: Middle East Intelligence Center - İngiliz Orta Doğu Entelijans Merkezi.

MI5: British Security Service - İngiliz Güvenlik Servisi

MI6: British Secret Intelligence Service - İngiliz Gizli Entelijans Servisi.

MI9: Escape and Evasion Service - İngiliz Kaçma ve Kurtulma Servisi.

MOSSAD: Ha Mossad, Le Modiyn ve Le Tafkidim Mayuhadim –İsrail Entelijans ve Özel Operasyon Enstitüsü

MUHABERAT: Mısır, Suriye ve birçok Arap devletinin istihbarat servislerine v erilen isim.

NIC: National Intelligence Council - ABD Milli Haberalma Konseyi

NIS: Naval Investigetive Service - ABD Deniz Kuvvetleri Soruşturma (İst) Servisi.

NSA: National Security Agency - ABD Milli Güvenlik Teşkilatı

OS: Overvaaksningst jeneste - Norveç İstihbarat Servisi

RCMP: Royal Canadian Mountain Police - Kanada Kraliyet Dağ Polisi.

SABO: Underrattelse Och Sakerhetsenhet - İsveç İstihbarat Servisi

SAVAMA: İran İstihbarat Servisi.

SB: Sluzba Bezpieczenstwa - Polonya İstihbarat Servisi.

SDECE: Service de Documentation Esterieur et Contre

Espiyonage: Fransız Dış Dokümantasyon ve Kontrespiyonaj Servisi.

SHABACK: İsrail İç Güvenlik Teşkilatı. FBI muadili

SIS: Secret Intelligence Service - İngiliz Gizli Entelijans Servisi (Ml6)'nın diğer adı.

STB: Stani Tajna Bezpecnost- Çekoslovakya İstihbarat Servisi
UB: Polonya İstihbarat Servisi. (Demirel, 2004, sy.11 -15)

1.GİRİŞ

İnsanlık tarihinde bir yolculuğa çıkıldığında, toplumların hayat tarzında ve kültürel yapısında büyük dönüşüme neden olan teknolojik buluşların kağıt, matbaa, telgraf, buharlı makine, elektrik ve bilgisayarın icadı olduğu kabul edilmektedir. (Yücel, 2005, syf.1)

Ancak, insanlık tarihindeki en büyük değişim, endüstri toplumuna geçişin yaşandığı 18. yy.'da, buharlı makinenin kullanımıyla başlamıştır. Endüstri Devriminin başlangıcı olarak kabul edilen buhar gücünün kullanımıyla insan gücüne olan ihtiyaç azalmış, insanoğlu maddeye hükmetmeye başlamıştır. Bu dönüşümde buharlı makineden sonraki en önemli adımlardan biri ise 1831 yılında elektriğin kullanılmasıdır. Elektriğin o dönem için anlamı, güç üretimindeki ucuzlamadır ki bu, sanayileşmeyi büyük ölçüde hızlandırmıştır.

Yine bu yüzyılda kullanılmaya başlanan telgraf ve telefon da, bilgi akışının hızlanması bakımından oldukça önemlidirler. Haberleşme sistemlerinin gelişimi, çok büyük bir hızla ve içinde bulunduğumuz yüzyılın en büyük icatları olan bilgisayar ve internet sistemleri ile paralel biçimde günümüzde de devam etmektedir.

Bilgisayarın tanımının esnekliği bakımından, ilk bulunduğu zamanı söylemek oldukça güçtür. Ancak günümüzde kullandığımız anlamda ikili sayı sistemine dayalı ilk dijital bilgisayar 1941 yılında Z3 adıyla Konrad Zuse tarafından geliştirilmiştir.

Görüldüğü gibi insanoğlu büyük bir teknolojik gelişim yaşamıştır ve hala yaşamaya da devam etmektedir. Bu gelişimin kaynağı düşünüldüğündeyse cevabın, bilgi ve bilim olduğu ortadadır. Bilgi; üzerinde kesin bir yargıya varılmış, anlamlı her türlü ses, görüntü ve yazıya denir. Bilginin değerli olup olmadığı; onun doğruluğu, güvenilirliği, ilgili konuyla alakadarlığı, bütünlüğü, anlaşılabilirliği, ulaşılabilirliği ve etkin maliyete sahip olup olmadığıyla değerlendirilir. Bilgi, insanoğlunun ihtiyaçlarını ve çevresinde olup bitenleri düşünmesinin, araştırmasının bir sonucu olarak meydana gelir. Teknolojik gelişimin diğer bir faktörü olan bilim

ise; "Dünyayı anlamak, olup bitenleri ve kendimizi kontrol altına almak, güvenli bir çizgi izlemek için belirlenen bir yoldur." (Yücel, 2005, sy.13)

Bilim, insanoğlunun tarihsel süreçte oluşturduğu bilgi birikimiyle beraber, bir düşünme şeklini de ifade etmektedir ki bu düşünme şekli, bilimsel bir yaklaşım ışığında; merakı, sormayı-sorgulamayı, anlatılanlara kayıtsız inanmamayı bizzat incelemenin kendisini kapsar. Örneğin yerçekimi yasasının bulunması, Newton'un başına elma düştüğünde onun bu elmanın neden aşağı düştüğünü anlamaya çalışmasının bir sonucuydu.

Bilginin artması ve bilimin ilerlemesi sonucunda yeni teknolojiler ortaya çıkmaktadır. Bu yeni teknolojiler ise, hayatımızın aslında her anında yer alan yeni tanımları ve yeni kavramları da beraberinde getirmektedir. Burada en dikkat edilmesi gereken nokta yeni teknolojilerin de bilgiyi arttırması ve bilimin ilerlemesine büyük katkı sağlamasıdır. Yani bilgi artışı, bilim ve teknoloji gelişimi, birbirlerini çaprazlama olarak beslemektedir. Bilgi ile bilim, bilim ile de teknoloji kavramı arasındaki bu karşılıklı ilişki, teknolojinin tanımını da kendiliğinden ortaya çıkmaktadır. Buna göre teknoloji; genel olarak bilimin, pratik hayatın ihtiyaçlarını karşılanmasına ya da insanın çevresini denetleme, şekillendirme ve değiştirme çabalarına yönelik uygulamalar bütünü olarak karşımıza çıkmaktadır. Başka bir tanımla teknoloji; bilginin ve bilgiye dayalı usullerin, herhangi bir işin yapımına uygulanmasıdır. Bir işe uygulanan bilgi ve bilgiye dayalı usul, o işin daha kısa zamanda yapılmasına imkân tanıyorsa burada bir teknolojik gelişmeden söz edilebilir.

Birbirleriyle çok yakın ilişkisi bulunan bilgi, bilim ve teknoloji arasındaki ilişkideki köprü görevini ise bilişim teknolojileri sağlar. Bilişim teknolojileri; "Günümüzün en temel zenginlik kaynağı olan bilginin toplanması, bu bilginin işlenmesi, saklanması ve gerektiğinde herhangi bir yere iletilmesi ya da her hangi bir yerden bu bilgiye erişilebilmesini, bugün için elektronik, optik vb. tekniklerle tanımlanmış belirli kurallara, protokollere göre otomatik olarak sağlayan teknolojilerin bütünüdür."(Akın, 1998, sy. 240)

Bilişim Teknolojileri bilgi ile teknolojini n beraber kullanılmasıyla elde edilen tüm sonuçları içermekte ve ana sistemlerden mikrobilgisayarlara kadar, bilgisayar temelli tüm sistemleri ifade etmektedir. Bilişim teknolojilerinin en önemli özelliği başka teknoloji alanlarını da derinden etkilemesi v e değiştirmesidir. Bilişim teknolojileri, verimliliği ve refahı arttıran anahtar faktör olarak yer almakta, bilginin gücünü harekete geçirebilmek ancak bu teknolojiler sayesinde mümkün olabilmektedir.

60'lı yıllarda ortaya atılan, 80'li yıllarda bilgisaya rların yaygınlaşmasıyla büyük bir ivme kazanan, günümüzde de bilişim teknolojilerinin en önemli bileşeni olan ağ kavramıyla kazanılan büyük gelişmelerle beraber kaybedilecek varlıkların da yaratacağı risklerin artmasıyla bilişim güvenliği kavramı da hayati bir önem taşır hale gelmiştir. Burada değinilecek en önemli noktalardan birisi de, bilişim sektöründeki aslında tahmin edilemez ölçüdeki hızlı gelişmenin beraberinde gelen güvenlik açıkları ve bunun neticesinde bunlardan yararlanma yoluna giden saldırganların bu açıkları kullanma eğilimleridir.

Çağın teknolojilerine sahip gelişmiş ülkeler, verimlilik ve üretkenlikleri ile rekabet güçlerini hızla arttırırlarken, bu teknolojilere sahip olmayan az gelişmiş ülkeler, bu ülkelere karşı rekabet gücü bulama maktadırlar. Hatta bu teknolojilere sahip ülkeler onların siyasal, hatta ve hatta sosyal yaşamları üzerinde bile belirleyici olmaktadırlar. Günümüzde bu gelişmiş olarak tabir edilen devletler, ekonomik gelişimlerini, refahlarını, mutlulukları ve güvenlikle rini bilim ve teknoloji politikaları yoluyla yürürlüğe koydukları stratejilerle sağlamaktadır.

Burada, teknolojiye tam anlamıyla sahip olmayan -olamayan ülkeler açısından dikkat edilmesi gereken en önemli nokta, teknolojiye sahip olan ülkelerin bu teknolojileri kullanırlarken, bunun kendileri için herhangi bir biçimde tehdit teşkil edip etmeyeceğidir. Nitekim çağımızda tehdit tanımı eski algılamaların içine teknolojiyi de dâhil ederek yapılmaktadır.

Bir ülke için en önemli unsurlardan birisi yukarıda saydıklarımıza ilave olarak sahip olduğu istahbarati gücüdür. Nitekim bir ülkenin sahip olduğu teknolojilere göre istihbarat biçimleri de gelişmiş, farklılaşmıştır. Örneğin istihbaratın elde ediliş

yöntemine göre yapılan bir sınıflandırmaya göre "insan is tihbaratı, görüntü istihbaratı, açık kaynak istihbaratı, sinyal istihbaratı ve iletişim ve elektronik istihbaratı yöntemlerinden sırasıyla saydığımız son iki yöntem, direkt olarak gelişen teknolojilere göre sınır ve şekilleri değişen istihbarat türleridir. " Sinyal istihbaratı; orijinal hedef tarafından gönderilen sinyal şeklindeki mesajların tespit edilmesidir. Bu mesajlar, elektromanyetik yayma vasıtaları ve sensörler vasıtası ile tespit edilebilir. İletişim ve elektronik istihbarat ise "yeni buluşların ge liştirilmesi için bilgi temin edilmesinin yanında, hedef ülkede bulunan iletişim düzenini kapsayacak hedef ülke iletişim olanak ve yetenekleri hakkında gerekli stratejik değerlendirmenin yapılmasına imkân verir "(Yılmaz, 2006, sy.169 –170)

"Bu bağlamda savunma sanayi alanında, ülkelerin tedarik ve teknoloji transfer modelleri, operatif ve taktik boyutta elektronik harp ve uzay savaşlarına yol açabilecek yeni senaryolar içinde, geleceğin bilgisayar donanımlı robotik savaş yöntemlerinin oynanacağı bilgi savaşlarına hazırlık düzeyi, fevkalade önem kazanan bir nitelik kazanmış bulunmaktadır."(Dindar, 2004, sy. 12)

Bu tez çalışmasında öncelikli olarak teknolojinin hızlı gelişimi çerçevesinde bilgi, bilim ve teknoloji arasındaki ilişkiye değinilmiştir . Bu kavramlar arasındaki köprü görevini sağlayan bilişim teknolojilerinin açıklanması amacıyla da veri ve internet erişimine vurgu yapılmış, bilişim sistemlerinin kullandığı protokoller genel hatlarıyla açıklanmıştır.

Sonraki bölümlerde teknoloji ile küre selleşme arasındaki ilişki açıklanarak, çağımızın yeni tehdit anlayışı çerçevesinde teknolojinin bilgi savaşı ile arasındaki ilişki açıklanmıştır. Bilgi savaşı ve bölümlerinin açıklanmasından sonra çağımızın önemli teknoloji ve sistemlerinden, kriptografi, haarp, uydu teknolojileri ve nanoteknoloji konularına değinilmiştir. Son bölümde de ülkemizin bilgi savaşına hazırlanması çerçevesinde dikkat etmesi gereken noktalar açıklanmıştır.

2 VERİ İLETİŞİMİ

2.1 Giriş

Bilgisayar ağları, günümüzde artık her türlü bilgiyi taşımakta, dolayısıyla endüstrinin her alanına girmektedir. Gerek evimizde gerekse işimizde bir ağa dâhil olmayan bilgisayar artık neredeyse kalmamıştır. İçinde yaşadığımız dünyada mali, askeri, sanatsal, bilimsel ve benzeri her türlü bilgiyi internet sağanağı altında yaşamımıza katabilmekteyiz. Bu noktada içinde bulunduğumuz bilgi çağında başarı, bu bilgilerin bir kaynaktan diğerine güvenli hatasız ve hızlı bir biçimde iletilmesinden geçmektedir.

2.2 İletişim Sistemleri

Veri iletişimini sağlayan bir modelleme yaparsak, bir iletişim sistemi; veriyi üreterek bir ya da daha fazla noktaya gönderen verici kısmı, bu veriyi alan alıcı kısmı ve bu iki nokta arasındaki iletişim kanallarından oluşur. Verici elektriksel sinyalin transmisyon ortamı ya da fiziksel kanal üzerinden iletimi için uygun bir şekilde çevirir. (Proakis and Salehi, 2002, sy.5)

İletişim kanalı, alıcıdan vericiye gönderilen verinin kullandığı fiziksel ortamı ifade eder. Bu fiziksel ortam, kablosuz uzay ortamını ifade edebileceği gibi, kablolu iletişim ortamları da olabilir. Alıcı kısmın fonksiyonu, alınan sinyal içinde yer alan mesaj sinyalini yeniden elde etmektir. Aşağıda bazı iletişim kavramlarına yer verilmiştir.

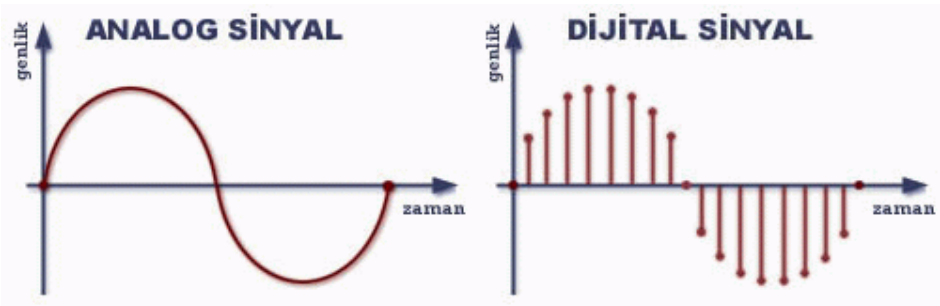
2.2.1 Sinyal

"Sinyal bilginin bir uçtan diğer uca taşınması için kullanılan elektriksel nicelik olup genlik frekans ve faz bileşenleri ile ifade edilmektedir. Genlik sinyalin Volt cinsinden elektriksel büyüklüğünü, frekans bir saniye içerisindeki sinyalin kendini tekrarlama sayısını, faz ise belirli bir referans açıya göre konumunu ifade etmektedir. "(Özbilen, 2005, sy.11)

Bir sinyalin genliği sürekli ve aralıksız değişiyorsa bu sinyale analog sinyal, işaretin bu haliyle yapılan haberleşmeye de analog haberleşme denir.(Başkan, 2002, sy.4)

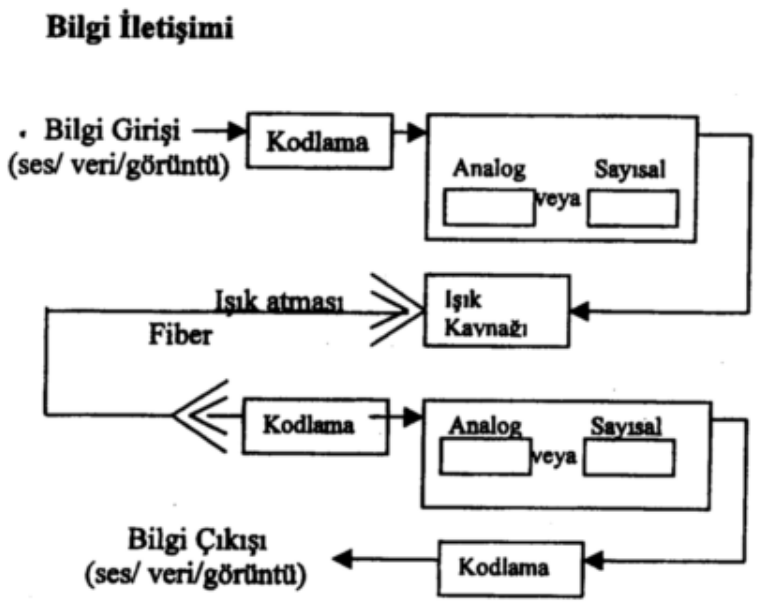
Analog sinyaller özellikleri nedeniyle genlik, frekans ve faz değişimlerine daha yatkındır.

Analog haberleşmenin bilinen sakıncaları nedeniyle sayısal haberleşme tekniklerine ihtiyaç duyulmaktadır. Bu amaçla analog işaretlerin sayısal biçime dönüştürülmesi gerekmektedir ve bunun için de en önemli nokta, analog işaretin uygun bir örnekleme frekansı ile örneklenmesidir. (Megep, 2007, sy.37)



Şekil 2.1: Sinyal Türleri

Çağımızın iletişim sistemlerinde eğilim, analog iletişime oranla yüksek performans, gürültüden fazla etkilenmemesi yüksek güvenlik ve esnek yönetim kabiliyeti sağlayabilen sayısal iletişim yönündedir. Şekil 2.2'de, optik kurallara göre çalışan, analog ve sayısal sinyallerin de taşınabildiği fiber iletişim görülmektedir.



Şekil.2.2 Fiber İletişim Sistemi

2.2.2 Eşzamanlama

Verici ile alıcı arasındaki verinin her iki uçta da anlaşılan uygun ortak bir dile çevrilmesi, iletişim teknikleri ve genel olarak alıcının verinin başladığı ve bittiği zamanı bilmesi ve sistemlerin aynı zamanı kullanması olarak tanımlanan eşzamanlama ile sağlanır.

2.2.3 Akış Denetimi

İletişimde önemli noktalardan birisi de akış denetimidir. Veri, alıcıların veriyi işleme hızlarının vericilerin işlem hızından daha düşük olması ya da alıcı sistemin yoğun bir trafiğe sahip olması durumunda karşı tarafa doğru biçimde iletilemez. İşte bu hızların ayarlanması akış denetimiyle yapılmaktadır.

2.2.4 Kodlama ve Modülasyon

Bilgi taşıyan bir sinyalin (veya mesaj sinyalinin),telefon hattı veya uydu kanalı gibi band geçiren bir iletişim kanalından iletimi, genellikle sinyalin frekans aralığının iletim için uygun bir frekans aralığına kaydırılmasını gerektirir. Modülasyon, taşıyıcı bir sinyalin bazı özelliklerinin modüle edici bir sinyalle uyumlu olarak değiştirilmesi işlemi olarak tanımlanır. Mesaj sinyaline modüle edici sinyal, modülasyon sonucunda elde edilen sinyale de modüle edilmiş sinyal denir.(Hsu, 1993, sy.48)

Modüle edilerek gönderilen bir sinyal karşı uçta modülasyonun ters işlemi olan demodülasyon işlemine tabi tutularak karşı tarafta ilk haline dönüştürülür.

Modülasyon uzayda yayılımı kolaylaştırmak, zayıflama ve gürültüyü azaltmak, çok sayıda kanalın aynı anda iletimini sağlamak ve cihazların ortaya çıkardığı sınırlayıcı etkileri yok etmek için yapılır. Zayıflama, gürültü ve girişim problemini çözmek için uygulanacak en iyi yöntem işaretin iletileceği ortamın özelliklerine uygun bir biçime dönüştürmektir.

Modülasyon analog ve sayısal olmak üzere ikiye ayrılır. Analog modülasyon; genlik, faz ve frekans modülasyon olmak üzere üç çeşittir. Sayısal modülasyon pcm, delta, ppm, pwm ve pam olmak üzere 5 çeşittir. Modülasyon türleri şekilde belirtilmiştir ancak konumuz gereği ayrıntılara girilmeyecektir.

Sesin iletim ortamında taşınabilmesi iç in uygun bir biçime dönüştürülmesi ses kodlama teknikleriyle yapılır. Kodlama işlemi analog ses işaretlerini sayısal işaretlere çeviren kodlayıcılarla yapılır. Kodlayıcılar "genelde ses giriş işareti üzerinde öngörülen dizilerin karmaşık işlemler ile anali zini ve uygun bir bant genişliğinden iletilebilmesi için sıkıştırılmasını da sağlamaktadır." (Güler, 2004, sy.27)

En bilinen ses kodlama biçimi PCM'dir. Genel olarak analog ses sinyali PCM kodlayıcı ile sayısallaştırılmış ses sinyaline dönüştürülür. Darbe Kod Modülasyon (PCM) sistemleri telefon şebekelerinin kapasitesini artırmak amacıyla kullanılmaktadır. PCM sistemlerde, az sayıda kanal içeren alçak kapasiteli sayısal sistemler çoklanarak çok sayıda kanal içeren yüksek mertebeli sistemler oluşturulur. Birinci mertebeyi oluşturan 30 kanallı 2.048 Mbit/s 4'lü çoklanarak 8.448 Mbit/s 120 kanallı sistem elde edilir. Bu sistemin 4'lü ve 16'lı çoklanmasıyla da sırasıyla 3. mertebeyi oluşturan 34.368 Mbit/s 480 kanallı sistem ve 4. mertebeyi oluşturan 139.264 Mbit/s 1920 kanalı sistemleri elde edilir. 139.164 MBit/s hızındaki sistem 34.368 Mbit/s hızındaki sistemin 4'lü çoklanmasıyla da elde edilir.

2.2.5 Genişbant

Band genişliği bir iletim ortamının ya da haberleşme kanalının kapasitesini ifade etmek için kullanılır. Başka bir deyişle bir kanal üzerinde taşınabilecek en fazla frekansa sahip sinyal, kanalın band genişliğidir. Haberleşme kanalının kapasitesi, analog sinyal kullanılıyorsa Hertz(Hz), sayısal sinyal kullanılıyorsa bps (bit per second) ile ifade edilir.

Genişband, son kullanıcıya ulaşan altyapının, örneğin yüksek hız gerektiren video hizmeti gibi bir hizmeti vermeye kapasitesinin ve teknolojisinin uygun olması ya da OECD'nin tanımındaki gibi müşteriye doğru olan hızın 200 kb/s'ı aşması ola rak

kabul edilir. Burada yapılan genişband tanımlarında dikkat edilecek nokta, genişbandın yüksek hız veri transfer teknolojisini ifade etmesidir.

Bir haberleşme sistemindeki 3 bileşenin band genişliklerinin de farklı olması durumunda haberleşme sisteminin kapasitesi minimum band genişliğine sahip bileşenin band genişliği kadar olacaktır. Verinin saklanabilme kapasitesi byte, iletilme hızı bit cinsinden ifade edilmektedir.

2.2.6 Kanal Çoklama (Multiplexing)

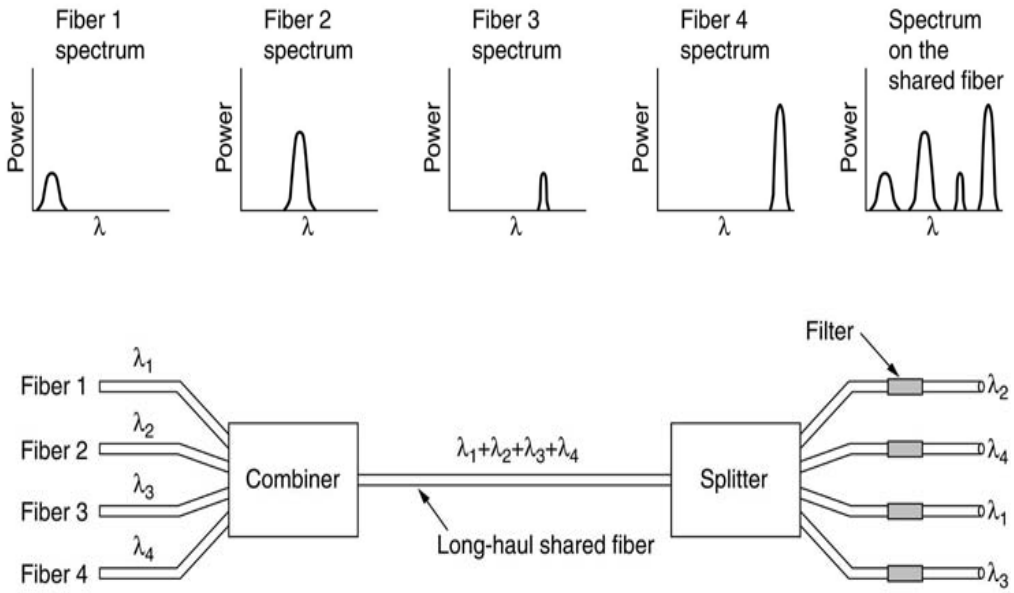
Çoklama teknikleri tek bir iletişim ortamında birden fazla haberleşme kanalı oluşturmak için kullanılır. FDM, TDM ve WDM olmak üzere üç tiptir. Çoklama; bilgi kaynaklarını birleştirmek, verimli iletim sağlamak, terminalin çalışmasını sağlamak ve maliyette tasarruf saplamak amacıyla yapılır.

FDM(Frequency division multiplexing): İletim bantlarının farklı frekans bölgelerinin kullanılmasıyla birden fazla haberleşme kanalının oluşturulmasıdır. Atmosferde aynı anda birden fazla yayının yapılabilmesi, adsl teknolojileri buna örnek verilebilir. FDM'de 3 kanal modüle edilip birleştirilerek pregrubu, 4 pregrup birleşerek 12 kanallı bir temel grubu, 5 temel grupta birleşerek 60 kanallı süper grubu oluşturur.

TDM(Time Division Multiplexing): Farklı zamanlarda farklı sistemlere ait verileri tek bir fiziksel hat üzerinden birden fazla haberleşme kanalı oluşturan çoğullama tekniğidir.

WDM (Wavelength Division Multiplexing): Dalga boyu bölmeli çoğullamada da frekans bölmeli çoğullamada olduğu gibi, aynı ortam üzerinde, aynı anda, farklı sinyallerin taşınması amaçlanmıştır. Farklı dalgaboyundaki sinyaller birleştirici

(combiner) kullanarak bir araya getirilir ve varış noktasında bir ayrıştırıcı (splitter) yardımıyla birbirlerinden ayrılırlar.



Şekil 2.3 WDM-Farklı Dalga Boylarının Çoğullanması (Oktuğ, sy.2)

2.2.7 Paralel ve Seri İletim

Paralel iletim; bilgisayarların kendilerine çok yakın uç birimleriyle aralarındaki bayt düzeyinde veri iletimini ifade etmektedir. Bayt içindeki herbir bit aynı anda farklı yollar üzerinden gönderilir. Yani 2 ortam arasında aynı anda 8 fiziksel iletim ortamı vardır. Ancak yakın mesafelerde kullanılan bu yöntem mesafenin artmasıyla teknik ve ekonomiklikten uzaklaşır. Bu bakımdan uzak mesafeli bağlantılarda tekbir iletim ortamından bitlerin tek tek gönderilmesi prensibine daya nan seri iletim kullanılır.

Seri iletim zamanlama bakımından senkron, asenkron ve isenkron olmak üzere üçe ayrılır. Asenkron iletimde, herhangi bir zamanlama bilgisi kullanılmadan verini başına ve sonuna başlangıç ve bitiş bitleri konulur. Başka bir değişl e, alıcı ve verici uçlar ortak bir zamanlama bilgisine sahip değildir. Senkron iletişimde, bazen veriyle bazen de veriden ayrı bir kanaldan gönderilen alıcı ve verici uçlar arasındaki ortak bir zamanlama bilgisi kullanılmaktadır. İsenkron iletim ise, haber leşmenin periyodik olarak yapıldığı senkron iletimin türevidir.

2.2.8 Haberleşme Kanallarının Çalışma Modları

Simpleks, half dublex ve full dublex olmak üzere 3 farklı çalışma modu vardır. Bunlardan simplex haberleşme; tv, radyo gibi tek taraflı bi r haberleşmeyi, Half dublex haberleşme; telsiz gibi haberleşmenin çift yönlü ancak sırayla yapılan haberleşmeyi, full dublex haberleşme ise, aynı anda yapılabilen çift yönlü haberleşmeyi ifade etmektedir.

2.2.9 Modemler

Uzak mesafe bağlantılarında kullanılan donanımlardır.

Çevirmeli Analog Modemler: İki telli kablolar üzerinden 56 kbps'ye kadar bağlantı sağlayan çevirmeli analog modemlerdir. Bu modemler için yapılan santrallerin herbir bağlantı için tahsis ettiği kanal band genişliği 64 kbps olduğun dan, teknolojik açıdan vadedilen hız maksimum bu hız olacaktır.

Kablo Modemler: Çevirmeli analog modemlerden farklı olarak bu modemlerde aktarım, koaksiyel kablolar üzerinden yapılmaktadır. Bu nedenle de bağlantı hızları çevirmeli analog modemlere göre da ha yüksek değerlere çıkmaktadır. Bu modemler

analog sinyaller üzerinden farklı frekans bandlarını kullanarak veri iletişimini yapmaktadır.

Sayısal Modemler: Yüksek band genişliği gerektiren uygulamalarda özellikle Xdsl teknolojisinde kulalnılan bu modemler in kullanımı büyük bir hızla artmaktadır.(Özbilen, 2005, sy.28 -29)

2.3 Bozucu Etkiler

Verinin gönderilme sürecinde sinyal, gürültü, zayıflama ya da gecikme gibi nedenlerden dolayı bozulabilir.

2.3.1 Gürültü

En genel anlamıyla gürültü, haber leşme sistemindeki istenmeyen sinyallerdir ve termal, intermodülasyon, diyafoni ve darbe gürültüsü olarak sınıflandırılır. İletim ortamında direnç gibi bir ortamda meydana gelen ısı termal gürültüyü oluşturur ve tüm elektronik sistemlerde sahip olunan bir durumdur. Özellikle çok kanallı sistemlerde frekansların birbirine karışmasından inter modülasyon gürültü oluşur. Diyafoni ise "komşu devrelerden istenmeyen haber geçişi ile ilgilidir."(Kayran, 1999, sy.18)

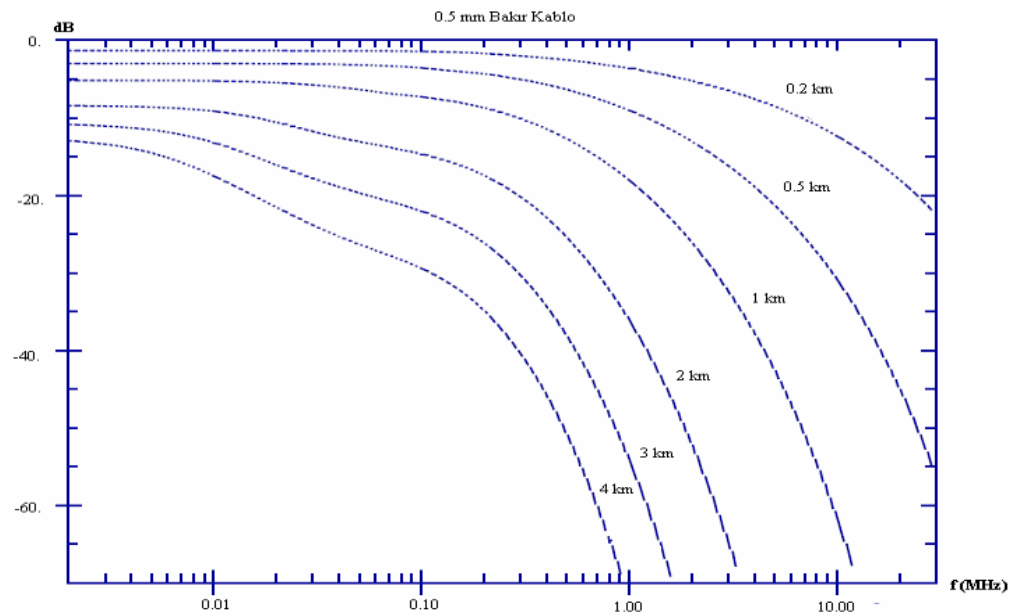
Analog Haberleşme]Bu sorun hatalı filtrelemeden v e FDM uygulanan sistemlerdeki hatalardan da kaynaklanabilir. Saydığımız bu üç gürültü, sistemlerde kapasite sınırlayıcı etki yaratırlar. RFI sinyalleri ve darbe gibi performans sınırlayan gürültüler de, genellikle doğada kesik kesik bulunan sinyallerden ka ynaklanan darbe gürültülerini oluşturur. Bu sinyaller coğrafi olarak değiskendirler ve önceden

belirlenemezler. Bu gürültüler sistemler üzerinde performans sınırlayıcı etki yaratırlar.

Bir hattın kalitesi Sinyal/Gürültü oranını temsil eden SNR değer iyle ifade edilir. Belirlenen band genişliği içinde desibel cinsinden işaret seviyesinin gürültü seviyesinden farkını ifade eder. Anlaşılacağı gibi bu oran ne kadar büyükse hattımızda o kadar kalitelidir.

2.3.2 Zayıflama

İletim ortamının direnci neticesinde sinyalin genliğinde meydana gelen düşmelerdir. Bu sorunun giderilmesi için alıcı ile verici arasına yineleyici ya da güçlendirici donanımlar yerleştirilir. Ancak bu cihazların iki uç arasında çok sayıda kullanımları bunların aynı zamanda ortamdaki gürültüleride yükseltmeleri nedeniyle sinyal kalitesinde düşmelere neden olmaktadır.



Şekil 2.4 Mesafe ve Frekansa Göre Kablo Kayıpları

Kablonun uzunluğu, kablo çapı, frekans, kablonun dallara ayrılması kanal zayıflamalarını etkileyen faktörlerdir. Zayıflama mesafe ve frekansa göre kablo kayıpları degrafik olarak görülmektedir. Frekans ve mesafe arttıgında kablo kayıpları da artmaktadır.

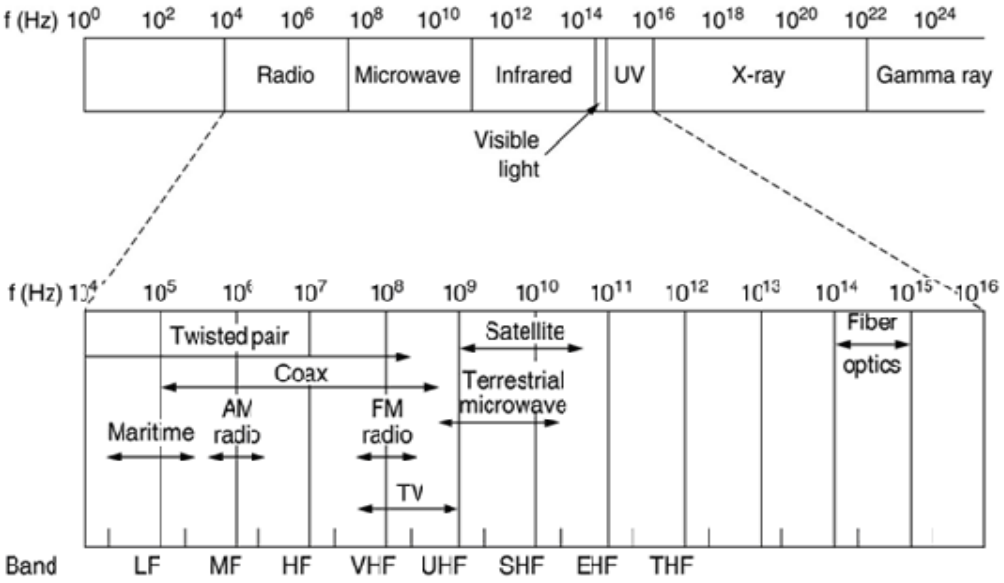
2.3.3 Gecikme

Mesajın farklı bileşenlerinin alıcıya farklı zamanlarda ulaşmasıdır. Gecikme kullanılan devrenin türü, ortamdaki bozucu etkiler, alıcı ve verici uçların trafik yoğunluğu ya da sistemde bulunan mesajın geçtiği uç birimlerdeki süreçlerden kaynaklanabilir.

2.4 İletişim Kanallarının Karakteristikleri

Daha önce iletişim kanalı alıcıdan vericiye gönderilen verinin kullandığı fiziksel ortamı ifade ettiğini belirtmiştim. Ortam üzerindeki veriler elektriksel ya da ışık halinde kablolar vasıtasıyla veya elektromanyetik dalgalar biçiminde uzayda kablosuz olarak taşınır.(Baykal, 2001, sy.37)

İletişim kanalı olarak kullandığımız manyetik kaset ya da hard disk gibi veri depolama aygıtları da iletişim açısından telefon ya da bir radyo kanalıyla aynı iletişim özelliklerine sahip olması bakımından bu ortam kavramı içinde kullanılabilir. Günümüzde en çok kullanılan iletişim biçimi optik kuralara göre çalışan Fiber Optik Sistemler vasıtasıyla yapılmaktadır. Geçmişte kullanılan RF dalgalarının kullanımıyla yapılan veri iletiminin yerini Fiber Optik iletişim almıştır. Günümüzde özellikle uzak mesafelerde popülerliğini daha fazla kaybeden RF iletişim, kısa mesafeli kampüs içi veri iletişimde kullanılmaktadır.



Şekil 2.5 Elektromanyetik Spectrum ve Haberleşmede Kullanımı

Bu frekansların genel kullanımı ise aşağıdaki tabloda özetlendiği biçimdedir.

Tablo 2.1 Frekansların Kullanım Alanları

Tanım Aralığı	**Frekans**	**Kullanıldığı Yer**
3-30 KHz	**VLF**	Navigasyon, Sonar, Radyo yayınları
30-300 KHz	**LF**	Radyo ile yön bulma-seyir, Navigasyon yardım
300-3000 KHz	**MF**	AM Yayını, deniz radyosu, sahil güvenlik haberleşmesi, yön bulma
3-30 MHz	**HF**	Telefon, Telgraf, Faks, Kısa dalga uluslar arası Radyo Yayını, Uzun menzili yerden yere, havadan yere ve gemiden havaya haberleşme, Radyo ile Seyir
30-300 MHz	**VHF**	TV, FM Yayını, Polis, Taksi Mobil Haberleşme, telsiz haberleşmesi
300-3000 MHz	**UHF**	Askeri amaçlı tek kanallı uydu haberleşmesi, TV, Radyo Dalgalarıyla Meteoroloji Merkezine data iletme, GPS
3-30 GHz	**SHF**	Askeri amaçlı çok kanallı uydu haberleşmesi için, Uçak Radarı, Mikrodalga linkler, Kara - Mobil Haberleşmesi
30-300 GHz	**EHF**	Radar, Deneysel Amaçlar

2.5 Kablolu İletişim Ortamları

Telefon ağları kablolu iletişimin en yoğun kullanıldığı uygulamalardır. Kablolu iletişim; iki telli açık kablo, çift burgulu kablo, UTP, koaksiyel olarak bilinen eşeksenli kablolar ve fiber optik kablolar kablolu kanallar olarak kullanılan ortamlardan yapılan iletişimi ifade etmektedir.

2.5.1 İki Telli Açık Kablo

En basit iletişim ortamı iki telli kablodur. Her tel diğerinden yalıtılmış ve her ikiside boşluğa açılmıştır. Bu tür kabl olar birbirinden yaklaşık 50 m. uzaklıkta ve en fazla 19,2 kbps ye kadar olan sistemler için kullanılabilir. (Baykal, 2001, sy.39)

2.5.2 Çift Burgulu (Twisted Pair) Kablolar

Özellikle LAN'larda kullanılan bu kablo tipinde, bir çift kablodaki her te l kendi eşiyle helezonik biçimde döndürülür. Bu sayede ortamda bulunan diğer tel çiftlerinin elektromanyetik karışımdan etkilenmemesini sağlayarak hem gürültüyü azaltır hem de hata oranını düşürür. Bu kablolar tekli olabilecekleri gibi dörtlü ya da sekizli de olabilir. Bu kablolar 100 m.ye kadar 1 Mbps 'ye kadar hızlarda veri iletimine imkan tanırken, hız mesafenin artmasıyla ters orantılı olarak bağıntılıdır. Bu kablolar diğer iletişim ortamlarına göre veri hızı ve band genişliği düşüklüğü ile iletişimin y apıldığı mesafede kısalık gibi handikaplara sahipken, özellikle kısa mesafede çalışan az kullanıcılı ağlarda ucuzluk ve kurulum kolaylığı bakımından tercih edilmektedir.

2.5.3 UTP Kablolar

İçerisinde bulunan 4 çift bakır kablodan her bir çiftin bir birleri üzerindeki elektromanyetik etkileri azaltmak üzere birbirine sarıldığı kablolardır.

CAT1 ve CAT2 kablolar düşük hızlı veri ve ses iletiminde kullanılırken 80'li yılların sonunda CAT3 ve daha sonra CAT5 kablolar kullanılmaya başlandı. Günümüzde neredeyse tüm yerel ağ bağlantılarında kullanılan CAT5 kablolar, cm.ye düşen bükülme oranı ile CAT3 kablolardan ayrılırlar. Yalıtımlarının teflonla yapıldığı "CAT5 ler 100 metreye kadar 100 Mbps hıza kadar veri iletimine olanak sağlamaktadırlar." (Özbilen, 2005, syf.25)

Daha yüksek bir teknolojiyle üretilen CAT6 kablolar ise 1000 Mbps hızında veri aktarımına imkan vermektedir. Bu kabloların kullanımında RJ-45 konnektörler kullanılmaktadır.

2.5.4 Eş Eksenli (Koaksiyel) Kablo

Özellikle elektriksel gürültünün yoğun olduğu çevre şartlarında kullanılan bu kablolar, kurulumlarının zorluğu ve pahalı oluşlarıyla diğer kablolara göre dezavantajlara sahiptir. Bu kablolarda bakır telin üzeri bir yalıtım maddesiyle kaplanmış olup onun üzeriyse bakır ya da aliminyum örgülü kabukla çevrilmişir. Bu tabakanın üzeride koruyucu plastik koruyucu kılıfla kaplanmıştır.

RG6, RG8 ve RG58 olmak üzere üç çeşit kullanımı olan bu kabloları birbirinden ayıran diğer karakteristik özellik de empedans değerlerdir. 75 ohm'luk em pedans değerine sahip olan RG6, ses ve veri taşımacılığında en güncel olarak da TV anteni ya da kablolu TV için kullanılan çeşitidir. 50 ohm'luk empedans değerine iki türden biri olan RG58, yerel ağlarda 180 metrelik mesafaye kadar kullanılırken; RG8 ise kalın tip olarak da bilinir ve yerel alan ağlarında 500 metrelik mesafeye kadar 10

Mbps hızına kadar veri aktarımına olanak sağlar. RG6 ve RG58 kablolar ucuz ve esneklikleriyle kalın olan RG8'e göre avantaj sağlarlarken verinin uzak measfelere iletimlerinde de RG8 kullanılır.

Bu kablolar, günümüzde 10 Mbps hızının artık çok yeterli olmaması ve bu kabloların UTP kablolara göre ekonomik ve fonksiyonel olmamaları nedeniyle yerel alan ağlarında neredeyse hiç kullanılmamaktadır.

2.5.5 Optik Lif Kablo

"Bakır tel, eş eksenli kablo gibi elektriksel sinyaller ya da radyolink (R/L), uydu haberleşmesi gibi radyo dalgaları ile yapılan iletişim sistemlerinde varolan; dinleme, karışma, gürültü, kapasite ve iletişim hızı düşüklüğü, band genişliği*uzaklık çarpanlarının ve esnekliklerinin az olması gibi olumsuz etkileri ortadan kaldıran optik iletim sistemi, iletişimde yeni bir dönem açmıştır.” (Çankaya ve Ertürk, 1999, sy.1)

Işıksal iletimi diğer iletim sistemlerinden farklı kılan özellikler şunlardır:

- Optik iletimde taşıyıcı frekansın çok yüksek olması; büyük bant genişliklerine ve daha yüksek hızda iletim imkanları verir. Başka bir değişle, geniş bantlı ve yüksek hızlı uygulamalar için oldukça yeterlidir.

- Sinyal zayıflamasının çok düşük olmasından dolayı diğer sistemlere göre çok daha uzun yineleyici aralıklarına olanak sağlar.

- Kabloların hafif ve ucuz olması, ayrıca bant genişliğinin yüksek olması nedeniyle istenen band genişliğinin daha az sayıda bağlantıyla sağlanabilmesi kanal başına maliyette ekonomi sağla maktadır.

- Bu kablolar, üzerinden gizli bağlantılar kurma ya da bilgi sızdırmanın zor olmasından dolayı, veri güvenliğinde avantaj sağlar. Bilgi çalınması ancak ışığı yerel olarak fiber damar içerisine verip diğer uçtan alma yöntemi olan "Local Injection and Dedection" olarak bilinen sistemlerle sağlanabilir ki bu hem güçtür, hem de yapılan saldırıların tespiti çok kolaydır.

- Bu kablolardaki iletişim, optik dalgalar vasıtasıyla yapıldığından bozucu elektromanyetik faktörlerden etkilenmesi mümkün değildir. Boz ucu elektromanyetik etkilerin olmaması ve kullanıcı sistemlerin daha teknolojik olması nedeniyle sahip olunan düşük hata oranı sağlanmıştır.

- Elektromanyetik etkilerin olmaması, yüksek gerilim iletkenlerinin içine fiber kabloların yerleştirilerek kullanılab ilmesi gibi farklı bir kullanım alanına olanak sağlar.

- Optik iletimde ışınlar, fiber dışına sadece kıvrımlardan çıkabilir. Ancak buralardan çıksa bile diğer sinyalleri etkilemez. Bu nedenle karışma sorunu yoktur.

- Alış-veriş uçlarında elektriksel yalıtım va rdır ve değişik çevre koşullarında da güvenli olarak kullanılabilir.

Optik Fiberlerin kullanım alanları

Fiber optik kabloların sahip olduğu avantajlar, bu kabloların haberleşme sistemlerinin büyük bölümünde, en önemlisi de internet omurgasında kull anımını cazip kılmıştır. Santraller arası bağlantılarda, bina içi iletim sistemlerinde, kapalı devre televizyon sistemlerinde, elektronik aygıtların birbiri ile bağlantısında, havacılık alanında yüksek hız gerektiren aygıtlar arası ve uçak iç donanımlarınd a, demiryolu elektrifikasyon ve sinyalizasyon uygulamalarında, trafik kontrol sistemlerinde, tıp alanında kullanılan aygıtlarda, nükleer enerji santralleri ve radyoaktif ışınların iletişimi bozduğu yerlerde kullanılır.

Ağ tasarımında; güvenlik, iletişim band genişliği, gürültü, hız, ağ arabirim kartları, yineleyici kullanımını, ortamın özellikleri ve kurulum maliyeti göz önünde bulundurulmaktadır. Dolayısıyla kablo seçimide bu kriterlerden öne çıkana göre yapılmaktadır. (Çankaya ve Ertürk, 1999, sy.7 -11)

2.5.6 Kablosuz İletişim

Kablosuz İletişimin keşfi Oersted, Faraday, Gauss, Maxwell ve Hertz'in çalışmalarından kaynaklanmaktadır. 1820 yılında Oersted, elektrik akımının bir manyetik alan yarattığını kanıtladı. 29 Ağustos 1831'de Michael Farad ay iletken bir maddenin etrafında bir mıknatısın hareketiyle bir akımın üretildiğini gösterdi. Bu değişen manyetik alanın elektriksel bir alan oluşturduğunu gösterdi. Bu çalımaların ışığında, 1864 yılında Maxwell elektromanyetik radyasyonun varlığını ve formülasyonunu temel bir teoriyle yayınladı. Maxwell teorisi 1877 yılında Hertz tarafından deneysel olarak ispatlandı. 1894 yılında İngiltere Oxford'da radyo sinyallerini algılayan hassas bir cihaz olan Dalga Alıcısı, mucidi Oliver Lodge tarafından kullanılarak 150 yard mesafede kablosuz iletişim sağlandı. (Proakis and Salahi, 2002, sy.3)

Bu mesafe 1895 yılında Guglielmo Marconi tarafından 2 km.'ye çıkarılmıştır. 1904 yılından vakum diyodun, 1906 yılında vakum triod yükselticilerin bulunması, yine bu yüzyılın başlarında radyo yayınlarını mümkün kılmıştır. Bundan sonraki yıllarda bu konudaki çalışmalar devam etti. İkinci Dünya Savaşı'da radyo haberleşmesi kullanılmaya başlandı ve bu haberleşme yöntemi savaştan sonra da günlük haberleşme ve güvenlik ihtiyaçlarının karşılanmasında kullanıldı. İlk televizyon sistemi 1929 yılında kurulurken, ilk ticari televizyon yayını 1936 yılında İngiltere'de gerçekleştirildi. Bu yıllarda elektronik sektörün yaşanan gelişmeler, haberleşme sistemlerine de büyük katkılar sağlamıştır. İlk TV yayını Telstar 1 uydusu yardımıyla Fransa'dan ABD'ye 1962 yılında aktarılır. Ticari uydu haberleşmesi servisi de 1965

yılında başlar. Bu konu ilerideki bölümlerimizde daha ayrıntılı biçimde incelenecektir.

2.6 Veri iletişim Tarihi

1799: "İletişimdeki en önemli buluşlardan birisi, Alessandro Volta'nın 1799 yılındaki elektrik aküleri keşfidir. Bu keşif, Samuel Morse'un 1837 yılında açıklayacağı elektrik telgrafının geliştirilmesini mümkün kılmıştır. İlk telgraf linki, Mayıs 1844'de Baltimore ile Washington arasında kurulmuştur. (Proakis and Salahi, 2002, sy.2)

1858: "Telgraf haberleşmesindeki en önemli mihenk taşı, 1858 yılında Birleşik Devletler ile Avrupa arasında kurulan ilk kıtalararası kablonun kurulumudur. Bu kablo, kurulumundan yaklaşık 4 hafta sonra denizaltı bağlantısı onarılamayacak şekilde arızalandı. İkinci kablo bundan birkaç yıl sonra Temmuz 1866 yılında kullanılabilir biçimde tekrar çekildi." (Proakis and Salahi, 2002, sy.2)

1876: Alexander Graham Bell, telefonun patentini aldı ve 1877 yılında Bell Telephone Company'i kurdu.

1880: A.Graham Bell tarafından 200 m.lik haberleşme sağlandı.

1887: Charles Vernen Boys, ilk ince cam fiberi gerçekleştirdi.

1906: "Triod yükselticilerin Lee De Forest tarafından 1906 yılındaki keşfi, telefon iletişim sistemlerinde sinyal yükseltimine ve bundan dolayı da çok uzak mesafalere sinyal iletimine imkân sağladı. Örneğin kıtalararası telefon iletişimi 1915 yılında kullanılmaya hazır hale geldi." (Proakis and Salahi, 2002, sy.3)

1950: Direkt görüntü iletiminde ilk kez cam fiber kullanıldı.

1958 -1960: Önce 300 bps ile 1200 bps hızlarında ve daha sonra 2400 bps hızında modemler piyasaya tanıtıldı. Bu tür modemler; dial -up ve düsük hız kiralık hatlarda full dupleks veri iletimlerinde örneğin bankalar ile bankala rın ATM (Para Çekme Makinaları) bağlantılarında kullanılmaktadır. Ayrıca 1960 yılında LASER'in başarıyla çalışması sağlanmıştır.(Yücel, 2005, sy.17)

1970: 70'li yıllarda X.25 standartı kullanılmaya başlanmıştır. Yine TCP/IP'nin ve fiber optik kabloların kullanılmaya başlanması da bu yıllara denk gelmektedir.

1980: 80'li yıllarda Frame Relay standartı X.25 in yerine kullanılması düşünülen bir standart olarak ortaya çıkmış ve LAN (yerel alan ağlarında) ethernet standartları belirlenmiştir.

1983': Bu yılın başlarında internetin babası ARPANET'in resmi protokolu TCP/IP olarak kabul edildi ve 1 Ocak 1984 tarihinde 100 adet bilgisayarın bağlantısı ile ilk internet bağlantısı kuruldu.

1984: Dünya telefon şirketleri, ISDN'i (Tümleşik Hizmetler Sayısal Şebekesi) haberleşme de kullanma konusunda fikir birliğine vardılar. ISDN, günümüzde hala kullanılan, ancak ADSL'in ortaya çıkmasıyla cazibesini kaybetmiş bir teknolojidir.

1990: "90'lı yıllarda ATM (Eşzamansız İletim Modu) tekniği piyasaya çıkmıştır.1992'de HDSL ve 1993'de de ADSL, telefon hatları üzerinden yüksek veri iletimini sağlayacak şekilde standartlaştırıldı. "(Yücel, 2005, sy.17]

Günümüzde de devam eden büyük ve hızlı dönüşüm ile çok yüksek hızlarda haberleşme imkanlarına sahibiz. Bu durumda da, bilgi teknoloji leri ve haberleşmenin önemini daha da artmaktadır.

3 İNTERNET VE TCP/İP

İnternet genel olarak, TCP/IP protokolü ile kontrol edilen, birbirinden tamamen farklı ağlardaki bilgisayar sistemleri arasında telekomünikasyon alt yapısını kullanarak veri iletimini destekleyen, küresel tek bir ağ gibi çalışan bilgisayar şebekesi olarak tanımlanır.

"Günümüzün gözde haberleşme sistemi olan internet, soğuk savaşın etkisiyle (bir taarruz esnasında bütün sorumluluklarını üstlenmiş bir bilgisayarın zarar görmesine karşılık)1960'da ABD savunma bakanlığı tarafından ARPANET adıyla kuruldu ve 1990'dan sonra hızla gelişerek bugünkü halini aldı." (Yılmaz, 2006, sy. 607)

TCP/IP, ilk defa ABD'de Arpanet (Advanced Research Projects Agency Network) adı altında, askeri bir proje olarak geliştirildi. Önceleri askeri amaçlı düşünülen proje, önce üniversiteler tarafından kullanılmaya başlandı. Ardından ABD'nin dört bir yanında birbirinden bağımsız geliştirilen ağlar, tek bir omurga altında NSFNet olarak adlandırıldı ve ulusal boyutu aşarak dünyaya yayıldı. İnternet'in doğuşu da bu tarihe denk gelir.

TCP/IP protokolü ağlar arasında evrensel bir dilin kullanılması ve iletişimin donanıma ya da yazılıma bağımlı olmaması amacıyla kullanılmaktadır. İlk olarak Unix işletim sistemlerinde kullanılan bu protokol bahsedildiği gibi daha sonra tüm ağlarda bir standart haline gelmiştir.

3.1 Osi Referans Modeli

Ortamın fiziksel tasarımı, bu ortam üzerinden bir noktadan bir noktaya veri aktarımı ve kodlamanın yapılması, paketlerin oluşturulması ve varış noktasına

yönlendirilmesi, veri aktarımı sırasında oluşan hataların çeşitli yöntemlerle giderilmesi, ağdaki bir hattın ya da birimin bozulması ya da ağda oluşan bir yoğunluk durumunda alternatif yolların değerlendirilmesi, paketlerin birleştirilmesi ve verinin kullanıcıya sunulması, değişik işletim sistemlerine sahip bilgisayarların birbiriyle olan haberleşmesi gibi daha pekçok işlemin yerine getirilmesi 1978 yılında ISO (International Organizations of Standarts) tarafından geliştirilen, Ağ iletişiminde standart bir model olan Osi Referans Modeli ile sağlanır.

Bu model, her katmanın görevinin belirlendiği 7 protokol katmanı ile tanımlanır ve her protokol katmanı karşı tarafta kendi katmanıyla haberleşir. Şekilde de ifade edildiği gibi her katmanda aktarılan veri, farklı biçimde isimlendirilmektedir.

Fiziksel Katman: Verinin fiziksel (bakır tel, optic lif, hava…) ortamda taşınması için gerekli yapıyı, kodlamayı oluşturur." (Oktuğ, sy.2)

Veri Bağlantı Katmanı: Bu katman, ağ üzerindeki bilgisayarların fiziksel olarak adreslenmesinden ve paketlerin aynı fiziksel bağlantı üzerinde olan bilgisayarlara taşınmasından, hata denetimi ile akış kontrolü görevinin yerine getirilmesinden sorumludur. Güvenli iletişim açısından önemli bir kavram olan MAC adresleri bu katmanda kullanılır. MAC kavramına ilerideki konularımızda değinilecektir.

Ağ Katmanı: Mesajların mantıksal adreslere taşınması için yönlendirme işleminin yapıldığı katmandır. Bu katman üzerinde yer alan mesaj birimleri ne paket ya da datagram denir. Bu katman veri bağlantı katmanı tarafından sağlanan noktadan noktaya bağlantı ilkesine göre çalışır. İnternet omurgasını oluşturan yönlendiriciler bu katmanda çalışırlar.

Taşıma Katmanı: Bu katman veri akış kontrolü, hata denetimi ve belirlenen hataların giderilmesi ile çoklama gibi hizmetleri sunar. Hata denetiminin yapıldığı son katmandır.

Oturum Katmanı: Bilgisayarlar arasında bağlantının kurulumunu, yönetimini, sonlandırılmasını ve uygulama veya sunum düzeyinde veri akışını kontrol eder. Ağ

üzerinde bir bilgisayara bağlanarak oturum açmak gibi işlemlerin yapıldığı bu katman da çift yönlü haberleşme yapılır.

Sunum Katmanı: İletilecek olan verinin yapısının belirtildiği katmandır. Verilerin şifrelenmesi-sıkıştırılmasıyla, kod formatı ve dönüşümlerini ve verilerin gösterimini sağlar.

Uygulama Katmanı: Programların ağ kaynaklarına erişimini sağlar.

Katmanlar arasında geçiş yapan bilgilere bulunduğu katmanın başlık bilgisi eklenir ya da çıkartılır. Yukarıda bahsettiğimiz verilerin farklı adları temel olarak bu başlık bilgilerinin eklenip çıkartılmasıyla ortaya çıkan yeni veriyi ifade etmektedir. (Oktuğ, sy.1-6)

3.2 İP ve Port Kavramları

TCP/İP protokolündeki ilk temel nokta, ağ üzerinde yer alan tüm noktalara bir ip adresi atanmasıdır. İnternet üzerinde yer alan her ağ birbirinden farklı ve çakışmaya yer vermeyecek biçimde adreslendirilir. Bu adresleri kullanan yönlendiriciler, sahip oldukları yönlendirme tabloları vasıtasıyla bir paketin iletimini sağlarlar.

İp adresleri bilgisayarların internet protokolü üzerinde çalışmasını sağlayan tanımlamalardır. Bilgisayarların bulundukları ağı temsil eden net id kısmı ve ağ içindeki bilgisayarların birbirinden ayrılmasını sağlayan host id kısmı olmak üzere iki kısımdan oluşmaktadır.

İPv4 ve İpv6 olmak üzere 2 çeşit ip adresi vardır. Günümüzde 32 bitlik adresleme sağlayan İpv4 kullanılmaktadır, ancak önümüzdeki dönemde işlevsellik ve kullanım kolaylığı sağlayan 128 bitlik adreslemenin yapıldığı ipv6 ya geçiş

hızlanacaktır. İPv6'ya geçişin en önemli nedeni ise; İpv4 de tanımlı adreslerin, tükenme noktasına yaklaşmasıdır.

İp adresleri, farklı sayıdaki ağları ve bu ağlardaki farklı sayıdaki bilgisayarları temsil etmesine göre A, B, C, D ve E olmak üzere 5 farklı sını fa ayrılmışlardır. A sınıfı adresler 127 ağı ve 16.777.214 bilgisayarı, B sınıfı adresler 16.383 ağı ve 65534 bilgisayarı, C sınıfı adresler 2.097.151 ağı ve 254 bilgisayarı ifade edebilmektedir. Görüldüğü gibi A sınıfı bilgisayarlar az ağı -çok bilgisayarı temsil etmekteyken bu sayılar diğer sınıflarda değişmektedir.

TCP/IP protokolünde açıklanması gereken kavramlardan biride port kavramıdır. Çünkü servisler port numaralarıyla birbirlerinden ayrılırlar. Port adresi servisin TCP'mi UDP'mi olduğu bilgi sini; ip adresi toplamı da soket kavramını açıklamaktadır.

Örneğin bir ip adresi hırsızların girdiği bir evin adresi, portları da bu evin kilitlenmiş ve kilitlenmemiş kapıları olarak varsaydığımızda; hırsızların eve girdiklerinde kolayca açarak girdikleri kilitsiz kapılar UDP portlarını, kilitli kapılar ise TCP portlarını ifade etmektedir.

Tablo 3.1 0-1023 Aralığındaki 'Bilinen Portlar'

PORT	AÇIKLAMA	DURUM
0/TCP,UDP	Ayrılmış; kullanımda değil	Resmi
1/TCP,UDP	TCPMUX (TCP multiplexer (çoğul plexer) port ser visi)	Resmi
4/UDP	NTP Zaman Protokolu	Resmi
5/TCP,UDP	RJE (Uzak(taki) Görevi Silme/Engelleme)	Resmi

7/TCP,UDP	ECHO protokolü	Resmi
9/TCP,UDP	Engelleme protokolü	Resmi
13/TCP,UDP	Zaman protokolü	Resmi
17/TCP,UDP	QOTD (Günün alıntısı) protokolü	Resmi
18/TCP,UDP	Mesaj Yollama Protokolü	Resmi
19/TCP,UDP	CHARGEN (Karakter Oluşturucu) protokol	Resmi
20/TCP,UDP	FTP - veri protokolü	Resmi
21/TCP,UDP	FTP – kontrol (veri gönderme/alma) portu	Resmi
22/TCP,UDP	SSH (Güvenli Shell) - Güvenli veri transfer işlemleri (SCP, SFTP) ve port yönlendirme işlemleri	Resmi
23/TCP,UDP	Telnet protocol – unencrypted text communications	Resmi
25/TCP,UDP	SMTP – E-Posta gönderme Protokolü E-mails	Resmi
26/TCP,UDP	RSFTP - A simple FTP-like protocol	Gayriresmi
37/TCP,UDP	TIME protocol	Resmi
38/TCP,UDP	Yönlendirici Erişim Protokolü	Resmi
39/TCP,UDP	Kaynak Belirtme Protokolü	Resmi
41/TCP,UDP	Grafik(ler)	Resmi

42/TCP,UDP	İsim Sunucusu	Resmi
49/TCP,UDP	TACACS Giriş barındırma protokolü	Resmi
53/TCP,UDP	DNS (AlanAdı İsim Sunucusu)	Resmi
57/TCP	MTP, Mail Transfer Protokolü	
67/UDP	BOOTP (BootStrap Protocol) sunucusu; ayrıca DHCP (Dynamic Host Configuration Protocol / Değişken Barındırma Ayarları Protokolü) tarafından kullanılmaktadır.	Resmi
68/UDP	BOOTP kullanıcısı; ayrıca DHCP tarafından da kullanılmaktadır.	Resmi
69/UDP	TFTP (Trivial Dosya Transfer Protokolü)	Resmi
70/TCP	Gopher protokolü	Resmi
79/TCP	Finger protokolü	Resmi
80/TCP	HTTP – web sayfaları gösterim/yayınlama protokolü	Resmi
80/TCP,UDP	Skype – CONFLICT with http listening ports	Anlaşmazlık
88/TCP	Kerberos - yetkilendirme aracısı	Resmi
101/TCP	HOSTNAME	
107/TCP	Uzak TelNet Servisi	
109/TCP	POP, Post Office Protokolü, sürüm 2	

110/TCP	POP3 – E-mail alım protokolü	Resmi
113/TCP	ident - eski sunucularda tanıtım sistemi, hâlâ IRC sunucuları tarafından kullanıcı tanımında kullanılmaktadır.	Resmi
115/TCP	SFTP, Simple Dosya Transfer Protokolü	
118/TCP,UDP	SQL Servisleri	Resmi
119/TCP	NNTP (Network News Transfer Protocol) - haber gruplarından mesajların alınmasında kullanılır	Resmi
123/UDP	NTP (Network Time Protocol) - zaman senkronizasyonunda kullanılır	Resmi
137/TCP,UDP	NetBIOS NetBIOS İsim Servisi	Resmi
138/TCP,UDP	NetBIOS NetBIOS Datagram Service	Resmi
139/TCP,UDP	NetBIOS NetBIOS Session Service	Resmi
143/TCP,UDP	IMAP4 (Internet Message Access Protocol 4) - used for retrieving E-mails	Resmi
152/TCP,UDP	BFTP, Arka Plan Dosya Aktarım Programı	
153/TCP,UDP	SGMP, Simple Gateway Monitoring Protocol	
156/TCP,UDP	SQL Service	Resmi
158/TCP,UDP	DMSP, Distributed Mail Service Protocol	
161/TCP,UDP	SNMP (Simple Network Management Protocol)	Resmi

162/TCP,UDP	SNMPTRAP	Resmi
179/TCP	BGP (Border Gateway Protocol)	Resmi
194/TCP	IRC (Internet Relay Chat)	Resmi
201/TCP,UDP	AppleTalk Routing Maintenance	
209/TCP,UDP	The Quick Mail Transfer Protocol	
213/TCP,UDP	IPX	Resmi
218/TCP,UDP	MPP, Message Posting Protocol	
220/TCP,UDP	IMAP, Interactive Mail Access Protocol, version 3	
259/TCP,UDP	ESRO, Efficient Short Remote Operations	
264/TCP,UDP	BGMP, Border Gateway Multicast Protocol	
318/TCP,UDP	TSP, Time Stamp Protocol	
323/TCP,UDP	IMMP, Internet Message Mapping Protocol	
366/TCP,UDP	SMTP, Simple Mail Transfer Protocol. ODMR, On-Demand Mail Relay	
369/TCP,UDP	Rpc2portmap	Resmi
384/TCP,UDP	A Remote Network Server System	
387/TCP,UDP	AURP, AppleTalk Update-based Routing Protocol	

389/TCP,UDP	LDAP (Lightweight Directory Access Protocol)	Resmi
401/TCP,UDP	UPS Uninterruptible Power Supply	Resmi
411/TCP	Direct Connect Hub port	Gayriresmi
427/TCP,UDP	SLP (Serivce Location Protocol)	Resmi
443/TCP,UDP	HTTPS – TLS/SSL üzerinden http Protokolü (Kriptolanmış aktarım)	Resmi
444/TCP,UDP	SNPP, Simple Network Paging Protocol	
445/TCP	Microsoft-DS (Active Directory, Windows shares, Sasser-worm, Agobot, Zobotworm)	Resmi
445/UDP	Microsoft-DS SMB file sharing	Resmi
464/TCP,UDP	Kerberos Change/Set password	Resmi
465/TCP	SMTP over SSL – CONFLICT with registered Cisco protocol	Anlaşmazlık
500/TCP,UDP	Isakmp, IKE-Internet Key Exchange	Resmi
514/TCP	rsh protocol - used to execute non-interactive commandline commands on a remote system and see the screen return	
514/UDP	syslog protocol – used for system logging	Resmi
515/TCP	Line Printer Daemon protocol - used in LPD printer servers	
524/TCP,UDP	NCP (NetWare Core Protocol) is used for a variety things such as access to primary NetWare server resources, Time Synchronization, etc.	Resmi

530/TCP,UDP	Rpc	Resmi
531/TCP,UDP	AOL Instant Messenger, IRC	Gayriresmi
540/TCP	UUCP (Unix-to-Unix Copy Protocol)	Resmi
542/TCP,UDP	commerce (Commerce Applications) (RFC maintained by: Randy Epstein [repstein at host.net])	Resmi
546/TCP,UDP	DHCPv6 client	
547/TCP,UDP	DHCPv6 server	
554/TCP	RTSP (Real Time Streaming Protocol)	Resmi
563/TCP,UDP	NNTP protocol over TLS/SSL (NNTPS)	Resmi
587/TCP	email message submission (SMTP) (RFC 2476)	Resmi
591/TCP	FileMaker 6.0 Web Sharing (HTTP Alternate, see port 80)	Resmi
593/TCP,UDP	HTTP RPC Ep Map	Resmi
604/TCP	TUNNEL	
631/TCP,UDP	IPP, Internet Printing Protocol	
636/TCP,UDP	LDAP over SSL (encrypted transmission)	Resmi
639/TCP,UDP	MSDP, Multicast Source Discovery Protocol	
646/TCP	LDP, Label Distribution Protocol	

647/TCP	DHCP Failover Protocol	
648/TCP	RRP, Registry Registrar Protocol	
652/TCP	DTCP, Dynamic Tunnel Configuration Protocol	
654/TCP	AODV, Ad hoc On-Demand Distance Vector	
666/TCP		Resmi
674/TCP	ACAP, Application Configuration Access Protocol	
691/TCP	MS Exchange Routing	Resmi
695/TCP	IEEE-MMS-SSL	
699/TCP	Access Network	
700/TCP	EPP, Extensible Provisioning Protocol	
701/TCP	LMP, Link Management Protocol.	
702/TCP	IRIS over BEEP	
706/TCP	SILC, Secure Internet Live Conferencing	
711/TCP	TDP, Tag Distribution Protocol	
712/TCP	TBRPF, Topology Broadcast based on Reverse-Path Forwarding	
720/TCP	SMQP, Simple Message Queue Protocol	

829/TCP	CMP (Certificate Managemaent Protocol)	
860/TCP	İSCSI	
873/TCP	rsync File synchronisation protocol	Resmi
901/TCP	Samba Web Administration Tool (SWAT)	Gayriresmi
981/TCP	SofaWare Technologies Remote HTTPS management for firewall devices running embedded Checkpoint Firewall-1 software	Gayrirresmî
989/TCP,UDP	FTP Protocol (data) over TLS/SSL	Resmi
990/TCP,UDP	FTP Protocol (control) over TLS/SSL	Resmi
991/TCP,UDP	NAS (Netnews Admin System)	
992/TCP,UDP	TLS/SSL Üzerinden Telnet Protokolü	Resmi
993/TCP	SSL üzerinden IMAP4 (Kriptolanmış aktarım)	Resmi
995/TCP	SSL üzerinden POP3 Protokolü (Kriptolanmış aktarım)	Resmi

Diğer portlar hakkındaki bilgilere "http://www.iana.org/assignments/port-numbers" adresinden erişilebilir.

3.3 Yeni Nesil İP Protokolü (İpv6)

Yeni nesil ip protokolünü daha iyi anlayabilmek için İpv4 ile İpv6'nın karşılaştırılmasını incelemek daha yerinde olacaktır. Buna göre;

1. İpv6'nın 128 bitlik adres büyüklüğüne sahip olması, 32 bitlik ipv4'e göre daha fazla adres tanımlamaya olanak verir. Ayrıca, ipv6 içerisinde tanımlanan faaliyet alanı, grupsal yayın paketlerinin ağ üzerinde yayılmasını oldukça kolay hale getirir.

2. İpv4 başlık alanı içerisinde bulunan bazı bölümlerin ipv6'da isteğe bağlı olarak tanımlanmış olması, hem bu mesajların yönlendirici mekanizmaları tarafından daha kolay yönetilebilmesine imkân tanır, hem de bu alanların olmaması nedeniyle veriye ayrılan bölümün artmış olması neticesinde daha fazla veri taşınabilmesi bakımından da verimliliği doğurur.

3. İpv6 protokolü veri akışı sırasında bazı bağlantılara öncelik tanıyan belirteçler kullanır ve bağlantılara daha iyi hizmet sunulması sağlanır.

4. Bağlantılar arasında doğruluğun kesinleştirilmesi, verilerin gerçekten bağlantı veri dizisi içinde yer aldığının tespiti, verilerin gizliliğinin sağlanması ipv6 mimarisi içerisinde tanımlanan güvenlik ve gizlilik tedbirleridir.(Dirican, 2005, sy.255-256)

3.4 Telekomünikasyon Alt Yapısı

Telekomünikasyon şebekesini genel olarak santral donanımı, transmisyon donanımı ve erişim sistemleri olmak üzere 3 kısımda inceleyebiliriz.

Telekomünikasyon şebekesinin genel yapısı bünyesindeki ADSL, X.25, ISDN, PSTN ile gösterilen anahtarlama birimleri; santral donanımını, santral birimlerinin uzak mesafelerde birbirleri ile irtibatını sağlayan sistemlere; transmisyon donanımı, santral donanımı ile müşteri arasındaki iletişimi sağlayan sistemlere ise; erişim sistemleri adı verilmektedir. Transmisyon ortamı olarak genellikle fiber optik veya R/L üzerinden SDH (Synchronous Hiera rchy-Eşzamanlı Hiyerarşi) sistemleri, ya da uydu sistemleri kullanılmaktadır. Erişim şebekelerinde iletim ortamı olarak; bakır iletkenli kablo, fiber optik kablo, koaksiyel kablo, uydu veya kablosuz sistemler kullanılır. (Yücel, 2005, sy.2-3)

Sayısal modemler en fazla 2 Mbps'e kadar iletime olanak sağlamaktadır. Bu noktada, daha yüksek hızlar için birden fazla modemin kullanılması düşünülebilir ancak bu, pratikte birçok dezavantajı da beraberinde getirmektedir. İşte SDH -PDH gibi donanımlar da bu yüksek hız ihtiyaçlarını karşılamak için ortaya çıkmaktadırlar. Türk Telekom transmisyon şebekesini oluşturan ana omurganın tamamında, tüm metropolitan şebekelerde ve bölgesel şebekelerin büyük bölümünde, fiber optik kablolar üzerinden irtibatlandırılan SDH tr ansmisyon teçhizatları kullanılmaktadır.

SDH sistemlerinin sağladığı bazı avantajlar aşağıdaki gibidir:

1. Tek bir uluslararası hiyerarşi kullanması nedeniyle tüm dünyada bir standartlaşma getirmesi,

2. GSM, veri, internet gibi hizmet şebekelerinin hızla artan t rafik ihtiyaçlarını karşılayabilecek yüksek kapasitelere çıkabilmesi,

3. Korumalı/yedekli devre imkânları sağlaması nedeniyle, yüksek kapasitelerde trafik kullanan hizmet şebekelerine yüksek hizmet kalitesi sunabilmesi,

4. Tek bir teçhizat üzerinde, hem yüksek hem düşük hızlara erişim imkânı olabilmesi ve değişik seviye sinyaller arasında doğrudan ekleme çıkarma yapılabilmesi,

5. Pratik ve güçlü bir işletim/yönetim sistemine sahip olması ve gelişmiş arıza, konfigürasyon ve performans yönetimi ile bu yönetim sisteminin esneklik ve güvenilirlik getirmesi,

6. Daha az sayıda teçhizat gereksinimi ve tek bir noktadan erişim imkânı da sağlayan gelişmiş işletim/yönetim sistemleri sayesinde, network yatırım ve işletme maliyetlerinde azalma sağlamasıdır. (http://www.gym-tech.net)

SDH'e göre bazı dezavantajlara sahip, PDH (Plesiochronous Digital Hierarchy - Yakın Eşzamanlı Sayısal Hiyerarşi) teçhizatları da, Türk Telekom alt yapısında hala kullanılmaktadır. Bu bakımdan bu cihazların SDH teçhizatları ile farklılıklarını irdelemek yerinde olacaktır.

PDH ile SDH arasındaki temel farklılıklar şunlardır:

1. PDH'de sistemler yakın eşzamanlı olarak çalışırken, SDH'de mikrosaniyeler seviyesinde dahi eş zamanlı olarak çalışan bir sistem mevcuttur.

2. Her iki sistemin zamanlama faklılıklarından kaynaklanan PDH'de bit-bit, SDH'de ise bayt-bayt çoklama teknikleri mevcuttur.

3. PDH 140 Mb/s'e kadar standartlaşmışken SDH, 155 Mb/s üzerinden STM-1 (155 Mb/s), STM-4 (622 Mb/s), STM-16 (2.5 Gb/s) ve STM-64 (10 Gb/s) olmak üzere standartlaşmıştır.

4. PDH'de iç içe geçmiş kanallara erişim, sadece ayırmadan sonra mümkünken SDH'de istenilen kanala istenilen anda erişim söz konusudur.

SDH, fiber optik ortamının yüksek band genişliği ve güvenilirlik avantajlarından yararlanmak için fiber optik transmisyon linkleri ve radyolinkler kullanır.

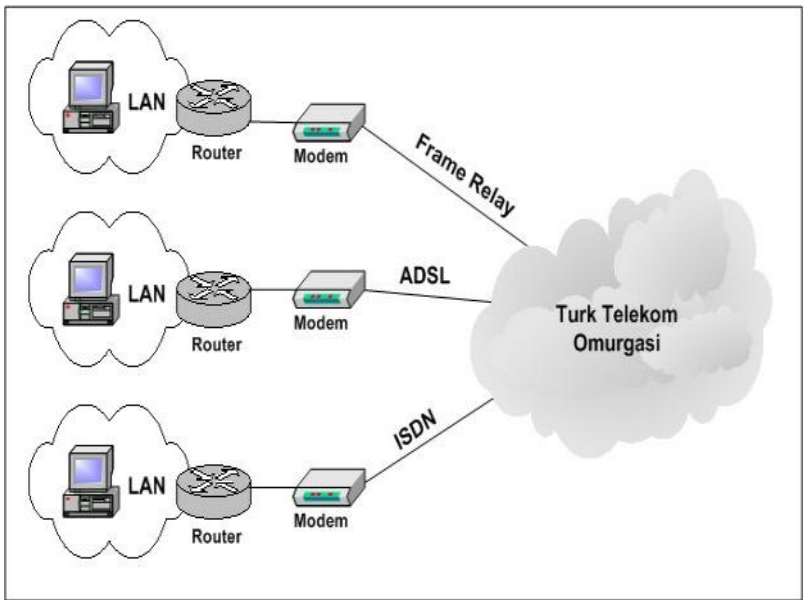
3.5 Kullanılan Teknolojiler

"ATM (Asyncronous Transfer Mode) anahtarlama temelli bir alt yapıda kurulan TTNetwork şebekesi ile ATM, FR (Frame Relay), ADSL (Asymetrical Digital Subscriber Line), LL (Leased Line) erişimi ile PSTN (Public Switched Telephony Network), B-ISDN (Integrated Services Digital Network) ve KabloTV üzerinden İnternet erişim şekilleri desteklenmektedir." (http://www.turktelekom.com.tr)

"TTNetwork Şebekesi başlangıç topolojisinde; Ankara, İstan bul (Ataköy, Tahtakale, Gayrettepe, Acıbadem, Kadıköy), İzmir, Adana, Samsun, Bursa, Antalya, Kayseri illerinde kurulan ana omurga 155 Mbps, diğer illerimiz ve Lefkoşe'de kurulan erişim noktaları ise 34 veya en az 2 Mbps hızında ATM protokolü ile TTNetwork şebekesine bağlanmaktadır. TTNetwork omurgasındaki tüm bağlantılar, alternatifli olarak tanımlanmıştır. Böylece, şebeke ve servislerin sürekliliği açısından güvenilir bir yapı sağlanmaktadır.

İnternet erişimi bakımından ev kullanıcıları genellikle, modem lerin kulllanıldığı 56 kbps hıza imkân tanıyan Dial-up veya yüksek hızlara imkân tanıyan, ülkemizde de yaygın bir kullanıma sahip ADSL ile erişim sağlarlar. Kurumsal kullanıcılar ise kiralık hat, ISDN, xDSL, FR veya ATM bağlantıları ile pop noktalarına eri şim sağlamaktadır. Dial-up erişiminin yüksek hızlı uygulamalar için yetersiz kalması ve yönetilme yeteneklerinden yoksun olması, diğer teknolojilere yönelime neden olmuştur. (http://www.turktelekom.com.tr)

Kişisel kullanıcılar, ISS'ler (internet servis sağ layıcı) üzerinden internete bağlanırlar. Servis sağlayıcılar, internet bulutuna aynı anda birçok verinin iletimine uygun olarak tasarlanmış ana iletim hattı olarak tabir edebileceğimiz bir omurga (backbone) ile bağlanan kurumlardır. Bir ülke, bir veya bird en fazla omurgaya sahip olabilir ve birbirine bağlı olan bu omurgalar interneti oluşturur.(Yücel, 2005, sy. 15)



Şekil 3.1 Türk Telekom Şematik Omurgası (Barkın, 2003)

3.5.1 Hücre Anahtarlamalı Şebekeler (ATM)

"Her geçen gün kendini daha güçlü his settiren bilgi çağı koşulları, bilginin daha yoğun ve güvenli gönderilmesi için bilgi otoyollarını zorunlu kılmaktadır. Bilindiği üzere kullanıcıların geniş alanda yüksek hız ve esnek band ihtiyaçlarını karşılamada ATM teknolojisi, bütün dünyada tek çözüm olarak kullanılmaktadır. Her türlü verinin yüksek hızlarda, aynı ortamda iletimine imkân sağlayan ATM; 2 Mbit/s'den başlayarak 622 Mbit/s hız seviyelerine kadar servis vermektedir." (http://www.turktelekom.com.tr)

Bağlantı temelli çalışan ATM'de veri bilgi si, sabit uzunluklu 53 byte hücreler halinde 5 byte başlık, 48 byte salt veri olmak üzere taşınır. Bu teknolojide hata düzeltme yapılmaması ve iletilen paketlerin çok küçük olması nedeniyle gecikmeler

azdır ve bu nedenledir ki; veri, ses ve video gibi uygu lamalar için çok uygun bir iletişim ortamı sunar.

Şu anda Türk Telekom veri haberleşmesi ana omurgasında, üniversiteler ve birçok kurum ile ISS'ler gibi büyük şirketlerin ana omurgalarında ATM kullanmaktadır.

3.5.2 X.25 ve Frame Relay

Verilerin küçük paketlere bölünerek çalışması prensibine dayalı paket anahtarlamalı sistemlerden X,25 ve Frame Relay, temelde aynı mantık da çalışırlar.

Farklı ağlardaki sistemlerin noktadan noktaya kurulan sanal devreler üzerinden iletişimini sağlayan kurallar bütünü olan X.25, yoğun hata kontrolü ve düzeltmesi yapan bir protokoldür.

Bu teknolojide, aynı fiziksel hat ya da port üzerinden değişik hız ve protokoldeki terminaller, birbirleri ile iletişim kurarlar. Arıza durumunda, ağda bulunan herbir düğümün birbirine bağlı olması nedeniyle yeni yollar kullanıcı hissetmeden otomatik olarak seçilir.

Türk Telekom tarafından, 2,4–64 Kbps arasında X.25 devreleri verilmektedir. Üzerinden geçen trafiğe göre değişken olarak ücretlendirilen bu servis, internet gibi yüksek hız gerektiren uygulamalar için kullanıma uygun değildir. Bu teknolojinin ülkemizdeki ilk uygulanması, yurt içinde ve dışındaki sistemlerin birbirleriyle iletişimini sağlayan sistemlerden biri olan TURPAK olarak kabul edilir. Bu sistem de iletişim; kullanıcı adı ve şifresi kullanılarak sadece arama, sadece aranma ya da belirli kullanıcıların birbirleriyle iletişimi biçiminde olabilir.

"Ekonomik, güvenilir ve kaliteli iletişim sağlayan TURPAK Şebekesine erişim ITI, DIAL-UP, X.25, SDLC, API, PRIVATE DIAL-IN, Frame Relay ve ATM protokolleri ile sağlanabilmektedir."(http://www.turktelekom.com.tr)

Paket anahtarlamalı bir teknoloji olan FR, 1997 yılından beri ülkemizde de yaygın biçimde kullanılmaktadır. Daha çok şehir dışı çoklu ofis bağlantıl arının sağlanmasında kullanılan bu teknolojide; birden fazla noktanın tek bir fiziksel hat üzerinden, ihtiyaca göre esnek bant genişliğine imkân sağlayan bağlantılar kurabilmesi amaçlanmıştır. Yüksek hızlı bu iletişim teknolojisi, düşük hızlardan başlayarak, 2, 34 ve 50 Mbps'ye varan hızlarla servis vermektedir. Tek fiziksel hat üzerinden sağlanan birden fazla iletişim olanağı kiralık hatlar ile kıyaslandığında, gerekli devre sayısında azalma ve maliyette tasarruf bakımından alternatif bir iletişim teknolojisi olarak karşımıza çıkmaktadır. FR'in yüksek hızlara çıkabilmesindeki en önemli faktörlerden birisi; uç cihazlar üzerindeki TCP/IP temelli uygulamaların hata denetim ve düzeltme mekanizmalarının da dikkate alınmasıyla, X.25'deki çoğu denetleme fonksiyonunun en alt seviyelere düşürülmüş olmasıdır.

İSS'lerin internet bulutuna bağlantıda da kullandıkları bu teknolojinin ATM teknolojisine açık oluşu onu cazip kılan diğer bir konudur. Ancak Frame Relay'in, kısa süreli yoğun trafiğe sahip bağlantılar için uygun ken ses ve normal data iletişiminde pek uygun olmadığını söyleyebiliriz.

Bu anlatılanlar doğrultusunda X.25 ile Frame Relay'in en temel farklılığı; X.25'in doğru veri iletimini, gecikmelere rağmen garanti etmesine rağmen, Frame Relay'in daha hızlı olmasına rağmen doğru veri iletimini garanti etmemesidir.

3.5.3 Metro Ethernet

Metro Ethernet, günümüz yerel ağlarının neredeyse tamamında kullanılan ethernet protokolünün, optik iletişimle F/O kablo üzerinden, yüksek bant genişliğini

kullanarak tüm şehire uygulanması fikrinden doğmuştur. Teknolojinin gelişmesi ve daha yüksek bant genişliği ihtiyacıyla, başlangıçta 10 Mbps bant genişliğine sahip ethernet protokol hızı, 1000 Mbps'ye kadar çıkarılmıştır.100 Mbps hızındaki portlar fast ethernet, 1000 Mbps portlar ise gigabit ethernet olmak üzere isimlendirilir. IEEE 802.3 olarak da adlandırılan ve 2.katmanda çalışan ethetnet protokolünde, ağ üzerinde çalışan birden fazla bilgisayardan, aynı anda sadece biri veri gönderirken diğerleri beklemelidir. Bekleme olmadan ağ ortamına veri gönderilmesi çarpışmalara neden olur. Ethernet protokolünün en büyük zaafiyeti olan bu durum, trafiğin az olduğu hatlarda fazla problem yaratmazken yoğun ağlarda uygun donanım seçimi ve planlamanın yapılmasıyla aşılır.

"Metro Ethernetler; fiber optik kablo bağlantısı ile Gigabit seviyesine kadar esnek ve düşük maliyette bağlantı seçeneği sağlar. Bağlantıları, yedeklemeli olarak kurulduğundan herhangi bir link kopması durumunda çok kısa bir sürede iletim yedeğe aktarılır. Uçtan uca ethernet paketi, taşıdığı - paket dönüşümüne ihtiyaç duymadığı - için SDH, router veya modem gibi ek yatırımlara ihtiyaç duyulmaz." (http://www.turktelekom.com.tr)

3.5.4 Isdn

Yaklaşık 20 yıl önce özellikle Amerika'da yaygın olarak kullanılmaya başlanan ISDN, günümüzdeki diğer yüksek hızlı teknolojilerle kıyaslandığında daha az kullanım olasılığı bulmaktadır. Devre anahtarlamalı bir teknoloji olan ISDN, aynı anda ses, veri hatta görüntü taşınmasına imkân verir. İletişim, telefon numarası bilinen bir müşteriye çağrı yapılarak kurulur ve iletişim gerçekleştikten sonra bağlantı kesilir.

ISDN hizmetleri; temel hız erişimi (ISDN BA) ve birincil hız erişimi (ISDN PA) olmak üzere iki temel standart erişime sahiptir. Temel hız erişimi; 2 adet 64 kbps B kanalı ile 1 adet 16 kbps hızındaki D kanalından oluşur. 2B kanalı veri aktarımında,

D kanalı ise kontrol ve senkronizasyon işlemlerinde kullanılır. Birincil hız erişimi ise; 30 adet 64 kbps B kanalı ile 1 adet D kanalından oluşur.

"ISDN teknolojisini alışılmış analog hatlardan ayıran en önemli özellik tamamen sayısal temiz bir ses kanalı sağlamasının yanında, aynı anda veri iletişimine de izin verebilmesidir." (http://www.turktelekom.com.tr)

3.5.5 Xdsl Teknolojileri

Mevcut bakır şebekenin atıl kapasitesinin, sayısal modem teknolojileri sayesinde örneğin; 1,5 Mbps ile santrale yaklaşık 5 km. uzaklıktan çevrimiçi film, ya da santrale yaklaşık 3,5 km. uzaklıktan 6 mbps ile sayısal televizyon yayınının izlenebilmesi gibi yüksek hızda veri iletişiminde kullanılmasıdır. XDSL teknolojileri farklı kullanım ve hızlar bakımından ADSL, HDSL, VDSL, SDSL ve IDSL olmak üzere gruplandırılır. Örneğin 20 Mbps veri transfer hızları gerektiren HDTV yayını ADSL ile değil, hat uzunlukları ile kıyaslandığında daha yüksek hızlara çıkabilen VDSL üzerinden daha iyi hizmet kalitesine sahiptir. Bu teknolojiler ile ayrıca uzaktan eğitim servisleri ya da görüntülü telefon ya da video konferans servisleri de verilebilmektedir.

Kurulu telefon altyapısının kullanılmasıyla yeni altyapı yatırımına ihtiyaç olmaması, veri iletiminde sağladığı çok yüksek bant genişliği, iletimin sağlanması noktasında kullanılan donanımların, sağladıkları hız, esneklik ve uygulama alanlarına göre diğer teknolojilere oranla sağladığı maliyet avantajları, aynı hat üzerinden aynı anda ses ve veri iletimini desteklemesi yanında sürekli bir bağlantı da sağlaması XDSL teknolojilerini cazip kılmaktadır.

HDSL (Yüksek Hızlı Sayısal Abone hattı)

En eski xDSL teknolojisi olan HDSL ile; yaklaşık 3.5 km l ik hatlar üzerinden her iki yönde de aynı hızda veri iletimini ifade eden kavramla ,simetrik olarak 2 Mbit/s' e kadar iletim yapılabilir. HDSL ile 2 twisted pair üzerinden T1 (1.544 Mbps) veya E1 (2.048 Mbps) hızlarında iletim yapılır.

HDSL ; Baz istasyonlarının birbirleri arasında kurulan 2Mbit/s'lik bağlantılarda ve mevcut bakır şebekesi ile maksimum sayıdaki aboneye 64kbit/s'lik ses kanalının sağlanmasında yaygın biçimde kullanılmaktadır.Hat bakımından dezavantaja sahip devrelerde bile HDSL modem ler kullanılabilmektedir.

SDSL (Simetrik Sayısal Abone hattı)

HDSL'de 2 twisted pair kablo kullanımının teke düşürülmüş biçimi olarak değerlendirebileceğimiz SDSL genellikle kiralık hatlarda kullanılan, 2 Mb/s data aktarım hızını ifade etmektedir. S antralden 3km. Mesafeye kadar kullanılabilen simetrik teknolojidir.

ADSL (Asimetrik Sayısal Abone Hattı)

HDSL'den sonra mevcut bakır şebeke üzerinden özellikle ev kullanıcıları için düşünülmüş ve bu doğrultuda kullanıcılar yönünde daha yüksek, sant rale doğru ise daha küçük hızı ifade eden asimetrik bir teknolojidir. Her kullanıcı kendine tahsis edilen hattı kullanır. Yani kullanıcıların bağlantıları, ortak bir şebekeyi paylaşan kablonet'te olduğu gibi birbirlerinin band genişliklerini etkilemez. Ads l'de konuşmanın yapıldığı frekans değerinin üzerindeki frekansların kullanılması aynı anda telefon görüşmelerine de olanak sağlar ki bu ADSL'in en önemli özeliklerinden biridir.

ADSL, "Bir yönde 6-8 Mbit/s hıza kadar iletim yaparken diğer yönde 640 Kbit/s ile 1 Mbit/s arasında iletim sağlayabilmektedir. (Alkan ve ark. Tekedere, Polat, 2001, sy.4)

Başlangıçta video-on-demand için tasarlanan ADSL teknolojisinin hızlı internet erişimi için uyarlanmış biçimi ise ADSL-Lite olarak adlandırılmaktadır ve yaklaşık 1.5 Mbit/s hızlarında sınırlıdır.

Türk Telekom'un yavaş yavaş hayata geçirmeye başladığı sms, video görüşme, tv izleme gibi interaktif servisler ADSL'i gelecekte daha da cazip kılacaktır.

VDSL (Çok Yüksek Hızlı Sayısal Abone Hattı)

Adından da anlaşılabileceği gibi kısa erişimli yapıda simetrik olarak 20 Mbit/s'in üzerinde, uzun erişimli yapıda ise asimetrik olarak 52 Mbit/s hızına kadar varan genişbant teknolojidir.

ADSL'e göre değerlendiridiğinde daha kısa mesafelerde çok büyük oranla rda hızları ifade ederken sistem karmaşıklığı bakımından da çok daha basit bir devre yapısına sahiptir.

IDSL (Tümleştirilmiş Sayısal Abone Hattı)

IDSL, isminden de anlaşıldığı gibi, 2 tane 64 Kbps B kanalın, 5,5 km.'ye kadar her iki yönde toplam 128 Kbps hızında veri taşıyan bir veri servisine dönüştürürüldüğü, simetrik, düşük düzeyde görüntülü konferans, İnternet ve LAN'lara uzaktan erişim için kullanılabilen bir servistir.

3.5.6 Kiralık Hatlar

İstenilen değişik hızlarda seçilebilen analog veya sayısal iletim, uçtan uca sabit fiziksel bir devreyle oluşturulur. Yönetiminin kolaylığı avantajıyken, yedeklemeli bir yapı için karışık ağ topolojilerine ihtiyaç duyması dezavantajı olarak sayılabilir. Türkiye'de kiralık devreler için genellikle TDM sistemi kullanılan "kiralık hat

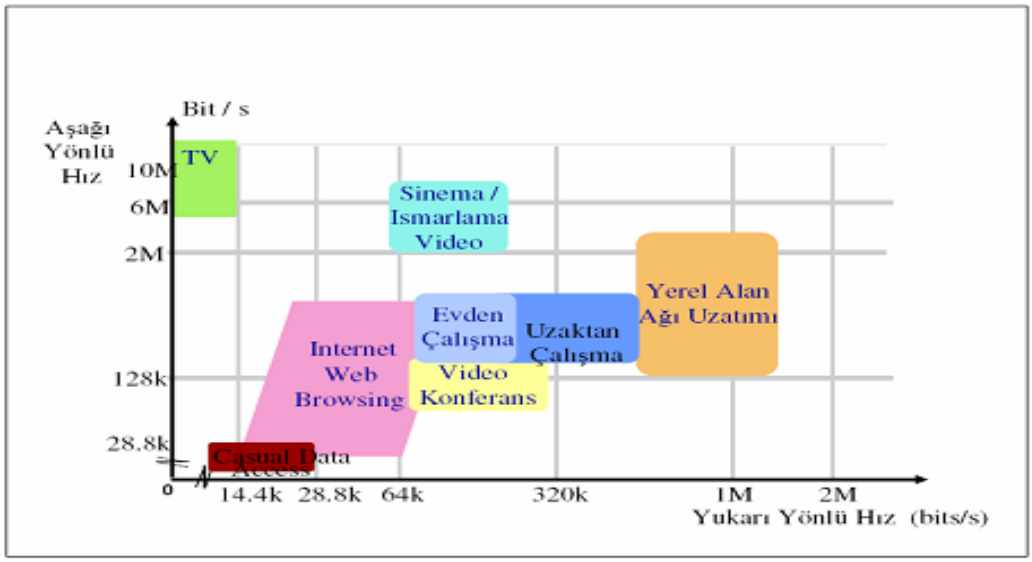
servisiyle 64 Kbps ile 34 Mbps hızları arasında uçtan uca yönetilebilen devreler tahsis edilebilir."(http://www.elkotek.com.tr)

Kiralık hatlar sağladıkları sabit bandgenişliği garantisi, kolay yönetilebilir olması ve müşteriye özel bir kanal tahsis edilmesi nedeniyle güvenilir olması bakımından tercih edilir. Özellikle ofisler arasında ses, görüntü ve veri trafiğinin aynı anda iletilmesinin istendiği uygulamalarda kiralık hat en iyi çözümü sunmaktadır. Kiralık hat uygulamalarını başlıca "internete erişim" ve "ofisler arasında bağlantılar" için kullanılmaktadır.

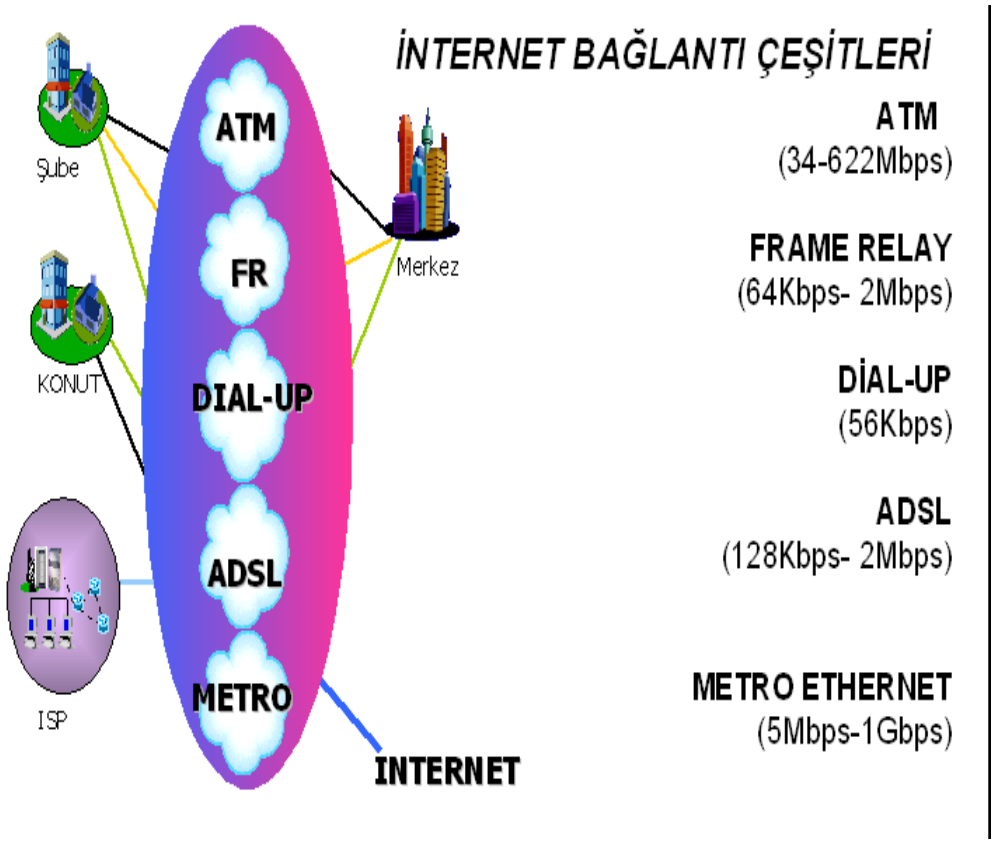
3.5.7 Kablo Tv Ağları

"Kablo TV, değişik transmisyon ortamlarından gelen analog ve/veya sayısal radyo, televizyon (TV) ve data sinyallerinin birleştiri lip çoklanarak sayısal paketler ve/veya analog sinyaller halinde, fiber ve/veya koaksiyel kablolar üzerinden abonelere/kullanıcılara, etkileşimli haberleşmeyi (interaktiviteyi) sağlayacak şekilde, iletilmesidir. Kablo TV işletmeciliğinde abonelere/kullanıc ılara geniş bantlı ve hızlı Internet erişimi, geniş band veri aktarımı, sayısal ve/veya analog TV ve radyo yayını, multimedya ve VoIP hizmetleri verilmektedir.

Dünyada hızlı bir gelişme gösteren kısaca kablo TV (Cable TV) olarak tanımlanan kablo ağı ilk döneminde sadece analog televizyon yayınlarının kesintisiz ve net bir şekilde tek yönlü olarak televizyon izleyicilerine ulaştırılmasına yönelik geliştirilmiş idi. Bu alt yapının özellikle fiber koaksiyel karma yapıya dönüşmesi, şebekenin çift yönlü olarak kurulmasına imkân sağlamıştır; bu sayede mevcut bakır kablolu telekomünikasyon altyapısı ile verilen tüm hizmetler Kablo TV şebekesi ile de verilebilir hale gelmiş ayrıca bir üstünlük olarak son kullanıcıya doğru daha geniş frekans bandı sağlandığı için geniş bantlı telekomünikasyon hizmetlerinin de verilebilmesine imkân sağlanmıştır."(Telkoder, KabloTV komisyonu Raporu Özeti, 2003)



Şekil 3.2 Servislerin Bant Genişliği İhtiyaçları



Şekil 3.3 İnternet Bağlantı Çeşitleri (Karaman İl Telekom Müdürlüğü, 20 06, sy.4)

3.5.8 Türk Telekom-Bgp

Blackhole Community (9121:666): DoS ataklar için; BGP kullanarak, belli bir grup IP bloğu boşa yönlendirilerek kullanıcıya doğru yapılan atak otomatikman engellenmiş olur.

Sadece Yurtiçi Community (9121:444) : Kullanıcılar kendilerine ait IP bloklarına erişimi engelleyerek, yurtdışından yapılan ataklara karşı tedbir alabilir. Bu durumda yurt içinde ki kullanıcıların erişiminde kesinti yaşanmaz.

Aşağıdaki tablo tüm bağlantı türleri bakımından özet niteliğinded ir

Tablo 3.2 Bağlantı Türlerinin Temel Özellikleri

(http://img157.imageshack.us/img157/92/wanservicesfl9.jpg).

Service	Bandwidth (Max.)	Line Type	Signaling Method	Characteristics
Public Switched Telephone Network (PSTN)	56 Kbps	POTS	Analog	Dialup over regular telephone lines
Leased lines	56 Kbps	POTS	Analog	Dedicated line with consistent line quality
X.25	64 Kbps	POTS	Analog	Dedicated line Variable packet sizes (frames) Ideal for low-quality lines
Frame Relay	1.54 Mbps	POTS T-1 T-3	Digital	Variable packet sizes (frames)
Asynchronous Transfer Mode (ATM)	1.2 Gbps	Coaxial, twisted pair, fiber-optic	Digital	Fixed-size cells (53-byte) High-quality, high-speed lines
Integrated Services Digital Network (ISDN)	144 Kbps (BRI) 4 Mbps (PRI)	POTS T-1	Digital	Basic rate operates over regular telephone lines and is a dialup service Primary rate operates over T-carriers
DSL	6.1 Mbps (1.544 or lower is more common)	POTS	Digital	Operates using digital signals over regular telephone lines DSL comes in many different flavors (such as ADSL and HDSL)

4.AĞ KAVRAMI VE YEREL AĞLAR

İki bilgisayar arasındaki veri aktarımının en basit yöntemi her 2 uçta bulunan bilgisayarların direk olarak bağlanmasıdır. Bu bağlantı biçimi birbirine yakın bilgisayarlar arasında avantajlıyken uzak noktalar arasındaki iletişimde maliyet, güvenlik ve verimlilik bakımından makul değildir. Bu bakımdan noktadan noktaya bağlantı yerine ağlar üzerinden sağlanan iletişim tercih edilir.

Bilgisayar ağları büyüklüklerine göre; LAN (Yerel Alan Ağları), MAN (Metropolitan Alan Ağları) ve WAN (Geniş Alan Ağları) olmak üzere 3' ayrılır. LAN'lar genellikle tekbir bina ya da yerleşke içerisindeki ağları tanımlarken, MAN'lar genellikle bir şehirdeki ağları kapsayacak şekildedir. WAN'lar ise dünyanın çeşitli yerlerindeki ağları birbirine bağlayacak büyüklüktedir.

Bilgisayar ağlarını kullandıkları teknolojilere göreyse; yayın ağları ve anahtarlamalı ağlar olmak üzere iki biçimde inceleyebiliriz. Yayın ağlarında tek bir iletişim ortamı ve buna bağlı bilgisayarlar vardır. Yayın tüm bilgisayarlarca dinlenir ve aynı anda tek bilgisayar iletişimde bulunabilir.

Anahtarlamalı ağlarsa paket anahtarlamalı ve devre anahtarlamalı olmak üzere ikiye ayrılır.

"Devre anahtarlamalı ağlarda iki bilgisayar arasında bulunan düğümler üzerinde yalnız gönderilen verinin kullanımına ayrılmış bir iletişim yolu kurulur. Bu yol düğümler arasında link olarak adlandıracağımız bir dizi bağı bir araya getirir. Her bağda bir mantıksal kanal kurulan bir bağlantı için ayrılır. Kaynak bilgisayarın ürettiği veri bu ayrılmış yol üzerinden hızlı bir biçimde gönderilir. Gelen veri düğümlerde herhangi bir gecikme olmaksızın uygun kanala yönlendirilir ya da anahtarlanır. Devre anahtarlamalı ağların en bilinen örneği telefon ağlarıdır.

Paket anahtarlamalı ağlarda ise veri, paket olarak adlandırılan küçük parçalar halinde gönderilir. Ağın aktarım kapasitesi aynı anda gönderim yapan birden fazla bilgisayar

tarafından kullanılmaya uygundur. Herbir paket kaynaktan hedefe varıncaya kadar düğümden düğüme aktarılır. Herbir düğümde paketin tamamı alınır, depolanır ve tekrar aktarılır." (Baykal, 2001, sy.161)

Bilgisayarların birbirleriyle iletişimi ağlar vasıtasıyla olur. İletişimde ise temel kural bilgisayarların aynı dili kullanmaları ve fiziksel bağlantılarının olmasıdır. Ayrıca bilgisayarların birbirleriyle iletişiminde belirl enmiş bazı standartlar, kurallar ve sınırlamalar mevcuttur ki bu da fiziksel bağlantılar ve cihazlar kadar ağ unsurunu oluşturan elemanlar olarak kabul edilmelidir. Bilgisayar ağlarında veri iletişimi kodlama, çerçeveleme ya da diğer adıyla kapsülleme, hat a saptama, iletişim hattının güvenliğinin saptanması ve erişim denetim mekanizmalarının sağlanması olmak üzere 5 kısımda incelenir.

Günümüzde yerel ağların neredeyse tamamında Ethernet Protokolü kullanılır. Ethernet protokolüne metro ethernet bölümü nde değinilmiştir. Bu protokolün haricinde Jetonlu Halka (Token Ring), Jetonlu yol (Token Bus), FDDI (Fiber Distributed Data İnterface) gibi protokoller kullanılmakla beraber bunlara geçerliliğini kaybetmiş olmaları nedeniyle ayrıntılı olarak değinilmeyece ktir.

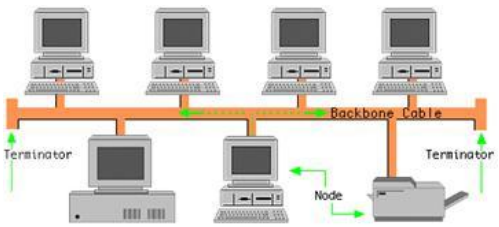
LAN'lara kullanıcıların çeşitli donanımları ve verileri paylaşma ihtiyacıyla, hızlı iletişimin sağlanması, kaynakların merkezi denetimden geçmesi zorunluluğu ve yeni uygulamaların işlevsel olabilmesi için birden çok bilgisayara ihtiyaç duymaları gibi nedenlerle ihtiyaç duyulur.

4.1 Ağ Topolojileri

Bir ağdaki bilgisayarların bağlantılarının nasıl yapılacağı ağ topolojileriyle ifade edilir ve en çok kullanılan ağ topolojileri; yol (bus), yıldız (star), ağaç (tree) ve ring topolojileridir.

4.1.1 Yol Topolojisi

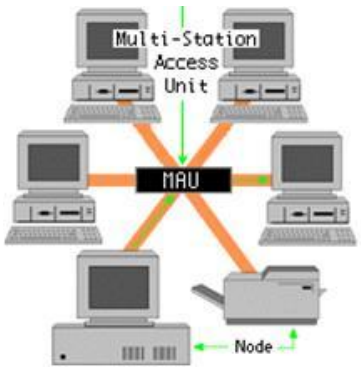
Sunucuların, iş istasyonlarının ve diğer çevre birimlerinin tipik olarak koaksiyel kablodan oluşan ve trunk adı verilen doğrusal bir kablo segmentini paylaşmasıyla oluşur. İletilen verilere diğer istasyonlarca da erişilebilir. Ethern et ağı bu topolojiye örnektir.



Şekil 4.1 Yol Topolojisi (www.sistemuzmani.com)

4.1.2 Halka Topolojisi

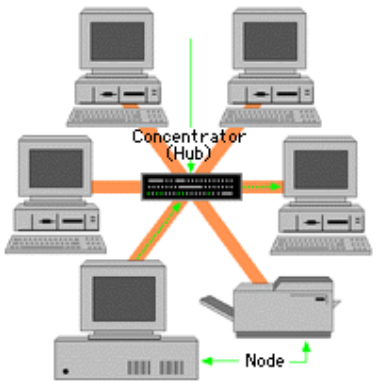
Tüm birimler, verinin tek yönlü olarak iletildiği çift yönlü bir halka biçiminde birbirine bağlıdır. FDDI ve Token Ring bu topolojiye örnektir.



Şekil 4.2 Halka Topolojisi (www.sistemuzmani.com)

4.1.3 Yıldız Topolojisi

Ağaç topolojiside aslında bir çeşit yıldız topolojidir. Bu topolojide Sunucu, İş istasyonları ve diğer çevre birimleri gibi uç birimler ağın tüm fonksiyonlarını yöneten bir anahtar veya hub ile direk olarak birbirine bağlanmıştır. Bu topolojinin en büyük dezavantajı ise merkezi birimin hayati önem taşımasıdır.



Şekil 4.3 Yıldız Yopolojisi (www.sistemuzmani.com)

4.2 Ağ Bağlantı Donanımları

Hub

Birinci katmanda çalışan bu ağ donanımlarının temel görevi; herhangi bir portundan gelen sinyali yükselterek diğer portlara göndermektir. Kendisine bağlı tüm bilgisayarlara ethernet'in temel felsefesinde olduğu gibi ortak bir paylaşım ortamı sunar. Ağ üzerinde merkezi bir nokta oluşturan bu cihazlar aktif ya da pasif veya aptal ya da akıllı olarak sınıflandırılırlar. Aktif hub'lar, sinyalleri güçlendirme işini bağlı oldukları güç kaynaklarından aldıkları enerji ile yaparlar. Akıllı hub'lar trafik akışını yönetmek üzere programlanmış hub'larken aptal hub'lar sadece sinyali alıp

kuvetlendirerek portlara dağıtan hublardır. Sinyali çoklu kullanıcı ortamı için bölen hublar ise pasif olarak adlandırılır. (Özbilen, 2005, sy.64)

Peşpeşe takılan hublar vasıtasıyla port sayısı artt ırılır ancak bir huba bağlı tüm bilgisayarlar aynı çarpışma alanında bulunduğundan bu durum çarpışma alanını daha da arttıracaktır. Hublar ucuz, tek çarpışma alanına sahip güvenli olmayan cihazlardır.

Köprüler

Osi referans modelinin 2.katmanında ça lışan bu cihazlar, topolojisi farklı olsa dahi aynı protokolleri kullanan İki Lan'ın birbirine bağlanmasında kullanılır. Köprüler ağ içerisinde iletilmek istenen verinin hangi ağa ait olduğnu inceliyerek eğer verinin varş noktası aynı ağ içerisinde ise ver inin gereksiz yere diğer ağa iletmeyerek trafik yaratmasını engellemiş olur. için kullanılan bu cihazlar 2. katmanda kullanılırlar. Ağ içerisinde iletimi yapılacak verinin doğru adrese iletilmesi köprünün görevidir.

Lan Anahtarları

Yüksek anahtarlam a ile bant genişliklerini, dolayısıyla ağ trafiğini hızlandırırlar. Sahip oldukları Mac tabloları sayesinde bir portundan gelen bir paketin nereye gönderileceğini bilen akıllı cihazlardır. Bu bakımdan sahip olduğu port sayısı kadar çarpışma alanı vardır. Örneğin 10 portlu bir anahtar 10 çarpışma alanına sahipken, 1 hub'ın sadece 1 çarpışma alanı vardır. (Özbilen, 2005, sy.64 -65)

Ağ Geçitleri

"Ağ terminolojisinde ağ geçitlerinin 2 türlü anlamı vardır. Birinci anlamı yönlendirme yapan cihazlarla diğer bir ağa ya da ağlara çıkışı tanımlayan adrestir. Diğer anlamı ise birbirine benzer olmayan, tamamıyla farklı teknolojiyle çalışan iki ağ arasında haberleşmeyi sağlayan fiziksel bir cihaz ya da yazılımdır."(Demirkol, 2001, sy.8)

İp adresleme mekanizmalarında anlatacağım ağ maskesi kavramını bu bölümde vermekte yarar görmekteyim. Çünkü ağ maskesi kavramı aslında ağ geçitleri ile yakından ilgilidir.

Bir İP adresindeki Host ID kısmı bitlerinin 0, Net ID kısmı bitlerinin 1 olduğu değerlerdir.Yani B sınıfı için 255.255.0.0, C sınıfı için 255.255.255.0 değeri ağ maskesini ifade etmektedir.

Ağ maskesi bir bilgisayarın verinin iletileceği bilgisayarla aynı ağda olup olmadığını kontrol amacıyla kullanılır.Bir bilgisayar kendi İpsi ile ağ maskesini mantıksal karşılaştırır.Ortaya çıkan değer, kendi İpsindeki Net İD kısmı ile aynı ise aynı ağda,değilse farklı ağda olduğunu anlar ve bu durumda veriyi yönlendiriciye yönlendirir.

Yönlendiriciler (Routerlar)

TCP/IP protokolüyle çalışan bu cihazlar köprül erden daha gelişmiş aygıtlar olup farklı ağlarda bulunan istasyonlardan gönderilen verilerin varış noktalarına iletilmesinden sorumludurlar. Ayrıca, örneğin İstanbul'da bulunan bir ağdaki verinin, Sivas'ta bulunan bir ağa iletimindeki tüm yolların değerlen dirilerek en uygun yoldan iletilmesi gibi bir görevi de üstlenmeleri bakımından önemlidirler.

5 PROTOKOLLER

Protokoller; iletişimin nasıl, ne zaman ve ne düzeyde yapılacağı noktasında iki noktanın aynı dili konuşmaları suretiyle birbirleriyle a nlaşmalarını, dolayısıyla iletişimi sağlayan standartlar kümesi olarak tanımlanır. " Bazı protokoller OSİ başvuru modelinin farklı katmanlarında çalışırlar ve o katmanın amacına uygun işlevler görürler. Bazı protokoller birlikte çalışarak protokol yığınlar ını oluştururlar." (Baykal, 2001, sy.172)

5.1 Donanım ve İP Adresi Dönüşüm Protokolleri

Bilgisayarlar yarattıkları datagramın, ağ üzerinde iletimini sağlamak için ip adreslerine, doğrudan bilgisayarlara ve hedeflere erişim içinse donanım adresleri ne ihtiyaç duyarlar. Bu etkileşim sayesinde bilgisayarlar arasında datagramların iletimi mümkün olur.

5.1.1 Adres Çözümleme Protokolleri (ARP)

Bilgisayarların haberleşmeleri ağ kartları vasıtasıyla olur ve bu kartlara fabrika ortamında MAC (Media A ccess Control) olarak adlandırılan numaralar verilir. İletişimin son aşamasında ağda bulunan bir veri alıcı adrese bu Mac adresleri vasıtasıyla iletilir. İletişim açısından ip adresleri kadar gerekli olan Mac adreslerinin bir diğer gerekliliği de TCP/IP pr otokolünü kullanmayan ağlarda kullanılma gerekliliğidir.

Veri bağlantı katmanı fiziksel donanım adreslerini kullanarak veri iletimini gerçekleştirir. Bu nedenle Ipv4 adreslerine karşılık gelen fiziksel adreslerin

çözümlenmesi ve belirlenmesi gerekir. Bu ise ARP protokolü kullanılarak yapılır. Bu protokol MAC adresi ile ip adresi arasında dinamik bağlantı kurarak bir bağlantı için tek başına yeterli olmayan ip adresi haricinde veri iletimi açısından hayati bir görev alır. İp adresleri değiştiği zaman bilgisayarlarda MAC adresine karşılık gelen ip adresleri de değişime uğrar.

DNS sembolik adreslerle ip adresleri arasında ilişki kurulmasında görev alır. İsimlerin ip adreslerine dönüştürülmesinde DNS. ip adreslerinin donanım adresleriyle eşleşmesinde de ARP protokolü kullanılır.

Ağ üzerinde bulunan bir bilgisayar başka bir bilgisayara veri gönderimi yapacaksa Arp istek paketi gönderir ve Mac adreslerini bildiği bilgisayarlara hedef ip'nin kime ait olduğunu sorar. Bu istek paketi ağ üzerindeki tüm bilgisayarlarca alınır ve bu pakette yer alan Mac adresine sahip olan bilgisayar bu pakete karşılık yanıt mesajı gönderir. Bu yanıt sonrasında veriyi gönderen bilgisayar yanıt mesajını gönderen bilgisayarın İp adresiyle Mac adresini ARP tablosuna ekle r.

Yönlendirme protokolleri ayrıca gönderilen bir verinin aynı ağdaki bir bilgisayara mı yoksa farklı ağdaki bir bilgisayara mı gönderileceğinin tespitinde de kullanılır. Eğer veri farklı bir ağa gönderilecekse ilgili yönlendiricinin, aynı ağdaki bir bilgisayara gidecekse de hedef bilgisayarın donanım adreslerinin tespiti ARP protokolü ile belirlenir.

Bir paket gönderilmeden önce kaynak bilgisayar önce kendi ARP tablosunu inceler. Eğer hedef bu tabloda yer almıyorsa istek paketi yayınlar. (Dirican, 2 005, sy.59-72)

5.1.2 Ters Adres Dönüşüm Protokolü (RARP)

Bilgisayarlar genellikle sabit diskleri üzerinde donanım adreslerine atanılan ip adreslerini depolarlar. Sabit diske sahip olmayan bilgisayarlar ya da ağ cihazları da

açılışları sırasında kullanacakları bilgileri başka bilgisayarlar üzerinden yüklerler. Bağlantının kurulması ve dosya transferinin gerçekleşmesi de TCP/IP protokolü şartıyla dolayısıyla ip atanması şartını getirir. İşte bu noktada ip adreslerinin belirlenmesi yapı ve çalışma itibarıyla RARP sunucularının ARP protokolüne çok benzeyen RARP protokolü ile çalışmalarıyla yapılır.

RARP sunucuları gelen istek karşısında belirtilen donanım adresine karşılık gelen ip adresini belirleyerek istekte bulunan bilgisayara iletirler. (Diri can, 2005, sy.73)

5.2 İnternet Protokolü

İnternet protokolü değişik türdeki ağlar arasında paket alış verişini sağlamak amacıyla tasarlanmıştır. İp adresleri arasında iletimi sağlayan protokol sadece kaynak ve hedef bilgisayarlar arasında paketlerin bitler halinde iletiminden sorumludur. Son noktalar arasında güvenli veri akışını, akış kontrolünü ve datagramın iletimini düzenleyecek herhangi bir mekanizmaya sahip değildir.

Bu protokol OSİ referans modeli içerisinde çalışan en işlevsel yapı olması bakımından da önemlidir. TCP, UDP, ICMP, IGMP protokolleri alacakları bilgileri ip datagramlar üzerinden temin ederler. İp datagramlar kolaylıkla taklit edilebilmeleri bakımından ve bağlantı tabanlı yani hedeflere ulaşma garantisinin olmaması bakımından güvensizdirler. Bu problem üst protokol katmanları içerisinde tanımlanan kontrol ve güvenlik birimleri vasıtasıyla giderilmelidir.

İnternet protokolü üzerinde çalıştığı ağı bant genişliği, donanım adresi, en büyük iletim birimi olan MTU (Maksimum Transmission Unit) gibi özellikleri soyutlayarak aktif hale getirir. Protokol kendi içerisinde hata denetimi yapan mekanizmalarına da sahiptir

MTU; Veri bağlantı katmanı kullanılarak gönderilebilecek en büyük datagramın boyutunu ifade eder. İnternet protokol katmanı datagramları ağ türüne öre değişen MTU değerini geçmeyecek şekilde tanımlar. Bu işleme parçalama (fragmentation) denir.

İp Datagram Yapısındaki Temel Kavramlar ise şöyle özetlenebilir:

Kaynak ve Hedef Adres: Datagramın iletildiği ve iletileceği adresi ifade eder.

Parçalama Bilgisi: Parçalanan paketlerin tekrardan birleştirilmesi için gerekli bilgileri içerir.

Datagramın Büyüklüğü: Datagramın büyüklüğünün, ne kadar veri taşındığının bilgisidir.

İp Başlığı Büyüklüğü: Burada güvenlik, veri yönlendirme vb. İşlemler için farklı büyüklüklerde kullanılacak büyüklükler değerlendirilebilir.

QoS Parametreleri: İp datagram başlığı üzerinde yer alan servis türü alanı, ağları talep edilen hizmet hakkında bilgilendirir. Bu servis bilgileri hizmet (QoS) parametreleri olarak adlandırılır. Bu sayede datagram için öncelik, güvenlik, gecikme gibi parametrelerin tanımlanmasına olanak verir. (Dirican, 2005, sy.79 -82)

5.3 Yönlendirme Protokolleri

"İnternet birbirine bağlanmış, birbirinden bağımsız organizasyonlar tarafından yönetilen değişik yapıdaki bilgisayar ağlarından oluşur. Bu noktaları birbirine bağlayan noktalar (backbones) birbirinden ayrı olarak idare edilir. Büyük organizasyonlarda bilgisayar ağlarını alt ağlara ayırarak, birbirinden bağımsız parçalar halinde yönetebilir. Bu sayede de ayrıştırılmış her ağ içerisinde bölümler

arası iş bölümü yapılabilir, küçültülen bilgisayar ağları daha kolay yönetilebilir, güvenlik ve organizasyon yönetim şemasına uygun atamalar daha kolay yapılabilir."

Birbirinden ayrı yönetilebilen ağlar otonom (özerk) sistemler kavramını ortaya çıkarmıştır. Bu sistemler daha kolay yönetim için alt ağlara ayrılmış olsalar bile dış dünya'ya tek bir yapı olarak görülürler. Her özerk sistem kendi yönlendirme protokolünü seçebilir ve kendi yönlendirme tablolarını diğer özerk sistemleri etkilemeden değiştirebilir. Yönlendiriciler tarafından kullanılan protokollere IGP (İnterior gateway protocol); Özerk sistemler arasındaki yönlendirme protokollerineyse EGP (Exterior Gateway Protocol) denir. Farklı ağlar üzerinde yer alan bilgisayarlar arasında TCP/IP tabanlı haberleşmenin gerçekleşmesi ağlar arasında datagramların yönlendirilmesiyle olur. Bu konuda kullanılan temel kavramlar aşağıda özetlenmiştir. (Dirican, 2005, sy. 173)

5.3.1 Datagramların Yönlendirilmesi

Osi modellemesinde de anlatıldığı gibi ağ katmanı ip datagramların yönlendirilmesi işlemlerinde kullanılmak için çeşitli kurallar dizisini bünyesinde barındırır. Bu işlemleri yürüten aygıtlar ise daha önce bahsedildiği gibi yönlendiricilerdir. Yönlendiriciler kendilerine gelen datagramların hedef ip adres alanını inceleyerek datagramları hedefe ulaştıracak diğer yönlendiriciye gönderir. Yönlendiriciler yönlendirme işlemlerini yaparken belleklerinde sahip oldukları yönlendirme tablolarını kullanılırlar.

5.3.2 Yönlendirme Tabloları

İp datagram yönlendirme tablosu bünyesinde, hedef ağ ve bu ağa ulaşmayı sağlayacak yönlendiricilerin bilgileri bulunur. Bu tablolar ayrıca datagramların en

uygun şekilde iletilmesini sağlayan bilgileri de içerirler. Datagram yönlendirme tabloları 2 şekilde oluşturulurlar:

Statik Yapılandırma Metodu

Bu metot ile yönlendirme tablosu isteğe bağlı olarak yapılandırılır. Hedef bilgisayar ile bağlantı kurulması için kullanılan yönlendirici i le aygıt arasındaki ilişki elle yapılandırılır. Bu metot sadece basit ve yapısı hiçbir zaman değişmeyecek ağlarda kullanılırlar.

Dinamik Yapılandırma Metodu

Bu metotta yönlendiriciler bünyelerinde yönlendirme tablo algoritmaları barındırırlar. Bu algoritma ve protokoller sayesinde diğer yönlendiricilerle haberleşerek en hızlı biçimde ip datagramları iletebilecek tabloları oluşturur. Bu tablolar değişken yapıda olup sürekli güncellenir. Günümüzde ağlar bu metodu kullanarak yönlendirme tablolarını oluşturmaktadır. RIP, OSPF ve BP en çok kullanılan dinamik yönlendirme protokolleri olarak karşımıza çıkmaktadır.

5.3.3 Yönlendirme Protokolleri

Yönlendirme Protokolleri ip yönledirme bilgilerinin yönlendiriciler arasında değişimini en etkin biçimde yapılması için tasarlanmışlardır. Yönlendiriciler arasındaki yönlendirme bilgileri ip datagramlar vasıtasıyla taşınır. Yönlendirme protokollerinden OSPF (Open Short Path First) İP protokolünü kullanarak; RIP (Routing İnformation Protocol) UDP protokolünü kullanarak; BGP (Border Gateway Protocol) ise TCP protokolünü kullanarak mesaj alış verişini gerçekleştirirler. Bu protokoller dinamik tablo yapısına sahiptirler.

5.3.4 Datagram İletim Türleri

Datagramlar aynı ağdaki hedef bilgisayara iletilecekse bu ARP protokolünün kullanılmasıyla, direk olarak birbirine iletmeleriyle sağlanır. Eğer datagram aynı ağdaki bir hedefe iletilmeyecekse ilk olarak yönlendirme tablolarının kullanılmasıyla rotanın belirlendiği dolaylı bir iletim gerçekleşir.

5.3.5 Datagram Yaşam Süresi (TTL)

Ağ üzerinde yer alan datagramların gereksiz bir yük yaratarak ağda dolanmasını engellemek amacıyla kullanılan bu kavram datagramın ağ üzerinde ne kadar kalabileceğini belirler. TTL süresi sıfırlanan bir datagram ıskartaya çıkarılı r ve ağdaki gereksiz yükte bu bakımdan engellenmiş olur.

5.3.6 Rip (Routing İnformation Protocol)

Bu protokol ipv4 ağları çerisinde yer alan yönlendiricilerin diğer ağlara erişimini sağlayacak en iyi rotayı belirlemelerini sağlayan tablo bilgi değişimlerini gerçekleştirmeye yarar. Hedef ağlara erişim ile ilgili toplanacak en önemli bilgi metrik bilgisidir. Metrik, basit ağlarda hedef bilgisayar ağına erişim için kullanılacak yönlendirici sayısını belirlerken, karmaşık ağlarda buna ilave olarak para, zaman verimlilik gibi değerleri kullanımını da temsil eder. Ağın topolojisinde meydana gelen değişimler sonucunda belirli aralıklarla yönlendirme güncelleme mesajları yayınlanır. Bunu alan yönlendirici bu mesajı inceler ve bu yeni donanımın eklenmesinin daha iyi bir rota yaratıp yaratmadığını değerlendirerek kendi yönlendirme tablosunu da günceller.

Çalışma prensibi ise temel olarak ağda yer alan bir yönlendiricinin bağlı bulundukları diğer yönlendiricilerin bilgilerini toplu yayın bilgileriyle alar ak bunu kendi tablosuyla karşılaştırarak daha iyi bir alternatif olması durumunda da kendi tablosunu buna göre güncellemesi olarak özetlenebilir. (Dirican, 2005, sy. 174)

5.3.7 Ospf (Open Shortest Path First)

Rip protokolünün geniş, karmaşık, değiş ik altyapıya sahip ağlarda yetersiz kalması nedeniyle geliştirilmiş gelişime açık bir protokoldür. Protokol, “en kısa rotayı kullan” olarak da bilinen “Dijkstra” algoritmasını kullanılır. Protokolü kullanan yönlendirici aktif hale geçer geçmez veri yapılar ını günceller ve kullanılan ağ donanım arabirimlerinin aktif hale geçmesini bekler ve aktif hale geçince komşu yönlendiricilere merhaba mesajı gönderir ve aktif olan tüm yönlendiricilerden de bu mesajı bekler.

OSPF yönlendirilen paketleri trafik yoğ unluğu gibi durumları da içine alacak biçimde en uygun yollardan gerekirse parçalı biçimde birden fazla rotayı da kullanacak biçimde hedefe yönlendirir. Bu sayede bilgisayar ağlarına binen yüklerde dengelenmiş olur. Protokol ayrıca basit sayılabilecek düze yde şifreleme mekanizması kullanır. (Dirican, 2005, sy. 184-185)

5.4 Icmp Protokolü

İnternet protokolü bu protokolü kullanarak datagramların iletimi sırasında meydana gelen hataları, uyarı ve kontrol bilgilerini bize iletir. Bu mesajların değerlendirilmesiyle ağ içerisinde meydana gelen aksaklıklar belirlenmiş olur.

ICMP mesajları genellikle, ip datagramların hedefe ulaşılamaması durumunda, ağ geçitlerinin datagramları hedeflere yönlendiremeyecek kadar yoğun olması durumunda ya da datagramların hedeflerine yönlendirileceği daha kısa bir rota bulunması durumunda kullanılır. Bu protokol sadece oluşabilecek hatalar noktasında bilgilendirme yapar. Ancak hata mesajları problemin yeri ve çözümü hakkında bize bilgi vermez. Gelen bir hata mesajını değerlendirecek ve hatayı bulacak farklı yöntemler kullanılır.

ICMP mesajlarının yaratılmasına neden olan bazı durumlar şunlardır:

- Bir paketin kaç tane ağ geçiti üzerinden geçebileceğini tanımlayan, ya da bir paketin yaşam süresi olarak açıklanan TTL(Time to live)'in dolması durumunda,
- İnternet protokolüne göre, parçalanan datagramların bazı parçalarının herhangi bir nedenden dolayı kaybolması neticesinde,
- Datagramın gönderildiği hedef bilgisayarın ağ üzerinde olmaması
- MTU değerinin çok büyük olması durumunda
- Yönlendiricilerin çok yoğun olması ya da ağ band limitinin aşılması durumunda; icmp mesajına neden olur.

5.4.1 Icmp Mesajlarını Kullanan Programlar

Ping: En çok kullanılan ağ analiz programıdır. Ping ile hedef bilgisayara ICMP echo istek mesajları gönderilir. Eğer paketin gönderildiği bilgisayardan bir yanıt echo mesajı gelirse o bilgisayarın ağ üzerinde aktif olduğu anlaşılır.

Bazı güvenlik duvarları bir ağın yapısı hakkında pekçok ipuçları veren ICMP ve benzeeri mesajların ağ içine ve dışına iletimin i yasaklayabilir.

Ping her pakete farklı numaralar atar ve bu sayede gelen yanıtlara göre ağdaki ikilemleri tespit eder.

Ping aldığı tüm datagramlar üzerinde hata denetimi yaparak ağ üzerindeki hatalar belirlenir. Ping ayrıca, gönderdiği paketlere gönderim zamanlarını yazar ve gelen paketlere göre paketlerin gelme zamanlarını belirler.

Ping taraması yapmak için çeşitli programlardan da yararlanabiliriz. Örneğin hacker'ların da olmazsa olmaz programlarından biri olan Nmap programı, ping taramaları bakımından oldukça güçlü özelliklere sahiptir.

Traceroute: Datagramların hedeflerine ulaşıncaya kadar izledikleri rotanın belirlenmesinde kullanılır. Program kısa ömürlü TTL paketleri yaratır.

Netstat: Kullanıcılar için ağ bilgisini gösteren bir araçtır.

5.4.2 Icmp Servisleri

Icmp'nin sunduğu temel servisler şunlardır:

Yankı (echo): Hedef bilgisayara erişebilmek amacıyla kullanılır.

Hedef Ulaşılamaz: Hedefteki bilgisayara erişilemez olduğunu belirtir.

Sıkışık Trafik: Rota üzerindeki yönlendiricilerin yoğun veya tıka lı olduğunu belirtir.

Yönlendirme: İp datagramların iletilmesinde kullanılabilecek diğer verimli rotaları belirtmek için kullanılır.

Zaman Aşımı: TTL süresinin sıfırlandığını belirtmek için kullanılır. Ayrıca datagramların parçalanması nedeniyle farklı yol lar üzerinden gelen parçalardan birinin ya da birkaçının kaybolduğunu belitmek amacışa kullanılır.

Parametre Problemi: İp datagramın iletilmesine mani bir durum olması durumunda datagram tamamen yok edilerek mesaj üretilir.

Zaman Belirteci(Time Stamp): İnternet üzerinde dolaşan paketlerle ilgili ölçümler yapmak için kullanılır.

Adres Maskesi: Ağ için belirlenmiş olan alt ağ maskesi değerinin öğrenilmesi için kullanılır. (Dirican, 2005, sy. 123-155)

5.5 Alt Ağlar ve Genişletilmiş Ağlar

İpv4 adreslerin kullanımının artması ile azalan ip sayısı, karşılaşılan sorunların başındadır. Bu problemin çözülmesi içinse “alt ağ kavramı” ortaya atılmıştır. Ağ numarası, (net id) birbirine bağlı ve alt ağ olarak adlandırılan küçük birimler tarafından paylaştırılmıştır. Alt ağların kullanılması; yönetimin kolaylaştırılması, güvenliğin artırılması ve dış ağda herhangi bir değişiklik yapılmadan iç ağda yapının değiştirilebilmesi gibi avantajlar sağlar. Yönlendirme olayında da yölendiriciler, ip datagram üzerinde yer alan hedef ip alanını, alt ağ maskesi ile mantıksal işleme sokarak hedefin aynı ağda olup olmadığına karar verir.

Ağ genişletme ise farklı ağ numarasına sahip ağları tekbir çatı altında toplamak ve tanımlamak için kullanılır.

5.5.1 Cidr (Classes İnternet Domain Routing-Adres sınıfından bağımsız yönlendirme)

Ağların oluşturulması sırasında C sınıfı adreslerin kullanımı, B sınıfı adreslerin çok çabuk şekilde kullanımını önlemiştir. Ancak bu seferde ağ sayısı artmış, dolayısıyla yönlendiricilerin yönlendirme tablolarında yığılmalar meydana gelmiştir. Bu problem de CIDR kullanılarak, birden fazla C sınıfı ağ tek bir yönlendirme girdisi altında toplanmasıyla giderilmiştir.

5.5.2 Toplu Yayın (Broadcasting) ve Grup Yayın (Multicasting)

Ağ üzerindeki tüm noktalara aynı datagramın gönderilmesi toplu yayın, ağ üzerinde tanımlı ve belirli gruplara datagramın kopyalarının gönderilmesi ise grup yayın olarak adlandırılır.

5.5.3 Igmp (İnternet Group Management Protocol)

IGMP, bilgisayarların grup yayınlarına dahil olmak ya da grup yayınlarından ayrılmak için kullandıkları, yönlendiricilere yönelik, ip modülü içerisinde yer alan ve ICMP ile büyük benzerlikler gösteren bir protokoldür. Başka bir deyişle yönlendiriciler, ağ üzerindeki grup üyeliklerini bu protokol ile tespit eder. (Dirican, 2005, sy. 159-170)

5.6 İletim Protokolleri

TCP/IP protokolü, OSİ modeli içerisinde uygulamalar arasında iletişimi sağlayan katmanı, yani iletim katmanını oluşturur. TCP/IP protokolü, bünyesinde TCP ve UDP olmak üzere veri iletişimini farklı yollardan sağlayan iki protokolü barındırır. Bu iki protokol de internet protokolünün üzerinde çalışır. UDP protokolü, gönderilen paketlerin yalnızca bir bilgisayarı hedef aldığı uygulamalarda kullanılır.

5.6.1 Tcp

Protokolün temel özellikleri aşağıda anlatıldığı gibidir:

- TCP protokolü, bağlantılı ve güvenli veri akışını sağlayarak iletim katmanına çok önemli hizmetler sunar. Çoğu uygulama kendi kontrol mekanizmasını oluşturmaktansa, TCP protokolünün sağlamış olduğu hizmetleri kullanır. TCP sunduğu hata denetimi, veri akış kontrolü gibi hizmetler sayesinde kendisini kullanan uygulamalara tatmin edici düzeyde güvenlik, hata kontrolü ve akış denetimi sağlar.

- İnternet protokolü bağlantısızdır ve paketlerin hedeflerine ulaşmalarını garanti etmez. Bu problemi ortadan kaldırmak için TCP protokolüne ihtiyaç duyulur.

- TCP protokolünün sürekli ve her iki yönde veri akışına olanak sağlaması diğer önemli özelliklerindendir. Protokol, gönderilen ve alınan her veri bitini işaretleyerek gönderdiği her parça içinde bağlantıda olduğu her uçta cevap bekler. Bu işaretleme sayesinde iletim sırasında kaybolan parçalar tekrar transfer edilebilir.

- TCP protokolünün en önemli özelliği ise iki nokta arasında güveli bağlantı sağlamasıdır. Bunun için TCP, zarar görmüş kaybolmuş, iki defa gönderilmiş veya düzenli sıraya göre gönderilmemiş datagramlarla uğraşmak ve bu hatalardan kaynaklanan sorunları gidermek zorundadır ve bunu bazı yöntemler kullanarak gerçekleştirir.

- Veri parçalarını alan ve gönderen bilgis ayarlar CPU hızı ve ağ genişliği gibi nedenlerden dolayı farklı hızda çalışabilirler. Bu nedenle, veri gönderen bilgisayarın karşı tarafın baş edemeyeceği hızda bilgi akışı olasıdır. İşte bu noktada TCP protokolü yaptığı akış kontrolü ile bu sorunu ortadan kaldırır.

- TCP protokolünün çoğullama özelliği ile tekbir makine üzerinden birden çok servisi verilebilmesidir.

- Bu protokolün bahsedeceğim en temel özelliklerinden birisi de bağlantıların gönderici ve alıcı tarafların port numaralarına göre yapılır. Bazı uygulamaların kullandığı sabit port numaraları vardır.

- Gönderilen mesajlar için öncelik ve güvenli tanımlaması yapılması ve sadece bağlantı kurulduktan sonra veri iletimini sağlaması güvenlik açısından önemlidir.

- TCP protokolünün sahip olduğu bayraklar, say açlar iletişim noktasında pek çok avantaj sağlarlar, ancak bu konular konumuzun özü bakımından ayrıntılı olarak anlatılmayacaktır. (Dirican, 2005, sy. 193 -224)

5.6.2 Udp (User Datagram Protocol)

Çoğu uygulamalar TCP protokolünün bünyesinde yer alan sağlamlık, akış kontrolü gibi özellikler gerek duymaz. Bunun yerine, bilgisayarda çalışan

uygulamanın varlığına ve basit hata denetiminin yapılmasını, çalışabilmeleri için yeterli bulurlar.

TCP gibi ip datagramları kullanan ancak TCP gibi bağlantı tabanlı olmayan UDP protokolü, bilgisayar ağları arasında paketlerin değişimine imkan sağlamak için tasarlanmıştır. Protokolün datagramların iletiminde oluşabilecek hatalara karşı sadece isteğe bağlı olarak yürütülen bir hata mekanizması vardır. Ayrıca protokol, datagramların iletimini garanti etmez.

Protokolü TCP ile kıyaslayabileceğimiz konulardan biri de hız ve kolaylıktır. Bu kriterler açısından avantajlı olan protokol, sağlamlık, güvenirlik gibi kriterler göz önüne alındığında TCP'ye nazaran çok fazla d ezavantaja sahiptir. Protokol ayrıca toplu yayın ve grup yayın mesajları içinde kullanışlıdır. (Dirican, 2005, sy. 231)

5.7 Ağ Konfigürasyon Protokolleri

Mevcut ağ yapısında meydana gelen değişikliklerde, BOOTP ve çoğunlukla da DHCP gibi protokoller kullanılır.

5.7.1 Bootp Protokolü

Protokol, ağ üzerinde bulunan bilgisayarların ağ alt yapısını kullanarak kendisi ile ilgili yapılandırma bilgilerini bootp sunucularından edinmelerini sağlar. Bootp protokolü, UDP ve IP protokollerini kullanarak çalışır ve genellikle diski olmayan bilgisayarlarca kullanılır.

Protokolün kullanılması iki aşamada değerlendirilebilir. Birinci aşamada bilgisayar, kendi ağ bilgilerini edinirken, ikinci aşamada genellikle TFTP protokolü kullanılarak

bootstrap (önyükleme) dosyasını elde eder. Disksiz bilgisayarlar bu dosyayı kullanarak ağ üzerinde çalışabilir hale gelirler.

Burada karşılaşılan temel durum; kendi ip adresini ve bootp sunucu adresini bilmeyen bilgisayarların karşılaştığı problemdir. Protokol bu problem için aşağıdaki adımları takip eden bir sistem geliştirmiştir.

1. Eğer bootp istemcisi, kendi ip adresini biliyorsa ip protokolünü normal yollardan kullanabilir. ARP istek mesajlarına yanıt verebilir.

2. Bootp istemcisi kendi ip adresini bilmiyorsa ip protokolünü kullanabilmesi için 2 çeşit yol vardır.

    a) Bootp istemcisi, kendi üzerinde yer alan bootp veritabanını kullanarak, kendisine gelen bootp istek paketinde yer alan donanım adresi ile ip adresi arasında eşleşme yapar. Elde ettiği ip adresi - donanım adresi ikilisini ARP tablosuna ekler.

    b) Bootp mesajları toplu olarak yayınlanır.

İP ve UDP protokolleri, gönderilen mesajların hedeflerine iletilmesini garanti, etmez. Bu mesajlar iletim sırasında değişime uğrayabilir ya da bozulabilir. Bu nedenle hata denetiminin kullanılması ve bootp protokolünün düzgün olarak çalışabilmesi için UDP hata denetim mekanizmasının kullanılması gerekir.

5.7.2 Dhcp Protokolü (Dynamic Host Configuration Protocol)

TCP/IP haberleşmesinde servis sağlayıcılar tarafından yapılan ip atamaları bu protokol vasıtasıyla olur. Protokol sadece bununla da kalmayıp subnet mask, DNS sunucu, WINS sunucu gibi yapılandırma değerlerini de tanımlar. Protokolün temel amacı; tek bir elden ağdaki bilgisayarları yapılandırmaktır. Protokol ayrıca kısıtlı sayıdaki ip adresinin verimli dağıtılması bakımından da önemlidir.

Protokol; elle, kalıcı ya da geçici olarak yapılandırılabilir.

- **Elle Yapılandırma:** DHCP sunucu üzerinde herbir bilgisayar için kayıt yaratılır. Ağdaki tüm bilgisayarlar sunucu üzerine girilen kayıtl arla eşleştirilir.

- **Kalıcı Yapılandırma:** Ağdaki bilgisayarlara sunucu tarafından değerlerin atanması ve verilerin kalıcı olarak DHCP sunucu üzerinde kalıcı olarak kayıtlı kalmasıdır.

- **Geçici Yapılandırma:** Ağdaki bilgisayarlara geçici sürelerle kullanılmak üzere yapılandırma bilgilerinin atanmasıdır. (Dirican, 2005, sy. 241-245)

5.8 Alan İsimlendirme Sistemi (Domain Name Server)

"İnternetin ilk ortaya çıktığı zamanlarda bilgisayar isimleri merkezi sunucularda hosts olarak adlandırılan dosyalar içinde t oplanırdı. Ağ üzerindeki bilgisayarlar açılırlarken, bu dosyaları kendi üstlerine yüklemek zorunda kalırlardı. Bilgisayar ağları ve barındırdıkları bilgisayar sayıları artıkça hosts dosyaları da çok büyük boyutlara ulaştı ve bu dosyanın bilgisayar ağlarınd a iletimi, ağa büyük yükler getirdi. Bu problemin çözümü amacıyla DNSoluşumu gündeme gelmiştir."

İnternet üzerinde kullanılan protokollerde, kaynak ve hedef bilgisayarlar 32 bitlik adreslerle ifade edilmektedir.

Ancak, bu adresler, insanlar tarafından hatırlanabilir olmadıklarından, DNS protokolü kullanılarak bu sorun giderilir. "DNS; ip adreslerini bilgisayar isimlerine, bilgisayar isimlerini de ip adreslerine dönüştüren yapıyı oluşturur." (Dirican, 2005, sy.269)

DNS'in görevlerinden biri, alan yönetimini parçalara bölerek görev sorumluluklarını atamak, diğeri ise farklı işletim sistemi ve uygulamalara sahip olan DNS sunucuların etkin ve verimli bir biçimde çalışmasını sağlamaktır.

DNS sunucular alan isimlerini " . " ile ayırarak tanımlarlar. Örneğin haber.milliyet.com.tr adresinde, tr Türkiye'yi, com tanımlaması ticari kuruluşları, milliyet kısmı milliyet gazetesinin sorumluluğundaki alan adını, haber kısmı ise milliyet gazetesinde haber kısmı için oluşturulan alt alan tanımlamasını ifade eder. Bu örnekte de, com.tr alan adlarının her ikisinde tüm sorumluluk ODTÜ'dedir. “haber.milliyet” alan adlarının sorumluluğu ise milliyet gazetesine aittir.

DNS protokolünün çalışma prensibi basit olup genellikle UDP protokolü üzerinden çalışır. Ancak TCP protokolünün de kullanıldığı durumlar vardır. UDP'nin tercih edilmesinin en büyük nedeni de bu protokolün tcp'den hızlı olmasıdır. Bir bilgisayar bir adrese bağlanmak istendiğinde bu adrese bağlı olan ip adres sorgulaması DNS sunucu üzerinden yapılır ve genellikle 53 numaralı UDP portundan çalışan DNS sunucu da gelen sorgu mesajlarını dinleyerek, sorguları yanıtlamaya çalışır.

İnternet üzerinden tanımlanmış kayıtlı milyonlarca alan adı vardır. Düşünüldüğü zaman tüm bu alan yönetimi ve sorguların yapılması oldukça güç bir iştir. Bu zorlukların üstesinden gelebilmek için DNS hiyerarşik bir sistem içerisinde yönetilir. Sistem içerisinde yer alan sunucuların tüm kayıtları tutmak gibi bir zorunluluğu yoktur. DNS mimarisine göre DNS sunucular, sadece derece olarak kendilerinin üzerinde ve altlarında bulunan diğer alan adı isimlerine ulaşmalarını ve yapacakları

sorguların yanıtlarını almalarını sağlayacak verileri bünyelerinde barındırır. Böylece bir DNS sunucu üzerinde onun için gereksiz olabilecek bilgiler toplanm az.

Örneğin Almanya'dan Türkiye'deki bir adres sorgulandığında, Almanya'daki dns, sorgulanan adresin Türkiye'de olduğunu kendi tablosuna bakarak bulur ve sorguyu Türkiye'deki dns'e yönlendirir. Türkiye'deki dns 'e yapılan sorgulama ile sorulan adresin ip'si bulunarak Almanya'daki sunucuya iletilir ve bunu da “cache” üzerine yazar ve daha sonra yapılan sorgulamalarda bu sorgulama tekrar tekrar yapılmaz.

Protokol de ayrıca, sunuculardan elde edilen verilere daha hızlı erişim amacıyla depolama (caching) mekanizmaları da bünyelerinde barındıran proxy sunucuları kullanımı tercih edilir. Bir sayfa ziyaret edildiğinde sayfa burada depolanır ve sayfaya erişim buradan daha hızlı bir biçimde gerçekleştirilir. Proxy sunucularda depolanan sayfaların güncelliği, yapılandırmaya göre zaman zaman yapılan kontrollerle sağlanır. Proxy sunucuların ve dolayısıyla bunu kullanan protokolün bu özeliği, band genişliği tasarrufu ve veri iletişimi açısından oldukça yararlıdır. Örneğimizde de bahsedildiği gibi DNS'ler de istemc ilere daha çabuk ve trafiği de gereksiz yere yoğunlaştırmayacak biçimde cache kavramını kullanır.

Caching temel olarak; Proxy caching ve istemci caching olarak iki türlü yapılır. Proxy caching; sunucu ile istemci arasında sunucu adına çalışan bir bilgisaya rla yapılırken, browser caching; browser'ın eriştiği dosyaların harddisk’de bir dosyada saklanması suretiyle yapılır.

5.9 WWW Kavramı ve Protokolleri

1990' lı yıllarda internet üzerinde ağırlıklı olarak ftp protokolü kullanılmakta iken bu protokolün yerini 2000'li yıllarda http protokolü almıştır.

5.9.1 Http (Hyper Text Transport Protocol)

Web siteleri web sayfalarından oluşur. Başka noktalara linkler vasıtasıyla ulaşan bu sayfalar, değişik türden veriler içerebilir. Bu ise html sayesinde taşınır.

Protokol diğer uygulamalarda olduğu gibi sunucu -istemci ilişkisiyle çalışır. Bir web sitesinin yayınlanması web sunucular vasıtasıyla olur ve bir sunucu üzerinden de pekçok site çalışabilir.

Büyük şirketler genellikle bu hizmet için kendi bünyel erinde web sunucu bulundururlarken, daha küçük şirketler sunucu sahibi olmak yerine bir sunucu üzerinden alan satın almayı seçmektedir.

İstemciler ise ağ tarayıcısı ya da web browser olarak adlandırılır. "Netscape Browser","İnternet Explorer" ve Mozilla F irefox, en çok bilinen istemcilerdir. Sunucular çok sayıda istemciye hizmet verebilecek biçimde tasarlanmışlardır.

Web istemci programları ile sunucular arasında iletişim kurulmasına yarayan protokole http protokolü adı verilir.Bu protokol uygulama katmanı seviyesinde hizmet verir ve TCP protokol tabanlıdır.TCP protokolünün sağladığı veri akışı,güvenilirlik gibi tüm özellikleri bünyesinde barındırır.

Protokol istek-yanıt sistemiyle çift yönlü, yani; istemciden sunucuya dosya alışverişine izin verirken aynı anda sunucudan istemciye de izin verecek biçimde

çalışır. Dünyadaki mevcut farklı diller nedeniyle web üzerindeki farklı karakterler istemci-sunucu arasındaki uzlaşma ile uyumlu hale getirilir.

Bu protokolde, DNS kavramında da açıklandığı gib i caching kavramını kullanmaktadır.

Burada bahsedilmesi gereken bir diğer kavram da Veri tabanları üzerinden araştırma yapılabilmesine olanak tanıyan CGI (Comman Gateway İnterface -ortak geçiş arabirimi) adı verilen arabirimlerdir. Örneğin, google si tesinde bir kelime aradığımızda bu kelime veri tabanları üzerinde araştırılarak elde edilen veri kullanıcıya aktarılır. Bu işlem de yine CGI arabirimleri ile mümkün kılınır.

Burada cookies (çerezler) kavramında da bahsetmekte yarar var. Cookies'ler istemcinin bilgisayarında saklanan, kullanıcı bilgi ve tercihlerinin saklandığı en fazla 4 kb büyüklüğündeki dosyalardır. Bu dosyalar sayesinde bir sayfanın sonraki ziyaretlerinde aynı bilgiler bize sürekli olarak tekrara tekrar sorulmaz. (Dirican, 2005, sy. 284-285)

5.9.2 Url Kavramı

Web sunucular üzerinde yaratılan dokümanların, web istemcileri tarafından alınabilmesi amacıyla bu dokümanlar birbirinden farklı olarak isimlendirilir. İşte sayfaların birbirinden bağımsız olarak isimlendirilerek birbi rinden ayrılmasını sağlayan bu özelliğe URL (Uniform Resource) denir. (Dirican, 2005, sy. 285)

5.10 Elektronik Posta İletim Protokolleri

İnternet üzerinde en çok kullanılan uygulamalardan biri de şüphesiz elektronik posta hizmetleridir. Gönderilecek bir postanın Dünya'nın diğer ucuna gönderilmesi de yine protokoller vasıtasıyla yapılır. Bu protokoller içinde en çok kullanılanı ise SMTP (Simple Mail Transfer Protocol) protokolüdür.

Elektronik posta iletimi de posta sunucularını kullanırlar ve posta sunucularının görevlerinden birisi, gönderilen postanın sunucuya gelmesiyle bunun alıcının sunucusuna teslim edilmesidir. Bir mesajın karşı tarafın sunucusuna iletilmesi, e-postaların alan adını kullanarak ve yapılır. Bu alan adının DNS'de sorgulanması neticesinde, ilgili posta sunucusunun ip adresi bulunur ve SMTP protokolüne uygun biçimde karşı sunucuya posta iletimi yapılır.

Sunucunun ikinci görevi ise; POP3 protokolünün çalışma biçiminde de değinileceği gibi postanın istenildiğinde saklanabilmesidir. Bir postanın, hedef sunucuya iletilememesi durumunda veri, sunucu üzerindeki alanda saklanır ve sunucu yapılandırılmasına bağlı olarak tekrar iletilmeye çalışılır. Uzun süre iletilememesi durumunda ise mesaj, göndericiye hata mesajıyla beraber geri gönderilir. Başka bir değişle; posta protokolleri bu özellikleri bakımından hatalara karşı anlık sorunlar yaşamamaktadırlar.

Bu hizmet de en çok kullanılan ve hayatımızda da önemli bir yere sahip başka bir kavram vardır ki bu; postaların iletim hedeflerini sunuculara anlatan elektronik posta adresleridir. (Dirican, 2005, sy. 295-297)

5.10.1 Smtp(Simple Mail Transfer Protocol)

"SMTP bilgisayarlar arasında elektronik postaların iletilmesini sağlayan protokoldür."

Uygulama katmanında çalışan protokol 25. port üzerinden çalışır. SMTP sunucuya bir posta geldiğinde sunucu alıcıya DNS'den yapılan sorgulamaya göre en iyi yoldan mesajı iletir ve bunu da kullanıcıya ayrıca iletir. Elektronik postaların iletimi ASCII modundadır. (Dirican, 2005, sy.298)

5.10.2 Pop3 (Post Office Protocol Versiyon 3)

SMTP sunucular gönderilen bir mesaj alıcıya gelmeden önce POP sunucusuna gelir ve kullanıcı çevrimiçi olana kadar burada depolanır. Bu mesaj TCP tabanlı çalışan POP3 protokolü kullanılarak sunuculardan istemcilere indirilir.

Bu işlem bazı komutlarla yerine getirilir ve bu komutlar genel olarak mesajların alınması, kullanıcıların kullanıcı işlemleri ve şifreleriyle sisteme giriş yapabilmeleri gibi yönleriyle POP3'e göre daha avantajlıdır. Ayrıca kullanıcı isterse, gelen bir mesajın kopyasını isteğe bağlı olarak burada depolayabilir.

5.10.3 Imap4 (İnternet Mail Access Protocol)

POP protokolü yerine geliştirilen bu protokolün temel mantığı; POP3 protokolündeki gibi posta kutularının tanımlanmasıdır.

IMAPv4'de istemciler her seferinde sunucular üzerinden elektronik postalarını almak zorundadırlar. Protokol, mesajın içinde kelime araması yapabilmek, mesajın bir kısmını indirebilmek gibi yönleriyle POP3'e göre daha avantajlıdır ancak IMAP sunucuların aynı anda çok fazla kullanıcı ile çalışmaları durumunda hızlarının düşmeleri yönüyle de dezavantaja sahiptir.

5.10.4 Mime (Multipurpose İnternet Mail Extensions)

Farklı formattaki verilerin karşı tarafa gönderilmesini ve karşı tarafta yorumlanarak anlaşılmasını sağlayan, güvenliğin ön plana daha çok çıktığı sürümdür. (Dirican, 2005, sy.302-304)

5.10.5 Binhex

Binary forma çevrilerek mail göndermeyi ve bunu karşıda alınmasını sağlar. Özellikle Machintosh makinalarla irtibata geçmenin en iyi yön temidir.

5.11 Uzaktan Erişim Protokolleri

Gelişen ağlar ve artan ihtiyaç nedeniyle uzaktaki sistemlere/bilgisayarlara erişim bir gereklilik haline geldi ve bu ihtiyaç da uzaktan erişim protokollerini ortaya çıkardı.

İki bilgisayar arasındaki uzaktan erişim, güvenilir bilgisayar ilkesine göre şifreye gerek duymadan kurulabilirken, kullanıcı adı ve şifresi de tanımlanabilir. Protokollerden bazılarına gönderilen verinin okunmasını engellemek amacıyla verileri şifreleyebilir.

5.11.1 Telnet

TCP tabanlı telnet; basit mimarisi ve kullanışlığı nedeniyle geniş ağlarda sıklıkla kullanılır. Ancak, bağlantı sırasında verilerin şifrelenmemesi, alıcı ve gönderen uçlar arasındaki aygıtlara erişim imkânına sahip insanların, bu bağlantılara erişiminin

mümküniyeti gibi nedenlerle, protokolün ele geçirme saldırılarına karşı zaafiyeti vardır.

Telnet protokolü NVT(Sanal Ağ Terminali) özelliği sayesinde bağlandıkları bilgisayarların mimarisi hakkında fazla bilgiye ihtiyaç duymaz. Sistemler arasında anlaşmanın sağlanması amacıyla telnet protokolü, internet üzerinde verinin ve komut dizilerinin tanımlanmasında da NVT'yi kullanır.

5.11.2 Bsd Rlogin Protokolü

Tcp tabanlı olan protokol, yapılandırmasına göre kullanıcı ve şifreye gerek kalmadan ve genellikle Unix tabanlı işletim sistemlerine sahip bilgisayarlarda kullanılan bir protokoldür.

İlk olarak BSD unix sistemler tarafından kullanılan Rlogin protokolüyle, güvenilirliği sağlanmış bilgisayarlar üzerinde dosya erişimi ve paylaşımını kullanıcılar için sağlayabilirler.

5.12 Dosya Erişim ve İletim Protokolleri

Bilgisayarlardaki veriler temel olarak dosya adıyla anılırırlar ve dosyaların bilgisayarlar arasndaki iletimi FTP (File Transfer Protocol) ve TFTP (Trivial FTP) protokolleriyle sağlanır.

"FTP protokolü TCP tabanlıdır. TCP protokolü sayesinde bağlantı kurulmuş iki nokta arasında güvenli veri alış verişi sağlanır. Protokol sayesinde tanımlanan erişim yetki sınırlamaları, isimlendirme, farklı işletim sistemleri tarafından kullanılabilme,

veri gösterim çeşitliliği gibi etmenler protokolü karmaşık bir hale getirir."(Dirican, 2005, sy.320)

Aynı anda birden fazla istemci bir FTP sunucu ile bağlantı kurabilir.

FTP sunucularında anonim ve şifreyle olmak üzere iki türlü erişim biçimi tanımlanmıştır. Şifreyle olan bağlantı da kullanıcılar, istenen kullanıcı adı ve şifreleri ile sisteme giriş yapabilirler.

FTP sunucular 21.port üzerinden çalışmaktadır. Burada bir noktaya dikkat çekmek istiyorum, zira internet üzerinden yapılan birçok saldırı ftp sunucular üzerinden yapılmaktadır.

Ftp'nin karmaşıklığına karşı geliştirilmiş bir protokol olan TFTP ise genellikle diske sahip olmayan, açılışları sırasında ROM bellek alanını kullanan cihazlar tarafından tercih edilir ve 69.port üzerinden çalışır. FTP TCP tabanlı olup güvenli veri alış verişini sağlarken, TFTP UDP tabanlıdır ve güvenli veri akışını sağlamaz.

5.13 Ağ Yönetim Protokolleri

"Geniş ağlara yayılmış ağlar üzerinde meydana gelen sorunların tespiti, giderilmesi ve aygıtların gözetlenmesi gerekir. Bu işlerin yerine getirilmesi için ağ yönetim protokolü tasarlanmıştır." (Dirican, 2005, sy.333)

Bu protokol ile ağ üzerinde bulunan yazıcılardan yönlendiricilere kadar tüm aygıtların yönetimi ve bilgi, toplanması tek bir elden sağlanmış olur. Bu nedenle sorunsuz ve güvenli bir yönetim içinde (authentication) doğrulama mekanizmasına sahiptir.

TP/IP ağları yönetim için SNMP protokolü kullanır. Aynı zamanda IPX, Apple Talk ve OSİ desteği de mevcuttur. SNMP protokolünde ağdaki farklı aygıtların farklı bilgilerinin depolandığı standart bir yapı vardır ve bu yapı MIB (Management Information Base) olarak adlandırılır. SNMP yaklaşımı sadece bilgilerin alınmasını - aktarılmasını sağlayan basit bir komut yapısına sahiptir.

6.BİLGİ SAVAŞI ORTAMI

6.1 Teknoloji ve Küreselleşme

Teknolojinin hızla gelişmesiyle beraber yaşanılan hızlı değişim, Dünya Savaşlarında da olduğu gibi, askeri ve coğrafi üstünlüğü ön plana çıkaran saldırılar yerine, bilgisayar sistemleri üzerinden daha kolay ve kısa sürede yapılabilen saldırıları mümkün kılmıştır.

Artık tek başına bir bilgisayar korsanı, yalnızca bir bilgisayar, modem ve telefon hattı ile bir şebekeye bilgi taarruz araçlarını kullanarak saldırabilmekte, kritik altyapı ağlarını kesintiye uğratabilmektedir. Bu nedenledir ki bir bilgisayar korsanı, kişisel bir nedenden dolayı, protesto hatta ve hatta hobi amaçlı olarak bile, gelişmiş sistemlere sahip ülkeleri tehdit edebilir konumdadır. Bu ortamda internet üzerinden gönderilen bir virüs, binlerce bilgisayarı etkileyerek çok büyük zararlara neden olabilmekte, altyapı sistemlerini çökertebilmektedir. Ya da, körfez savaşında da olduğu gibi, karşı tarafın birliklerine ait haberleşme bilgisayar ortamında yapılan müdahalelerle etkisiz hale getirilebilmekte, bazı ülkelerdeki farklılıklar yapılan propaganda ve psikolojik saldırılarla körüklenerek kullanılabilmekte, iletişim sistemler üzerinden çok önemli istihbarati bilgiler kolaylıkla temin edilebilmektedir.

Bilginin hâkim olduğu çağımızın toplumsal yaşamı; bilgi artışındaki büyük hız, bu bilginin gelişmiş iletişim imkânlarının kullanılmasıyla sağlanan hızlı aktarımı ve bunların sonuçlarından biri olarak da yeni teknolojilerin ortaya çıkmasıyla, bireysel anlamda yaşantı biçimlerini, devletler anlamında da güvenlik, strateji ve birbiriyle ilişkili benzer pek çok kavramı etkileyen bir süreç olarak karşımıza çıkmaktadır. Bilgi teknolojilerindeki son gelişmeler, yaşadığımız Dünya'da da kurumlar açısından;

- Yaratılan zenginliğin değişimi;
- Güç dağılımının değişimi;
- Karmaşıklığın artması (sistemlerin bütünleşmesi anlamında);

- Mesafelerin kısalması;
- Yaşam tempomuzun artmasıyla zamanın sıkışması biçimindedir. (Alberts vd. Garstka, Stein, 1999, sy.15)

Küreselleşme süreci artık herkesin tanıdığı a ma birçok kişinin içeriğini tam kavrayamadığı veya farklı amaçlarla kullandığı bir kavram. Kimileri bu sürecin yeni bir sömürü yöntemi olduğunu ileri sürerken kimileri de küresel gönenç artışı için bir fırsat olduğunu iddia etmektedir. Kimilerine göre küre selleşme iktisadi açıdan liberalizm, kimilerine göre demokratik kavramların ve kuralların evrenselliği, kimilerine göre evrensel insan hakları, kimilerine göre çevreyle ilgili sorunlar, kimilerine göre ise yukarıdakilerin hepsini kapsayan bir süreç ile ilg ili bir kavramdır. (Gürak, 2003, sy.1)

“Küreselleşme kavramının popülerliğine ve bu konudaki literatürün genişliğine rağmen, kavramın kesin bir tanımı yoktur. Genel ifadelerle küreselleşme, bütünleşen, ama aynı zamanda parçalanan, evrenselle yerelliğin iro nik bir şekilde birbirine geçtiği ve karıştığı bir dünya imgesi olarak karşımıza çıkıyor. Kısaca 20. yüzyılın insanı Karl Polanyi’nin ifadesiyle “büyük dönüşüm”e tanıklık ediyor.” (Hasanoğlu, 2001, sy.69)

“P.G. Cerny’nin ifade ettiği üzere: “Küreselleşme yeni bir dünya düzeninin değil fakat yenidünya düzensizliğinin, hatta üst üste gelen ve rekabet halindeki otoritelerin, çoklu bağlılıkların ve kimliklerin, prizmatik uzay ve inanç nosyo nlarının oluşturduğu “yeni bir ortaçağ” işaretçisi olarak görülebilir.

Kısaca, küreselleşme; dünyanın tek bir mekân olarak algılanabilecek ölçüde sıkışıp küçülmesi anlamına gelen bir süreci ifade etmektedir.

OECD’nin küreselleşmeyle ilgili olarak önerdiği tanım üç faktörden oluşmaktadır;

1. Ulus aşırı şirketler gibi güçlü ve yeni aktörlerin siyasal sahneye girişi;

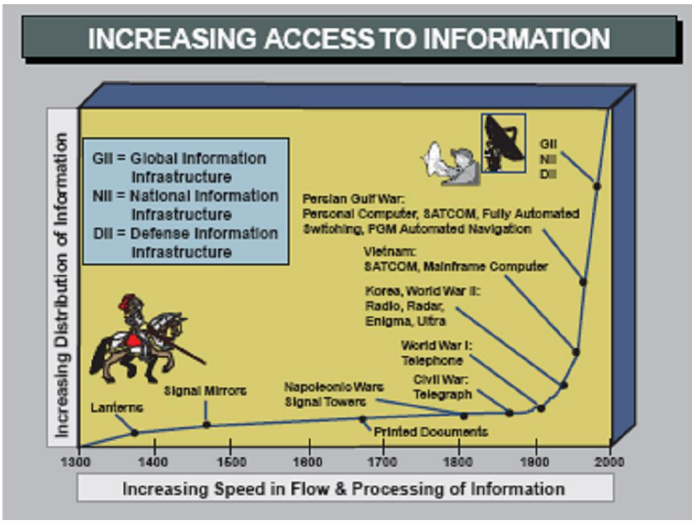
2. Bilgisayar teknolojisinin iletişim ve enformasyon alanındaki hızlı yayılımı.

3. Çoğu ülkede de-regülasyon politikalarının benimsenmesi" (Bağçe , 1999, Sy.9-10)

Teknoloji artık Dünya'nın çehresini öyle değiştirmektedir ki, teknolojinin küreselleşmesi küreselleşmenin en önemli boyutu, hatta küreselleşmenin lokomotif olarak kabul edilmektedir. Küreselleşme üzerinde teknolojinin etkisini inkâ r etmek mümkün görülmemektedir.

Küreselleşmenin en önemli boyutu olan teknolojik küreselleşmenin en önemli özelliği;"internet ağı ve diğer şebekeler ile fiziki sınırları ortadan kaldırarak, kritik altyapıyı, resmi ve kamu hizmetlerini ve kuruluşlarını, yaz ılı, görsel, sesli medya kuruluşlarını, sivil toplum örgütlerini, çıkar gruplarını, meslek kuruluşlarını, uluslar arası organizasyonları, endüstri ve ticari kuruluşları, üniversiteleri, teknoloji ve AR - GE kurumlarını, strateji kuruluşlarını ve tüm askeri g üç unsurlarını şebekelendirmekte, farklı ve yeni yeteneklerin oluşmasını sağlamaktadır. (Bayazıt, sy.1)

Özellikle 1980'li yıllardan itibaren enformasyon teknolojilerinin yaygınlık kazanması, Dünya'da mesafe kavramının eski anlamını ortadan kaldırmıştır. Ni tekim 1945 yılından beri, okyanus ötesi nakliye bedelleri %50, hava taşımacılığı maliyetleri %80 ve transatlantik telefon bedelleri de %99 oranında gerilemiştir. 1999 yılı BM İnsani Kalkınma Rapor'una göre, 1990 değerleriyle, New York'dan Londra'ya üç dakikalık telefon görüşmesi bedeli, 1930 yılında 245 dolar iken, bu oran 1998 yılında 35 cent'e inmiştir. (Bozkurt Küreselleşme kavram, gelişim yaklaşımlar, 2005)



Şekil 6.1 Bilgiye Erişimin Hızlanma Süreci (Joint Pub 3 -13, 1998, I-17)

İkinci olarak, ticari sektörde, bilişim teknolojileri'nin oluşturduğu "şebekelerin şebekesi" yaklaşımı, askeri alanda "Sistemlerin Sistemi" şeklindeki sistemsel yaklaşım olarak kullanılmaktadır. Muhasıma, müttefike, dosta ve tarafsızlara siyasi, askeri, ekonomik, bilgi ve altyapı/teknoloji sistemlerinin oluşturduğu bir sistem olarak yaklaşılmakta ve sistemi meydana getiren önemli sistemlerin işlevsiz kılınması, akabinde stratejik felç yaratılması amaç edinilmiştir. Bu yaklaşım tehdit değerlendirilmesinden stratejik planlamaya ve operasyon icrasına kadar tüm süreçlerde kullanılmaktadır.

Üçüncüsü, zaman, mekân ve güç etkileşiminin değişmesidir. Bilişim teknolojileri, sürati artırarak zamanı yoğunlaştırmıştır (bir internet senesi klasik anlamdaki 7 yılımıza eşittir.) Üç boyutlu değerlendirilen harekât ortamına uzay ve bilgi boyutlarını ekleyerek, yeni harekât ortamını 5 boyuta çıkarmıştır. Bunun sonucu, muharebe sahasını derinleştirip, genişleterek siyasi, askeri, ekonomik, sosyal, bilgi ve altyapı, sistemlerini de kapsamıştır." (Baya zıt, sy.1-3)

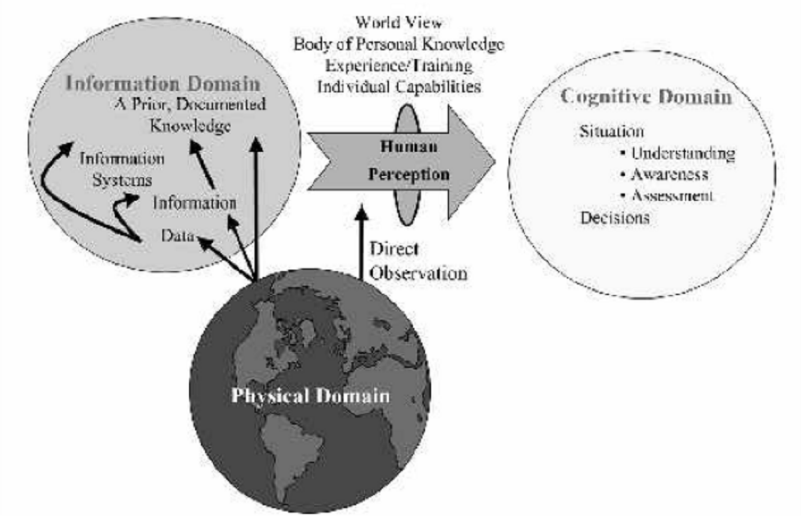
Teknolojik küreselleşmenin en temel dayanağı da kendi ihtiyacı olan bilginin güvenliğinin sağlanmasıdır. Bu iletişim çağında teknolojik küreselleşmenin bir diğer özelliği de medyayı bir güç haline getirmesidir. Bu durum ise bir noktada daha ilerde

bahsedeceğimiz psikolojik harp kavramına vurgu yapmaktadır. Teknolojik küreselleşme stratejik anlamda bazı değişiklikleri de zorunlu kılan özelliklere sahiptir. Bunlar;

1. “Zaman, mekân ve güç etkileşimini değiştirmesi,
2. Asimetrik yaklaşımlar üzerindeki etkileri,
3. Güvenlik ortamının dinamik ve akışkan bir şekilde belirsizliklerin artması,
4. Güvenlik alanındaki aktörlerin sayısının artması ve yapılarının değişmesi,
5. Askeri operasyonların siyasi, ekonomik, sosyal, bilgi ve altyapı sistemlerini kapsaması,
6. Yeni savaş teorisi, yeni muharebe ve operasyon konseptleri,
7. Yeni Harekât nevileri, Savaş Dışı Askeri Operasyonlar
8. Bilgi Güvenliği.

Bu parametreler direkt olarak milli menfaatlerin tespitini, milli hedeflerin saptanmasını, milli politikanın belirlenmesini ve milli stratejilerin oluşturulması güçleşmiştir. Teknolojik küreselleşmenin getirdiği yeni stratejik bağlam, bireylerin ve kurumların bilgiyi üretme, yapısallaştırma, değerlendirme, kullanma ve yönetme yetenekleri ve bilgi çağının şartlarına uyum sağlama kabiliyetleri üzerine inşa edilmektedir.” (Bayazıt, syf10)

Emre Kongar’ın, Küresel Terör ve Türkiye adlı eserinde küreselleşmeye teknolojinin ve Sovyetler Birliği’nin dağılmasından sonra ortaya çıkan siyasi tablonun kaynaklık ettiğini belirtmektedir. Soğuk savaş döneminde komünizme karşı ön plana çıkarılan milliyetçilik ve dini eğilimlerle, Türkiye’nin Sovyetler Birliğine karşı batıya yaklaşması, ülkemizin bugün içinde bulunduğu tehditkâr ortamla yüzleşmesinin bir nedeni olarak düşünülebilir. Bu bakımdan soğuk savaş döneminden en fazla etkilenen ülkelerden birinin Türkiye olduğunu söylemek yanlış olmayacaktır.



Şekil.6.2 Domainler (Alberts et al.Garstka, Hayes and Signori, 2001, sy.11)

Bilginin güvenliğini sağlama yeteneğini açıklamak için yukarıdaki şekilde de belirtildiği gibi fiziksel domain, bilgi domaini ve kavramsal domain olmak üzere 3 domain gereklidir.

Fiziksel domain askeri olayların var olan etkilerinin; kara, hava, deniz ve uzayda çarpışma, koruma, taktik tatbikatın olduğu; ya da fiziksel platformların ve iletişim ağlarının bağlandığı yer olarak tanımlanabilir. Kuvvetler zaman ve mekân uzayında bu domain üzerinde hareket ederler. Karar verme sürecinin hızlandırılması ve durumsal bilincin geliştirilmesini mümkün kılar. (Alberts et al.Garstka, Hayes and Signori, 2001, sy.12-13)

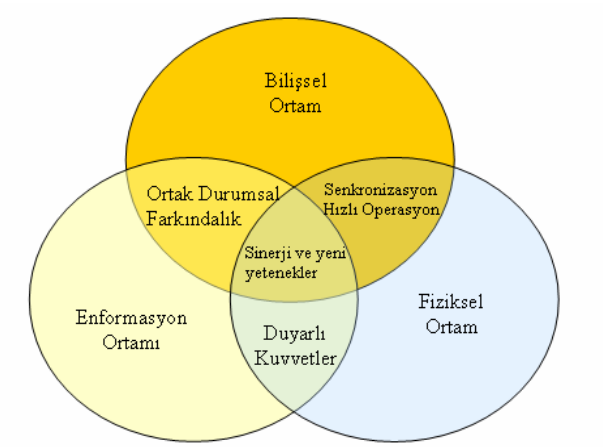
Fiziksel ortamda güvenlik, kara, hava ve deniz kuvvetlerinin haberleşme, sensör, elektronik harp, komuta-kontrol, silahlar, lojistik koruma vb. fonksiyonlar ve sistemlerle sağlanır. (Vural, Bilgi Teknolojisindeki Gelişmenin Yarattığı Uluslar Arası Yeni Güvenlik Ortamı)

Bu domain eskiden beri var olan en önemli domain olarak kabul edilmekteyken yaşanılan teknolojik gelişmeler bu domaini önem bakımından bilgi domainine göre daha art sıraya atmıştır.

Bilgi domaini bilginin yaşadığı her türlü optik, manyetik vb. her türlü yeri ifade eder. Burada bilgi üretilir, işlenir ve paylaşılır. Bu domain savaşanlar arasında iletişimi kolaylaştırır. Bu domain, modern askeri kuvvetlerin komuta kontrolünün yapıldığı yerdir.

"Enformasyon ortamı, sayısal harita, sensör ve radar verileri, ülkelerin enerji, politika ve ticaret bilgileri vb. çok değişik nitelik ve nicelikte bilgileri içerir. Bu ortam fiziksel ortama göre daha yenidir ve teknolojideki gelişimlerin hızına paralel olarak değişmektedir. Enformasyon ortamında enformasyon kuvvetlerinin geliştirilmesi için gerekli kavram ve doktrinler henüz gelişme aşamasındadır." (Vural, Bilgi Teknolojisindeki Gelişmenin Yarattığı Uluslar Arası Yeni Güvenlik Ortamı)

Kavramsal domain katılımcıların zihinlerindedir. Algılamalar, bilinç, anlayış, inanışlar, değerler ve bunlara bağlı olarak kararların alındığı domaindir. Pek çok savaşın gerçekte kazanıldığı ya da kaybedildiği yer burasıdır. Liderlik, kavramlar, doktrinler, taktik, prosedürler ve teknikler bu domaine bağlı olarak şekillenir. (Alberts et al.Garstka, Hayes and Signori, 2001, sy.12 -13)



Şekil 6.3 Güvenlik Ortamlarının Birlikte Ele Alınması ile Kazanılan Yetenekler (Vural, sy.3)

Vural'a göre enformasyon ortamı, bilişsel ortam ve fiziksel ortam olarak adlandırılan bu üç ortamın karşılıklı etkileşimi, bütünleşik bir yapı içerisinde sinerji ve yeni yetenekleri oluşturur. Fiziksel ortamla enformasyon ortamı birlikteliğinden son derece duyarlı askeri güç doğar. Fiziksel ortamla bilişsel ortam birlikteliği senkronizasyon ve hızlı operasyonları doğururken, bilişsel ortamla enformasyon ortamı da durumsal bilgi ve farkındalık da artışı sağlamaktadır.

Bilginin güvenliğinin sağlanması için bu üç ortam bakımından, bilgi operasyonu stratejilerinin başarımı; pek çok yetenek ve aktivitenin entegrasyonu ile sağlanabilmektedir. İstihbarat ve iletişim sistemlerinin desteği hem defansif hem de saldırı anlamında bilgi operasyonları için çok kritik bir öneme haizdir. İstihbarat desteği, bilgi operasyonlarının planlanması ve yürütülmesi açısından oldukça önemlidir. İstihbaratın ilgili birimlere, zamanında, doğru, tam, kullanışlı, objektif ve etkili biçimde destek verecek biçimde ulaştırılması sağlanmalıdır.

6.2.Çağımızın Güvenlik-Tehdit Anlayışı ve Teknoloji

Günümüzde artık, ülkelerin güvenlik anlayışı teknolojiyi kapsayacak biçimde değişmektedir. Daha önce bahsettiğimiz gibi teknoloji-bilgi arasındaki etkileşim ve her iki kavramın bu etkileşimle karşılıklı gelişimi, bu teknolojik gelişmeyi yakalamayan ülkeler açısından en önemli tehdit kavramı olarak karşımıza çıkmaktadır.

"Uluslararası güvenliğin bugünkü hegamonik güçleri; yeni aktörler ve yöntemler yanında, uzaya dayalı sistemler ve elektronik alanındaki teknolojik üstünlüklerini kullanarak, özellikle görüntü, açık bilgi toplama ve dinleme alanında; uydular internet, echelon, çift kullanımlı teknolojiler gibi yeni vasıtalar ile teknolojinin keskin uçlarından önemli bir güç kaynağı olarak istifade etmekteler."(Yılmaz, 2005, sy.5)

ODTÜ Enformatik Enstitüsünden Doç.Dr. Nazife Baykal, bu yeni tehdit kavramı nedeniyle, içinde bulunduğumuz çağda yurt kavramının artık elektromanyetik spektrumun tüm bölgelerini de içine alacak biçimde yapılması gerektiğini şu biçimde belirtmektedir;

"Her türlü veri iletişiminin sağlandığı bu alan, en az kara, hava ve deniz sınırlarının savunulması kadar önemlidir. Kısaca siberyurt adını vereceğimiz, bu bölgeye yapılacak sızmalar ile, her türlü elektronik iletişim ve etkinlik kontrol edilebilir, durdurulabilir ve tahrip edilebilir" demektedir. (Baykal, sy.3)

Uluslararası ve Avrupa Etütleri Enstitüsü'nde araştırmacı olan Johnny Ryan, bir analizinde bu yeni tehditi, Estonya'da yaşanan şu örnekle açıklamaktadır:

"27 Nisan 2007 tarihinde aniden bir DDoS atakları (distribution denial of Service/servis dışı bırakma) fırtınası başladı ve bu durum Haziran ortalarına kadar devam etti. Devlet Başkanlığı, parlamento, bakanlıklar, siyasi partiler, belli başlı haber ajansları, ve Estonya'nın iki önemli bankası bu saldırılara hedef oldu. Estonya Savunma Bakanı olayla ilgili olarak "bu bir ulusal güvenlik konusudur ve limanlarınızın denize kapatılmasından farkı yoktur." açıklamasını yapmıştır.(Ryan, 2007)

Emekli Tuğgeneral Nejat Eslen, "yeniçağın güvenlik sorunları" adlı yazısında tehdit kavramıyla ilgili olarak şunları söylemektedir:

NBC silahların yayılması, çok yönlü terör, etnik ve dini çatışmalar, organize suç örgütleri, uyuşturucu kaçakçılığı ve kriminal anarşi geleneksel olmayan tehditlerdir. Bunlara ek olarak ticari ve finansal harp ve siber terör askeri olmayan tehditler arasında yer alır. Geleneksel olmayan tehditler, bir devletten, devlet dışından veya ülkelerarası organlardan oluşabilen asimetrik yani belli bir cephesi veya yönü olmayan tehditler haline dönüşmüştür.

Çağdaş güvenlik politika ve stratejileri, geleneksel tehditlerin yanı sıra, geleneksel olmayan asimetrik tehditlere de tedbirler almak zorundadır. Kitle imha silahları, terör ve siber terör bu tehditler içinde ayrı ayrı önem taşımaktadır.”(Eslen, 2001)

7.BİLGİ SAVAŞI KAVRAMI VE ÖZELLİKLERİ

7.1 Bilgi Savaşı Kavramı

Çağımızın yeni biçimli savaş meydanlarında bilgisayar ve sistemler üzerinden gerçekleştirilen bu savaşın, bugüne kadar ortak bir tanım yapılmamıştır. Askeri boyutunun yanında sahip olduğu sosyal, kültürel, biyolojik, psikolojik, teknolojik boyutları bu savaşı alışılagelmiş savaş tanımlamaların dışına çıkarmaktadır. Bir başka değişle, bilgi savaşı tanımını tam olarak yapmak mümkün değildir, çünkü bilgi savaşı tanımı farklı bakış açılarından farklı biçimde yapılabilir.

Libicki'de, kavramı açıklamak için kitabında şunlara yer vermiştir.

"Bilgi Savaşları ile ilgili ilk teknik tanım ilk kez konuyla ilgili bir seminerde Dr. John Alger tarafından verilmiştir. Bu tanımda bilgi savaşı, sahip olduğumuz bilgilerimizi ve bilgi tabanlı yapılandırmalarımızı korurken; rakibin bilgilerini, bilgi sistemlerini ve bilgi tabanlı yapılanmalarını etkileyerek bilgi üstünlüğünü sağlamamıza yarayacak her türlü faaliyetlerdir" şeklinde ifade edilmektedir."(Özdemir, 2003, sy.51)

"Konuyla ilgili benzer bir tanımı da amerikan hava kuvvetleri yapmıştır. Bu tanımlamaya göre bilgi savaşı düşmanın sahip olduğu bilgi ve onun fonksiyonlarını engellemek, imha etmek, bozmak ve kendi çıkarımız doğrultusunda kullanmak için yapılan hareketlerle, düşmanın bu faaliyetimize karşı önlem almasını engellemek ve benzeri harekâtına karşı koymaktır şeklindedir."

Leeds Üniversitesi Haberleşme Enstitüsü'nde çalışmalar yapan Profesör Philip M. Taylor, bilgi savaşı ile ilgili düşüncelerini şöyle açıklamaktadır:

"Dışarıda bir savaş var, bir dünya savaşı ve bu savaş kimin daha fazla mermiye sahip olduğuyla ilgili olmayan bilgiyi kimin kontrol ettiğiyle, nasıl gördüğümüz -

duyduğumuz, ne yaptığımız ve ne düşündüğümüzle ilgili. Hepsi bilgi hakkında..” (Taylor, 2006)

Winn Schwartau ise bilgi savaşları ile görüşlerini kitabında şöyle ifade etmektedir;

Bilgi Savaşı endüstriye, politik küresel etkilere, ekonomik güçlere hatta tüm ülkelere karşı sürdürülebilir. Bu teknolojiye karşı teknolojinin kullanılmasıd ır; bu, sırlar ve sırların çalınmasıyla ilgilidir; bu, bilginin sahiplerine karşı bu bilginin kullanılmasıyla ilgilidir, bu, bir düşmanın kendi bilgi ve teknolojisini kullanma kabiliyetinden yoksun bırakmakla ilgilidir. (Schwartau, 1994, sy. 291)

Türkiye’de 90’lı yıllarda literatüre giren bu kavram, özellikle TSK Komuta Kontrol Sistemlerinin güvenliği ve etkin kullanımının ancak bilgi güvenliği ile sağlanacağı fikriyle üzerinde en çok durulan konulardan biri haline gelmiştir. Daha önce bahsettiğim comsec, compusec ve bunların birleşiminden oluşan infosec kavramlarının askeri literatüre girişi de bu yıllara denk gelmektedir.

Ali Tatar’ın 2001 yılında yayınlanan “Bilgisiz Harp Olmaz” makalesinde ise Nato bilgi harekâtı konseptine göre bilgi harekâtı; politik v e askeri hedefleri desteklemek amacıyla kendi bilgi ve bilgi sistemlerini etkili bir biçimde kullanarak ve korurken, hasmın bilgiye dayalı işlemlerin, komuta kontrol (C2), muhabere ve bilgi sistemlerini etkileyerek karar vericilerin müessir olmalarını sağl amak maksadıyla icra edilen faaliyetlerdir” şeklinde açıklanmaktadır.

Türk Silahlı Kuvvetlerinin tanımına göre bilgi savaşı çeşitli bilgi harekâtlarından oluşmaktadır. Bilgi harekâtı ise “ karar vericiler tarafından ortaya konulan hedeflere ulaşılmasını desteklemek için kendi bilgi ve/veya bilgi sistemlerini etkin kullanırken ve korurken başkalarının bilgi ve/veya bilgi sistemlerini etkileyerek yapılan faliyetler”den oluşmaktadır. (Özdemir, sy.56 -57)

Bilgi savaşını bilgi avantajının kullanılmasıyla düşman üzerinde üstünlük ve yönetimi amaçlamaktadır. Yani bilgi savaşının başarısı hem savunmayı hem de taarruzi çalışmaları kapsamaktadır. “Hayati bilgiyi, bilgi proseslerini ve bilgi

sistemlerini savunamayan bir strateji, kaybedilecek kötü bir son gibidir." (A lberts, 1996, sy.2)

Bu noktada zaten IW-D olarak adlandırılan savunmaya dayalı bilgi savaşı kavramı karşımıza çıkmaktadır ki bu kavram, bilgi saldırılarına karşı alınabilecek tüm savunmaya dayalı hareketleri ve tedbirleri ifade etmektedir.

Tablo 7.1 Potansiyel Bir Bilgi Savaşı Örneklemesi (Banks, 2001 sy.16)

PSTN ağına kontrolü tamamen ortadan kaldıracak gizli bir yazılımın yüklenmesi ya da saklanması
Kişisel bilgisayarlarla yapılan yoğun arama saldırılarıyla telefon sistemini etkilemek
Sisteme yerleştirilecek bir virüs ile tren hareketlerini yanlış yönlendirme ya da direk çarpışmalara neden olacak şekilde değiştirmek
Düşman radyo ve televizyon ağını elektroniksel olarak ele geçirerek, yapılabilecek yayınları propoganda ya da diğer bilgi amaçlı kullanma k, ya da düşmanın kendi yayını üzerinden ayırt edilmesi olanaksız biçimde değişen gizli mesajlar iletmek
Medikal formüllerin ya da kan tipi gibi kişisel sağlık bilgilerinin uzaktan değiştirilmesi
Koordineli saldırı ile belirlenmiş bir ağa saldırmak
Banka bilgisayarlarında yanlış gösterilen birikimler veya bilgi sürekliliğine zarar verecek biçimde veri bankalarına yapılacak bir saldırı ya da büyük bir karışıklık ya da paniğe neden olacak tüm girişimler
Gizli kişi, ilaç veya finansal bilginin çalınması ve açığa çıkarılması
Bilgisayar solucanları veya virüsleri ile bilgilere ya da sistemlere zarar verme
Komuta kontrol altyapısını bozarak birliklerin birbirleri ya da komuta merkezi ile aralarındaki iletişimi bozmak
Telefon sisteminin, elektrik güç şebekes inin, kentsel ya da hava trafik kontrol sistemlerinin bozulmasıyla beraber fiziksel yıkım veya yaşam kaybının meydana gelmesi ya da bilgi blokajı

Yukarıdaki tabloda potansiyel bilgi savaşı örnekleri verilmektedir.

Konuyla ilgili olarak 31 Mayıs 2007 tarihinde Genelkurmay Başkanı Orgeneral Yaşar Büyükanıt'ın yaptığı "Güvenliğin Yeni Boyutları ve Uluslararası Örgütler" konulu sempozyum açılış konuşmasının bir bölümünü aynen aktarmak istiyorum:

"Özellikle, 1990'lı yıllarla birlikte bilgi ve iletişim teknolojisinin hızla yaygınlaşması; dünyada mal, hizmet, sermaye ve fikir hareketlerinin serbest ve hızlı dolaşımı çerçevesinde ülkelerin başta ekonomik, güvenlik ve kültür olmak üzere çeşitli alanlarda birbirine daha bağımlı hâle gelmeleri sonucunda bütün ülkeler, küresel sorunlar karşısında ortak değer, yaklaşım ve tavırlar benimsemeye zorlanmışlardır.

Bunun sonunda, uluslararası güvenlik ortamı son derece değişken ve öngörüleri zorlaştıran bir hâl almıştır. İşte bu değişim sürecini doğru algılayabilen toplumlarla algılayamayan veya yanlış algılayan toplumlar kendi geleceklerini olumlu veya olumsuz yönde etkileyeceklerdir. Değişim sürecini zamanında algılamayan toplumlar, maalesef sadece, değişim sürecinin sonucunu seyretmekle yetineceklerdir.

Bu noktada ifade edilmesi gereken en önemli husus, ülkelerin tehdit algılamalarıdır. Soğuk Savaş Döneminde sade olan tehdit algılamaları günümüzde çok değişmiştir. 2003 yılında, bu salonda yapılan "Küreselleşme ve Güvenlik Sempozyumu"nda da ifade ettiğim gibi, yaşadığımız günlerde, güvenliklerini ithâl malı tehdit algılamalarına dayandıran ülkelerin güvenliklerini tehlikeye atacakları da bir gerçektir.

Diğer önemli bir husus ise tehditler ve krizlerin yönetim süreçleri ile ilgili olup, bu süreçlerin kolay yönetilebilmesi ile ilgili olarak kullanılabilecek yöntemlerdir. Halen bu konuda yüzlerce karar verme yöntemleri kullanılmaktadır. Pareto Analizleri, Fütz, Swot, Kepner-Tregoe Matrisi bunlardan birkaçıdır.

Bugün risk ve tehditlerin yanlış algılanması ve uygulanması ve bu hususun, karar verme süreçlerini olumsuz etkilemesi, sonuçları itibarı ile güvenlik anlayışına yeni boyutlar getirmiştir.

Aynı konuşmasında Orgeneral Büyükanıt güvenlik ve güvenliği tehdit eden unsurları ise şöyle açıklamaktadır:

"Soğuk Savaş sonrasında; içinde dünyanın en duyarlı bölgelerini oluşturan Balkanlar, Karadeniz ve Akdeniz Havzaları, Kafkasya, Orta Asya ve Orta Doğu coğrafyasında son on, on beş yıl içerisinde meydana gelen gelişmeler, güvenlik ve tehdit algılamalarında geçmişe nazaran önemli değişikliklere neden olmuştur.

Güvenlik algılamalarında meydana gelen değişimin en önemli sebeplerinden birisi, tehdidin tek boyutlu, devletten devlete olma klasik konumundan çıkarak, asimetrik ve çok boyutlu bir konuma ulaşmasıdır. Bu durum, günümüz tehditleri ile mücadelede klasik yapılanma ve anlayışların geçerliliğini tamamen yitirdiğine işaret etmektedir.

Genel tanı olarak bir güvenlik olgusundan bahsedebilmek için, tehdidin ve tehdide yönelik algılamaların ve tahminlerin doğru olarak tanımlanması önemlidir. Nedir tehdit? Alışık olduğumuz tanımıyla bir ülke ordusunun başka bir ülkeyi işgal etme olasılığı mıdır? Yoksa bunu, bugünün doğruları ile yeniden tanımlamaya mı ihtiyaç vardır?

2003 yılında meydana gelen 14 savaş içinde çatışan her iki tarafın devlet olduğu tek bir savaş meydana gelmiştir: ABD-Irak Savaşı. Bu durumdan anlaşıldığı üzere yeni dönemde savaşan aktörler değişmiştir.

Gelinen bu noktada, acaba diyorum, soğuk savaş yerini "karanlık savaşlara mı" bırakmıştır?

“Karanlık Savaş” kavramı içine o kadar çok aktör ve etken yerleştirilebilir ki bu aktör ve etkenlerin incelenmesi doğal olarak benim yaptığım açılış konuşması sınırlarını aşar. Umarım bu konu, sempozyum sırasında tartışılır.

Güvenlik, hepinizin çok iyi bildiği gibi, çok boyutlu bir kavramdır. Bugün artık güvenliği, içinde sadece askerî değil, siyasi, hukuki, ekonomik, sosyolojik ve psikolojik etmenlerin olduğu bir çerçevede tanımlamak gerekmektedir.

Bunun yanında risk ve tehditlerin kaynağının, zamanının ve şeklinin önceden tahmin edilmesinin, Soğuk Savaş Döneminin aksine imkânsız bir hâle geldiği yeni güvenlik ortamında, mücadele alanı bütün dünya olarak ortaya çıkmıştır.

Çünkü tehdidin ne şekilde ve ne zaman karşımıza çıkacağı belli değildir. Tehdit, ülkelerin gücü ve kabiliyetleri karşısında çok cılız gibi görünse de sahip olduğu imkânları ile istediği yer, zaman ve şekilde istediği etkiyi yaratabilecek asimetrik güce sahiptir. Bu nedenle, küresel mücadelenin ve işbirliğinin yürütülmesi zorlaşmıştır.

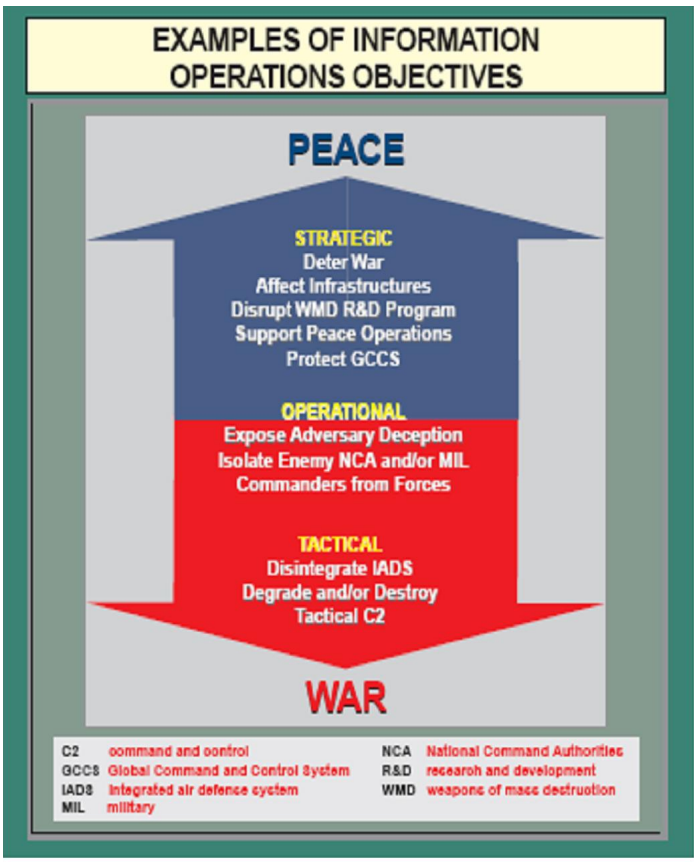
Bu noktada vurgulanması gereken önemli husus, ülkelerin güvenlik bağlamında çifte standart uygulamamasının bir ön şart olması gerekmektedir.

Bu alanda bir diğer önemli değişiklik ise, güç kavramının tanımlanmasında olmuştur. Daha önce askerî imkânlar ve ekonomik kapasite gibi parametreler vasıtasıyla belirlenen güç kavramının, artık “bilgiye ulaşabilme” ve “bilgiyi kullanabilme” yeteneğini kapsaması dikkat çekmektedir. Bunun nedeni, küreselleşme sürecinde insan faktörünün ön plana çıkmış olmasıdır. İnsan kaynaklarından azamî ölçüde istifade edebilme imkân ve kabiliyetine sahip ülkeler, diğer ülkelerin siyasi uygulamalarını, ekonomik politikalarını ve güvenlik stratejilerini etkiler duruma gelmişlerdir.

Güvenlik ortamının bu yeni yapısı şüphesiz ki, yeni tehdit algılamaları ışığında şekillenmiştir ve içinde yaşadığımız bu süreçte şekillenmeye de devam etmektedir.” (Büyükanıt, 2007)

7.2.Bilgi Savaşının Özellikleri

- Her türlü hedefe karşı zaman ve mekâna tabi olmaksızın yürütülebilen bilgi savaşı toplum anlamında her kesime yayılması amacıyla askeri, ekonomik, politik, ideolojik hatta dini sorunları temel alarak stratejik, taktik ve operatif seviyedeki hedeflere uygulanabilir.



Şekil 7.1 Bilgi Savaşı Nesneleri (Joint Pub 3-13, 1998, II-2)

Şekilden de görülebileceği gibi stratejik seviye ile taktiksel seviye arasında barış ve savaş zamanlarına göre değişen uygulamalar yer almaktadır. Stratejik seviyede küresel komuta kontrol sistemi ni korumak varken bu taktik seviyede komuta kontrol harbine dönüşmektedir.

- Bu savaşın başladığını ya da başlayacağını haber veren herhangi bir mekanizma yoktur. Yani biz bir füzenin geldiğini o hedefe ulaşmadan görebiliriz ancak örneğin hayati hedeflerimi zi hedef alan bir bilgi savaşı saldırısına karşı sadece daha önceden bu savaşa karşı aldığımız tedbirlerle savunma anlamında cevap verebiliriz.

- Çağımızın yeni tehditlerinden bahsederken değindiğimiz gibi, bilgi savaşı da asimetrik savaş türlerindendir. Çünkü asimetrik savaş, bilgi savaşında da olduğu gibi, meşru olarak harp etmeden özel hayati hedeflere alışıla gelmişin dışında yöntemler kullanarak saldırmayı, halkın yaşam ve psikolojisini etkilemeyi, her türlü silahın kullanılarak yapılabileceği savaş şek lini ifade etmektedir. Milli Güvenlik Kurulu Genel Sekreterliği de, kendi web adresinde asimetrik tehditten "yarattığı ani ve hazırlıksız durum nedeni ile ülkelerin siyasi, sosyal ve ekonomik sistemlerinde istikrarsızlıklarına neden olan, düşük seviyede kuvvet ve teknoloji kullanarak etkin olmayı amaçlayan tehdit algılamasıdır" şeklinde bahsetmektedir. (http://www.mgk.gov.tr)

- Bir bilgisayar sahibi ve yeterli bilgi birikimine sahip bir kişi özellikle bilgisayar korsan savaşı olarak belirttiğimiz çeşidi itib arıyla bu savaşı yürütebilmektedir. Bu yönüyle de ülkeler açısından yürütülecek savaşlarda zenginlik farklılıkları savaşın kazanılması noktasında belki de baskın güç unsuru olmaktan çıkmaktadır. Çünkü onlarca tankın yapacağı bir saldırının bu bilgisayarla daha etkili bir biçimde yapılabileceği gerçeği gözden kaçırılmaması gereken bir noktadır. Burada dikkat edilmesi gereken bir diğer nokta da bu savaşların sadece bir bilgisayara sahip olma maliyeti kadar bir bedelle gerçekleştirilebilmesidir. Bir başka değişle, bu savaş vasıtasıyla uzaktaki bir hedefe yönelik saldırılar alışılagelmiş askeri saldırılara göre, çoğu zaman büyük maliyet ve çabaları gerektirmeden çok hızlı bir biçimde yapılabilir.

- Gelişen teknolojiyle sürekli gelişen bilgi savaşı silahları, hem savunma hem de saldırı amaçlı kullanılabilir. Yapılacak bir saldırıya karşı koyabilme, sahip olunan bilgi-teknolojiyi kullanma imkân ve kabiliyetine bağlıdır.

- Bazı kaynaklar bilgi savaşı yerine siber savaştan bahsetmektedir. Ancak unutulmaması gereken nokta siber savaşında aslında bilgi savaşlarının bir türü olduğudur. Bilgi savaşı ya da siber savaşın ilgilendirdiği ortak nokta ise ulusal güvenliktir.

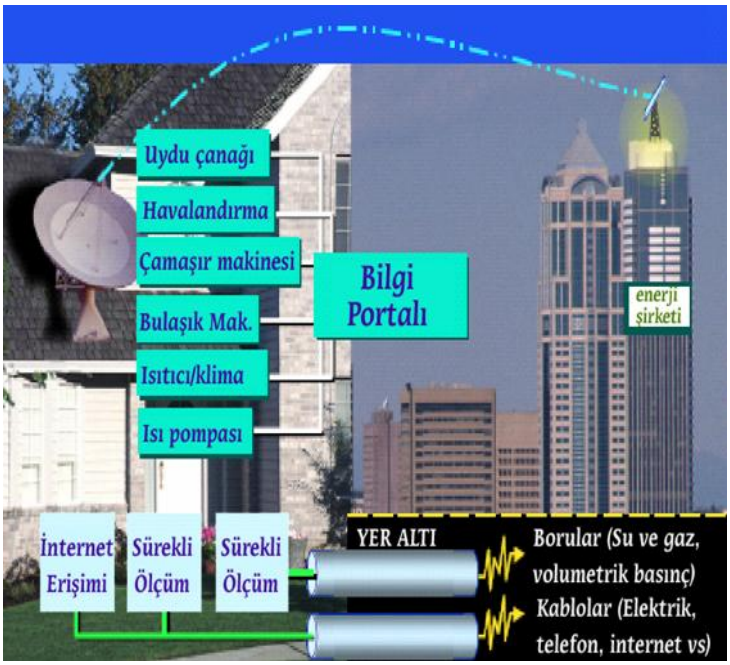
- Bilgi savaşının önemli özelliklerinden birisi de kuşkusuz saldırıyı gerçekleştiren kaynağın tam olarak tespitinin mümkün olmamasıdır. Saldırıyı gerçekleştiren saldırgan bunu." kolaylıkla inkâr edilebilir ve cezalandırılması son derece güçtür. Bugün hala Estonya saldırılarının bilgisayar korsanların bir siber ayaklanması mı yoksa resmi bir otorite tarafından onaylanmış saldırılar mı olduğunu söylemek güçtür. İşin içinde resmi bir onama vardıysa dahi, bir devletin başla bir devletin iSavaş saldırısına nasıl mukabele edebileceği açık değildir." (Ryan, 2007)

- Bu savaşın hedefi bir ülkenin enerji sistemleri, iletişim ağları, hava kontrol sistemleri, finansal sistemler ve taşımacılık işlemlerini destekleyen bilgi sistem ve yapıları gibi hayati yapıların bilgisayar ve ağlarına karşı yürütülen tahrip edici tüm güç uygulamalarını içermektedir.

Şekil 7.2 Bilgi Savaşının Hedefleri

Gelişen ve gelişmekte olan tüm teknolojiler tüm askeri operasyonlarda tehdit kavramının alanını yaygınlaştırmaktadır. Şekil.5'te de gösterildiği gibi bu hedefler liderler, sivil yapılar, askeri yapılar ya da askeri sistemler olabilmektedir.

Bir başka örnek olarak, özellikle gelişmiş ülkelerde su, elektrik, doğalgaz gibi alt yapı hizmetleri ile eğitim, sağlık, hukuk gibi hizmetler bilgi teknolojileri ile büyük bir ilişki içinde olması verilebilir. Dünya'da üzerinde çalışılan ve bir bütünleşme sağlanmasını amaçlayan e-Devlet projeleri, zaman ve maliyette tasarruf sağlarken, bilgi savaşları bakımından da tehdidin bir boyutunu da gözler önüne sergilemektedir.



Şekil 7.3 Bilgi çağı teknolojileri sayesinde enerji, güç, su ve iletişim siste mlerinin birbiri ile entegrasyonu (Baykal sy.1)

- Bilgi savaşında güvenliğin sağlanması, iletişim güvenliğinin sağlanması temelindedir. İletişim güvenliği ise kripto güvenliği, iletim güvenliği, yayılım güvenliği, fiziksel güvenlik kavramlarını içine almakta dır. Kripto güvenliği konusuna ileride değinilecektir. Ancak özetle kripto güvenliği şifreleme ve şifreleme sistemlerini kapsamaktadır. İletim güvenliği iletim güvenlik ihlallerinin önlenmesi olarak tanımlanırken, yayılım güvenliği, iletişim sistemlerinde yapılan yayılımların yetkisiz kişilerce ele geçirilip analizinin engellenmesidir. Fiziksel güvenlik ise daha önce de bahsettiğim gibi tüm sistemlerin her anlamda fiziksel olarak korunmasını kapsamaktadır.

- Bilgi savaşı şahsi hayata dönük biçimde herhangi bir kişinin şahsi bilgilerinin kullanılmasıyla yapılabilir. Gelişen teknolojiler bilginin gizliliği ve sürekliliğinin yanında kişisel mahremiyeti de ortadan kaldırarak kişilere ait bilgileri açık bir biçimde tüm Dünya'ya ifşa etmektedir. Geçmişte olduğu gi bi bir kişi hakkında bilgi sahibi olabilmek, çok derin araştırmalara gerek olmaksızın mümkün olabilmektedir. Google arama motoru üzerinden ya da

son dönemde ülkemizde de yaygınlaşan arkadaş bulma sitesi olarak değerlendirilen facebook tarzı web siteleri ile bir kişi ile ilgili çok derin bilgilere sahip mümkün olabilmektedir.

Bilgi savaşının diğer bir hedefi de şirketlerdir. Şirketler arasındaki rekabet neticesinde rakip firmanın veri tabanındaki verilere saldırarak silme, değiştirme ya da kullanma ile rakip firmaya çok büyük zararlar verilebilir. Bir kuruluşun terör örgütüne destek verdiğinin, bir firmanın yasadışı faaliyetler yürüttüğünün, ya da piyasada bulunan ürünlerinden birinin zararlı kimyasallar içerdiğinin internette yayılması çok büyük kitlelere çok kısa zamanda ulaşabilir ve rakibe büyük zararlar verebilir.

Bunun yanında bir terör örgütü kendi sempatizanlarıyla olan haberleşmesini internet üzerinden yaparak eylem yapabilmekte, maddi destek sağlayabilmektedir.

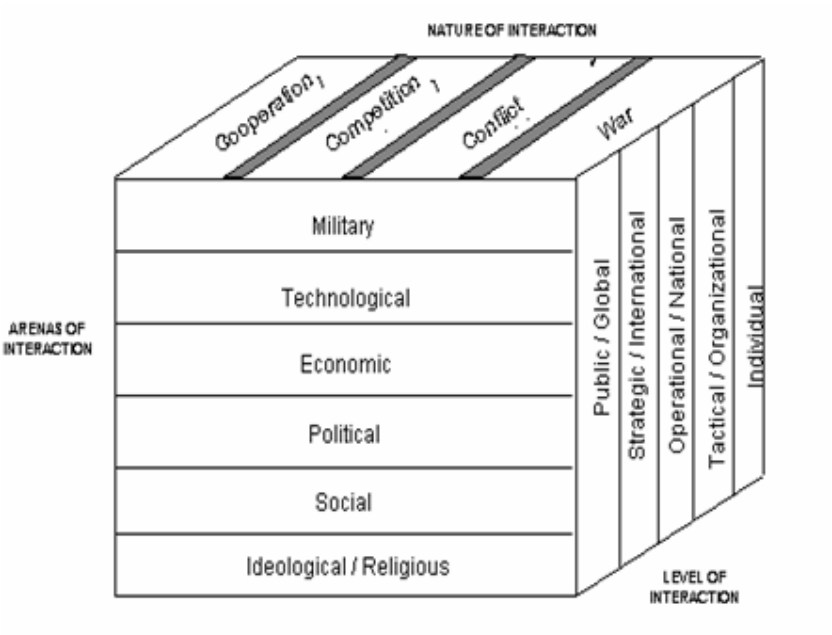
Bilgi savaşının icra edilebileceği son hedef ise ülkeler ve küresel güçlerdir.

- Emekli Korgeneral Şadi Ergüvenç, bilgi ve iletişim teknolojilerinde yaşanan çok hızlı gelişmelerin sonucunda barış, kriz ve savaş ortamlarının birbirlerinden kesin hatlarla ayrılmasının çok zor olduğunu ifade etmektedir. Çağımızın yeni çatışma modeli, gelişen bu teknolojilerle beraber gerçekleştirilen bilgi savaşlarıdır ve gelişmiş devletler geleceğin bilgi savaşları için hazırlanmaktadır.

- “Bu yeni savaşlar hassas askeri varlıklar, kritik altyapı varlıkları, savaş alanı iletişimi ve uydu istihbaratıyla bağlantılıdırlar. Örneğin, Çin’in Aralık 2006’da hazırladığı savunma konusunda devlet politikasını açıklayan belgede

(Beyaz Kitap) uydular gibi enformasyon varlıklarını kontrol edebilmek için uzayda üstünlük kazanılmasından söz edilmektedir." (Ryan, 2007)

- Şekil bilgi savaşı arenasını tanımlamak ve ele geçirmek için gereken bağımsız üç farklı yönelimi izah etmektedir. Anlaşmazlık/fikir birliğinin derecesi; teknolojik, politik, askeri, sosyal, ekonomik seviyelere direk olarak odaklanmaktadır. Aktörlerse bireyler, taktiksel/organizasyonlar, operasyonel/devletler, stratejik/uluslararası, medya, genel yayınlar vb.leridir.



Şekil.7.4 Bilgi Uzayı (Alberts, 1996, sy.2)

- Bilgi Savaşları terimi birçok düşünceyi anlatmak için kullanılabilir. Fakat bilgi savaşı genellikle bilgisayarların hâkim olduğu siber savaş ya da askeri etki alanı üzerinde odaklanmaktadır. Günümüzde askeri, ulusal, yerel, özel bilgi sistemlerini izole etmek mümkün değildir. Çok önemli askeri trafiğin bile ulusal altyapı sistemi üzerinden taşınması olasıdır.

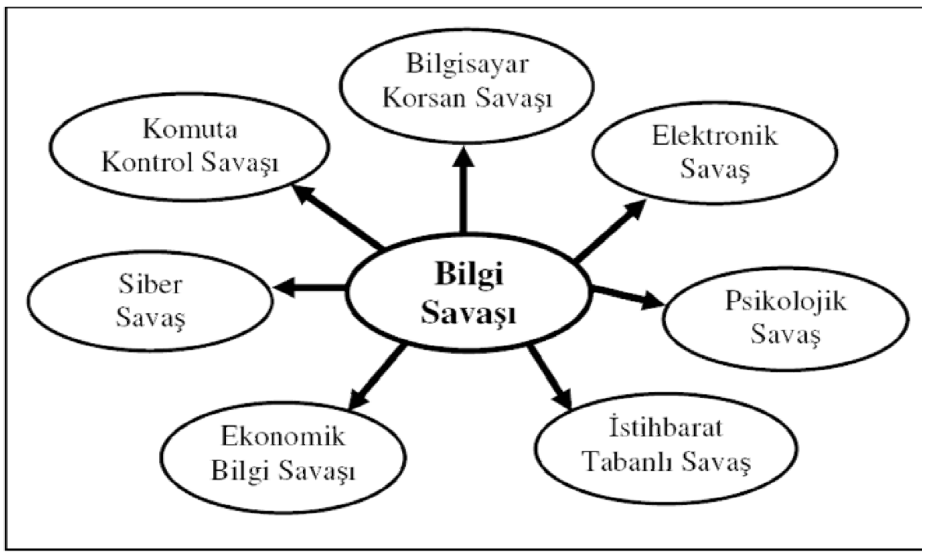
- Savaşlarda ilk saldırıyı gerçekleştirmek, ani baskınlar yaratmak oldukça önemlidir. Bu bakımdan topyekun bir savaşa girilmeden önce önemli altyapılara yapılacak ve onları çökertecek saldırıların önemli avantajlar

sağlayacağı bir gerçektir. Ayrıca bu savaş çok hızlı bir biçimde yaygınlaştırılarak devam ettirilebilir. Örneğin “2007 yılında Estonya’ya yapılan saldırılarda, web siteleri anında bu saldırılara nasıl katılınabileceği konusundaki basit bilgileri anında yayıverdiler.”(Ryan, 2007)

- Bilgi savaşının temel hedefi olan bilgi üstünlüğü; bilgi edinerek, düşmanın bilgi toplamasını ve süreçleri engelleyerek, düşmanı yanlış bilgi ile aldatarak ya da düşmanın alt yapısını tahrip ederek sağlanabilir.

8. BİLGİ SAVAŞI BÖLÜMLERİ

Bilgi savaşları; komuta kontrol savaşı (C2W: Command-and Control Warfare), istihbarat tabanlı savaş (IBW: Intelligence-Based Warfare), elektronik savaş (EW: Electronic Warfare), psikolojik savaş (PSYW: Psychological Warfare), bilgisayar korsan savaşı (Bilgisayar korsanı Warfare), ekonomik bilgi savaşı (EIW: Economic Information Warfare) ve siber savaş (Cyber Warfare).olmak üzere değerlendirilebilir **.** (Libicki, 1995, sy.1)



Şekil 8.1 Bilgi Savaşı Türleri (Erdal, Teknoloji ve Ulusal Güvenlik)

8.1.Komuta Kontrol Savaşı

Harp alanı ile komuta merkezi arasındaki iletişim, geçmişte olduğu gibi günümüzde de Komuta Kontrol sistemleri vasıtasıyla sağlanmaktadır. Bu anlamda komutanlar kendi kuvvetleri üzerindeki yetkilerini, kom uta kontrol sistemleri üzerinden sağladıkları bilgi ve istihbarat ile taktik, stratejik ve harekâtsal açıdan değerlendirerek, yine bu sistemler üzerinden savaş alanına iletirler.

Karar vericiler üzerinde odaklanan komuta kontrol sistemleri sivil karar vericilere ve askeri komutanlara stratejik, konvansiyonel ve özel operasyon kuvvetlerinin yönetimi için gerekli imkânları, sensörleri ve donanımları sağlar. Çeşitli konvansiyonel ve stratejik kuvvetlerle ilgili olan komuta kontrol sistemleri savunma mimarisinin bütünleşik bir yapısıdır ve caydırıcılığa ve savaşma yeteneklerine de katkıda bulunmaktadır.(Perry, 1995, sy. 228 –229)

Tüm sensör ve silahların bir ağ sistemi ile bütünleştirildiği bir ortamda karar vericiler ortak bir bilgi sistemini kullanırlar. Bu durumda şeffaf olmayan hiyerarşik emir komuta sistemindeki her komuta katı, operasyonlarda zaman kaybına neden olur. Böyle bir organizasyon yerine misyona göre adapte edilen bir organizasyon çok daha hızlı ve güvenli olacaktır. Misyona göre adapte edilmiş organizasyonda da hiyerarşinin tamamen ortadan kalkması söz konusu değildir. Birçok kritik kararın klasik düzende verilmesi gerekebilir.(Vural, Bilgi Teknolojisindeki Gelişmenin Yarattığı Uluslar Arası Yeni Güvenlik Ortamı)

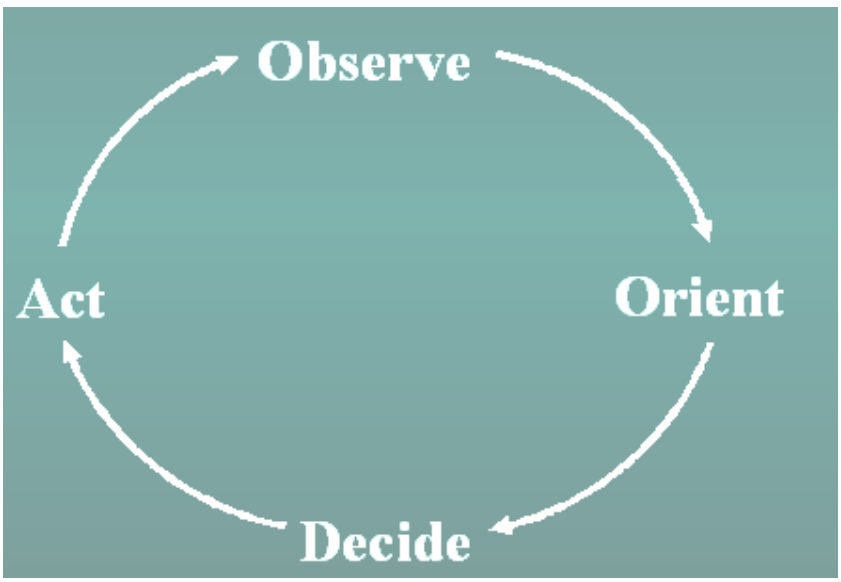
Libicki bu savaşı bilgi savaşının savaş alanlarında psikolojik yıkımla bütünleşik bir askeri strateji olarak tanımlamaktadır.(Libicki, 1995, sy.10)

“Komuta kontrol savaşı, gizlilik, askeri aldatma, psikolojik operasyonlar, elektronik harp, fiziksel tahribat operasyonlarının istihbarat ve istihbarata karşı koyma, düşman komuta kontrol yeteneğini dağıtma ve yok etme, dost komuta kontrol yeteneğini koruma amacı ile bütüncül olarak kullanımı anlamına gelmektedir.

Komuta kontrol savaşında hedefe ulaşmada beş araç kullanılmaktadır. Bunlar operasyonel güvenlik, askeri aldatma, psikolojik operasyonlar, elektronik savaş ve fiziksel tahribattır. Operasyonel güvenlik, bir tarafından kendi operasyonu hakkında düşmanın komuta kontrol sistemi tarafından keşfedilmesini engellemektir. Askeri aldatma operasyon hakkında düşman komuta kademesine yanlış bilgi sızdırmasıdır. Psikolojik operasyonlar, düşman kuvvetlerine düşman liderinin kuvvet ve nüfusunu

etkileme ve kontrol etmesini zorlaştırıcı bilgiler yayılmasıdır. Elektronik savaş taarruz yada savunma amaçlı olabilir. Fiziksel yıkım, düşman komuta kontrol sistemine saldırılar yapılmasıdır "(Baykal, Bilgi Teknolojisinin, Ulusal Güvenlik ve Ulusal Güvenlik Stratejisi ile İlgili Boyutu)

Komuta kontrol savaşının temel amaçları düşmanın Komuta kontrol s istemini yok ederek düşmanı yenmek, düşman komutasıyla birliklerini birbirinden ayırmak ve kendi komuta kontrol sistemimizi korumaktır.



Şekil 8.2 Komuta Kontrol Karar verme Mekanizması (www.owlnet.rice.edu)

Komuta kontrol karar verme mekanizmasını ise; Gözlemlemek, yönlendirmek, karar vermek, harekete geçmek şeklinde birbirini takip eden kavramlarla açıklamak mümkündür.

"Modern silahlı kuvvetleri yöneten komutanlar, mutlak başarıya ulaşabilmek için komuta kontrol inisiyatifini ellerinde bulundurmak zorundadırlar. Komuta katına iletilen en temel veriler dahi komuta kararına doğrudan etki edebilmektedir.

Dolayısıyla etkili karar alınabilmesinde C2 sistem mimarisine çok büyük işler düşmektedir. Bu sistem mimarisinde oluşabilecek en ufak aksama, mevcut liderlik otoritesini temelinden sarsabilecek, hatta kaosa dönüşebilecektir." (Vural, 2002, sy.217)

Rusya-Ukrayna Araştırmaları Masası Asistanı Elnur Soltan tarafından çevrilen makalesinde Profesör George J. Stein; "Enformasyon savaşı, 21. yüzyılın temel ulusal güvenlik meselesi olabilir. Bu yüzden, ABD yeni enformasyon savaş teknolojilerinin stratejik ve askerî kullanımı için kapsamlı ulusal-düzeyli politika geliştirmelidir. Bu amacı kolaylaştırmak için, ABD silâhlı kuvvetleri, komuta kontrol savaşı başlığı altında, "siber savaş" yeteneği sağlayabilecek teknoloji ve sistemler geliştirmektedirler." Şeklinde ABD'nin bu savaşa hazırlığını özetlemektedir. (Stein, 2002, sy.181)

Teknoloji çağımızın en değerleri ürünü olduğu kadar komuta kontrol savaşlarının da en önemli unsurudur. Çünkü "Bir C2 sistemi algılayıcıların, seyrüsefer unsurlarının, komuta ve füzyon merkezlerinin muhabere irtibatlarının ve karar sistemlerinin (yani bilgisayarlar) çevriminden oluşan bir dizi tali sistemden meydana gelen bir sistemdir." (Schleher-Kara, 2004, sy.25)

Körfez savaşı İngiliz ve Amerikan birliklerinin Irak komuta ve kontrol merkezlerinin imha edilmesiyle uygulanmış bir savaştır.(Özdemir,2003, sy.58)

İşte komuta kontrol savaşı da, hem düşman komuta merkezinin bilgi edinmesini engellemeyi hem de düşman komuta kontrol merkezleri ile savaş meydanındaki birlikleri arasındaki iletişimin kırılmasını amaçlamaktadır. Bu bağın kırılması hem komutanın hem de savaş alanındaki birliklerin bilgisiz kalmasını sağlayarak dilimizdeki tabiriyle elini kolunu bağlamaktadır. Bu anlamda komuta kontrol harbi bilgi savaşının askeri harekâtlara uygulanması bakımından bir alt kolu olarak değerlendirilmektedir. (Schleher-Kara, 2004,sy.24)

Bilgi savaşı siyasi altyapı, ekonomik altyapı ya da fiziki altyapıyı hedef olarak alırken komuta kontrol harbi fiziki altyapılarla askeri altyapıları hedef olarak almaktadır.

Komuta kontrol savaşları bir otorite ve düşman komutanına yöneliktir. Komuta kontrol, kendi KK sistemimizi koruma amaçlıyken düşmana saldırıyı içeren bilgi savaşlarının askeri uygulamasıdır. Komuta kontrol savaşı psikolojik operasyonları, elektronik harbi, istihbaratı ve bunların birbirleriyle olan karşılıklı ilişkilerini tanımlar.

Bilgi savaşı stratejik, taktik ve harekâtsal düzeyde icra edilirken komuta kontrol harbi taktik ve harekâtsal seviyelerde yapılmaktadır.

Bilgi harbi hem savaş hem de barış zamanlarında icra edilmektedir. Komuta kontrol harbi ise savaş yâda çatışma anlarında yapılmaktadır.

Tüm teknolojiler için öncelikli hedefimiz milli teknoloji altyapısını oluşturmak olmalıyken, bunun ilk adımı da; milli bir politika çerçevesinde, belirlenecek kritik teknolojilere ağırlık verecek bir hamle olmalıdır. Ancak konu, vatanımızın savunulmasıyla ilgili en önemli konulardan biri olan komuta kontrol sistemleri olduğunda, bunun için gerekli tüm sistemin, silahın, aracın ve donanımın ülkemizin kendi mühendisi, tesisi ve projesi ile ülkemizde kurulacak ya da geliştirilecek bir savunma sanayii ile sağlanması daha da büyük önem kazanmaktadır. Bu bakımdan bir yandan belirli kalite standartları çerçevesinde, ordumuzun ihtiyacını karşılayacak ve bunları ordumuza aktaracak diğer yandan da sürekli gelişen teknolojiyi takip ederek, ihtiyaçları anında karşılayabilecek, dış ülkelerde üretilen yeni gelişmiş teknolojiler üretildiğinde de bunları geliştirebilecek milli savunma sanayiinin kurulması ülkemiz açısından büyük bir gereklilik olarak sağlanmalıdır.

8.2.İstihbarat Temelli Savaş

İstihbarat, kelime manası itibariyle Arapça istihbar kelimesinin çoğulu olarak; haberler veya yeni öğrenilen bilgiler, haber alma demektir. Teknik olarak istihbarat, muhtelif imkân ve vasıtaları kullanarak herhangi bir konuda enformatik materyal temini ve temin edilen bilgilerin ham halden kurtarılarak işlenmesi, kıymetlendirilmesi ve yorumlanarak bunlardan bir netice çıkarılmasıyla ilgili faaliyettir. Ve insanların fıtrî bir melekesi olan merak ve öğrenme arzusu ile doğmuştur. Batı dillerinin bilhassa ingilizcenin hâkim olduğu ülkelerde kelime "intelligence" kelimesiyle karşılanmaktadır. Bu kelime zekâ anlamını taşımaktadır. Bu da Batı'da bu meşgalenin hangi seviyede yapıldığını göstermektedir. (Avcı, 2007, sy.13)

İstihbaratı buradan yola çıkarak haber ve zekânın birlikte oluşturduğu bir kavram olarak özetlemek de yanlış olmayacaktır.

İstihbarat pek çok kaynakta akıl, zekâ, anlayış, malumat, haber, bilgi, vukuf, işletilen haberler, muteber olan havadis, duyulan şeyler, toplanan ve alınan haberler, bilgi toplama, haber alma olarak tarif edilmektedir. (Demirel, 2004,sy.29)

Cia'nın kendi sayfada yapılan istihbarat tanımı ise; "ülkemizi yönetenlerin, güvenliği sağlamak için ihtiyaç duydukları bilgi şeklinde açıklanmaktadır." (https://www.cia.gov)

Başka bir tanımla istihbarat, ülkeler ya da bölgeler için de elde edilebilir bilgilerin, toplanarak işlenmesi, bütünleştirilmesi, analiz edilmesi, değerlendirilmesi ve yorumlanmasının sonucu olarak ortaya çıkan üründür. Bir rakip ya da düşman hakkında, gözetleme, araştırma, analiz ve anlayış ile elde edilen bilgidir. (Joint Publication, 1998, sy. I-02)

Devlet istihbaratı ise devletin bütünlüğünü, rejimin emniyetini sağlamak için, milli politika ile tespit edilen milli hedefleri elde etmek üzere devlet organlarının yaptığı istihbaratın tümüdür. (Demirel, 2004,sy.29)

Bilgi savaşlarının önemli bir bölümü olan istihbarat temelli savaşta ise savaşın bilinen bir parçası olan sürprizleri engellemek ve komuta merkezlerine planların şekillendirilmesinde yardımcı olmak " temel amaçtır. Taktik resmin elde edilmesi maksadıyla kullanılan tüm vasıtalar ve sensörler ile bu bilgileri işleyen, değerlendiren ve askeri birliklere yayan tüm sistemleri kapsamaktadır. (Özdemir, 2003, sy.58)

Bilgi savaşının temel dayanak noktası olan bilgi alt yapısının çözümlenmesi; o ülke ile ilgili olarak yapılacak her türlü teknolojik istihbarat çalışmalarının başarılı olacağı anlamına gelmektedir. (Sağsan, 2002, sy.219)

İstihbarat temelli savaşı anlayabilmek için özellikle tek nolojik istihbarat çeşitlerinin neler olduğunu bilmek gerekir. Teknolojik istihbarat çeşitlerinin izah edilmesiyle istihbaratın herhangi bir savunma veya saldırı amaçlı çatışma esnasında nasıl kullanılması gerektiği açıkça ortaya çıkmaktadır. Dünyada 100 ü lkenin kayıtlı yaklaşık elli bin bilgisayar ağı olduğunu düşünürsek; teknolojik istihbaratın bilgisayar destekli çeşidinin 21. yüzyıldaki kapasitesini algılamak hiç de zor olmayacaktır. Bilgisayar teknolojilerinden istifade edilerek gerçekleştirilen ve bilgisayarın bilgiyi toplama, sistemleştirme ve dağıtma amacına yönelik olarak kullandığı bu teknolojik istihbarat türüne kısaca "bilgisayar tabanlı istihbarat" denilebilir. Bir diğer teknolojik istihbarat türü ise, iletişim araçlarının kullanılarak yapıldığı bilgi toplama faaliyetleridir. Örneğin, dijital iletişimin en önde gelen araçlarının (telefon, TV, faks) kullanılarak yapıldığı bu tür, popüler olarak yapılan istihbarat çalışması niteliğini taşımaktadır.(Sağsan, 2002, sy.228)

İstihbarat faaliyetlerinde tasnif ilk aşamadır. Bu aşamada benzer bilgiler bir araya getirilir. İkinci aşama kıymetlendirmedir. Yani, haberin istihbarat değerinin, haberin alındığı kaynağın güvenilirliğinin ve haberin doğruluk derecesinin tespit edilmesidir.

Bu aşamadan sonra bir yorum yapılır. Yorum kesin bir yargıya varmak için mevcut bilgilere dayanılarak olayların, gelişmelerin ve benzer durumların anlamını ve önemini ortaya koyma işlemidir

Son aşamada ise, üretilen istihbarat, ihtiyacı olan kurumlara, gerekli zamanda ve uygun formda ulaştırılır.(Demirel, 2004, sy.30)

Şekil 8.3 İstihbarat Çarkı (http://www.atin.org/isthsair.asp)

İstihbarat kaynaklarına göre açık ve gizli istihbarat olmak üzere ikiye ayrılır. Açık istihbaratta kamuya açık her türlü bilginin değerle ndirilmesi yapılır. Gizli istihbaratta ise belirli operasyonlar sonucunda bilgi edinimi yapılır. (Avcı, 2007, sy.29)

İstihbaratın büyük bir bölümü açık kaynaklıdır.

İstihbarat yapısal olarak taktik ve stratejik olarak ikiye ayrılır. Taktik istihbara t; güncel konularla ilgili ve güncel olaylar üzerine yapılan çalışmalarıdır. Stratejik istihbarat ise; büyük ve önemli olaylarda, uzun vadeli planlamalarla ortaya konan çalışmalarıdır. (Atay, 2003, sy.18.)

Burada değinilmesi gereken bir diğer istihbarat tü rü ise operasyonel istihbarattır ki o, stratejik ve taktik istihbarat arasındaki bağı oluşturur.(Headquarters Department of the Army, 1995,sy. 9-I)

Modern stratejik istihbaratın kurucusu sayılan, II. Dünya Savaşı sırasında Yale üniversitesinde tarih profesörü olarak çalışan Sherman Kent'in istihbarat konusunda pek çok çalışmaları bulunmaktadır. (http://en.wikipedia.org)

Prof. S. Kent, stratejik istihbaratın teorik temellerini geliştirdiği "Stratejik İstihbarat" adlı kitabında stratejik istihbaratı:" Karar alıcıların hatalı plânlama ve hareketleriyle kendi politikalarına zarar ve taahhütlerine zarar vermeyecek şekilde diğer devletlerle ilgili olarak sahip olmaları gereken bilgi türüne verilen addır." şeklinde tanımlanmaktadır. (Özdağ, 2002, sy.113)

Kent, "Stratejik İstihbarat" adlı kitabında stratejik istihbarat sürecinin yedi aşaması olduğunu belirtir. Bu yedi aşamayı şöyle sıralamaktadır:

1) Bir stratejik istihbarat grubunun dikkatini çekecek bir sorunun doğuşu,

2) Bu sorunun hangi aşamalarının ülke için önemli olduğunu tespit için analizin ve hipotezin geliştirilmeye başlanması,

3) İkinci aşamada ortaya konulduğu şekli ile sorun, yani hipotez ile ilgili bilgi toplama,

4) Toplanan bilginin tasnifi ve analizi, hipotezlerin test edilmesi,

5) Dördüncü aşamadaki bilginin özünü tespit için tekrar değerlendirme,

6) Olası başka hipotezlerin ortaya çıkması durumunda daha fazla bilgi toplânarak hipotezin doğrulanması veya yanlışlanması için sona gidiş,

7) Son hipotezin belirlenmesi (Özdağ, 2002, sy.117

Stratejik, operasyonel ve taktik istihbaratın yöneldiği temel hedefler bir devletin/toplumun bütün yaşam alanlarını, diğer bir ifade ile millî gücü oluşturan bütün unsurları kapsamak zorundadır. Bu istihbarat alanları şunl ardır:

1) Askerî İstihbarat: Kara, Deniz ve Hava kuvvetleri ile füze sistemleri ve kitlesel imha silâhlarına yönelik bilgi toplama amacı ile yapılan istihbarattır.

2) Biyografik İstihbarat: Bir ülkede askerî, siyasî, kültürel, ekonomik elite yönelik yapılan bilgi toplama faaliyetidir.

3) Ekonomik İstihbarat: Ekonominin genel kapasitelerine, zayıf ve güçlü yanlarını tespit etmeye yönelik ve çok uzun zaman genellikle ekonominin silâhlı kuvvetleri destekleyebilme derecesini tespite yönelik istihbarattır.

4) Bilim ve Teknoloji İstihbaratı: Bütün dünyada ve aktüel ve muhtemel düşmanlarla ilgili bilimsel çalışma ve teknolojik gelişmeleri toplamaya yönelik istihbarattır.

5) Ulaşım ve İletişim İstihbaratı: Ulaşım ve iletişim istihbaratı ülkelerin ulaşım altyapılarına ve iletişim tesislerine yönelik olarak yapılan bilgi toplama faaliyetidir.

6) Askerî Coğrafya İstihbaratı: Askerî coğrafya istihbaratı, askerî operasyonları etkileyecek her türlü fiziksel ve kültürel çevrenin tespit ve analizine yönelik çalışmadır.

Stratejik istihbaratın gerçekleşmesi istihbaratın kapsamına, zaman ve mekân perspektifine de bağlıdır.

7) Siyasal İstihbarat: Bir ülkenin siyasal yapısını oluşturan, devlet sistematiğinin yani anayasal düzenin yapısında yer alan bütün unsurlara karşı yapılan i stihbarattır.

8) Sosyolojik İstihbarat: Toplumsal yapıya yönelik olarak gerçekleştirilen bilgi toplama faaliyetidir.

Bütün bu alanlara yönelik olarak gerçekleştirilen istihbarat faaliyetleri çok boyutlu, girift, karmaşık ve sistemleştirilmiş, kendi içinde uzmanlaşmayı gerektiren bir yapı arz etmektedir ve aşağıda bu yapıların her birisi kendi içinde incelenmiştir (Özdağ, 2002, sy.121–122)

İstihbaratın değinilmeyen bazı özellikleri ise aşağıdaki gibidir:

- Geleceği görebilmek, olası sorunları önceden tespit ed erek çözümünü bulabilmek, iyi bir istihbarat sağlandığında daha kolaydır.

- İstihbaratın, yaşanan teknolojik gelişmelere rağmen en önemli unsuru hala insandır.

- İstihbaratın bir diğer olmazsa olmazı da milli olması gerekliliğidir. Çünkü ülkeler arasındaki ilişkiler çıkara dayalıdır ve öylede olması gerekmektedir.

- Yazılımlar ve internet istihbaratın en önemli kaynakları durumundadırlar. Uydular, cep telefonları ve daha pek çok teknoloji, istihbarat açısından kullanılmaktadır. Bilgisayar istihbarat amaçlı bu iki kılavuzu kullanarak açık ve kapalı casusluk yaparlar. Bu konulara ilerideki konularda değinilecektir.

- İstihbarat bir savaş açısından, savaşta esas unsur değil, yardımcı kuvvettir. Savaşın kazanılması bakımından önemlidir ancak savaşı kazanmayı garanti etmez. İstihbarat savaşın kazanılmasına hizmet eder.(Kahn, çeviren:ASAM, 2002, sy.12-13)

- İstihbarat, savunmanın belirleyici bir özelliğidir; diğer taraftan saldırıya sadece eşlik eden bir özelliktir

Hemen hemen istihbaratın anlatıldığı tüm kaynaklarda M.Ö 500 yıllarında yaşamış meşhur Çinli komutan ve filozof Sun Tzu Savaş Sanatı adlı kitabına atıf yaparak, casusluk faaliyetinin fevkalade önemli olduğunu bariz bir şekilde vurgulamıştır. Sun Tzu'ya göre; bilge hükümdarlarla iyi bir komutanın kolaylıkla savaş kazanıp zafere ulaşması istihbarata bağlıdır. (Avcı, 2007, sy.13)

Ümit Özdağ istihbaratın önemini ilginç bir benzetmeyle ifade etmektedir.

“İstihbarattan kopuk bir devlet yönetiminin gözleri bağlı maraton koşmaktan hiçbir farkı yoktur. Nereye gittiğinizi, rakiplerinizin önümüzde mi arkanızda mı olduğunu, ne kadar koştuğunuzu özetle hiçbir şeyi bilmeden koşarsınız. Oysa karar alıcılar

uluslarının karşı karşıya olduğu fırsatları ve tehditleri öngörmekle yükümlüdürler.”(Özdağ, 2002, sy.111)

Bu tarifler toparlandığında istihbaratı şu şekilde de değerlendirebiliriz. ‘Ülkelerin ulusal, askeri, ticari, teknolojik, ekonomik vs. faaliyetlerinin yakından izlenmesi; bu bilgilerin değerlendirilmesi ve ileriye dönük olabilecek gelişmelerle ilgili önceden analizlerinin yapılabilmesidir’

İstihbari faaliyetlerde gizlilik, doğruluk, devamlılık, çabukluk, tarafsızlık, erişebilirlilik ve açıklıktır. (Demirel, 2004,sy.32)

"ABD ve İngiltere'deki üniversitelerde "güvenlik ve istihbarat" her türlü politik, ekonomik, sosyal ve askeri gelişmeyi anlamayı ve derhal öngörmeyi amaçlayan, evrensel bir sosyal bilim" olarak açıklanmaktadır. (Yılmaz, 2006,sy.27)

Ancak son dönemde yaşadığımız hızlı gelişmeler güvenlik kavramının artık teknolojiyle de çok yakından ilişkili olduğunu göstermektedir.

Soğuk savaş döneminden günümüze kadar geçen süreçte, güvenlik ortamının geçirdiği devrimsel değişimler; stratejik dengenin değişimi, stratejik sistemin değişimi ve askeri teknolojide yaşanan değişimler olmak üzere üç başlık altında toplanmaktadır. Jeo-stratejik devrim niteliğindeki yeni denge, ABD üstünlüğüne dayalı tek kutuplu dünya düzeninin ortaya çıkış ile tanımlanmaktadır. Yeni güvenlik ortamının ikinci önemli özeliği ise, stratejik sistem değişimlerinin getirdiği post-modern çatışma şekillerinin ortaya çıkmasıdır. Post-modern çatışma ise; "

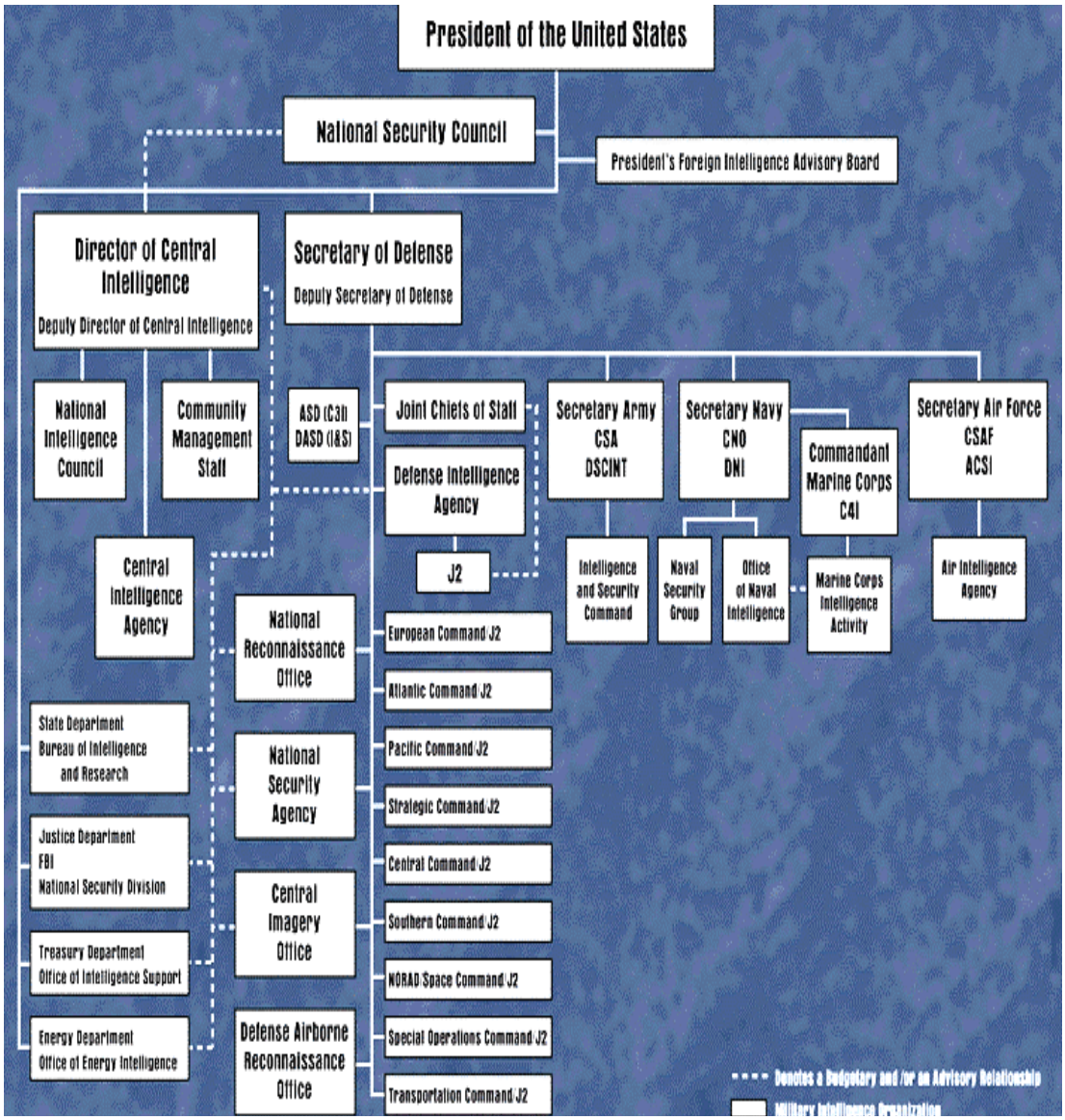
(1) Güvenliğin ulusallaşan boyutunun daha önemli hale gelmesi ve ulus-devlet yapılarına nüfuz eden sosyal hareketler şeklinde görülen devlet dışı aktörlerin, sistemde etkin rol edinmesi, (2) Uzayın ve siber savaşın çatışmalarının gittikçe daha önemli güvenlik çarpanı haline gelmesi ile tanımlanmaktadır. "(Yılmaz, 2006,sy.27)

"Sherman Kent, II. Dünya savaşı sonrası güçlü bir müttefiğe ihtiyaç olmadan, ABD'nin tüm Dünya üzerindeki çıkarlarını korumak için temel ihtiyacın, stratejik

istihbarat olduğunu ifade etmişti. Bu tanımı biraz daha genişletirsek stratejik istihbarat, bir devlet için gelecekte ortaya çıkabilecek fırsatları, tehditleri araştırıp tespit ve öngörerek, karar alıcıların önüne olabileceklerle ilgili seçenekler koyarak, onların politika üretme sürecini daha doğru bir zemine çekebilmek amacıyla yapılan istihbarat türüdür."(Yılmaz, 2006,sy.27)

II. Dünya Savaşın'dan sonra Cia'de de görev alacak olan Sherman Kent'in de belirttiği gibi, geleceğe dönük doğru politikaların üretilmesi noktasında temel ihtiyaç, stratejik istihbarattır. Bu kavramın önemi ilk çıktığı dönemden günümüze giderek artmıştır. "Teknolojik gelişmelere ilave olarak, uluslararası ilişkilerde savaş dışı yöntemlere daha fazla yer verilmesi ile birlikte istihbaratın kapsamı da genişledi. Örtülü operasyonların yanında, propoganda faaliyetleri de güvenlik ve ulusal çıkarların muhafazasında güncel hale geldi. Gelinen bilgi ve iletişim ortamında bilgilerin toplanması kadar toplanan bilgilerin istihbarat haline getirilmesindeki süreç de zorlaştı." (Yılmaz, 2006, sy.172)

İstihbaratın giderek değer kazanması ülkeleri bu konuda daha teknolojik ve yerleşik olmaya itmiştir. Tüm milli varlıklarla beraber yürütülen istihbarat faaliy etleri, milli gücü oluşturan tüm varlıkların ortak çalışması ile tüm kaynakları değerlendirecek biçimde olmalıdır. Aşağıdaki şekilde ABD'de istihbarat faaliyetlerinin hangi kurumlarca yürütüldüğü ve birbirleriyle olan ilişkileri değerlendirilmektedir.



Şekil 8.4 ABD'nin İstihbari Yapılanması (http://www.atin.org/isthsair.asp)

Ancak unutulmaması gereken bir konu da istihbarat veya istihbarat servislerinin, her olayın kahramanı veya her derdin dermanı olmadıklarıdır. İstihbarat örgütlerinin ulusların kaderini veya tarihini tek başlarına tayin etme veya yapma durumunda olmadıkları da açıktır. Askeri, ekonomik, politik açıdan istihbarat, önemli olmakla birlikte başarıda veya başarısızlıkta tek başına belirleyici değildir. Ancak bugün

dünyanın içinde bulunduğu ekonomik ve siyasi durum, bu birimlerin varlıklarını ve yaptıklarını yaşamsal düzeyde önemli kılmaktadır. (Özkan, 2007, sy.3)

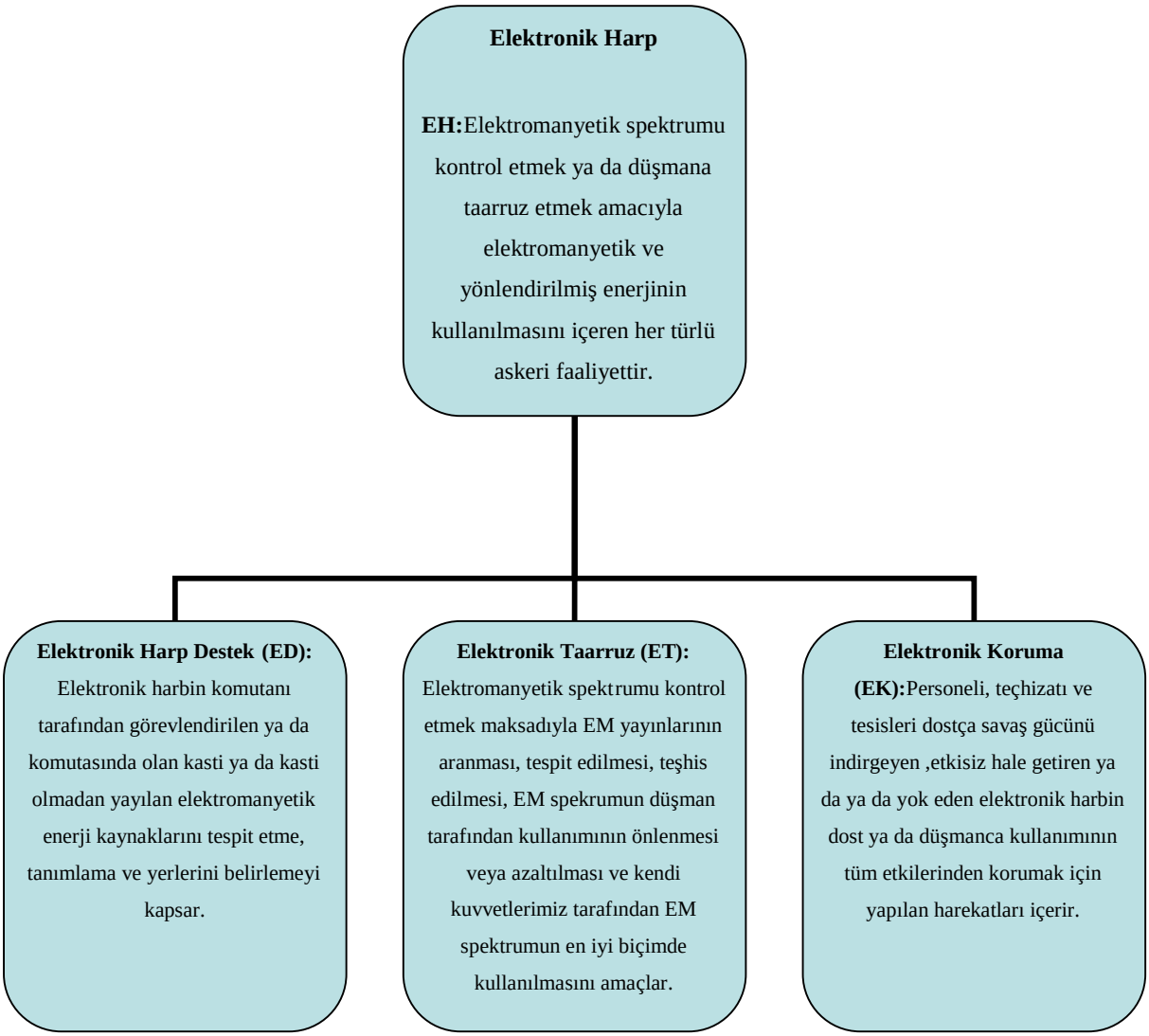
Yaşanan teknolojik gelişmeler istihbarat örgütlerinin çalışma biçimlerini de büyük ölçüde değiştirmiştir. Örneğin geçmişte k ullanılan yöntemleri, echelon ile ya da uydu sistemleri ile karşılaştırmak mümkün bile değildir. Bu bakımdan sağlanan avantajlar istihbarat örgütlerinin teknolojiyi kullanma yönündeki isteklerini de arttırmıştır. İstihbarat örgütlerinin de bu noktadaki tem el yardımcıları tabii ki bilgisayarlardır. "Bilgisayarlar akla gelebilecek herşeyden evvel bilgi işlemek içindir. Yüksek performanslı istihbarat bilgisayarlarının en önemli başarıları; ses ve resim analizleri, şifreleme ve şifre çözme, uydu kontrolleri ve yönetiminde görülmektedir. İstihbartat servislerinin ülkeleri ve ticari faaliyetleri incelerken başarılı şifre kırma çalışmalarının ardında ve temelinde bilgisayarlar bulunmaktadır." (Yılmaz, 2006,sy.608)

Sonuç olarak, ülkemizin en önemli değerlerinden bi ri olan Millî İstihbarat Teşkilâtının da modern bir istihbarat kurumu olarak, ülkemizin bölünmez bütünlüğüne, anayasal düzenine, varlığına, bağımsızlığına, güvenliğine ve Millî gücünü meydana getiren unsurlarına karşı var olabilecek muhtemel tüm tehditler hakkında bilgi toplaması ve istihbarat oluşturması vazgeçilmez bir ihtiyaçtır. Bu görevlerin yerine getirilmesi bakımından günümüzün hızla gelişen en ileri bilgi ve teknolojik imkanlarını MİT'nın kullanımına sunmak yapılması gereken işlerin başında gelmektedir. Bununla beraber, kamu mali yönetiminde yapılan temel değişikliklere de kısa sürede adapte olabilen, gelir, gider, varlık ve yükümlülüklerinin etkili, ekonomik ve verimli şekilde yönetilmesine olanak veren bir yapı istihbarat teşkilatımız bakımından d a oldukça önemlidir. (Milli İstihbarat Teşkilatı, 2007 Faaliyet Raporu)

Önemli olan bir diğer konuda istihbarat teşkilatımızın mevcut personelinin çağın değişen ihtiyaçları doğrultusunda eğitilmesi gerekliliğidir.

8.3. Elektronik Harp

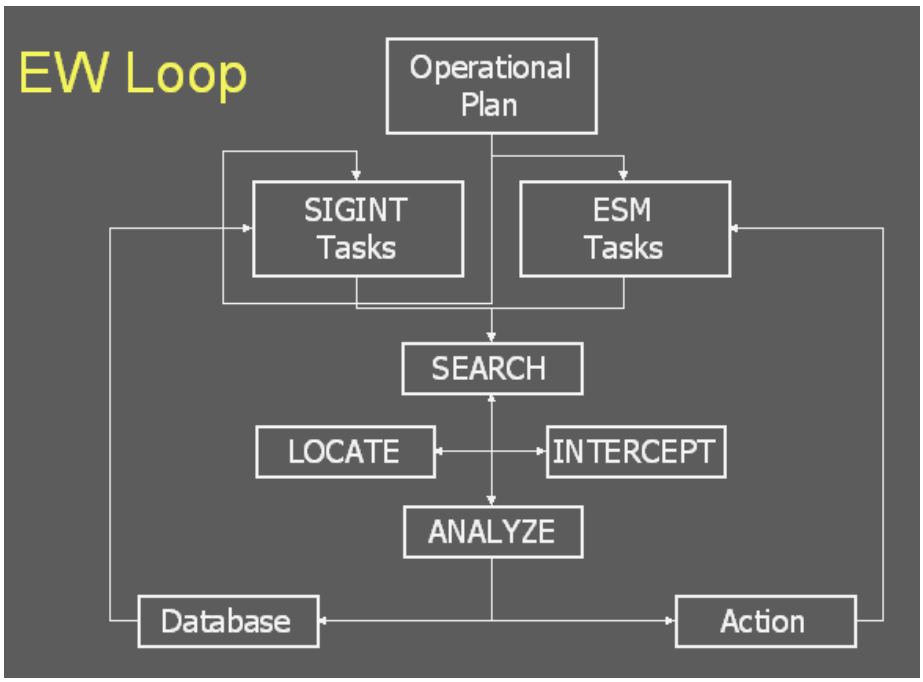
Elektronik harp (EH) aslında elektromanyetik spektrumun kontrol altına alınması için gerçekleştirilen bir muharebedir. Ancak günümüzde elektromanyetik spektrumun aslen tüm askeri harekâtlarda esas olan bilgi taşıyıcısı ya da sağlayıcısı olarak işlev görmesi gerektiği anlaşılmış ve kabul edilmiştir. Bu yüzden elektronik harp bilgi harbi olarak kabul edilen kavramın temel unsurudur.(Schleher -Kara, 2004, sy.10)



Şekil.8.5 Elektronik Harp Terminolojisi (Schleher -Kara, 2004, sy.20)

Elektronik Savaş, Hedef birliğin elektron ve enformasyon akışını kesmek, bozmak veya müdahâle etmek üzere tasarlanan komuta kontrol veya istihbarat merkezli savaşa uygulanabilir teknikler bütünüdür.(Sağsan, 2002, sy.228)

Aşağıdaki şekilde Elektronik savaşa ait döng ü ifade edilmektedir.

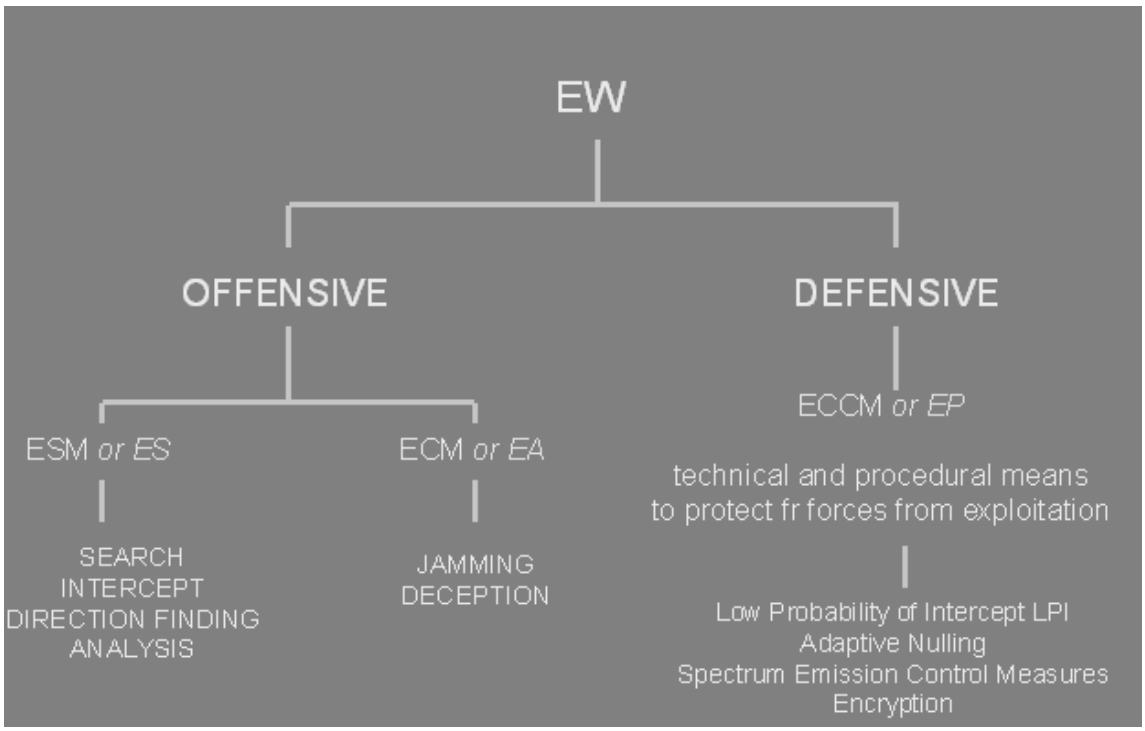


Şekil 8.6 Elektronik Savaş Döngüsü (Paul,2004)

Elektronik harpte amaç bahsedildiği gibi elektromanyetik spektrumun kendi kuvvetlerimiz adına mümkün olduğunca etkin bir biçimde kullanılması ve düşmanın ise bu spektrumu kullanmasının engellenmesi ya da etkisinin azaltılmasıdır. EH'in temel amacı olan elektromanyetik spektrumun kontrol altına alınması, taarruzi olarak hem elektronik taarruza (ET), hem de savunma amaçlı elektronik korunma (EK) faaliyetlerine ihtiyaç duymaktadır. Son olarak da ET ve EK'yı mümkün kılan istihbarat ve tehdit tanımlamalarının yapılmasını Elektronik Harp Destek (ED) karşılamaktadır. Yani elektronik harp; Elektronik Harp Destek (Electronic Warfare

Support), Elektronik Taarruz (Electronic Attack) ve Elekt ronik Koruma (Electronic Protection).olmak üzere üçe ayrılmaktadır. (Schleher -Kara, 2004,sy.19)

Aşağıdaki şekilde Paul, elektronik savaşı savunma ve saldırı olarak 2 bölümde tanımlamaktadır. Zaten benim de daha önce değindiğim gibi Elektronik koruma, elektronik taarruz ve desteğe yardımcı olarak hizmet etmektedir.



Şekil.8.7 Elektronik Savaş Bölümleri(Paul,2004)

Elektronik Destek, sinyallerin tespitini, bu sinyallerin yerlerinin belirlenmesini, düşman haberleşme ve radar sinyallerinin kendi çıkarla rımız için kullanılmasını, komuta merkezinin acil ihtiyaçları doğrultusunda, düşmanın niyetinin anlaşılmasını ve tehditle ilgili bilgilerin toplanmasını hedeflemektedir. (Bengür ve ark. Atmaca, Şener, sy.1)

Başka bir değişle ED; “ET, EK, silahtan sakınma (weapon avoidance), hedefleme yada kuvvetlerin diğer taktik koşullanması gibi konuları içeren acil kararların desteklenmesi amacıyla gerçek zamana yakın olan tehdit bilincine varılması için gerçekleştirilen faaliyet üzerinde yoğunlaşır. Burada ele alınan k onu önemli faaliyetleri dinlemek, tanımlamak, analiz etmek ve düşman yayınlarının yerini belirlemektir. Elektromanyetik yayınlar genellikle önemli tehditlerle bağlantısı olan frekans bandlarını kapsayan hassas alıcılar kullanılarak tespit edilmektedir.” (Schleher-Kara, 2004,sy.20)

ET, elektromanyetik enerji kullanarak bozmak, zarar vermek, karıştırmak amacını içermektedir. Düşman etkinliğinin azaltılması ve etkisiz hale getirilmesi işlevini de yerine getirir. Elektronik Karıştırma (Electronic Jamming) düşman cihazlarının etkinliğinin zayıflatılması amacıyla, Elektronik Aldatma (Electronik Deception) düşmanı şaşırtmak, yanlış yönlendirmek amacıyla ve Elektronik Etkisizleştirme (Electronic Neutralization) düşman cihazlarına geçici veya kalıcı hasar vermek amacıyla yapılan elektromanyetik yayınlardır. (Bengür ve ark. Atmaca, Şener, sy.1)

Elektronik Koruma; personel, yetenek veya donanımların dost ve düşman haberleşme veya radar sinyallerinden kaynaklanan enerjilerden dolayı EH kabiliyetlerinin azal masının veya yok olmasının engellenmesini amaçlamaktadır. İyi elektromanyetik önlemler düşman ataklarına karşı koymak için başarılı bir savunma oluşturur. Elektromanyetik oluşumların iyi yönetimi sayesinde düşman tarafından algılanmak zorlaşır ve sistemler in dayanıklılığı artar. (Bengür ve ark. Atmaca, Şener, sy.1)

“Elektronik korumanın kullanımı sadece elektronik teçhizatın korunması (ECCM) için değil, elektromanyetik kontrol (EMCON), elektromanyetik direnç arttırma (electromagnetic Hardening), EH frekans uyumluluğu ve muhabere emniyeti (COMSEC-Communication Security) gibi tedbirlerin kullanımı için de daha kapsamlı bir hale getirilmiştir.” (Schleher -Kara, 2004,sy.19)

Elektronik Taarruz sistemleri aktif ve pasif olmak üzere değerlendirilebilir.

Aktif Koruma Sistemleri;

- Jamming (Yayını Bozma): Düşmanın haberleşme ve tespit sistemine tesir,
- Deception (Aldatma):Düşmana ait bilgiyi yanlış yönlendirme ya da geçersiz kılma,
- Active Cancellation (Etkin İptal): Radar sinyallerini örnekleme, analiz ve fazın dışına verme,
- EMP: Nükleer bir patlama veya bir elektromanyetik bomba ile yoğun manyetik akım üretmeyle elektromanyetik yayılım üretme,

Gibi kavramları içerir.

Pasif sistemler ise; Chaff (Yanıltıcı, uçaklarda radar güdüm yanıtma amaçlı), Towed Decoys (Çekici Yem), Balloons, Radar Reflectors (Radar yansıtıcılar), Winged Decoys (Kanatlı Yem) ve stealth (Gizleme)'yi içerir. Gizleme kızılötesi, görünmezlik, radar emen boyalar ve metalik olmayan uçak iskeleti gibi uygulamaları içerir.

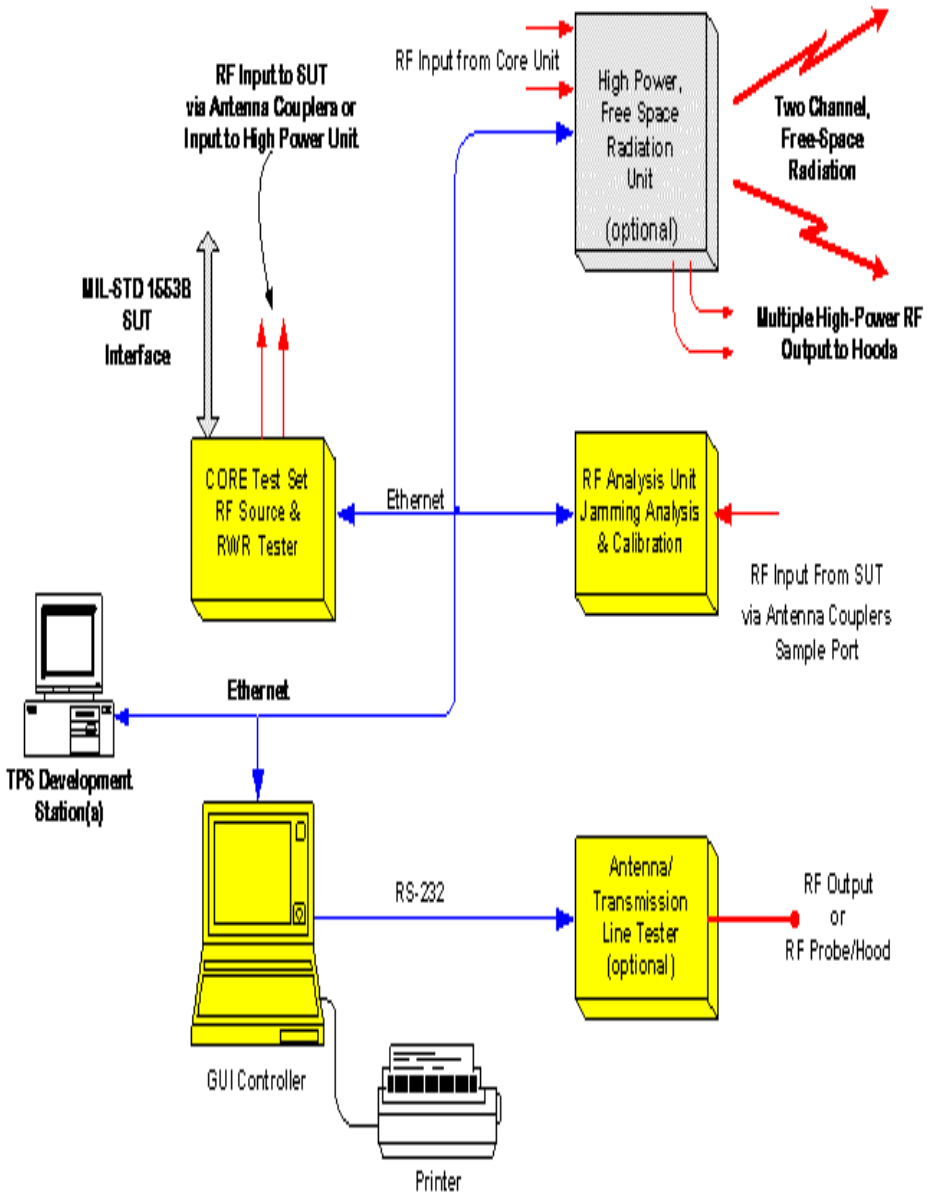
Elektronik Koruma da aynı şekilde aktif ve pasif olmak üzere iki kısımdan oluşur. Aktif Elektronik Koruma, Radyo ekipmanının teknik modifikasyonunu, Pasif EK ise savaş alanında kullanılacak operatörlerin eğitimi, onların askeri disiplin ile eğitilmesini içerir.

Elektronik destek, ise ELINT (ELectronic Signals INTelligence), SIGINT (SIGnals INTelligence). Communications Intelligence (COMINT) olarak 3 kısımda incelenir.

- ELINT (ELectronic Signals INTelligence): Radar dalgaları roket ve telemetrik bilgisayar bilgilerinin toplanması, Dost yada düşman ayrımının yapılması ise, ELİNT ile gerçekleşir.
- SIGINT (SIGnals INTelligence): Stratejik olarak, Radar veya radyo sinyallerinden bilginin toplanmsı ve analizini tanımlar.

- Communications Intelligence (COMINT): Tüm sinyallerin dinlenmesi, çözülmesi ve analizini kapsayan istihbaratı tanımlar.(Speer and Searles, Elektronik Savaş)

Konuyla ilgili son olarak elektronik savaşa ait bir test akış şemasına yer vermek istiyorum.



Şekil 8.8 EH Test Akış Şeması (http://inosci.blogspot.com)

Bir kriz anında düşman silahlı kuvvetlerine karşı kullanılabilecek en etkin silahlardan biri olan Elektronik harp sistemleri, bu özelliği ile ülke savunmasında kullanılan silah sistemlerinin ayrılmaz bir parçası konumunda görülmektedir.
Barış zamanında istihbarat bilgilerinin toplanması ile başlayan, savaş zamanında da düşman silah sistemlerini etkisiz hale getirilmesi suretiyle zaferin en önemli mimarlarından biri kuşkusuz elektronik harp sistemleridir. Bu özellikleri nedeniyle elektronik harp sistemleri ülkelerin Milli Savunma Doktrini içerisinde önemli bir yere sahiptir.

Günümüz dünyasında, ülkelerin silahlı kuvvetleri tarafından; pasif veya aktif, koruyucu veya elektronik saldırı amaçlı kullanılabilen elektronik harp sistemleri; kara, hava ve deniz platformlarında saldırı ve savunma silah sistemlerinin etkinliğini artıran en önemli sistemlerden biri olarak karşımıza çıkmaktadırlar. (Yıldız, Milli Elektronik Harp Yaklaşımı ve Teknolojik Öncelikler)

8.4.Psikolojik Harekât

Bir ülke açısından tüm konularda olduğu gibi güvenliği konusunda da en önemli faktör insandır. Bir ülke, verimli ve stratejik noktalar üzerinde bulunan topraklara yada zengin maden yataklarına sahip olabilir, ancak unutulmamalıdır ki bir ulusun var olması için gereken esas zenginliği o ülkenin sahip olduğu bilinçli, eğitimli, ülke menfaatlerini kendi şahsi çıkarından üstün tutabilecek bireyleri kadardır.

Çünkü bu bilince ve eğitime sahip olmayan toplumlar, sahip oldukları zenginliklerin diğer ülkeler tarafından sahiplenilmesine karşı durabilecek gücü ya da gerekli hareketleri yapma cesaretlerini, kendilerinde bulamazlar.

Bu nedenle onların zenginliklerinin ele geçirilmesi ya da bu toplumları kendi çıkarlarına uygun kullanma amacıyla; toplumların var olan bilinçlerinin yok edilerek

insanların korku, endişe ve güçsüzlük duygularına itilmesinde de, tarihte de pek çok kez örneklerini bulabileceğimiz psikolojik saldırılar kullanılmaktadır.

Günümüz Dünyası mücadeleleri, artık bilindik savaş kavramından uzaklaşma eğilimi sergilerken, ülke ve toplumlara fiziki zarar vermek yerine, zihni(mental) zararların verilmesi hedeflenmektedir. Rakip fert ve toplumların inanç sistemleri, duygu ve düşünceleri hedef alınarak, dil, düşünce, görüş birliği, milli güç ve mücadele azimleri gibi milli ve kültürel değerler t örpülenerek tahrip edilmektedir. (Kumkale, 2006, sy.11)

Savaş ilan etmeden hedef ülkede bu çeşit tahribatların yaratılması; kültür savaşı, psikolojik savaş ve enformatik cehaletin sağlanması ile mümkündür. Birbiriyle iç içe geçmiş bu kavramlar genellikle beraber yürütülmeleri bakımından da, bir nokta da buluşmaktadırlar. (Baştürk, 2005, sy.8)

Psikolojik harekâtın silahları olan yıkıcı fikirler, zararlı duygular ve kötü alışkanlıklar hem psikolojik harpte, hem de kültür savaşında kullanılmaktadır. Psikolojik harbin buna ilave olarak kullanılan malzemesi yalana, iftiraya ve karalamaya dayanan bilgiler, haberler, yorumlar ve şayialar; kültür savaşının malzemesi bunlarla beraber yabancı kültür unsurları; enformatik cehaletin malzemesi ise yalan yanlış, lüzumsuz ve zararlı bilgiler haberler ve yorumlardır. Kültür savaşı ve enformatik cehalet kesintisiz, psikolojik harp safha safha uygulanır.“(Baştürk, 2005, sy.8)

Bu olguları bundan 700 yıl önce yaşamış olan tarih filozofu ve sosyolojinin kurucusu İbn Haldun’un Mukaddime adlı eserinde, aslında şöyle özetlemektedir: “Yenilmiş kavimler, yenmiş kavimlerin din, mezhep, örf, adet, gelenek, giyim ve kuşamlarını alırlar. Çünkü nefis ve kalp kendini yenenlerin üstünlüğüne inanır.” (Arslanoğlu, Misyonerlik Batı Emperyalizminin Silahıdır)

Buradan aslında şu sonucu da çıkarabiliriz: Bir kavime karşı onun din, mezhep, örf, adet, gelenek, giyim ve kuşamlarını kabul eden kavimler, yenildiğini kabul eden ya da gerçekten yenilen kavimler halini alırlar.

8.4.1.Psikolojik Savaş

Psikolojik harekâtlar, seçilen bilgi ve göstergelerin yabancı hükümet, organizasyon, grup ve bireylere yönlendirilerek onların duygularını, güdülerini, bir olaya verdikleri reaksiyonları ve davranışlarını etkilemek amacıyla planlanırlar.

Psikolojik harekât gündeme gelmesini hazırlayan sebepler çok çeşitlidir. Bunların başında kendilerini Dünya'nın tek hâkimi olarak gören küresel kuruluşların, tarihin her devrinde ülkeleri yönetmek ve kendi emelleri doğrultusunda toplumları yönlendirmek gayretleri gelmektedir.(Kumkale, 2006, sy.41)

Barış zamanından çatışmaya kadar olan süreçte yapılan bu operasyonlar aslında askeri harekâtların bir parçasıdır. Bu savaşta verilen ana mesajlar; sözler, tehditler, hayatta kalma şartları ve güvenliğin sağlanması gibi konuları içerebilir. Verilen mesajların başarısı, mesajı verenin bunları yerine getirme yeteneği ve gücüyle orantılı olarak algılanır.

Psikolojik operasyonlar öncelikle; askeri arenanın dışında yürütülen ve stratejik etki yaratmayı amaçlayan stratejik operasyonlar, savaş ya da çatışma zamanlarında tanımlanan coğrafya üzerinde düşmanlıkları arttırarak kendi stratejimizi uygulamaya imkân verirken hedef ülkenin stratejilerini yürütmesini engellemeyi amaçlayan operasyonel, yine savaş ya da çatışma zamanlarında karşı kuvvetlerin komutanlarına karşı yürütülen taktiksel ve yabancı topraklar üzerinde bulunan birliklerin başarısı amacıyla oradaki insanların birbirleriyle olan düşmanlıklarını ya da olası anlaşmazlıklarını kullanmak amaçlı birleşme operasyonları olarak 4 bölüme ayrılır.(Byrd, 1996)

Libicki'ye göre psikolojik savaş türlerini; ulusal iradeye karşı faaliyetler, rakip komutanlara karşı faaliyetler, rakip birliklere karşı faaliyetler ve kültürel anlaşmazlık ve çatışmalara yönelik faaliyetler olmak üzere sınıflandırabiliriz. (Libicki, sy.34)

"Psikolojik harbin hedefinde hedef ülkenin milli güç unsurları (siyasi güç, askeri güç, coğrafi güç, sosyo-kültürel güç, bilimsel ve teknolojik güç) bulunur. Düşman psikolojik harpte hedef ülkenin harp planlamasını teşkil eden Milli Güç unsurlarını ele geçirerek emeline ulaşır. Daha açık bir ifadeyle psikolojik harp; hedef ülke milli güç unsurlarının yönlendirilmesi ya da yok edilmesidir." (Şahin, 2003, sy.11)

Psikolojik tehdidin hedefi; insanın duygu, düşünce inanç ve davranışları olmakla birlikte, bu tehditle her sınıf ve kesitteki insanlar aynı yoğunlukta muhatap olmamaktadır.

Psikolojik harekât öncelikle hedef aldığı fert, grup ve toplumlar ayrı ayrıdır.hedef alınan kişi ve grupların sahip oldukları potansiyel ve toplumu etkileme gücü oranında düşmanın psikolojik harekat baskısı artar.(Kumkale, 2006, 77 -78)

Bir anlamda psikolojik harekâtın doğal özelliği çok gizli bir faaliyet olmasıdır. Çok gizlidir; çünkü insan karakteri kendisine dışarıdan dikta ettirilen doğruları değil, kendi kültürü çerçevesinde algılayacağı doğruları seçer ve kendisine dışarıdan yönlendirilen ve zorlama olduğu anlaşılan fikirleri asla kabul etmez. Sonunda doğal olarak yönlendirilen fikre karşı savunmaya geçer ve bunu şiddetle reddeder. İşte bu yüzden gizlilik bu harekât temel özelliğidir.

Bunun sonucu olarak, tamamen gizli olarak yapılan bu harekât uygulama sonuçlarını da tam anlamı ile tespit etmek mümkün değildir. Veya ortaya çıkan sonuçlara bakılarak bu olayın psikolojik saldırı sonucu mu, yoksa doğal bir davranış sonucu mu meydana geldiğini tespit edebilmek her zaman mümkün değildir.(Kumkale, 2006, sy.79)

Psikolojik harekât Dünya'da bazı ülkeler tarafından o kadar planlı bir biçimde yapılmaktadır ki; Oktay Sinanoğlu "ABD'nin Florida'da sadece bu konuda ordu mensuplarına hizmet veren bir üniversitesinin bulunduğunu ifade etmektedir."(Sinanoğlu, 2002, sy.119)

Klasik anlamda savaşın kazanılması veya kaybedilmesinde, ya da savaştan sonraki dönemde üstünlüğün devam etmesinde yahut sorunların çözülmesinde, insanların ruh haline etki ederek sonuç almak olarak tanımlanan psikolojik savaşta temel kural; kendini ve düşmanını çok iyi tanımaktır. Bir diğer nokta ise, baskı ve ikna yöntemlerini iyi bir şekilde kullanarak hedef ülkede psikolojik bir çöküntünün uyandırılmasıdır. (Tarhan, 2002, sy.5)

Uzun süre savaş alanlarında kullanılıp çoğunlukla düşmanı etkileme gayretleri olarak ele alınıp değerlendirilen bu harekât, bugün tamamen farklı olarak algılanmakta ve uygulanmaktadır. Bu faaliyet artık sadece savaş zamanlarını değil, barış dönemlerini de içine almaktadır. Sadece düşman tarafına değil dost birliklerine, tarafsız ve yabancı toplumlara da uygulanan ve birbiriyle koordineli olarak yürütülen bir seri beyinleri etkileme faaliyeti şeklinde kullanılmaktadır. (Kumkale, 2006, sy.80)

Anlatılanlardan sonra psikolojik harp kavramını tanımlamak yerinde olacaktır.

Psikolojik harp, çeşitli nedenlerle, sınırdan silahlı saldırı halinde harekete geçmeyen düşmanın, diğer araçlarla milli bünyeye, vatan yüzeyine girerek ve yerli personelden istifade ederek içten bölücü, içten yıkıcı metotlarını uygulamak suretiyle devleti sarsmak ve ele geçirmek hususunda yapılan propaganda ve ilgili tedbirlerin planlı olarak kullanılmasını kapsayan bir saldırı, bir savaş olarak ortaya çıkmıştır. (Şahin, 2003, sy.1)

Eşref Özdemir Bilgi Savaşları adlı kitabında propaganda/psikolojik savaştan, “politik ve askeri hedefleri ele geçirmek maksadıyla, düşman, dost ve tarafsız olan kesimlere yöneltilen davranış ve tutum değiştirmeye yönelik planlanmış psikolojik etki faaliyetleridir” şeklinde bahsetmektedir.(Özdemir, sy.60)

Örneğin ”Körfez savaşında Irak’ın basın yayın organlarına müdahale edilerek yayın yapması engellenmiştir. Amerika ve İngiltere gelişmeleri çıkarları doğrultusunda kendi basın yayın organları ile yönlendirerek halkına ve Irak halkına duyurmuştur. Hatta yanlı yayın yapan El Cezire televizyonunun yayınları da engellenmeye çalışılmıştır. “(Yayla, 2004, sy.589)

Amacı insanları ikna etmek ve değiştirmek olan psikolojik savaşın saldırı ve savunma silahı propaganda, eğitim ve provokasyon iken yöntemi de insanların fikir ve beyinlerini etkilemektir.

Sinanoğlu psikolojik savaşın en önemli 2 aracı olarak, eğitim kurumları ve basın - yayın ile bunlara nüfuz edip kullanmak olarak açıklamaktadır. (Sinanoğlu, sy.192)

"Propaganda hedef olarak seçilen toplulukların morallerini bozmak, onların her alanda başarma gayretlerini, mücadele azim ve iradelerini yok etmek, insanların inançlarını zayıflatarak kendilerine olan güvenini kaybettirmek ve nihayet kendileri tarafından tarafından tespit edilen belirli fikirleri aşılamak maksadı ile psikolojik harekât başvurduğu en etkili vasıtadır.

Propaganda belli hedef gruplarının düşünce, inanç tutum ve davranışlarını et kilemek maksadını güden haber bilgi ve özel dokümanların kitle iletişim araçları yardımı ile planlı ve devamlı olarak hedef seçilen toplum üzerine gönderilmesi işlemidir."(Kumkale, 2006, sy.105)

Psikolojik harbin etkilerinin nasıl yaratılabileceği aslında, Mahir Kaynak'ın belirttiği şu biçimde özetlenebilir. Kaynak'a göre "İnançlarımız bizim hem gücümüz hem de sınırımızdır. İnancımızı bilenler bizim hangi etkilere nasıl tepki vereceğimizi de bilirler." (Kaynak, sy.99)

Ülkemize yapılan psikolojik saldırılarla ilgili pek çok örnek verilebilir. Örneğin, 19. yüzyılda İngilizlerin Suudi Arabistan'da Vahabilik mezhebini ortaya çıkartmaları da buna örnektir. Çünkü Vahabiliğin ortaya çıkması aslında, hem dinsel hem siyasal olarak Hicaz bölgesinde Osmanlı Devleti'ne bir başkaldırı niteliği taşımaktaydı. Vahabi isyanları, Osmanlı Devleti'nin bütünlüğünü bozmakla kalmamış aynı zamanda imparatorluğun parçalanmasında katalizör rolü oynamıştır.(Vurmay, 2005)

Bu durumu Prof. Dr.Tayyar Arı ise şöyle açıklamaktadır:

1902 yılında başa geçen Abdul Aziz bin Abdurrahman el -Suud'un bu yıldan 1. Dünya Savaşına kadar geçen süre içinde bölgedeki Arap kabileler üzerinde otorite sağlanmasında Vahhabizm olarak bilinen dini anlayışı referans alası ve iktidarının meşru aracı olarak kullanması önemli bir etken olmuştur.(Arı, sy.184)

Mahir Kaynak'ın kitabında verdiği bir örnek de bize psikolojik savaşı çağrıştırması bakımından dikkat çekici birörnek niteliğindedir. Kaynak, "acaba teröristler dinsel amaç güttükleri için mi ABD bu çizgiy e geldi, yoksa ABD çatışmanın din temelinde olmasını kurgulamıştı ve karşısındaki gücün de aynı nitellikte olmasını mı istemişti? Her iki tarafında aynı çizgide olması sadece bir tesadüften mi ibaret?" diyerek, bugün ABD'nin yürüttüğü bazı tutum ve politik alarını ifade etmektedir. (Kaynak, sy.71)

Amerikan ordusunda görevli Serookiy, Psikolojik harbin en önemli örneklerinden biri olarak askeri operasyonların desteklenmesinde, psikolojik savaşla idaren edilen ve düzenlenen ciddi bir dersin Afganistan'da, Sovy etler Birliği müfreze ve birlikleri tarafından öğrenildiğini ifade etmektedir.

Bir tarafta birlikler, yerel savaş konusunda oldukça iyi durumda bulunurlarken, diğer tarafta yabancı topraklar üzerindeki çatışmalarda psikolojik savaşı, psikolojik faaliyetleri ve moralin önemini hafife aldıklarını belirtmektedir. (Serookiy, sy.196)

Bu örnekte esas vurgulanmak istenen nokta aslında Sovyetler'in bu nedenlerle bu savaşı kaybettiğini ifade etmektir. Bunu tam olarak ispatlamak zor. Ancak şu bir gerçektir ki ABD'nin bu savaşta, o güne kadar görülmemiş gizli, bir harekâtının varlığıdır. Nitekim Charlie Wilson'ın Savaşı adlı gerçek olayları anlattığı ifade edilen filmde "Afganistan'daki Sovyet işgali sırasında komünizme karşı direnen mücahitlere gizli yollardan silah ve finans desteği sağlayan Teksas'lı kongre üyesi Charlie Wilson'un gerçek yaşam öyküsü anlatılıyor." (http://beyazperde.mynet.com)

8.4.2.Kültür Savaşı

Bir toplumu var eden ve onu yaşatan o toplumun kendine has kültürüdür. Bu bakımdan kültürünü koruyup geliştiremeyen toplumlar için söylenecek tek şey onların başka toplumların kültürü içinde eriyip yok olacağıdır

Sosyologlar kültürü somut ve soyut olarak ikiye ayırmaktadırlar. Somut kültür; bir toplumun kullandığı kap–kacak, giyim eşyaları, her türlü alet ve teknik araçlardır. Soyut kültür ise, bir toplumun başta dili, edebiyatı, sanatı, bilimi, felsefesi, örf ve adetleri, düğün şekilleri, yemek yeme şekilleri vb. şeylerdir. Sanat alanına ait olan müzik, resim, mimarlık, halk oyunları da soyut kültürün öğelerindendir.(Arslanoğlu, Ulusal eğitime neden gereksinim vardır?)

Toplumları millet yapan dil, din ve ahlak, örf ve adetler, milli alışkanlıklar ve zevkler, sanat, hukuk, milli tarih şuuru, ideal birliği ve sanat eserlerinden meydana gelen ahenkli bütünü "milli kültür" olarak tanımlamaktadır. Kültür savaşı ya da kültür emperyalizmi, hedef ülkenin milli kültürünün yok edilmesidir. Kültür savaşlarında bir taraftan hedef ülkenin milli kültürü tahrip edilirken, bir taraftan da hedef ülke insanlarına yabancı kültür aşılanarak yabancılaştırılmaktadır. .(Baştürk, 2005, sy.8)

Kültür empozesi ayrıca, "psikolojik savaş kapsamında değerlendirmekle birlikte, savaşın öncesinde düşman ülkenin değer yargılarına ve bilinç seviyesine, özellikle iletişim vasıtaları kullanarak, bir yönlendirme yapılmakta ve toplumda kabulleniş yaratılmaktadır. Uzun sürelidir. Sonuç sonunda kimi zaman düşman ülkenin kuvvetleri bir kurtarıcı gibi algılanılabilmektedir." şeklinde açıklanabilmektedir. (Özdemir, sy.59)

Küreselleşmenin toplumlar üzerinde etkisinin en fazla sosyo-kültürel alanda kendini hissettirdiğini söylemek yanlış olmayacaktır. Ocak 1997'de Le Monde Diplomatique'de yayınlanan bir makale küreselleşme olgusuna eleştirel bir bakışla küreselleşmeden; "tek düşünce doğması olarak sunulan küreselleşme olgusu, başka

hiçbir ekonomi politikasına şans tanımamakta; yurttaşın sosyal haklarını sosyal rekabetin insafına bırakıp hüküm sürdükleri toplumlarda, bütün faaliyetlerin yönetimini finans piyasalarına bırakmaktadır şeklinde bahsetmekte dir.(Miman, 2007, sy.75)

Teknolojinin etkilediği alanlardan birisi de kültürün küreselleşmesidir. Nitekim Dünya'ya ulaştırılan bütün haberler, 4 haber ajansının tekelindedir. Yine Dünya haberlerinin %65'i ABD tarafından Dünya'ya ulaştırılmaktadır. Bu durum , teknolojiden faydalanarak medya gücünü elinde bulunduran ülkelerin kendi kültürlerini yaymalarında daha çok başarılı olmalarını sağlayarak, ortak kültür oluşturma çabalarını kolaylaştırmaktadır. (Miman, 2007, sy.74)

Milletimizde tarih boyunca pek çok kez bu saldırılara maruz kalmıştır. Örneğin; Çin Seddi ile kendilerini güvende hissetmeyen Çinliler, Türklerle baş etmenin yolunu Göktürk Yazıtlarında da belirtildiği gibi, Türklerin Çinli kadınlarla evlendirilmesi ve çocuklarına Çince isimler verilerek Çinlileştirilmesi olarak bulmuşlar ve bunda da bazı dönemlerde başarılı olmuşlardır.

Ya da Tanzimat döneminde yabancılar kendi okullarını açarak yetiştirdikleri gençleri siyasal bakımdan bilinçlendirerek Osmanlı İmparatorluğu'nun parçalanmasında kullanmışlardır. Bu okulların kullanılması Atatürk dönemine kadar devam etmiş, Atatürk bu okulları Lozan Barış Antlaşması görüşmeleri sırasında kapatmış hatta bu yüzden görüşmeler belli bir süre çıkmaza girmiştir. (Arslanoğlu, Ulusal eğitime neden gereksinim vardır?)

"Hayatı boyunca onu en çok meşgul eden, geceleri konuşmalarını Türkçe kelime ve terimlere ayıran Atatürk, Türkiye Cumhuriyeti gibi, dilin de söz varlığı, ek, kök ve kurallarıyla bağımlılıktan kurtulmasını istemiş, dilin millet hayatındaki önemini tam anlamıyla kavramış bir liderdir. Onun Türkiye Cumhuriyeti'nin kuruluşunda, yaptığı dönüşümlerle (inkılâplarda) güttüğü "her yönüyle uygar bir toplum yaratma" amacı dilde de yansımasını bulmuştur. Ulu önderin "Yaptığımız ve yapmakta olduğumuz inkılâpların gayesi, Türkiye Cumhuriyeti halkını tamamen asrî ve bütün mana ve eşkâliyle medenî bir hey'et-i ictimaiye (uygar bir toplum) hâline isâl etmektir

(ulaştırmaktır). İnkılâbımızın umde-i asliyesi (asıl ilkesi) budur." biçimindeki açıklaması yaptığı kültürel etkinliğinin özetidir."(Zülfikar, 2007, sy.778)

Yabancı okulları günümüzde de bir tehdit olarak değerlendirebiliriz. Çünkü bu okullarda hem yabancı dilde eğitim verilmekte, hem din derslerinde ağırlıklı olarak hıristiyanlığa vurgu yapılmakta hem de burada okuyan gençlere karşı yapılan kültürü bozucu saldırılar doruğa ulaşmaktadır.

Bu tür saldırılar günümüzde de büyük bir hızla devam etmektedir. Bu saldırılara yukarıda da bahsettiğim gibi yabancı dilde eğitimin zorunlu olması da örnek olarak verilebilir. Artık işe ya da herhangi bir eğitim programına başvurmak için dahi, yabancı dil sınavlarında belirlenen bir baraj puanı istenilmektedir. Oysa bu resmi bir zorunluluk değil çağın getirdiği bir gereklilik olarak değerlendirilebilir. Liselerimizde yabancı dilde eğitim verilmesiyle de, gençlerimiz kültür empozesi mücadelesinde örümcek ağının tam ortasına bırakılmaktadır.

Türk Dil Kurumu Başkanı Sayın Prof. Dr. Şükrü Haluk Akalın, Ankara Üniversitesi Eğitim Bilimleri Fakültesinde toplanan Ulusal Eğitim Kurultayında yaptığı konuşmada yabancı dilde eğitim yapan ülkelerin Nijerya, Kenya, Etiyopya, Uganda, Tanzanya, Filipinler, Macaristan, Bulgaristan ve Türkiye olduğunu söylemiştir. (Arslanoğlu, Ulusal eğitime neden gereksinim vardır?)

Yabancı dilde eğitimin yanında müzik konusunda da bir kültür empozesinden bahsetmek mümkündür. Hemen her yerde karşılaşılan yabancı müzikle, bizim gibi hissetmesi mümkün olmayan toplumların duyguları yaşama biçimi bile bize dayatılmaktadır. Dilimizdeki tahribatı artık alışveriş yaptığımız dükkânların tabelalarında bile görmek mümkündür.

Günlük hayatta direk olarak karşılaşabileceğimiz kültürümüzü bozma çalışmalarından birisi de dini olarak toplumumuzu etkileme çalışmalarıdır. Kimi zaman sokakta karşılaştığımız bir misyoner, kimi zaman televizyonumuzu açtığımızda bir kanaldan yayınlanan bir program ya da dini öğrenmek isteyen bir

vatandaşımızın aldığı bir kitap, insanların dini duygularını istismar ederek onları bazı düşüncelere kanalize etme amaçlı olabilmektedir.

Öyle ki, televizyonda gördüğümüz ak sakallı bir dede; insanlara dini korku vererek, geniş bir kesime hitap eden bir lider; dinler arası diyalog çağrısı yaparak yada popüler bir manken; din değiştirerek, görünenin de ötesinde başka bir amaca hizmet edebilmektedir.

Sovyetler Birliğinin dağılmasıyla Sovyetler tehdidi ortadan kalkarken batının kültür emperyalizmi, özellikle misyoner faaliyetleri şiddetlenmiştir. Misyoner faaliyetlerin etkisiyle dini inancı saptırılan kişiler din adına anarşist ve terörist olarak dı ş güçler tarafından Devletimizi ele geçirmek üzere 1990'lı yıllarda faaliyete geçirilmiştir. (Baştürk, 2005, sy.31)

Misyonerlerin son taktiği diyalog adlı çalışmasında Günay Tuncer şunları belirtmektedir. Dinler arası diyalog, ilk olarak 1962 -67 yılları arasında gerçekleştirilen 2. Vatikan konsülünde ortaya çıkmıştır. Konsülde Müslümanlar ve hıristiyan olmayan kişi ve kesimlere karşı yaklaşım konusunda bazı kararlar alınmıştır. Bu kararlar da üzerinde özellikle vurgulanan konu ise dinler arası diyalog kavramıdır. Burada hıristiyan olmayan insanlara karşı yapıcı, olumlu ve hoşgörülü yaklaşılması, çatışmadan kaçınılması üzerinde durulmakta bu sayede onları kazanma şansının artacağı ifade edilmiştir. Bu çerçevede farklı dinlerin temsilcileri ile yapılan görüşmeler vasıtasıyla kendi görüşlerini diğer inanç çevrelerine aktarma fırsatı bulmuşlardır.(Cevizoğlu, 2005, sy.164)

Vatikan'ın bu tutumu da aslında psikolojik bir harekât olarak da değerlendirilebilir. Çünkü bu yaklaşım bazı akademik çevrelerde hatta bazı ce maatlerce de kabul görmüş, bu kabulün arkasındaki fikrin ne olduğu konusunda da tereddütler yaratan bir durumdur.

Ülkesindeki misyonerlik çalışmalarının sonuçlarını Afrikalı bir yazar şöyle anlatır: Misyonerler Kenya'ya geldiğinde topraklarımız bizim, kuts al kitap onların elindeydi. Bize gözlerimizi kapatıp dua etmemizi söylediler. Gözlerimizi açtığımızda kutsal

kitap bizim, topraklarımız ise onların eline geçmişti “Hıristiyanlar ülkemize geldiğinde bizim topraklarımız onların elinde İncil vardı. Bize gözle rinizi yumun dua edin dediler. Gözlerimizi açtığımızda bizim topraklarımız onların olmuş bizim elimizde ise sadece İncil kalmıştı.(Demir, Yeniçağ Gazetesi, 03.12.2007)

8.4.3.Enformatik Cehalet

Enformatik cehalet, hedef toplumun dış güçler tarafında n yalan, yanlış lüzumsuz ve zararlı bilgiler, haberler ve yorumlarla istenilen yönde yönlendirilmesidir. (Baştürk, 2005, sy.8)

Bu konuda kullanılan temel silahlardan birisi medyadır. İnsanlar yeterli bilgiye ve bilince sahip değillerse medyanın tara flı düşünceleriyle çok kolay bir biçimde yönlendirilebilmektedirler.

Enformatik cehaletin kullandığı bir diğer silahta düşünce özgürlüğü fikridir. Herkes istediğini düşünebilir ancak unutulmamalıdır ki Dünya’nın hiçbir ülkesinde suçu teşvik eden fikirler sınırsız bir biçimde ifade edilemez. Burada bahsedilen iki kavram arasındaki farklılık da aslında birmiş gibi ülkelere empoze edilerek hedef ülkelerde terör ve anarşi ortamının yaratılması bakımından kullanılmaktadır. (Baştürk, 2005, sy.15-16)

Kullanılan bir başka yöntemde doğrularla beraber yanlışların verildiği yalan yanlış asılsız iddialardır. Burada amaç iddialarla varsayımların sunulduğu hedeflere, doğruları görünce yanlışları da doğru olarak kabul ettirme eğilimidir. (Baştürk, 2005, sy.18)

Ayrıca bir toplumun kültürüne uygun olmayan eserlerin seçilerek eser sahibine çok prestijli ödüller vermek, böylece hedef ülkeyi kötülemek ya da felaket tellallığı

yaparak toplumda kötümser duyguların ya da panik ortamının yaratılması da kullanılan yöntemlerdendir.

Yukarıda bahsettiğimiz örnekler gibi daha pek çok yöntem sayılabilir ancak burada unutulmaması gereken nokta, iyi eğitilmiş bilinçli bir toplumun hiçbir zaman bunlardan etkilenmeyeceğidir. Bu saldırılara karşı yapılması gereken bir diğer eylemde, karşı psikolojik harekât planlarının hazırlanmasıdır.

Prof. Dr. Hasan Gürak'ın, "www.bilgiyonetimi.org" sitesinde yayınlanan bir makalesiyle beyin göçü konusuna da değinmek istiyorum.

"Eğitimli insan kaynakları ekonomik açıdan her ülkenin en değerli varlıklarıdır. Çünkü ülke ekonomisinin ve ülke içindeki işletmelerin gelişip büyüyebilmesi, uluslararası piyasalarda söz sahibi olabilmesi, verimliliğini arttırabilmesi için en önemli araç insanın "zihinsel" emeğidir. Başka bir deyişle, bir ülke ekonomisinin veya bir işletmenin uzun vadede başarısı sahip olunan insan gücü kaynaklarının nitelikleri ile sınırlı ve orantılıdır. Fiziksel (makineler/tesisler), mali veya doğal kaynaklar ne denli büyük olursa olsun nitelikli insan gücü olmadan ne ülke ekonomisinin ne de işletmelerin uzun vadede istikrarlı bir başarıya ulaşması olası değildir.

Çağımızda beyin göçü nedeniyle gelişmekte olan ülkeler sürekli olarak bu en değerli varlıklarını yitirmekte, buna karşın gelişmiş ülkeler ve küresel yatırımcı firmalar ise masraf ve zahmete girmeden sürekli olarak kazanmaktadırlar. Beyin göçünü durduracak önlemlerin bir an önce alınması, hatta "tersine" beyin göçünün teşvik edilmesi gerekir. Beyin göçü denince sadece gelişmekte olan ülkelerden gelişmiş ülkelere göç edenlerin geri dönüşünü anlamamak gerekir. Gelişmiş ülkelerin yüksek nitelikli yüz binlerce insanı işsizdir ve gelişmekte olan ülkeler bu kişilerin niteliklerinden yararlanabilir. Ayrıca emekli olmuş ama hala aktif olarak katkıda bulunabilecek kapasitedeki yüz binlerce insan potansiyelinden de yaralanmak mümkündür. Bu sayede gelişmiş ülkelerden gelişmekte olan ülkelerin ekonomilerine ve işletmelerine paha biçilemeyecek bir "bilgi, beceri ve deneyim" akımını aktarma olanağı olacaktır. Böylece bir yandan batının daha gelişmiş teknolojik ve örgütsel

becerileri gelişmekte olan ülkelere aktarılırken bir yandan da üretilen katma değerin daha hızlı büyümesi, yani hızlandırılmış verimlilik artışı, mümkün olacaktır."

Türkiye "tersine beyin göçü" konusunda önemli bir avantaja sahiptir. Çünkü kısa dönemde yararlanabileceği büyük bir potansiyeli vardır; Türkiye dışında yaşayan ve gelişmiş ülke okullarında çağdaş ekonomilerin gerektirdiği eğitimi almış ve almakta olan on binlerce Türk kökenli insan. Bu potansiyelden etkin bir şekilde yararlanılabilmesi durumunda nitelikli insan açısından Türkiye ekonomisi büyük bir kazanım elde etmiş olacaktır. (Gürak, Küreselleşme Nereye Götürüyor?,2003)

Özet olarak psikolojik harekatlar bireylerin ve toplumların düşünce, davranış ve değerlerinin saldırgan tarafın amacına uygun bir biçimde değiştirilmesi için yapılan girişimlerdir. Bu saldırılardan milletimizi korumanın en önemli yolu onlara Ulu Önderimizin "Ne Mutlu Türküm Diyene! İlkesini aşılayabilmekten geçmektedir. Bunun yapılması da milli eğitim sisteminden geçmektedir. Bu çerçevede yetişecek kültür unsurları sağlam bireyler de, bu savaşa karşı milletimizin en etkin gücü olacaklardır.

Psikolojik harekatların en etkin silahları; medya, internet, kitap, gazete, dergi, televizyon, konferanslar, paneller ve benzeri iletişim ortamlarıdır. Bu bakımdan bunların denetlenmesi ve kontrolü büyük önem taşımaktadır. Bu kontrolü yapacak kurumların yeni teknolojilerden en iyi biçimde yararlanmaları sağlanmalı, onlara rekabet imkanı sağlayacak maddi ve manevi destek verilmelidir.

Toplumumuza özellikle ekonomik, politik, askeri ve kültürel alanlarda psikolojik destek vermek de onlara karşı uygulanacak psikolojik savaşın en önemli panzehiri olacaktır.

8.5.Bilgisayar Korsan Savaşı

Bilgi alt yapısını hedef alan bir diğer saldırı biçimi de bilgisayar korsan savaşlarıdır. Bu eylemler doğrudan altyapıya yönelik değillermiş gibi görünseler de, bu altyapıya ait bir sistem üzerinden onu etkilemek ya da d irek olarak ele geçirmek suretiyle, tüm sistemi etkilemeleri bakımından, bilgi savaşlarında en önemli konulardan birini teşkil etmektedirler.

Bilgi savaşının bu türü askeri, stratejik ve politik açıdan maliyet, zaman, yer ve hatta bir noktaya kadar teknol ojiden bağımsız yürütülmesi nedeniyle oldukça caziptir. Bu savaş direk olarak insanları değil onların bilgilerini ve sahip olduklarını hedef almaktadır.

Çağımızın en temel hazinesi olan bilginin korunması da, yine karşı bakış açısına göre istihbaratın toplanması da, teknolojinin kullanımı ile sağlanmaktadır. Yani teknolojiyle bilginin korunması, ya da bilginin sağlanması bu noktada kesişmektedir.

Servis sağlayıcılar bir omurga üzerinden internet bulutuna bağlanır. İnternete yapılan kişisel bağlantıl arda, daha önce de anlattığımız gibi servis sağlayıcılar üzerinden genellikle mevcut telefon şebekesi üzerinden yapılır. İşte bu noktada da kişisel bir bilgisayarın, bu internet bulutuna diğer kullanıcılar, bankalar, devlet kurumları, ticari organizasyonla r, askeri kurumlar, istihbarat teşkilatları ile aynı biçimde internet üzerinde olduğunu söyleyebiliriz. Tüm bu kullanıcıları birbirinden ayıran kavram ise, kendilerine göre geliştirdikleri güvenlik yapılandırmalarıdır. Yetersiz güvenliğe sahip sistemler ba kımından, gelişmiş teknolojilere sahip olan kurumların istedikleri bu tarz veri bankalarına girerek istedikleri bilgileri almaları mümkün olabilmektedir.

"The Washinghton Post gazetesindeki bir değerlendirmeye göre, internet üzerinde (yani istihbarat ve gü venlik açısından açık sayılabilecek) 150 binden fazla askeri bilgisayar bulunmaktadır. 1994 yılında istihbarat kurumları (enformasyon sistemleri ajansı) ve ordu bu bilgisayarlara saldırı yapılması adına bir grubu serbest bırakmış,

bu bilgisayarların yüzde 90'ına yakınına giriş yapılmış ancak yüzde 4'ü fark edebilmiştir." (Yılmaz, 2006,sy.609)

Örneğin, kaydettikleri tüm verilerin ve yazışmaların ABD gizli servisleri tarafından öğrenildiğini fark eden Alman ordusu ve Dışişleri Bakanlığı, Microsoft yazılımlar ını kullanmayacaklarını açıkladı. Alman Der Spiegel Dergisi'nde yer alan iddiaya göre, asrın casusluğu Microsoft programlarındaki gizli ana şifreyi kullanan Amerikan Ulusal Güvenlik Ajansı (NSA) tarafından gerçekleştirildi. (Milliyet Gazetesi, 19.03.2001)

Bu nedenle Almanya'nın yanı sıra Fransa, Rusya, Finlandiya gibi ülkeler de, özellikle devlet kurumlarında açık kaynak kodlu Linux işletim sistemlerine geçmekte ve Linux'un yaygınlaşması için çaba harcamaktadırlar. (Şen, Elektronik Gözetim)

Bu çerçeveden bakıldığında bilgi güvenliğinin farklı bir tanımı daha karşımıza çıkmaktadır. Buna göre bilgi güvenliği, üretilmiş her türlü bilginin bütünlüğünün korunması, izin verilen kişiler tarafından kullanımının ve erişimlerinin sürekliğinin sağlanması, yetkisiz erişimlerin engellenmesi ve bilgilerin kesintisiz akışının sağlanması sürecidir.

Bilgi güvenliğinin temel amacı veri bütünlüğünün korunması, erişim denetimi, mahremiyet ve gizliliğin korunması ile devamlılığın sağlanmasıdır (Fatih Özavcı, Bilgi Güvenliği Temel Kavramlar, 2002)

Bilgi güvenliği olmadan kaybedebileceğimiz varlıklar veriler, sistem kaynakları ve saygınlıktır. Varlıklarımızın kaybedilmesi, kabul edilebilir bir durum değildir.(Soğukpınar, Veri ve Ağ güvenliği, sy.6)

8.5.1 Güvenlik Prensipleri

Güvenliğinin birçok boyutu olmasına karşın, gizlilik, veri bütünlüğü ve süreklilik güvenliğin olmazsa olmaz özellikleridir. Temel güvenlik prensipleri ve beraber anılan erişim denetimi kavramları ise özetle şunlardır:

Gizlilik: Gizli bilgilerin korunması ve mahremiyetinin sağlanması ya da bir verinin yalnızca yetkili kişilerce erişilebilirliğinin garanti edilmesidir. Gizlilik manyetik ortamda saklanan veriler için olabileceği gibi ağ üzerindeki verileri de kapsamaktadır. Kimlik tanıma sistemleri de bu kapsamd a değerlendirilir.

Bütünlük: Temel amaç, verinin göndericinin alıcıya ilettiği biçimde hiçbir değişikliğe uğratılmasına mahal vermeden doğru bilginin iletilmesiyle kullanıcılara en güncel bilgilerin sunulmasıdır.

Süreklilik/Güncellik: Kullanıcılar, erişim yetkileri dâhilinde verilere güncel, güvenilir ve sürekli bir biçimde erişmeleridir. Bir bilgisayar korsanı sürekliliği etkileyebileceği gibi, yazılımsal hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındak i değişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilir. (Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003,sy.8)

Erişilebilirlik (availability): Bir veriye istenildiği zaman erişilebilmesidir. (Danışman, 2007)

Kurtarılabilirlik: Herhangi bir verinin kaybolması durumunda, bu verilerin kurtarılabilir olmasıdır. Bu kendi içinde yedeklemeden tutun, veritabanı bütünlüğünün tekrar oluşturulabilmesine kadar birçok alt unsur barındırır. (Labris Teknoloji, Yazılımı Güvenliği Yaklaşımı)

İzlenebilirlik ya da Kayıt Tutma: Sistemde meydana gelen tüm olayların, faaliyetlerin kayıt altına alınarak saldırılara karşı bir tedbir olarak düzenli biçimde

kontrol edilmesidir.(Pro-G Bilişim Güvenliği ve Araştırma Ltd. Bilişim Güvenliği, 2003, syf.10)

Kimlik Sınaması (Authentication): "Kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik sınama sistemleri yaygın olarak kullanmaya başlanmıştır."(Pro-G Bilişim Güvenliği ve Araştırma Ltd. Bilişim Güvenliği, 2003, syf.11)

Bilgi güvenliğini sağlanabilmesi için korunacak bilginin niteliği çok iyi belirlenmesi, güvenlik politikalarının uygulanması bakımından çok önemlidir. Ancak unutulmaması gereken en önemli nokta, hiçbir güvenlik tedbirinin, bizi yüzde yüz güvenli kılmayacağı ve hiçbir sistemin yüzde yüz güvenli olmadığıdır.

"Carnegie Mellon Üniversitesi tarafından 2001 yılında literatüre tanıtılmış ve "güvenlik yaşam döngüsü" olarak bilinen yaklaşımın dikkate alınarak, güvenliğin; statik değil dinamik bir sürece sahip olduğu, koruma ve sağlamlaştırma ile başladığı, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gerektiği ve sistemde her zaman iyileştirme yapılması gerektiği vurgulanmaktadır."(Canbek ve Sağıroğlu, sy.11)

8.5.2 Saldırı Kavramı

"Bilgi hırsızlığı, başka bilgisayarlara sızma, hack etme işlemleri, ileri düzey programlama bilgisi olan, gelişmiş bilgisayarlara ve modem-telefon hattı gibi erişim kanallarına sahip uzmanlar tarafından, önce sızılacak bilgisayarların işletim sistemlerinde veya yazılımlarında bir açıklık veya zayıf nokta bulunarak yapılmaktadır. Saldırılar, profesyonel suçlular, genç kuşak saldırganlar, kurum

çalışanları, endüstri ya da teknoloji casusları ya da dış ülkeler tarafından gerçekleştirilebilir.

Saldırıları gerçekleştirenler için“bilgisayar korsanı” kelimesini kullanmak dilimiz açısından daha doğru olacaktır. Zira bu kavram aslında, sadece kötü amaçlı saldırganları değil iyi amaçla çalışanları da içine almaktadır. Ben de çalışmam da, iki anlamı da içine alan anlatımlarda bilgisayar korsanını, kötü amaçlı kişiler içinse saldırganı tercih edeceğim.

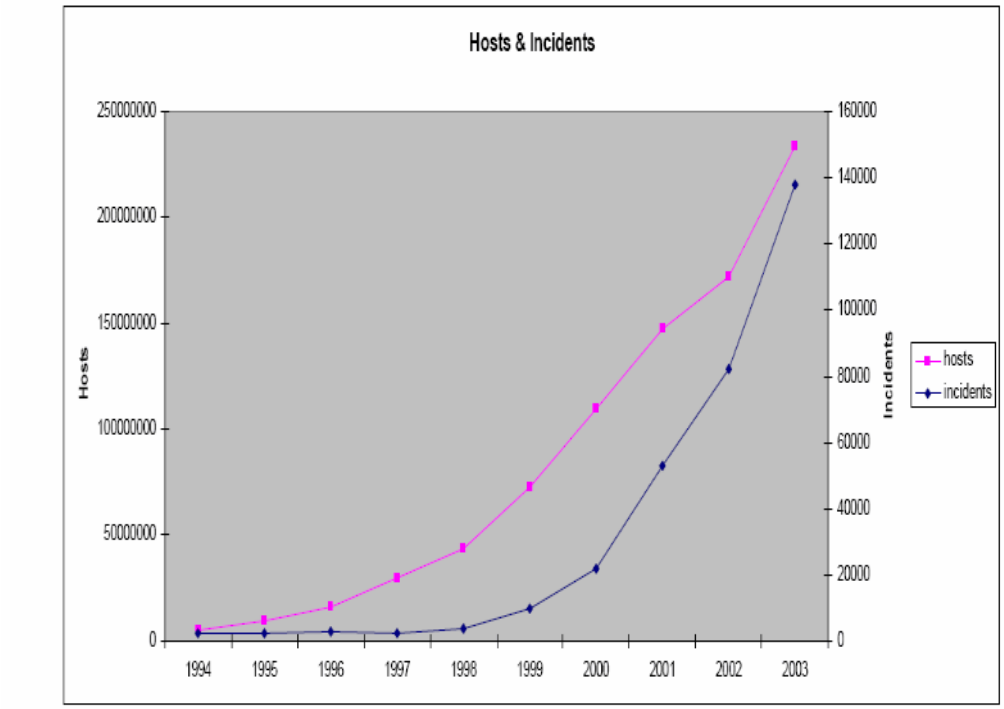
Bir bilgisayar korsanı, sızılacak bilgisayarın şifresini kendi geliştirdiği programlarla kırarak ya da bir şekilde öğrenerek, bu bilgisayarına girer. Ayrıca bilgi elde etmek isteyenler; dinleme istasyonları, telefonlara konulan çiplerden de faydalanmakta ve bu işlemler için bilgisayarların yardımına başvurmaktadırlar."(Yılmaz, 2006,sy.611)

Bilgisayar korsanları, internetin ilk yaygınlaşmaya başladığı dönemlerde saldırıları sadece idealistlik, dikkat çekme güdüsü ya da hobi amaçlı olarak yaparlarken, günümüzde çok çeşitli amaçlar için bilgisayar sistemlerine karşı farklı saldırı yolları aramakta ve denemektedirler. Artık saldırı, bir sektör haline gelmiştir ve çeşitli nedenlerle yapılmaktadır. Bu bakımdan da uygulanan saldırı yöntemleri de büyük bir hızla karmaşıklaşmakta ve hızlı bir artma eğilimi göstermektedir. 2005 yılında CERT/CC istatistiklerine göre saldırı çeşitleri 2000-2005 yılları arasında 6 kat artmıştır. (Canbek ve Sağıroğlu, 2007, sy.2)

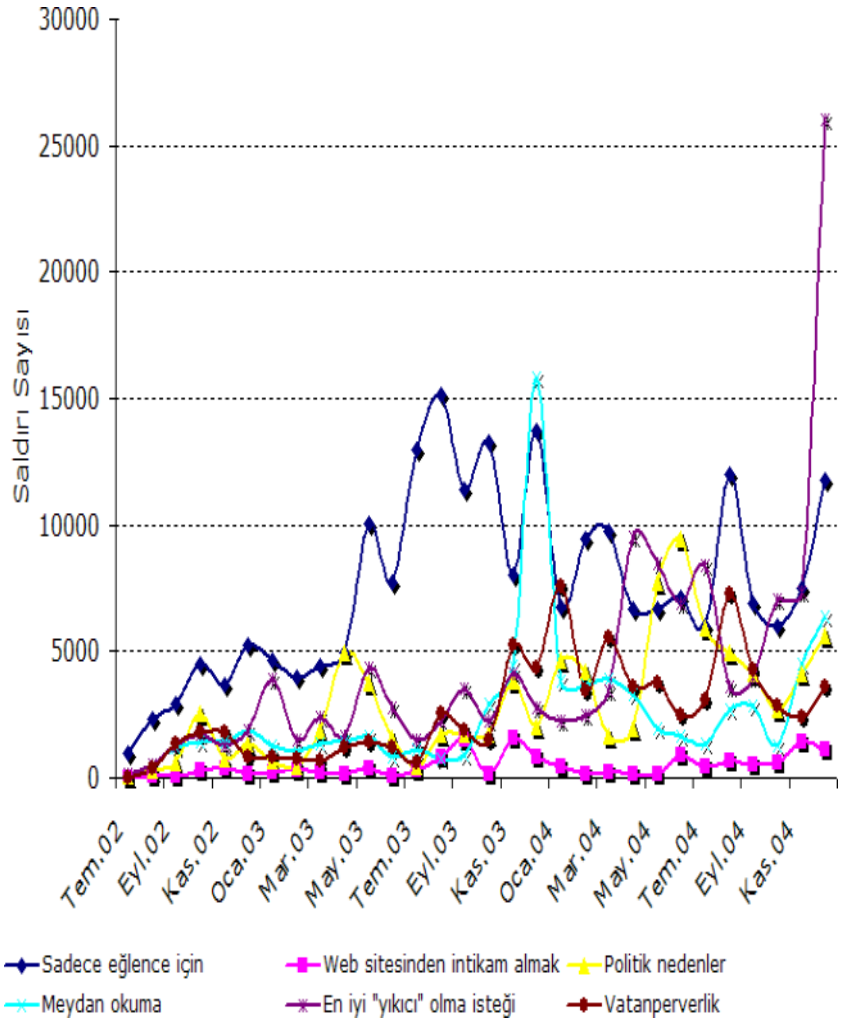
Bu bakımdan yapılan saldırılar bir güvenlik analizi açısından da çok iyi analiz edilmeli ve sistem güvenliği açısından alınacak tedbirler bir bilgisayar korsanı gözüyle sisteme dışarıdan bakış açısıyla yapılmalıdır.

Bilgi ve bilgisayar güvenliği sistemini aşma, kırma veya atlatma yöntemlerini kullanarak, zafiyete uğratma, durdurma, yavaşlatma, zayıflatma ya da tamamen bitirme, saldırı ya da atak olarak adlandırılır. (Canbek ve Sağıroğlu, 2007, sy.2)

Aşağıdaki şekilde 1995-2003 yılları arasında gerçekleştirilen saldırıların nedenleri istatiksel olarak gösterilmektedir.



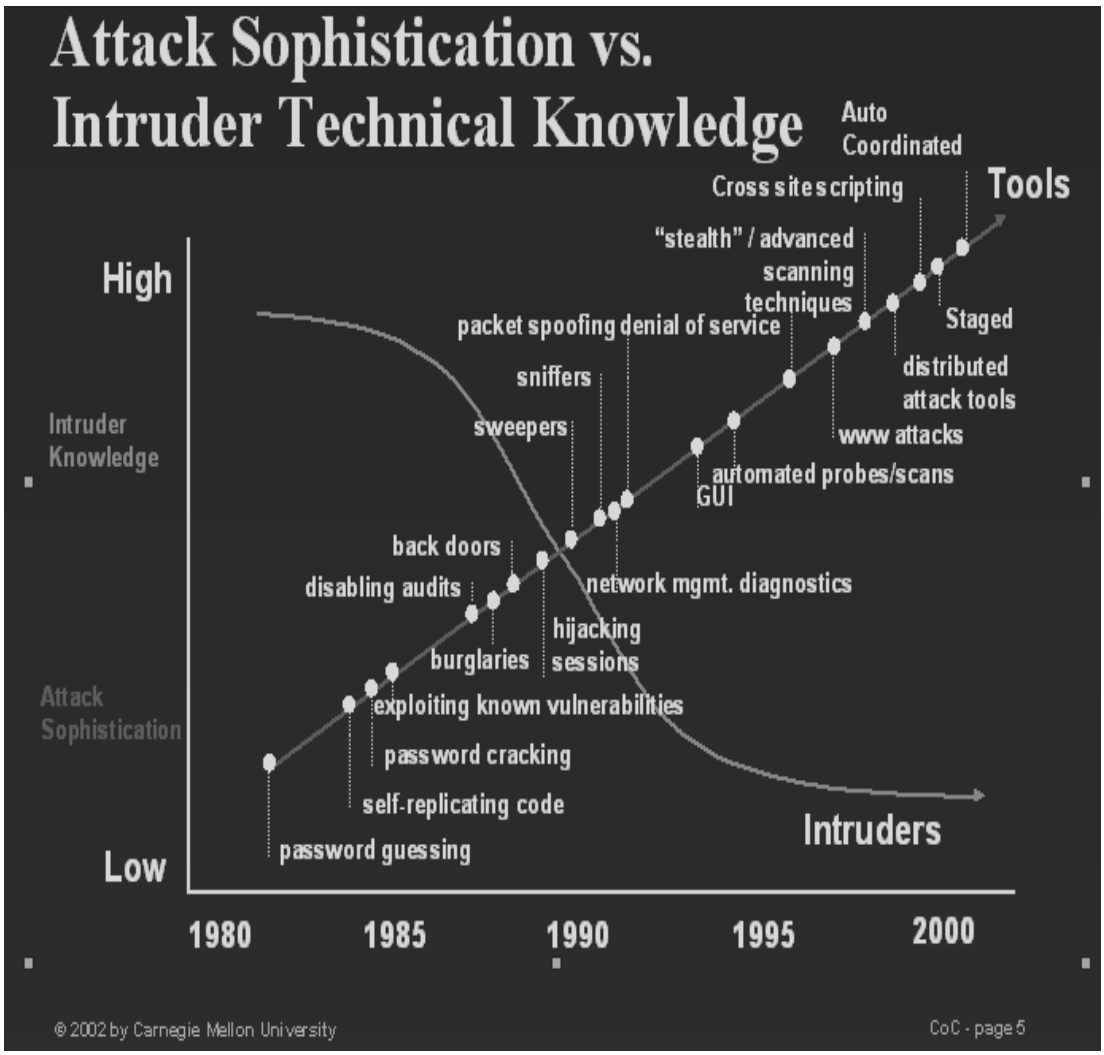
Şekil 8.9 Saldırı ve Host Sayıları İlişkisi (http://www.cert.org)



Şekil 8.10 Sistemlere Yapılan Saldırı Nedenleri (Canbek ve Sağıroğlu, 2007, sy.3)

Saldırganların saldırılarını gerçekleştirebilmeleri için sahip olmaları gereken teknik araçlar ve teknik bilgi ile bunların kullanılmasıyla yaptıkları saldırı çeşitleri de aşağıdaki biçimde ifade edilmektedir. Örneğin, 80'li yıllarda parola tahmini ile başlayan süreç, zaman ve gelişen teknolojilerinde kullanımıyla dağıtık -koordineli saldırıları mümkün hale getirmiştir. Şekilden de anlaşılacağı gibi eğlence, meydan okumak ve en yıkıcı olma isteği neden olarak saldırıların büyük bir kısmını teşkil etmektedir.

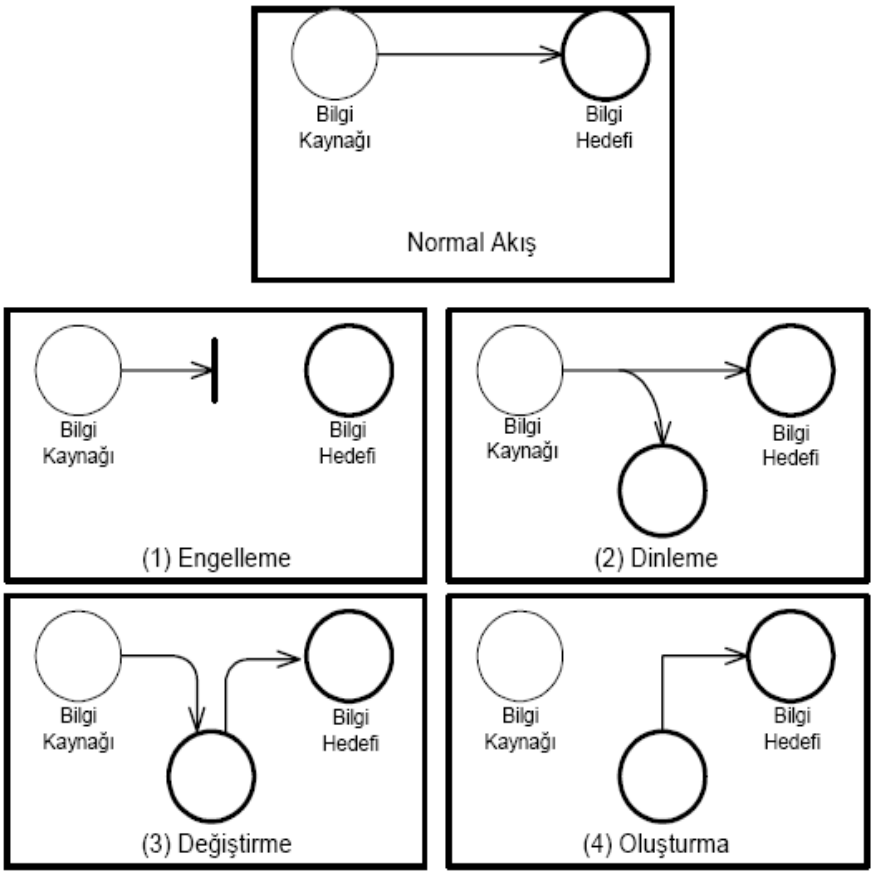
Yine dikkat edilmesi gereken bir diğer nokta ise saldırganların bilgi seviyesiyle zaman arasındaki ters ilişkidir. Yani saldırganların bilgi seviyeleri, saldırıları gerçekleştirebilmeleri bakımından düşmesine rağmen giderek yeterli hale gelmiştir. Saldırı türlerinin çeşitlenmesi ve saldırı sayılarının artması, saldırılar sonucunda oluşacak zararları artırırken, saldırıları önlemeyi de zorlaştırmaktadır.



Şekil 8.11 Saldırı Karmaşıklığı ile Teknik Bilgi İlişkisi (Shimeall, 2002)

Aşağıdaki şekilde de gösterildiği gibi bilgi akışına yapılan saldırılar şöyle özetlenebilir.

İlk şekilde; A ve B noktaları arasındaki normal akışı gösterilmektedir. 1'de; iki nokta arasındaki bilgi akışının yani erişimin engellendiği "engelleme" durumu ifade etmektedir. 2'de; iki nokta arasındaki veri akışına yapılan gizli müdahaleyle; "dinleme" ifade edilmektedir. Burada veriye gizli erişim yapıldığı kullanıcılara farkettirilmeyebilinir. 3'de; verinin yapılan müdahalelerle değiştirilerek varış noktasına iletilmesi yani "değiştirme", 4'de ise; yaratılan sanal bir bilginin, A'dan geliyormuş gibi B noktasına gönde rilmesini ifade eden "oluşturma" gösterilmektedir.



Şekil 8.12 Süreçsel Sınıflandırma (Soğukpınar, veri ve ağ güvenliği, syf.9)

8.5.3 Saldırı Mimarileri

8.5.3.1 Keşif

> Bir hırsızın ilk yapacağı iş gireceği evle ilgi bilgi toplamaktır. Onu ilgilendiren, evde bulunan değerli varlıkların eve girmesi için alınabilecek bir riske ve evin aldığı güvenlik tedbirlerinin kendini yakalatacak niteliğe sahip olup olmadığıdır. Bir evde bulunan altınlar; kameralar, şifreli kasalar özel güvenlik ekipleriyle korunuyorken elmasların bulunduğu ancak alınan tedbirler bakımından bu kadar yeterli olmayan bir eve girmek tabii ki anlamlı olacaktır. İşte iyi bir bilgisayar korsanında yapacağı ilk iş, saldıracağı sistem hakkında bilgi toplamak ve o sistemin, sahip olacakları bakımından ne denli güvenli olduğunu araştırmaktır.(D.Yılmaz, 2005, sy.128)

Aşağıda bazı keşif amaçlı kullanılan yöntemlere değinilmiştir.

Ağ Bilgi Toplama Teknikleri

"Organizasyonlar içerisindeki sistemler kadar organizasyondaki her insan da ağ üzerinde yaratacağı açıklar bakımından bir saldırı için başlangıç noktası olabilir. Bu insanların e-posta adresleri, hesap bilgileri saldırı için zemin hazırlayabilir. Bu nedenle çalışanların her türlü bilgilerinin gizliliğinin sağlanması için sınıflandırma yapılması gerekir. Arama motorları ya da e-devlet uygulamaları sayesinde bile, kişisel bilgilere erişim kolaylaşmış ve bu siteler üzerinden bilgi toplama yöntemi saldırganlar tarafından da yaygın biçimde kullanılır hale gelmiştir.

"Bilgi edinme işlemi; ağın kapsamını genel hatları ile içerdiği bilgisayar sistemlerini, bilgisayar sistemlerinin sunmuş oldukları servisleri, servis sunan bilgisayar veya aygıtların kullandıkları sürümleri, ne kadar zaman boyunca aktif olduklarını, güncelleme bilgilerini ifade eder." (Dirican, 2005, sy.416)

Saldırgan bilgi toplama teknikleri ile ağdaki arka kapıları, işletim sistemi bilgilerini ve hizmetleri öğrenerek saldırı için zemin hazırlar.

Açık Kaynak Araştırması

Sistemde kullanılan tüm yazılımlar, atlanan, unutulan, önemsenmeyen ya d a bilerek bırakılan eksiklik ya da hatalarına karşı bilgisayar korsanları tarafından sık sık kullanılırlar. Bunu, bir keşiften sonra bulan bilgisayar korsanları, bu noktalar üzerinde yoğunlaşarak sisteme zarar verebilirler. Bu bakımdan sistemde kullanılan cihazların adlarının bile gizlenmesi var olabilecek bu riskleri minimuma indirecektir.

Sistem üzerindeki cihazlarda, ilk üretildiklerindeki ayarların bırakılması, ağ donanım ayarlarının yanlış yapılması, kullanıcı hesaplarının güvenlik düzeylerinin düşük tutulması ya da şifrelerin kolay kırılabilir şifreler olması, yapılandırma zayıflıkları sınıfına; TCP/İP zafiyetleri, işletim sistemi zafiyetleri, network donanım zafiyetleri teknoloji zafiyetleri sınıfına; yazılı bir güvenlik politikasının bulunmaması, şir ket içi politik çekişmeler, hızlı personel sirkülâsyonu, donanım erişim kontrollerinin zayıflığı, güvenlik yönetim ve politikalarının takibinde aksaklıklar yaşanması, saldırıya uğranıldığının anlaşılmaması, belirlenen politikaya uygun olmayan yazılım ya da donanım kullanılması güvenlik politikası açıkları sınıfına dahil edilebilir. (D.Yılmaz, 2005, sy.129)

Yukarıda bahsedilen zayıflıklardan işletim sistemi zafiyetleri, bir bilgisayar korsanı tarafından, işletim sistemine ait bazı zayıflıkların kullanılmasıy la, sosyal mühendislik tekniklerinin uygulanmasında sağladığı kolaylıklar bakımından oldukça önemlidir.

Bir işletim sistemi; ağ trafiğini izleyerek paketlerin yakalanması ya da, bu paketlerdeki işletim sistemlerine ait karakteristik ttl, df bayrağı vb. kar akteristik değerlerin takibiyle tespit edilebileceği gibi, protokollere ya da programlara göre yapılan taramalar sonucunda elde edilen verilerin incelenmesiyle de öğrenilebilir.

Arama Motorları ile Diğer Bilgi Kaynakları

Bir web sitesinden saldırganın hede fine ait irtibat adresleri ve telefon numaralarına, iş ortaklarına, hedefin kullandığı teknik donanım bilgisine, yani ip adres bilgilerine, dns adreslerine, sistem mimarisine, hedefle ilgili son haberlere, ulaşması oldukça kolaydır.(D.Yılmaz, 2005, sy.129)

Örneğin internet üzerinde "type=hidden name=password" ile yaptığım basit bir kaynak kod araştırmasında bile 1000 civarında şifre ve kullanıcı adını veren siteye rastladım.

Bu sınıflandırma da belirtmem gereken bir diğer yöntemde DNS kayıtlarının kullanılmasıdır. "DNS sayesinde alan adına ait İp aralığı; bu adres aralığı içerisinde yer alan kayıtlar, posta sunucuları, yetkili isimler hakkında bilgi sahibi olunabilir. İp adres değerleri kullanılarak ters yönde sorgular yapılabilir. Ağ içerisinde bulunan sunucular, yönlendiriciler, anahtar ve diğer ağ aygıtları hakkında bilgi sahibi olunabilir.

Saldırı için hedef hakkında bilgi sahibi olmak isteyen kişilerin ilk yöneldikleri adresler DNS sunucularıdır. DNS sunucularının sorgulanması ile birlikte alan adı ve ağ ile ilgili çok önemli bilgiler elde edilir." (Dirican, 2005, sy.422)

nslookup komutuyla DNS Sorgulama yapılırken kullanılan dig uygulaması ile DNS problemlerinin belirlenmesi, ip-adres arasında ters dönüşüm sorgulamalarının yapılması ile ağ üzerinde çalışan sunucuların ne olduğu hakkında bilgi toplanabilir. (Dirican, 2005, sy.424)

Whois Veritabanı

“WHOIS, internet kullanıcılarına bir directory servisi sunar. Bu servis, e-mail adresleri, posta adresleri, telefon numaraları, organizasyonların adresleri vb ile ilgili bilgilere ulaşmanın yollarından biridir. WHOIS servisi bu isi bir ana veri tabanını tarayarak yapar. Bu veri tabanı (database) Network Information Center (NIC)'da bulunur. WHOIS'in kullanımı;

whois [-h servis-adi] tanımlamalar

Burada servis adı sorgulamak istediğimiz veri tabanının bulunduğu servisin adresidir. Eğer verilmezse, varsayılan (default) adres kabul edilir. Aşağıdakiler geçerli whois sorgularıdır:

whois dec.com

whois itu.edu.tr

whois -h ns.nic.ddn.mil knuth

whois -h whois.internic.net jones" (http://www.bid.ankara.edu.tr)

İP Veritabanı

İp adreslerine ulaşma noktasında çok sıkıntı çekmeyecek iyi bir bilgisayar korsanının bundan sonraki hedefi, kaynak veritabanlarının bulunduğu adreslerdir. Çünkü saldırgan hedefine ait tüm ip adres bloğunu bilmelidir. Nedeniyse tabii ki, daha geniş alana yayılan ip bloklarının açık verme ihtimallerini kullanma eğilimidir. ARIN, RIPE, APNİC ya da LACNİC ip veritabanları kullanılarak hedefin sahip olduğu ağ bloklarını tespit etmek mümkündür. (D.Yılmaz, 2005, sy.141)

Topoloji Araştırması

Bir bilgisayar korsanı, daha önce anlatılan traceroute komutu ya da bazı grafik arayüzüne sahip programları kullanarak hedefine ait bir topoloji araştırması yapabilir.

8.5.3.2 Tarama Yapmak

Keşif konusundaki verilen örnekteki hırsız, hatırlanacağı gibi önce gireceği evi seçmişti. Bundan sonraki adım da ise hırsız, gireceği evin içine en kolay hangi

yoldan girebileceğini tespit etmek isteyecektir. Kapılara, pencerelere ya da açık unutulan bir girişe bakarak güvenlik açıklarını değerlendirmeye çalışır. Burada bizi ilgilendiren girişler de tabii ki portlar ve ip adresleridir. Keşif yapılarak elde edilen bilgileri kullanan saldırgan, hedef sistemi tarayarak açık olan portları, çalışan servislerin ne olduğunu, hangi uygulamaların çalıştığını, işletim sisteminin ne olduğunu ve bunlarla ilgili açıkları rahatlıkla bulabilmektedir. (D. Yılmaz, 2005, sy.156)

Bilgisayar korsanları hedefleri üzerinde tarama yapabilmek için tarayıcı olarak adlandırılan bazı programlar kullanmaktadırlar. Tarayıcı programlar vasıtasıyla, ağın kuvvetli ve zayıf yönlerini rahatlıkla tespit edebilmektedir. En basit tarama, daha önce değindiğimiz ping uygulamaları vasıtasıyla yapılır. Bilgisayar korsanları ayrıca, ping haricindeki diğer icmp sorgulamalarını ve bazı zaafiyet tarama programlarını da kullanmaktadır. Bu programlar sistem yöneticileri açısından da açıkların tespiti bakımından da oldukça kullanışlıdır.

Hedef sistem üzerindeki ip adresleri, dns adresleri artık biliniyor ve ku llanılan icmp sorgulamalarıyla da sistemin canlı olduğu anlaşılmışsa, bundan sonra yapılan port tarama işlemi ile de portların değerlendirilmesi yapılır. Yani, port tarama işlemi, bilgisayar korsanı tarafından uygulanacak bir sonraki adımdır. Tarama için k ullanılan protokollere göre farklı teknikler ve programlar kullanılmaktadır. (D. Yılmaz, 2005, sy.163)

8.5.3.3 Sisteme Sızmak

Sistemi keşfeden, daha sonra tarayan bilgisayar korsanı, bundan sonra sisteme sızmak için yollar arayacaktır. Kullanılan yöntemlere daha sonraki konularda ayrıntılı olarak değinilecektir.

8.5.3.4 Kalıcılığı Sağlamak

Sisteme sızan bilgisayar korsanları, aynı sisteme daha sonra yeniden girmek istediklerinde, geçtikleri zorlu yollardan bir daha geçmemek için arka kapıları ve trojanları kullanırlar. (D.Yılmaz,2005, syf.380)

8.5.4 Saldırı Türleri

Başlıca saldırı türleri arasında, açık kaynak kod saldırıları, gizli dinleme (eavesdropping), hizmet aksattırma saldırıları (DoS), dolaylı saldırılar, arka kapılar (backdoor), doğrudan erişim saldırıları, sosyal mühendislik ve kriptografik saldırıları saymak mümkündür. Bunlardan başka saldırı türleri arasında, iletişim protokollerini kullanan saldırılar, ip saldırıları, işletim sistemine yönelik saldırılar ve uygulama katmanına yönelik saldırılar sayılabilir. Bunlar arasından en çok yapılan saldırılara, ileride değinilecektir.

8.5.5 CERT Gruplandırması

Tablo 8.1 CERT Saldırı Gruplandırması(Soğukpınar, veri ve ağ güvenliği, syf.10)

Probe,Scan,Scam	Bir sistemdeki açık ve kullanılan portların taranmasıyla, bu portlardaki hizmetlere yönelik yapılan saldırılardır.
Prank	Kullanıcı hesaplarının yanlış ayarlanmasından doğan açıklara yönelik yapılan saldırılardır.
E-mail Spoofing	Başka bir kullanıcının adresini sanki o kişiymiş gibi kullanarak gönderilen sahte e-posta saldırılarıdır.
E-mail bombard	Bir posta adresine genellikle farklı posta adreslerinden çok fazla sayıda posta gönderilmesidir.
Send mail Attack	SMTP portuna yönelik saldırılardır.
Break in	Verilen hizmetlerin devere dışı bırakılmasına yönelik saldırılardır.
İntruder gained root Access	Sisteme normal kullanıcı olarak girerek sistemden süper kullanıcı olarak çıkması..
İntruder İnstalled Trojan Horse Program	Bilgisayar korsanı'ın sistemde kalıcılığı sağlamak için yaptığı saldırılardır
İntruder İnstalled Packed Sniffer	Sisteme giren ve çıkan paketlerinin sniffer vasıtasıyla toplanması
NIS Attack	Ağ kullanıcı yönetim sistemine yönelik saldırılardır.
NFS Attack	Genellikle ağ erişimini devre dışı bırakmaya yönelik yapılan, Ağ dosya yapısına yönelik yapılan saldırılardır.
Telnet Attack	Uzaktan erişim protokollerinin açıklarından yararlanarak yapılan saldırı türüdür.

RLogin and RSH attack	Uzaktan erişim servislerinin açılarına yönelik yapılan saldırılardır
Cracked Password	Genel olarak kolay tahmin edilebilir şifrelerin tahmin yoluyla kırılmaya çalışılması
Anoymous FTP abuse	Anonim erişim izni verilen dosya aktarım sunucularına yapılan saldırılardır.
İp spoofing	İp adres yanıltmasıyla yapılan saldırılardır.
Configuration error	Konfigürasyon hatalarından ve eksikliklerden yararlanma.
Missuse of host resources	Konak kaynaklarının yanlış kullanımı ile ortaya çıkan açıklıklardan yararlanma.
Worn, Virus	Solucan ve virüslerin kullanıyla yapılan saldırılardır.

Yukarıda bahsedilen sınıflandırma CERT (Computer EmergencyResponse Team)'e aittir. Ancak burada bir sınıflandırmaya tabi olan saldırıların pek çoğu, diğer saldırı sınıflandırmalarına da dahil edilebilmektedir

8.5.4.2 Genel Saldırı Yöntemleri

Çöpleri Karıştırma

Bu yöntem, değerli olabilecek her türlü bilginin ele geçirilmesi bakımından bilgisayar korsanlarınca hedeflerine ulaşma noktasında başarıyla kullanılan bir tekniktir.

"Paylaşılan çöpler ile ilgili potansiyel güvenlik zayıflıkları olarak; şirket telefon rehberleri, organizasyon şekilleri, kısa notlar, şirketin siyaset tarzı, toplantı

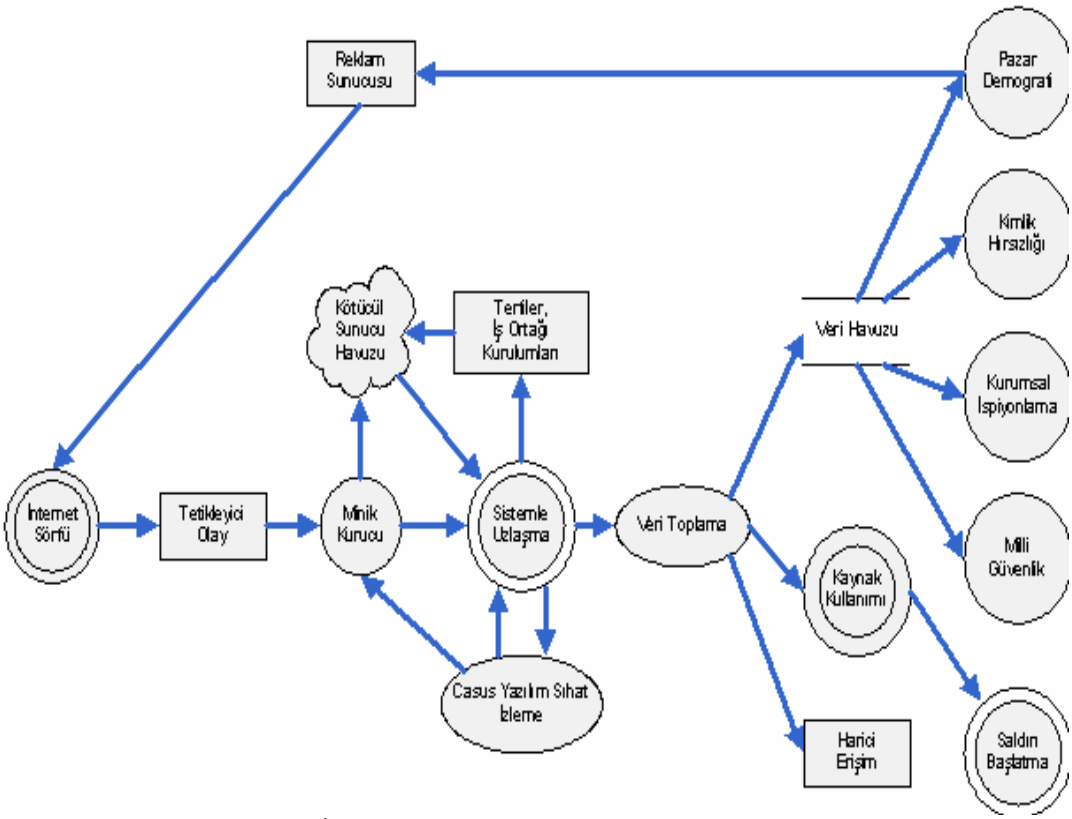
zamanları, sosyal olay ve tatiller, elle yapılan sistemler, bağlantı isim ve parolalarını içeren hassas yazıcı çıktıları, diskler ve kayıt üniteleri, şirket mektup başlıkları ve kısa not formları, zamanı geçmiş donanımlar belirlenmiştir." (Şeker, Amerikan Örneklemi Işığında Kamu Alanında Bilginin İnternet İle Sunumu ve Önündeki Tehlikeler, 2002)

Kaynak Kod İstismarı (Code Exploit)

“Sistemde kullanılan (işletim sistemi için hazırlanan sistem prog ramları dâhil) tüm yazılımlarda var olabilecek arabellek taşması (buffer overflow), CGI betikleme (scripting) hataları ve şifreleme hataları gibi yazılım kusurları, bir bilgisayar sisteminin kontrolünün ele geçirilmesine veyahut o bilgisayarın beklenmedik bir şekilde çalışmasına neden olabilir. Bu, son yıllara kadar gözden kaçırılan bir konu olarak, birçok saldırıya açık kapı bırakmış bir korunmasızlıktır.” (Canbek, 2005, sy.21)

Aşağıdaki şekilde, internet üzerinde bize göre aslında güvenli görülen bir web sayfasında gezinirken, bu web sayfasında yer alan kötü betik kodların, kullanıcının tarayıcısında saptadığı uygun bir güvenlik zaafiyetinden yararlanarak, kullanıcının haberi dahi olmadan, sistem üzerinde bilgi toplama amaçlı kurucu bir programı çalıştırması ve sonuçları özetlenmektedir. Bu yöntem ile kaybedilebilecek bilgiler, her türlü amaçlar için, hatta ve hatta milli güvenlik bakımından risk teşkil edebilecek nitelikte dahi olabilmektedir. Ya da bu bilgiler başka sistemlere saldırı amaçlı da kullanılabilmektedir.

Burada, sistemde çalışmakta olan bu yazılım sürekli olarak sistemi takip ederek, onu silme girişimleri durdurulmaya çalışır. Yazılım bir şekilde durdurulduğunda ise saldırgan tarafından yapılacak iş; onu tekrar ayağa kaldırmayı denemek olacaktı r. Bir bilgisayar korsanı, kendi casus yazılımını çeşitli tekniklerle yeniden ayağa kaldırabilir.(Canbek ve Sağıroğlu, 2007, sy.7-8)



Şekil 8.13 Kaynak Kod İstismarı Yaşam Döngüsü (Canbek ve Sağıroğlu, 2007, sy.7)

Gizli Dinleme

İki nokta arasında iletilen verinin, üçüncü kişiler tarafından araya girilerek elde edilmesidir. Bu yöntemde, verinin iletimine devam ettirilmesinden dolayı her iki nokta açısından da fark edilmeme ihtimali kuvvetlidir.

"Whacking" olarak bilinen yöntem de bu konu bakımından örnek teşkil etmektedir. Whacking; "temel olarak kuvvetli darbe kablosuz sistem kırma (hacking) dır. Kablosuz ağı (network) gizli dinleyen sistemlerin hepsi doğru bir radyo kanalını bulmayı ve kablosuz iletimin içinde bulunabilmeyi gerektirir. Gerekli donanım ile ofis binalarının dışından sinyallerin toplanabilmesi mümkündür. Bir defa yüklenen bir kablosuz şebeke sistemi ile davetsiz misafir genelde şifrelenmemiş (kriptolanmamış) olarak ağdan (network) gönderilen bilgiyi toplarlar.

Ortak bilgide (corporate espionage) telefon düşmesi başka bir yol olarak kullanılmaktadır. Dijital kayıt yapan alet ile faks cihazının iletim ve kabulünü izleyen bir sistemi oluşturmak,

faks cihazına bir bilgi gelmeden önce kimsenin bilgisi olmadan bir kopyasının alınması, telefon ile görüşmede bir kişinin sesleri toplanarak, banka hesabına erişmesi mümkündür." (Şeker, Amerikan Örneklemi Işığında Kamu Alanında Bilginin İnternet İle Sunumu Ve Önündeki Tehlikeler, 2002)

Bu konu içerisinde değinilmesi gereken bir diğer konuda "sniffing "'dir. Sniffing temel olarak bir ağ üzerinde gidip gelen paketlerin dinlenmesi işidir. Bu suretle ağ ve bilgisayarla ilgili temel bilgilere ulaşılması amaçlanır.

Doğrudan Erişim Saldırıları

Sistemlere fiziksel erişim sağlayan bir sistem yöneticisi, kendisi için ileride kullanabilecek bazı değişiklikler yaparak ya da hesaplar yaratarak, kurduğu sistemler üzerinden ileride kullanılmak üzere, uzaktan erişim yöntemleri deneyebilir. Hatta ağda bulunan mevcut bilgileri kendi isteği doğrultusunda kullanabilir ya d a yedekleyebilir. Bu bakımdan, bir sistemin yönetimi üçüncü şahıslara asla verilmemelidir. Sistem yönetiminin herhangi bir nedenden dolayı el değiştirmesi durumunda da gerekli güvenlik mekanizmaları çalıştırılmalıdır. (Canbek ve Sağıroğlu, 2007, sy.8)

Sosyal Mühendislik Yöntemleri

Bilgisayar sistemlerinde karşılaşılan güvenlik ile ilgili birçok olay, insan faktöründen kaynaklanmaktadır. İnsan faktöründen kaynaklanan bu zafiyet, insanların bilerek veya bilmeyerek yaptıkları nedenlerden kaynaklanabilir.

"Bilgisayar güvenliği terimleriyle Sosyal Mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri açıklıklar olarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir." (Bican, sy. 4)

"Bilgisayar güvenliğinde sosyal mühendislik, bir bilgisayar korsanının, ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve

sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel addır. Sosyal mühendislik de kullanılan taktikler, hedefe ulaşmak amacıyla değişik biçimlerde sürekli denenir. Özellikle telefon ile kullanıcı ve şifre bilgilerini elde etme, buna en tipik örnektir."(Canbek ve Sağıroğlu, 2007, sy.9)

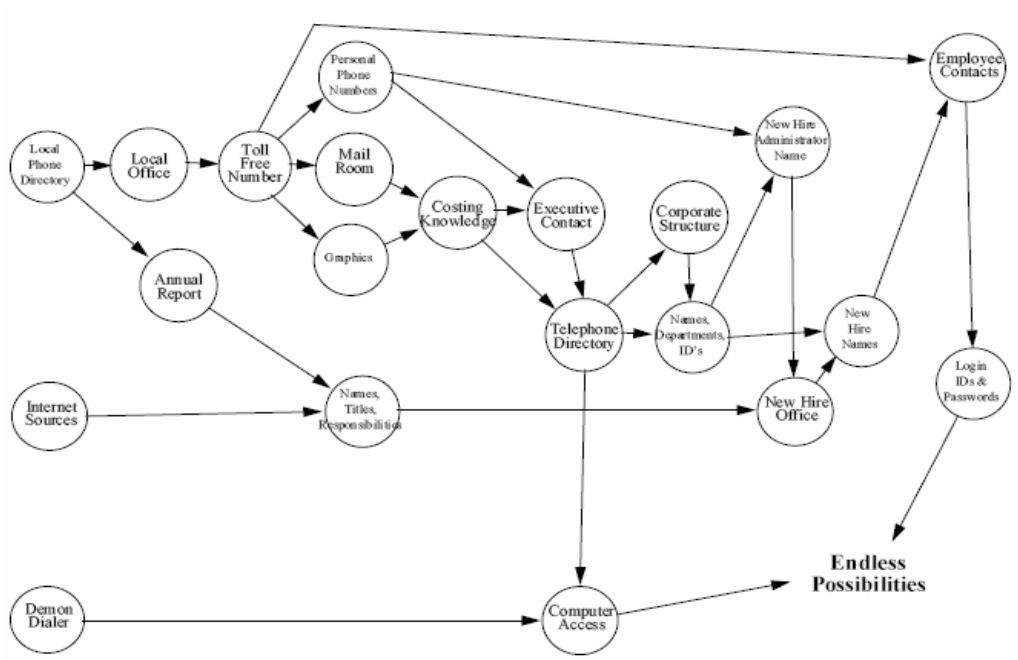
Sosyal mühendislik saldırıları, ağın işleyişine ya da direk bilgiye dönük yapılan saldırılardır. Sosyal mühendislikten elde edilen bilgiler diğer ağa saldırmak için kullanılabilirken, ağa yapılacak saldırılar bakımından keşif niteliği de taşıyabilmektedir.

Sosyal mühendislerin kullandıkları en önemli yöntem, karşılarındaki kişileri kendi amacına ulaşmasını sağlayacak herhangi birşeye inandırmaktır. Bu işi bazen öyle iyi yaparlar ki, karşıdaki kişiyi bir karar verme noktasında zorlayarak istediği bilgiyi elde ederler.

Bilgisayar korsanları, kullanılan tüm teknolojik sistemleri, alınan tüm güvenlik önlemlerini, belki de bazı noktalarda insanoğlunun en zayıf yönü olan duygularını kullanarak aşarlar. Daha önce de bahsettiğimiz gibi güvenlik en zayıf halkanın gücü kadardır.

Bu noktada telefon, bilgisayar korsanlarının kullandıkları en önemli cihazdır. Bundan başka bilgisayar korsanılar çalışanları izleme suretiyle bazı bilgilere ve şifrelere erişim sağlayabilirler. Örneğin bilgisayarınıza herkesin rahatlıkla görebi leceği bir konumda şifrenin girilmesiyle, bunun görülmesi suretiyle çok önemli erişim şifreleri saldırganlarca öğrenilmiş olabilir.

Ayrıca hassas bilgilerin çalınması ya da önemli sistemlerin bulunduğu yerlere saldırganın girerek müdahale etmesi olasılığın a karşı, fiziksel güvenli tedbirleri çok sıkı bir biçimde denetlenmelidir.



Şekil 8.14 Sosyal Mühendislik Saldırı Anatomisi (Winkler and Dealy, 1995, Sy.4)

Kriptografik Saldırılar

Şifrelenmiş bilgilerin şifresini kırmak veya çözmek amacıyla yapılan bu sal dırılar, kriptoanaliz yöntemleri kullanılarak gerçekleştirilmektedir. "Bunlar arasında kaba kuvvet saldırısı (brute force attack), sözlük saldırısı (dictionary attack), ortadaki adam saldırısı (man in the middle attack), sadece şifreli metin (chipertext on ly), bilinen düz metin (known plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext), uyarlanır seçili düz metin (adaptive chosen plaintext) ve ilişkili anahtar (related key attack) saldırılarını saymak mümkündür (Canbek, Sağıroğlu , 2007, syf.9)

Hizmet Aksattırma Saldırıları (DoS, Denial of Service)

Bu saldırılarda temel amaç; bir bilgisayar, sunucu veya ağın kaldırabileceğinden fazla yük bindirilmesiyle kullanılamaz hale getirilmesidir. Bu tip saldırılar genelde sistemin bant genişliğini ve kaynaklarını tüketmek, yapılandırma bilgilerini ya da fiziksel ağ bileşenlerini bozmak şeklinde yapılmaktadır. Bu saldırılar tek bir

kaynaktan olabileceği gibi, bazen ip yanıltma teknikleriyle bazen de birden fazla bilgisayarın saldırgan tarafından ele geçirilmesiyle çok sayıda bilgisayar tarafından gerçekleştirilebilmektedir.

Bu saldırılarda genel olarak üretim kolaylığı bakımından en çok ICMP ECHO paketleri kullanır. Fakat teorik açıdan her türlü paket bu saldırılar için kullanılabilmektedir. (Berkay, Hack Teknikleri, sy.14)

Bu saldırılarda hedefler genellikle küçük bant genişliğine sahip olan, ya da ağa herhangi bir servis sunan sistemlerdir. Bu bakımdan akıllı tasarlanmış bir band genişliği yönetimi, güvenlik duvarlarının kullanımı ve sistem üzerinde kullanılan uygulamaların yazılımlarının güncellenmesi, alınabilecek tedbirlerden bazılardır.

DoS saldırıları aşağıdaki gibi sınıflandırılabilir:

Smurfing

Bu saldırılarda saldırgan, yarattığı ping paketler kaynak ip kısmına saldırmak istediği bilgisayarın ip adresini yazarak bunu bir yayın adresine gönderir. Bunun sonucunda, ağ üzerindeki bilgisayarların bu istek paketine cevap vermesiyle, sistemin bant genişliği tamamen tüketilir, dolayısıyla herhangi bir isteğe karşı cevap veremez hale gelir. (Canbek, 2005, sy.51-52)

Syn/Rst Seli (SYN/RST Flooding)

Bu saldırılarda TCP mesajlaşmasındaki temel ilke olan el sıkışması kullanılır. Örneğin bil bilgisayar karşı bilgisayara bağlanma isteği gönderdiğinde, bu bilgisayardan da ona yanıt gelir. Ancak bağlantı talebinde bulunulan bilgisayar, bağlantıyı başlatacak bilgisayardan da bu yanıta cevap vermesini bekler ve bir süre bağlantıyı açık tutar. Burada bu durum ardı ardına olduğunda bir süre sonra bu isteklerin sıraya konduğu kuyrukta dolma olur ve bu bilgisayar üzerinde, gelen isteklere cevap verememe durumu ortaya çıkar. (Berkay, Hack Teknikleri, sy.17-18)

Yazılımsal Saldırılar

Mantıksal bombalar, arka kapılar, solucanlar ve virüsler bu sınıfta incelenir.

- **Mantıksal Bomba (Logical Bomb) Saldırıları:** Mantıksal bombalar çeşitli etkilere sahip, zarar verme amaçlı yazılmış program parçalarıdır. Örneğin bir kullanıcı işten kovulduğunda, bu programın çalıştırarak programın sistem kaynaklarına (bellek, hard disk, CPU, vb.) büyük zararlar vermesine neden olabilir. Bu program parçacıkları, sistemdeki dosyaların yıkımını sağlayabilirler. Mantıksal bombalar, üzerinde yazıldıkları bilgisayarın yanı sıra, internet üzerinden de gönderilerek ağa bağlı sistemlerin güvenliğini de tehdit ederler. (Türkiye Bilişim Derneği, 2006)

- **Solucan (Worm):** Kendisini dosyalara eklemek yerine, bulaşmak için ağ bağlantıları üzerinden sistem açıklarını kullanan ve büyük bir hızla yayılabilen virüs çeşididir. (Daşkıran, 2005, syf.5]

- **Truva atları (Trojans):** Çoğalma ya da yayılma eğilimlerinin olmamaları yönüyle virüslerden ayrılan Truva atı, görünüşte zararsız bir programın içine gizlenmiş bir program (backdoor) veya kendi başına uzaktan kontrole veya programın özelliklerinin çalışmasına imkân tanıyacak özel bir sunucu kodu olan programlardır. Bugün internet literatüründe trojan programı denildiğinde hemen netbus, boo, subseven ve benzeri belli başlı programlar akla gelir. (http://www.zonguldak.pol.tr)

8.5.5 Virüsler

Bilişim sektöründe çalışan yöneticilerden, interneti sohbet ya da eğlence amaçlı kullananlara kadar, internet dendiğinde ilk akla gelecek kavramlardan birisi muhakkak virüslerdir. Genel olarak virüsün tanımı istendiğinde de büyük bir

çoğunluk virüsü; bilgisayarlara zarar veren, sistemlerini yavaşlatan hatta tamamıyla durdurabilen programcıklar olarak tanımlayacaklardır. Biraz daha dikkatli kullanıcıların bu tanıma ekleyecekleri ise virüslerin yayılma eğiliminde olduklarıdır. Eskiden sadece disketlerle bulaşan virüsler, kullanılan yöntemler ve gelişen teknoloji ile artık protokolleri de kullanarak bilgisayarlarımıza girmeye çalışmaktadırlar.

Virüsler hakkında anlatılanlara ilave olarak, tabii ki söylenecek çok söz var. Örneğin virüsler kendilerini bir dosyaya farkedilmeden ekleyebilirler ve sisteme zarar verirler. Bu zararlar beklemediğimiz anlarda anlık olarak bilgisayarımızın kilitlenmesi olabileceği gibi, tüm bilgilerimizi kaybedebileceğimiz sonuçlar da doğurabilmektedir. Virüslerin etkilerini genel olarak şöyle özetleyebiliriz:

- Gereksiz mesajlar görüntüleyebilir (W97M/Jerk)
- İşletim sistemi zarar görebilir
- Diskte kayıtlı bilgiler silinebilir (Navidad)
- Diskteki bilgiye erişim engellenebilir
- Flash – BIOS silinebilir (CIH)
- Kontrol dışı e-posta gönderebilir (Sircam)
- Gereksiz ağ trafiği yaratabilir (Nimda) (Çalışır, 2002)

8.5.5.1 Tarihsel Süreç

1983:İlk bilgisayar virüsü. Deneysel amaçlı ve bir doktora tezinin parçası olarak yayımlandı.

1986:Bilinen ilk kötü amaçlı bilgisayar virüsü olan “Brain” yazıldı. Bu virüs sadece disket üzerinde etkili olup sabit diskteki dosyalara bulaşmıyordu.

1987:Dosyalara bulaşabilen ilk virüs olan “Lenigh” ortaya çıktı.

1988:İlk bilgisayar solucanı “Tanenbaum”. IBM bilgisayarlarında yayılmaya başladı.

1989:“Washburn” isimli ilk polimorfik virüs ortaya çıktı.

1990:Peter Norton, Symantec firması bünyesinde “Norton A ntivirüs” yazılımını geliştirdi ve dünyanın en zenginleri listesine girdi.

1991:Virüs programlama yarışmaları düzenlenmeye başlandı.

1992:İlk virüs paniği “Michaelangelo” ile birlikte başladı.

1994:E-posta iletileriyle yayılan ilk virüs olan “Good Times” o rtaya çıktı.

1995:Word dosyalarına bulaşan ilk makro virüsü “Baza” yazıldı.

1997:İlk Linux virüsü yazıldı.

1998:Bilgisayar donanımına zarar veren ilk virüs “Chernobil (CIH)” yayılmaya başladı.

1999:E-posta programlarını kullanarak kendi kendini gönderen i lk bilgisayar solucanı “Melisa” ortaya çıktı

2000:“I LoveYou” virüsü bütün dünyada çok büyük zararlara (20 Milyar Euro kadar) yol açtı.

2001:Bilgisayardaki adres defterlerindeki bütün adreslere kendisini gönderen ilk virüs “Nimda” Internet'te yayıldı.

2003:Bilgisayarın sürekli olarak kendi kendine kapanıp açılmasına yol açan “Blaster” solucanı yayılmaya başladı.

2005:Bir Türk programcının yazdığı “Zotob” virüsü hızla yayılarak milyarlarca dolar zarara neden oldu. (http://blog.milliyet.com.tr)

8.5.5.2 Virüs Türleri

Dosya Virüsleri: COM, EXE, DRV, DLL, BIN, OVL, SYS uzantılı dosyalara bulaşarak, her çalıştırıldıklarında belleğe yerleşip kendilerini aynı uzantılı başka dosyalara kopyalayan aslında programların kendilerine denilen virüslerdir. Bunlar bu uzantılı dosyaları etkileyen ve genellikle ve o dosyanın çalıştığı anda harekete geçen virüslerdir. (Daşkıran, 2005, syf.5)

Açılış (Boot) Virüsleri: Bulaştıkları DOS formatlı disketlerin açılış sektöründen kullanıldıklarında o bilgisayara ve daha sonrada bilgis ayara takılan tüm disketlerin açılış sektörüne bulaşan virüslerdir. Bu virüsler, “bilgisayar açılırken disketten boot etmeye çalışlar ve böylece disketten sisteme girerler.

Bu tip virüsleri önlemek için; bilgisayarı açarken sürücüde bir disket olmadığında n emin olmak gerekir. Çünkü bu virüsler, fabrika etiketli orijinal yazılımlarda bile bulunabilir." (Daşkıran, 2005, syf.4)

Makro Virüsleri:”Bazı programların, uygulama ile birlikte kullanılan "kendi yardımcı programlama dilleri" vardır. Söz gelimi, popüler bir kelime işlemci olan "MS Word", "Makro" adı verilen yardımcı paketlerle yazı yazma sırasında bazı işleri otomatik ve daha kolay yapmanızı sağlayabilir. Programların bu özelliğini kullanarak yazılan virüslere "makro virüsleri" adı verilir. Bu virüsler, sadece hangi makro dili ile yazılmışlarsa o dosyaları bozabilirler. Bunun en popüler ve tehlikeli örneği "Microsoft Word" ve "Excel" makro virüsleri. Bunlar, ilgili uygulamanın makro dili ile yazılmış bir şekilde, bir Word ya da Excel kullanarak hazırladığ ınız dökümana yerleşir ve bu dökümana her girişinizde aktif hale geçer. Makro virüsleri, ilgili programların kullandığı bazı tanımlama dosyalarına da bulaşmaya (normal.dot gibi) çalışır. Böylece o programla oluşturulan her döküman virüslenmiş olur. Microso ft Office (Word, Excel vb) makro virüsleri ile baş etmek ve korunmak için,

http://www.microsoft.com/msoffice adresinde gerekli bilgiler bulunabilir.” (www.bim.gazi.edu.tr)

Polimorfik Virüsler: “Polimorfik” adı verilen özel tip virüsler kendilerini sistemde boyut değiştirerek ya da yeni virüsler türeterek gizleme özelliğine sahiptirler.(Yeniçeri, 2004, sy.5)

Stealth (Casus) Virüs: Kendilerini gizleme yeteneklerinin olan virüslerdir.

Kılavuz Virüsler: Örneğin sıkça kullanıldığımız paint uygulamasının ismiyle , kendi ismini değiştirerek, bizim yanlışlıkla bu programı çalıştırmak istediğimizde önce kendi kodunu, hemen ardındanda gerçek paint programını çalıştırmak suretiyle, kendini gizleme yoluna giden virüslerdir. (Daşkıran, 2005, syf.4)

Taşıyıcı: Saldırılacak sisteme bu zararlı yazılımları taşıyan dosyalardır.

8.5.5.3 Virüslere Karşı Alınacak Tedbirler

Sistemimizde virüs olup olmadığı noktasında hiçbir zaman kesin bir kanaate varamayız. Ancak alabileceğimiz bazı tedbirler, bizim açımızdan yine de koruyucu olacaktır.

Virüslere karşı alınabilecek en önemli tedbir; sürekli arka planda çalışan ve güncellemeleri sürekli yapılan bir antivirüs programı kullanmaktır. Ayrıca tanımadığımız e-postaların açılmaması, dosya indirmelerinin ancak güvenli sitelerden yapılması, zararlı scriptlerin açılmaması ya da bilgilerimizin her ihtimale karşı sürekli yedeklerinin bulunması bizim virüslerden gelen saldırıları minimuma indirmeye yarayacaktır.

Bilgisayarımıza yükleyeceğimiz dosyaları ya da programları öncelikle virüs kontrolünden geçirerek sistemimize kabul etmek ve internetten yapacağımız yüklemelerde güvenilir kaynakları tercih etmek, doğabilecek virüs tehditlerini baştan

ortadan kaldıracaktır. Ayrıca, e-postalarla gelen ekleri açma noktasında temkinli davranmak da, bizim açımızdan alınacak tedbirlerden biridir.

Son olarak, bilgisayarımızı, sistemi disketten açmayı denemeyecek biçimde ayarlamak ve bilgisayarımızda da takılı disket bulundurmamak da disket yoluyla bulaşabilecek virüsler bakımından izi koruyacaktır.

Sistemimizi bilgisayarımız haricinde bir yerde yedeklemek, doğabilecek en büyük zarar durumunda bile en azından kaybedebileceğimiz verileri kaybetmemek bakımından oldukça yararlı olacaktır.

Eğer makinemize virüs bulaşmışsa bu noktada bazı tedbirler almalıyız. Örneğin virüsü temizleyene kadar o bilgisayarda hiçbir çalışmaya izin vermemek, bir ağdaki bilgisayarlardan birinde virüs varsa diğerlerinde de olma ihtimalini de dikkate almak ve bunları taramaya tabi tutmak, alınabilecek tedbirlerin başındadır. Ayrıca, bilgisayarımıza antivirüs programımızda tanımlanmayan bir virüs bulaşmışsa, sadece bu virüslere yönelik çalışan yazılımların kullanılması bu problemin çözümünde kullanılabilir.

Çağımızda en çok karşılaşılan terimlerden birisi olan phissing konusuna da burada değinmekde yarar görüyorum. Özetle phissing; gerçek süsü verilmiş mesajların kulanılmasıyla güvenilir bir kuruma olan inancı kötüye kullanıp bundan yararlanarak, özellikle fazla deneyimli olmayan kulllanıcıları hedef alan dolandırıcılık olarak ifade edilebilir. Bu kelime, eskiden kullanılan telefon sistemlerinde ücretsiz görüşme yapmak için kullanılan bir aldatmaca sistemi olan phreaking ile balık avlama yani fishing kelimelerinin birleşiminden ortaya çıkmıştır. Tanım olaraksa phishing, genellikle e-posta ya da web sitelerindeki açılır pencereler yoluyla karşımıza çıkan kişisel ya da finansal anlamda bizi zarara sokabilecek bilgi hırsızlığı olarak yapılır. Amaç, karşımıza çıkan bir aldatma sayfası ile; bilgilerimizi güncellememiz noktasında bizi ikna etmektir. Örneğin kişisel hesaplarımızın bulunduğu bir bankadanmış gibi gelen bir mesaj bizden bilgilerimizi güncellememiz aksi takdirde hesaplarımızın kapanacağı noktasında bizi ikna edebilir. Burada tuzağa

düşüp bilgileri güncellememizse, tabiiki bu bilgilerin bizi aldatmaya çalışan insanlarca kullanılarak hesabımızın kullanılması olarak bize dönecektir.

Bu dolandırıcılık yönteminden korunmak için, internette dikkatli davranmalı, bilgilerimizi direk olarak isteyen bir mesaja aldanmamalı, bizden istenen bilgileri girmek için e-postalarda ya da linklerle verilen bağlantılara tıklamamalı, gelen mesajların bizi yönlendirdiği adreslere dikkat etmeli, açılan sayfaların sağ alt köşesinde iletişimin güvenli olup olmadığını gösteren simgeye dikkat etmeli, bu aldatmaya yönelik güvenlik sağlayan bazı antivirüs yazılımlarını tercih etmeli, ayrıca kullandığımız istemci uygulamalarını güncel tutarak, onların sağladığı güncel güvenlik uyarılarından da yararlanılmalıdır. (Daşkıran, 2005, syf.5 -9)

8.5.6 Protokolleri Kullanan Saldırılar ve Alınacak Tedbirler

Bazı protokoller saldırganların kullanabileceği zayıf yönlere sahiptir. Bu yönleri iyi değerlendiren bilgisayar korsanları sisteme istedikleri biçimde sızabilirler.

“Bu saldırılardan korunmak için çeşitli sistemler geliştirilmiştir. Bunlardan bazıları muhtemel saldırılara karşı firewall yazılımları, e-maillerin virüslere karşı ve saldırı kodlarına karşı korunabilirliğini sağlayacak virüs yazılımları, saldırıları tespit etmek için IDS(Intrusion Detection System) yazılımları, güvenli bir ağ altyapısı için switch’li yapılar, şube veya birimler de doğrudan Internet üzerinden değil de Sanal Özel Ağlar (VPN) kullanılarak internete çıkılması, haberleşmede bilgilerin şifrelenerek gönderilmesi (Cryptology) yöntemleri kullanılabilir.”(Fındık, Sadıay, 2003, sy.1)

8.5.6.1 ARP Protokolüne Yönelik Saldırılar

Paketlerin Monitör Edilmesi

Bu saldırı türünde, bağlantıda olan iki bilgisayarın arasına giren bir bilgisayar, bu 2 bilgisayarın ip adresi-mac adresi ilişkisini bozmak için taklit edilmiş arp yanıt paketleri gönderir. Birinci bilgisayarın arp tablosunda yer alan B'ye ait ip değerine karşılık gelen mac adresi yerine kendi mac değerini tabloya yazar. Yine aynı şekilde ikinci bilgisayarın arp tablosunda da, A'ya ait ip değerine karşılık gelen mac adresi yerine de kendi mac adresini yazar. Bu sayede iki bilgisayar arasına giren bir bilgisayar iletişimi kendi üzerinden yönlendirmiş ve iletişimi kontrol etmiş olur.

Toplu Yayın Saldırısı

Bir ağda bulunan bilgisayarlardan birisinin mac adresi, taklit edimiş arp yanıt mesajları kullanılarak "FF FF FF FF FF FF" olarak değiştirilirse bu bilgisayara gönderilen bütün paketler toplu yayın mesajı olarak algılanır ve ağdaki tüm noktalarca da monitör edilir.

ARP Protokolüyle Yapılan DoS Saldırıları

Bilgisayar ağlarında taklit edilmiş arp yayın paketleri kullanılarak, arp tabloları içerisinde yer alan mac adreslerine kaşılık gelen ip adres değerleri değiştirilebilir. Böylece ip adresi yanlış algılanan bilgisayara gönderilecek hiçbir veri ulaşamaz. Yine aynı şekilde o bilgisayardan gönderilen verilerde ağda yayınlanmaz.

Bu saldırılar anlatıldığı gibi temel olarak MAC adresi yanıltma amaçlıdır. Bu sayede de, ya bilgisayarlar arasına girilerek iletişim dinlenir ya da bağlantı tamamen kesilir. Bu problemi çözmek amacıyla alınacak bazı önlemler sorunu büyük ölçüde etkisizleştirecektir.

Uygulanacak adımlardan birincisi; statik arp tablolarının yaratılması ve böylece mac - ip adresi değişiminin önüne geçilmesidir. Ancak statik yapılandırma, bazı Windows

tabanlı işletim sistemleri tarafından kabul edilmeyerek güncellenebilir ve bu durumda alınan bu önlem kendiliğinden geçersiz hale gelmiş olur.

Alınacak tedbirlerden ikincisi ise, ağ üzerinde güvenlik olarak korumalı, şifreli gelişmiş yapıda anahtarların kullanılmasıdır. Bu gelişmiş anahtarların kullanımı ile ARP protokol paketlerinin doğruluğu sürekli kontrol edilebilir ve bu sayede ağ üzerinde gerçek ve taklit edilen protokol paketleri izlenmiş olur.

Bir diğer tedbir ise geniş ağlarda kullanılması zor olmasına karşın, anahtar üzerindeki tanımlı port-mac adreslerinin, sadece ve sadece ağ yöneticisi tarafından, elle değiştirilmesidir.

Bu saldırılardan korunmanın bir diğer yolu da daha önce anlattığımız ve ağ üzerinde mac adresi bilinen bir bilgisayarın ip adresini bulmaya yarayan RARP istek paketlerinin kullanılmasıdır. Bu yolla yapılan sürekli kontrollerle mac-ip ikilisinin bozulup bozulmadığı incelenebilir.

Son olarak alınabilecek bir tedbir de, ağlarda yapılan bilgi toplama yöntemiyle ağ üzerinde Mac adresi bilinen bir bilgisayarın, tüm bilgilerinin kontrol edilmesiyle bunlarda meydana gelen değişimlerin saldırı olabileceği düşünülerek incelenmesidir. (Dirican, 2005, sy.345–353)

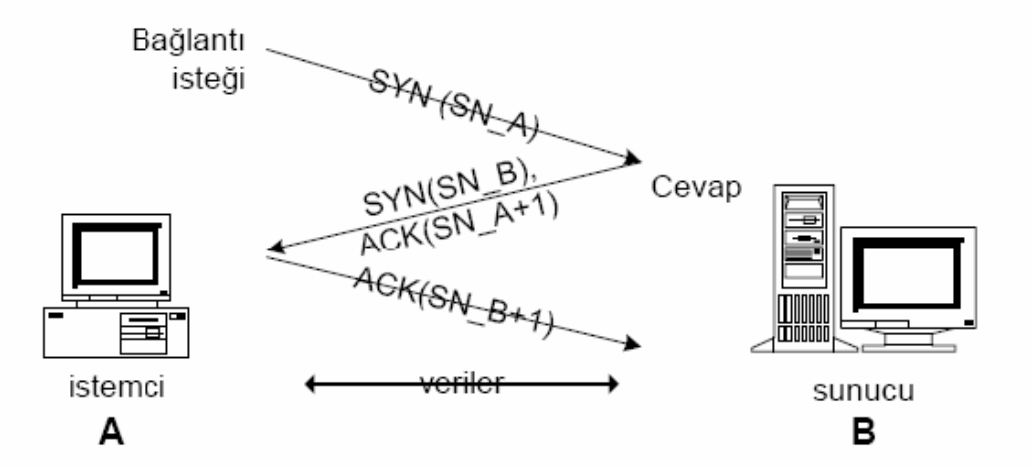
8.5.6.2 TCP Protokolüne Yönelik Saldırılar

İstek (Syn) Bombardımanı

TCP protokolü el sıkışması prensibine göre çalışır. Buna göre bir bilgisayar bağlantı istek paketini bir sunucuya gönderir. Bu bağlantı istek paketini alan sunucu, bağlantı kurulmasını kabul ederse bir yanıt paketi yollar ve bu yanıt paketinin alınmasıyla da bağlantı kurulmasına yönelik bir paket gönderilir ve bağlantı kurulur. İşte bu tam da bu noktada, bir bilgisayarın bir sunucuya bağlanmasındaki bir zaafiyetten bahsedebiliriz. Bir sunucuya yapılan bağlantı istekleri sunucu tarafından değerlendirilerek cevaplanır. Ancak, sunucuya onun başedemeyeceği kadar taklit

edilen sahte ip datagram istek paketleri gönderilirse, bu durum da sunucu işlevlerini yerine getiremez ve yeni bir bağlantı da artık yapılamaz hale gelir.

Bu saldırılardaki temel amaç sunucuları etkisiz kılmak ve oturumu ele geçirme ktir.



Şekil 8.15 TCP El Sıkışma Kuralı (Soğukpınar, veri ve ağ güvenliği, syf.13)

Dizi Numaralarının Belirlenmesi

TCP protokolü, doğru dizi numarası ile gelen paketleri otomatik olarak güvenilir kabul eder. Bu bakımdan bir saldırgan, ilgili bağlantıdaki d izi numarasını tahmin ettiği zaman bu durum, güvenlik zaafiyetlerine yol açar. Bunu bulan saldırgan bağlantıya keyfi veriler gönderebilir.

TCP Oturumlarının Ele Geçirilmesi

TCP bağlantılarının diğer bir zafiyeti de, bağlantının kurulmasından sonra devam eden iletişimin güvenli olduğu varsayılarak tekrar kontrol edilmemesidir.

Bu saldırılarda önce, ilk dizi numarası belirlenir. Daha sonra sunucu, istek bombardımanı ile susturulur. Böylece bağlantıda olduğu istemci ile haberleşmesi de engellenmiş olur.

Bu saldırıların tespit edilebilmesi, saldırganın izlediği yolu tahmin etme ve bilme becerisine sahip olunarak yapılabilir. Bu bakımdan yapılan bazı incelemeler bir saldırının yapılıp yapılmadığı noktasında bize ipuçları vermektedir.

Saldırılardan korunmak için s sh protokolünün kullanılması önerilebilir.

"Bilgisayar ağları üzerinden yapılan Telnet, FTP, TFTP gibi protokol bağlantılarının bir bölümünde iletilen giriş şifresi, kullanıcı adı gibi bilgiler açık yazı olarak iletilir. SSH bağlantı içerisinde iletilen bi lgilerin şifrelenmesini sağlar; oturum ele geçirme saldırılarının yapılmasını zorlaştırır." (Daşkıran, 2005, sy. 369)

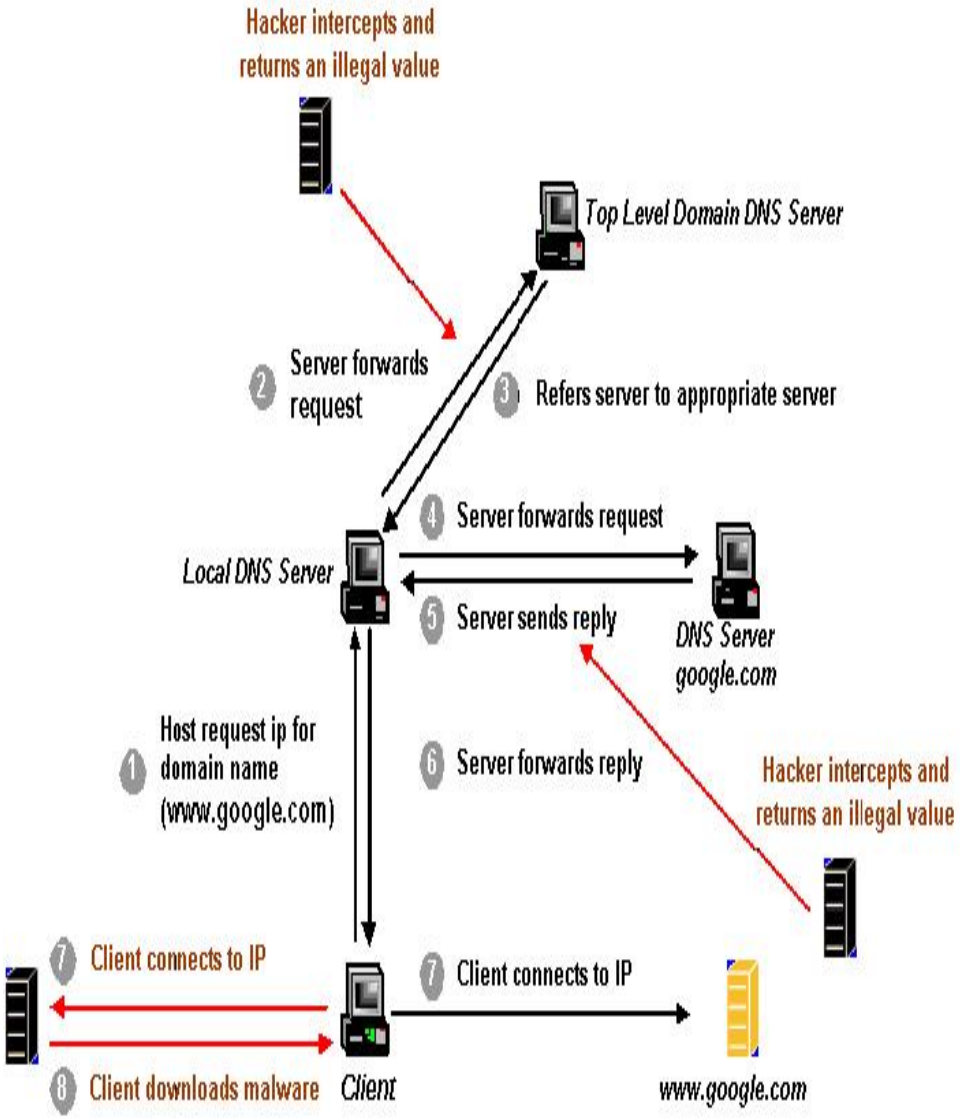
SSH sahip olduğu çok güçlü şifreleme mekanizması sayesinde birçok saldırının engellenmesinde etkindir. SSH protokolü, ağ alt yapısına ve sunuculara güvensiz yaklaşım sergiler. SSH bağlantısı kurulumunda istemci ve sunucu, RSA doğrulama sistemi yürütür.

TCP saldırılarından korunma yöntemlerinden biri de durum tablosu ve bağımlı filtreleme uygulamalarıdır. "İşletim sistemleri ağ üzerinde aldı kları her paket için belleklerinde yer ayırır. Ancak bu, paketlerin o an bağlantıda olunan noktalarla ilgilerini denetim altında tutmaz. Bu amaçla bazı güvenlik duvarları, ağ içerisine giren ve çıkan her paketin iletiminin engellenip engellemeyeceğini, değ işikliğe uğrayıp uğramayacağını, gönderilen paketlere karşılık yanıt iletilip iletilmeyeceğini denetler. Bu amaçla güvenlik duvarının yerel ağ ile dış dünya arasında bulunan tüm bağlantıları belirlemesi lazımdır. İletilen paketleri tek tek ele almayan, ile tim içerisinde bütünün parçaları olarak gören güvenlik işlemlerine "stateful" paket filtreleme adı verilmektedir." (Daşkıran, 2005, sy. 369)

8.5.6.3 DNS Protokol Güvenliği

DNS protokolü, internet üzerinde oldukça yaygın olarak kullanılan protokollerdendir. İnternet üzerindeki paket trafiğinin yaklaşık yüzde 20'sini DNS'e ait paketler kullanılır. Bu bakımdan DNS sunucuların, sürekli çalışabilecek düzeyde kontrolleri gerekir.

- **Ortak Kullanılan Dns Sunuculara Yönelik Saldırılar :** İki dns sunucu arasında yapılan sorgu-yanıt sistemi, bazı güvenlik problemlerini yaratabilmektedir.
- **DNS MİM saldırısı:** DNS sunucu ile bilgisayar arasına yerleşen bir bilgisayar, istemcinin yaptığı sorgulamalara dns'den önce yanıt verebilir. Bu sayede de sorgulama yapılan adresle, ip'si arasında yanlış bir eşleşme yapabilir. (Daşkıran, 2005, sy. 375-378)



Şekil 8.16 Sahte Yönlendirmeler (Uzunay, 2005)

- **DNS Sunuculara Yönelik Band Genişliğinin Tüketilmesi:** Bu saldırlarda, sunuculara boyutları büyük paketler gönderilerek yavaşlamaları sağla nır. Birden fazla kaynaktan, ip adresi taşımayan veriler DNS sunuculara aynı anda gönderildiklerinde bu sunucular için sıkıntılara neden olur.

DNS sunucularına yapılan saldırıları engellemek için bazı tedbirler alınabilir.

- ✓ DNS sunucuların sürümlerinin gün cellenmesi,
- ✓ Birkaç değişik hat üzerinden erişilebilecek biçimde birbirleriyle ilişkili birden fazla dns sunucunun kullanılması,
- ✓ İç ve dış ağa hizmet verecek biçimde kurulmuş yetki alanı belirlenmiş ve bunun haricindeki isteklere yanıt vermeyecek sunucu yap ılandırması,
- ✓ Sadece dns sunucunun kurulduğu ve başka işlemlere izin vermeyen, dolayısıyla da verilmeyen hizmetlerden kaynaklanan güvenlik açıklarının olmadığı bir yapılandırma,
- ✓ Dns sunucuların bölge yapılandırmalarının, sadece o bölgeden gelen dns sorgulamalarına yanıt vermesi ya da kısıtlandırılması, belirli ip adresinden gelen sorgulamalara cevap verilmesi,
- ✓ Dns sunuculara ait kullanıcı yetki seviyelerinin minimum seviyede ve kontrollü olarak verilmesi,

Alınabilecek önlemlerden bazılarıdır. (Daşkıran, 2005 , sy. 381-384)

8.5.6.4 Ağ ve Hizmetlere Yönelik Saldırılar

DoS saldırıları, ağ trafiğinin ya da çalışan servislerin yaratılan gereksiz ve aldatma amaçlı paketlerle yavaşlatılması ya da tamamen durdurulmasını amaçlayan sistemsel kayıplardan ziyade pa ra ve zaman olarak kayıplara neden olan saldırılardır. Bu bakımdan, yapılan tüm saldırılar bu kapsam içerisinde değerlendirilebilir. Bir DoS saldırısı kaynakları, yapısal ayarları ya da fiziksel aygıtların çalışmalarını

engelleyecek biçimde gerçekleştirile bilir. Daha önce anlatılan istek (syn) bombardımanı saldırıları da en çok kullanılan DoS ataklarındandır. Virüs saldırıları, sisteme fiziksel zarar verecek saldırılar bu grup içerisinde değerlendirilebilir.

Kaynakları hedef alan saldırılar, bilgisayar ağ bağlantılarını hedef alarak ağ bağlantısını yavaşlatmayı ya da tamamen durdurmayı, sistem kaynaklarının saldırı amaçlı kullanımını, ağ band genişliği tüketimini ya da sisteme ait kaynakların suistimal edilerek kullanımı neticesinde sisteme ek yük getirmeyi hedefliyor olabilir.

Yapısal ayarları hedef alan saldırılarda temel amaç, ağ üzerinde yer alan bilgisayarların yapılandırma ayarlarında yapılacak değişikliklerle bu cihazların etkin ve verimli kullanımını engellemek hatta tamamen durdurmaktır.

Fiziksel saldırılar ise, direk olarak sisteme yapılan fiziki müdahaleleri ifade eder. Önemli ağ cihazlarının bulunduğu sistem odalarının kontrolü ve bu odalara giriş izinlerinin kontrollü ve sınırlı verilmesi alınabilecek önlemler arasındadır.

DoS saldırılarının çoğu yaptıkları saldırıları toplu yayın adreslerini kullanarak yaparlar. 255.255.255.255 adresini hede alan paketler tüm ağa, 10.255.255.255 adresini hedef alan paketler ise 10'lu bilgisayar ağı üzerinde bulunan tüm noktalara iletilirler. Bu bakımdan bu adresi hedef alan paketlerin, yönlendiriciler tarafından ağ sınırları dışına yönlendirilmemeleri gerekmektedir. (Daşkıran, 2005, sy. 387 -390)

Daha önce bahsettiğimiz Smurf Saldırıları bu grupta değerlendirilen saldırılardır.

Teardrop Saldırıları: MTU değeri farklı ağlarda, Bir IP paketi karşı tarafa yollandığında bu paket tekrar verilere ayrılırken paketin içinde bulunan “offset” bilgisi kullanılır. Bu “offset” bilgilerinin birbirleriyle çakışmaması yani üst üste gelmemesi lazımdır. Özel ayarlanmış bir paket bu senkronizasyonu bozabilir ve paketler üst üste gelirse ve bunu kontrol edebilecek bir mekanizma da mevcut değilse bu işletim sistemini çalışmaz duruma getirebilir. Bu saldırı yönteminden korunma yöntemi IP protokülünün kodlanması ile ilgili olduğundan tam amen işletim sistemi

ile alakalıdır. Günümüzde çoğu işletim sistemi bu tür saldırılara karşı dayanıklıdır. (Atabey, Temel Saldırı Teknikleri)

8.5.6.5 Koordineli Dağıtık Saldırılar

Saldırılar tek bir bilgisayar kullanılarak yapılabileceği gibi birden fazla bilgisayar tarafından koordineli olarak da yapılabilir. Bu saldırılardaki temel amaç, saldırının yapıldığı, genellikle internet erişimi iyi bilgisayarlarında ele geçirilerek kullanılmasıdır. Msstream, TFN, trinoo en bilinen koordineli saldırılardır.(Daşkır an, 2005, sy.405)

Plansız yapılan saldırılardan ziyade, koordineli ve planlı biçimde yapılan saldırılar her zaman, daha büyük tahribatlar yaratan ve durdurulmaları da bir o kadar zor olan saldırılardır. Bu bakımdan bu saldırılar bizim için her zaman daha önemlidir.

8.5.6.6.Uygulama ve Hizmet Protokolleri

Dış dünyaya hizmet veren sunucular, dışarıya kullandıkları sürümleri ve türleri hakkında bilgi verebilir. Bu bilgiler sayesinde de bir saldırgan sunucudan kaynaklanan ya da kaynaklanabilecek açıkları değerlendirme yoluna gidebilir. Bu sunucuları kullanan saldırganlar, ağ hakkında bilgi toplayabilir hatta ve hatta ağ haritasını bile çıkarabilir. Bu bakımdan sunucuların güvenliği oldukça önemlidir

Sadece sunucular değil, evlerimizde kullandığımız modem lerin bile yapılan basit ip taramaları ile modelleri hakkında bilgi edinmek mümkün olabilir. Modeli bilen bir saldırganın yapacağı ilk işlem de, modemin ayarlarının fabrika ayarlarında olup olmadığını kontrol ederek, modeme erişimi sağlayan bilinen fabrika çıkış şifreleri denemektir.

Örneğin, verilen bir ftp hizmeti için yapılan bir bağlantının takibiyle, sunucunun türü hakkında, bahsettiğimiz protokollerin izleriyle ağlar ve sistemler hakkında, kullanılan bir traceroute komutuyla ağların bağlantı noktalarının ve yolların

belirlenmesi hakkında, ya da kullanılacak basit bir tarama programları ile port durumları hakkında çok önemli bilgiler elde edilebilir.

8.5.7 Erişim Denetimi

Bilgisayar sistemlerinde yaşanan hızlı gelişme neticesinde, güvenlik bilg isayar ya da ağdaki cihazların herbirine ayrı ayrı uygulanan biçimde mümkün olmazken, bu cihazların bulunduğu ağın kontrolü şeklinde şekillenmektedir. Ancak, bu gerçekleştirilirken sadece dış ağ değil iç ağımızda da bazı tedbirlerin alınması bir zorunluluktur.

Bu noktada kullanılan yöntemlerden biri olan erişim kontrolü, temel olarak ağa gelen paketlere karşı nasıl davranılacağının belirlenmesidir. Erişim kontrol, iyi bir güvenlik politikası ve kuralları iyi yazılmış bir firewall ile sağlanır. (Soğukpınar, Veri ve Ağ Güvenliği, sy. 18)

“Sistemdeki her nesne için ayrı erişim kontrol listesi (acl) tutulur. Bu listede ikililer halinde nesneye erişecek özneler ve öznelerin erişim bilgileri bulunur. Eğer bir özne acl içinde geçmiyorsa ilgili nesne üzerinde herha ngi bir erişim hakkına sahip değildir. Çok sayıda özne aynı nesne üzerinde aynı erişim haklarına sahipse grup tanımlayarak acl listesi uzatılmadan erişim hakları tanımlanır.” (Çiçek, 2004, sy.3)

Genel olarak erişim kontrol listeleri, kaynak ya da varış ip adreslerine, kaynak ya da varış portlarına ya da ip potokol numaralarına bağlı olarak trafiği kabul ya da reddebillirler. Bu işlev daha çok firewall'lar için kullanılır. Yönlendiriciler, her paketi ayrı ayrı inceler. Liste içindeki adres ya da port numaral arına bakar ve adres ya da portlar için özel kurallara göre trafiğin geçmesine izin verirler. Firewallar sadece bağlantı için kullanılacak bu değeerlere değil TCP/İP bağlantısının kendine has özelliklerini de, her bağlantının durumu için ayrı ayrı araştırı rarak incelerler. (Strassberg, et al Gondek, Rollie, 2002, sy.42)

8.5.7.1 Erişim Denetiminde Önemli Noktalar

Bir bilgi varlığındaki açıklıkları kullanarak varlığa kısmen ya da tamamen zarar veren etkenlere tehdit denilmektedir. Tehdit insanlar tara fından bilerek ya da bilmeyerek meydana gelecekleri gibi doğal afetler, yanlış konfigürasyonlar ve sistemsel ya da yazılımsal hatalardan da kaynaklanabilir.

Bir tehdit tarafından kullanılarak, bilgi sistemlerinde zarara neden olan zayıflık ya da açıklıklar da zafiyet olarak değerlendirilir. (Özeren, Güvenlik Yönetim Sistemleri)

Saldırganların sistemimize karşı oluşturdukları tüm tehditler, güvenlik boşluklarına yöneliktir ve bir güvenlik boşluğu ortadan kaldırılırsa o boşluğu yönelik tehdit de ortadan kalkmış olur.

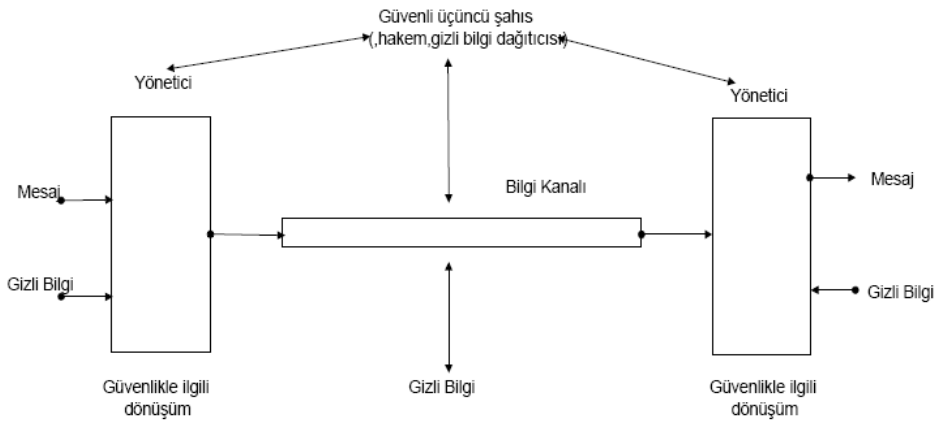
Erişim Denetimindeki diğer önemli kavramlarda daha önce bahsedilen Kimlik Onaylama (Authentication), ilerideki konularda bahsedilecek şifreleme ve “takip”tir. Takip; Güvenlik politikasının tanımlanmasından sonra, politikanın ne ölçüde uygulandığının kontrolüdür. Bu, bir güvenlik açığının oluşması ya da eksikliklerin giderilmesi bakımından oldukça önemlidir.

8.5.7.3 Ağ Güvenliği

Ağ güvenliği için yapılan bir modelleme şekilde gösterilmiştir. "Burada gönderici, alıcı arasında veri ilet iminde verinin dağıtıcısı olan güvenli bir üçüncü kişi bulunduğu görülmektedir. Bu genel güvenlik mimarisi, güvenlik servislerinin tasarımında dört temel işi gösterir.

- Güvenlik ilişkili dönüşümler için bir algoritma tasarımında,
- Algoritma ile kullanılacak bilginin üretiminde,
- Gizli bilginin dağıtımı ve paylaşımı için yöntem geliştirilmesinde,

- Güvenlik algoritması ve güvenlik servisini sağlayacak gizli bilgi kullanımını sağlayacak bir protokol belirlemede."



Şekil 8.17 Ağ Güvenlik Modeli (Soğukpınar, Veri ve Ağ Güvenliği, sy. 5)

Ağ güvenliğinin sağlanmasında bazı yazılımsal ve/veya donanımsal sistemlere ihtiyaç duyulmaktadır. “Saldırılardan korunmak için çeşitli sistemler geliştirilmiştir. Bunlardan bazıları muhtemel saldırılara karşı firewall yazılımları, e-maillerin virüslere karşı ve saldırı kodlarına karşı korunabilirliğini sağlayacak virüs yazılımları, saldırıları tespit etmek için IDS(Intrusion Detection System) yazılımları, güvenli bir ağ altyapısı için switch’li yapılar, şube veya birimler de doğruda n Internet üzerinden değil de Sanal Özel Ağlar (VPN) kullanılarak internete çıkılması, haberleşmede bilgilerin şifrelenerek gönderilmesi (Cryptology) yöntemleri kullanılabilir.” (Fındık, Saday, 2003, sy.1)

Tablo.8.2 Güvenlik Prensip ve Sonuçları(http://savassaygili.net)

Tehdit kaynağı Saldırı Örneği	**Açıklama**	**Zarara Uğrayan Güvenlik Prensibi**
Kimlik Bilgilerinin Çalınması	Kullanıcıların kişisel işlemlerini yapmalarını sağlayan kimlik bilgilerinin ele geçirilmesi	Gizlilik, Veri Bütünlüğü
Hizmet aksatma Saldırıları	Hizmet veren sunucu yada sitemlerin çalışmaz duruma getirilmesi	Süreklilik, Erişilebilirlik
Ağ Trafiğinin Dinlenmesi	Ağ ortamında aktarılan verinin şifrelenmemiş kanal üzerinden iletildiği durumlarda	Veri Bütünlüğü, Gizlilik
Yanlış Yapılandırılmış ErişimDenetimi Ayarlamaları	Yetkisiz bir kullanıcının yetkili bir kullanıcı yerine geçerek yaptığı değişiklikler	Gizlilik, Veri Bütünlüğü
Doğal Afetler	İstem dışı oluşan dış etkenler	Süreklilik, Erişilebilirlik
Zararlı Kod Parçaları	Virüs, Solucan (worm), Truva atlarının (trojens), klavye kaydediciler (keylogger) sistemlere bulaşması	Gizlilik, Veri bütünlüğü Erişilebilirlik
Uygulama Zafiyetleri	Geliştirilen uygulamalar üzerinde yeterli girdi denetimlerinin yapılmadığı durumlarda gerçekleştirilen saldırılar (sql sokuşturması, siteler arası betik çalıştırma (XSS)..	Gizlilik, Veri bütünlüğü Erişilebilirlik

8.5.8 Firewalls (Ateş Duvarları)

Firewall ingilizceden dilimize ateş duvarı olarak çevrilebilir. Aslında itfaiyecilerin kullandığı bir tabir olan Firewall kelimesinin nereden geldiğini anlatmak, ne işe yaradığını daha iyi özetleyecektir. Binalarda meydana gelebilecek bir yangında, yanan bir odadaki alevlerin diğer odalara sıçramaması için ateşten etkilenmeyen ve ateşin yayılmasını büyük ölçüde etkileyen özel oda duvarları yapılmıştır. Bu duvarlara itfaiyecilerin verdiği isim ise Firewall' dur.(Fındık, Saday, 2003, sy.1)

Bir firewall'un temel işlevi, bir bilgisayar ağına yetkisiz erişimin önlenmesi amacıyla ağ iletişimini görüntülemektir. Firewall'lar değişik şekil ve biçimlerde, bazen birden fazla bilgisayarın toplaması şeklinde ortaya çıkarlar. Firewall'lar, Özel ağlarımızı, birçok güvenlik tehditi barındıran internet ve benzeri ağlardan ayıran, sadece politikalarla belirlenmiş olan trafiğin geçişine izin veren cihazlardır. Bir ağa dışarıdan gelen paketleri incelemek ve belirlenen kurallar çerçevesinde geçişine izin vermek ya da paketi düşürmek için; ağ adreslerini, filtreleri, vekil sunucuları kullanır. Servis ve protokoller, firewall üzerinde kapatılabilir ya da açılabilir. Firewall'ların kullanımının en basit cevabı, yetkili ve yetkisiz iletişime karar vermektir.(Strassberg, et al Gondek, Rollie, 2002, sy.3)

İnternet bizim tarafımızdan kontrol edilemez ve politikalarımızı internette uygulamamız mümkün değildir. Açık ağlar hızla büyümektedirler ve güvenlik açısından da denetlenebilirlikleri her geçen gün azalmaktadır. Bu ağların çevresi net bir biçimde belirlenmiştir ve genellikle de tek bir giriş çıkış noktası bulunur. Kayıtları tutmak ve ağ istatistiği toplamakla beraber, güvenlik politikasının oluşturulduğu noktayı olma bakımından da önemli olan firewall'lar, farklı ağ segmentlerinde farklı biçimde çalışabilirler. Firewall'ların güçlü ve zayıf yanları aşağıdaki gibi özetlenebilir.

Güçlü Yanları

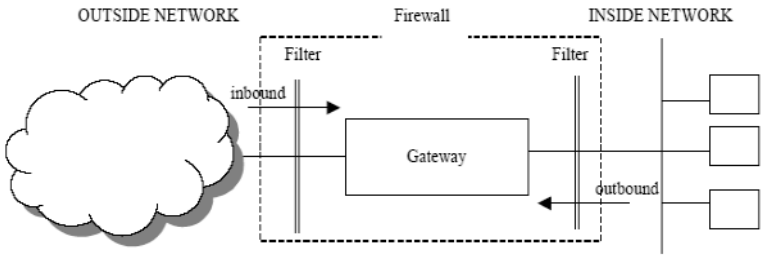
- Bir güvenlik politikasının uygulanması noktasında kullanılabilecek mükemmel cihazlardır.
- Farklı servislere sınırlı erişim sağlayarak güvenliği arttırmaları bakımından oldukça kullanışlıdırlar. Örneğin web'e erişime izni verirken, ağa dışarıdan telnet ya da diğer erişim yöntemleriyle bağlanmayı engelleyebilirler.
- Firewall'lar mükemmel izleyicilerdir.
- Firewall'lar herhangi normal olmayan bir olay olması durumunda bunu mükemmel bir biçimde olan uyarıcı özelliği ile firewall yöneticisine bildirirler.
- Firewallar ayrıca, VPN, URL filtering, Virus Checking gibi ek hizmetler de sağlarlar.

Zayıf Yanları

- Firewall'lar yetkili erişimlere karşı oldukça zayıftır. Yani, firewall politikalarında belirtilmeyen ya da önlenecek bir politikanın yazılmadığı durumlarda, yetkili kişilerin yaptığı bilinçli ya da bilinçsiz saldırı imkânlarına karşı açıktır.
- Firewall politikaları eğer yeterince iyi belirlenmemişse, bu açığı tespit ederek bunlardan yararlanma yoluna gitmek firewall'u etkisiz hale getirebilecektir.
- Firewall'lar sosyal mühendisliği engelleyemezler.
- Firewall'lar zayıf yöneticilerini ya da onların yazdığı zayıf politikaları belirleyemezler.
- Üzerlerinden geçmeyen bir trafik ile yapılan saldırıları engelleyemezler.
- Bilinmeyen yeni güvenlik açıklarından bizi koruyamazlar.
- Virüsleri engelleyemezler."(Strassberg, et al Gondek, Rollie, 2002, sy.6)

Erişim kontrol politikasına göre ağlar arasındaki trafiğin değişimini filtre ederler. Firewall’lar iç ağın güvenli trafiğini, dışarıdaki güvensiz trafikten korurlar. Her bağlı ağın içerisinden ve dışarısından geçen yetkili trafiğe izin verirler. Ağın tehlikeye

düşmemesi açısından bir firewall kendini saldırılara karşı her yönüyle güçlendirmelidir. (Roeckl, 2004, sy.3)



Şekil 8.18 Firewall'ların Yerleşimi (Tosun, Vekil Sunucular ve Güvenlik Duvarları, sy.3)

Firewall genellikle TCP/IP bazında kaynak ve varış adresleriyle ve port numaralarına dayalı olarak çalışır. Buna göre Firewall, ip paket yapısını inceler ve kurum içi İP adreslerini saklar. TCP syn saldırılarını önlerken ip spoofin g veya TCP hijacking saldırılarını zorlaştırır ancak yüzde 100 engellemez. Data bölümünde gizlenmiş saldırıları da engelleyemez.

Firewall'u olmayan bir sistem belki kolay yönetilebilir ya da yüksek işlevsellik içinde çalışabilir ancak bu sistem için "güven liği sağlanmıştır" diyemeyiz. Unutulmamalıdır ki bir sitemin güvenliği o sistem üzerinde bulunan en zayıf halka ile değerlendirilir.

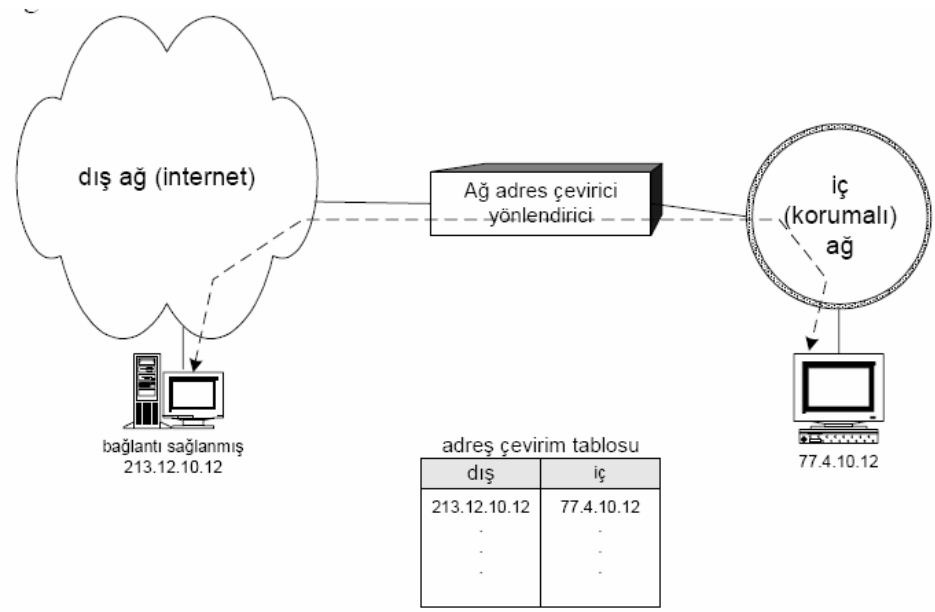
Özet olarak firewall kullanımı ile dışarıdan yapılabilecek saldırılar, ağ içerisindeki yetkisiz kişilerin dışarıya bilgi gö ndermesi ve internet'te dolaşımın sınırlandırılması ile de sisteme bulaşabilecek virüs tehlikesi önlenmiş olur. Ayrıca, iş kaybına neden olacak sohbet programları, çalışanların internette gezinmelerinin engellenmesi gibi uygulamalarla da iş kaybının engell enmesi bakımından yararlıdır.

8.5.8.1 NAT ve PAT Kavramları

NAT (Network Adress Translation)

NAT olarak bilinen “Network Address Translation” teknolojisi network mühendisliği ve güvenliği bakımından iki önemli konuya hitap etmektedir. Bunlardan birincisi, NAT’ın firewall’un arkasında yer alan ağa ait adresleme şemasını gizlemek için etkili bir araç olmasıdır. İkincisi ise; İç ağlarda kullanılan tahsisli olmayan ip numaralarıyla, daha az sayıda ip kullanılmasının sağlanmış olmasıdır. (Budanur, Security Via Fırewalls)

Dış ağlarla olan iletişimde, güvenlik duvarının sahip olduğu internette bilenen ip adresi kullanılır ve yönlendirici, iç ağdan gelen paketin hangi bilgisayardan geldiğini bilerek kendi ip'sini pakete yazar. Aynı şekilde kendisine gelen paketle ri de ilgili bilgisayara iletir.



Şekil 8.19 Adres Çevrimi (NAT) (Soğukpınar, Veri ve Ag Güvenliği, sy.115)

PAT

Birçok bilgisayarın TCP oturumlarını ve UDP aktarımlarını, bir ya da birden çok ip adresine aktarır. İçerdeki bir bilgisayara dışarıdan bir o turum açmak mümkün olmadığı için güvenliği bir miktar daha arttırmış olur.

8.5.8.2 Firewall Tipleri

Paket Filtreleme Yönlendiricileri

Ağ üzerinde ayrıntılı erişim denetimlerini tanımlayabilen ilk temel teknolojidir. Tek yönlü, servis bağlantılarının kullan ıldığı ağlar için yeterli ve güvenli bir çözüm olabilir. Temel olarak ağımız üzerinde iletilen verilerin hangilerinin iletilip hangilerinin iletilmeyeceğini, ya da hangi servislere izin verileceğini ayrı ayrı ya da sadece içeri ya da sadece dışarı olabilec ek şekilde, izin vermeyi ifade etmekte kullanılır. Tabi bunun sağlanabilmesi de uygulanan politikalarla desteklenmelidir. Bu yöntemde, daha önce bahsettiğim access list'ler kullanılmaktadır.

Paket filtrelemeye bağlı olarak çalışan bir firewall yapılandırma sı genel olarak kullanılan yönlendiricilere de bağlı olarak yapılır

İzin verme kurallarına uymayan anlamsız paketlerin ağ içine gönderilebilmeleri, karmaşık politikaların uygulanması durumunda yönetimlerinin çok zor olması, ip paketlerin parçalanarak ağın içine gönderilebilmeleri zayıf yanlarıdır.

Kalkanlanmış Host

Paket filtreleme yönlendiricisi tarafından sağlanan bu mimaride, sadece yönlendirici tarafından erişilen “bastion host” iç ağ üzerindedir.

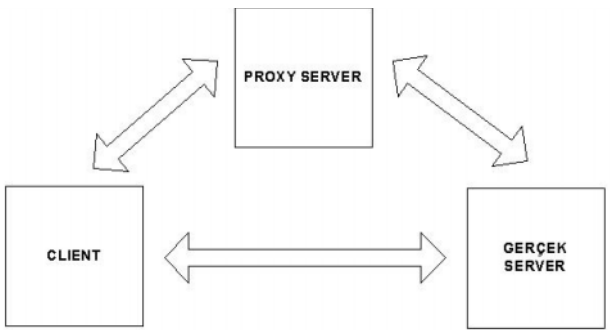
Kalkanlanmış Subnet

Çevre güvenliği yaklaşımında kullanılan mimari yapıdır. Yönlendirme güvenliği, ağlar arasına yönlendirmenin konulmasıyla daha da arttırılmıştır. İç ağa ek olarak, güvenlik için DMZ ara ağı oluşturulmuştur. Dış ağa verilmekte olunan servisler DMZ'e yerleştirilmişlerdir ve DMZ' den de iç ağa erişim çok kısıtlanmıştır. Ayrıca bastion host içerideki LAN'dan ile ekstra bir yönlendirici vasıtasıyla ayrılır. Böylece iç ağa girebilmek için iki yönlendiricinin de aşılması gerekir. Bu sayede DMZ'de bulunan bir sunucunun ele geçirilmesi d urumunda atağın iç ağa taşınması engellenmiş olur.

Güvenlik yazılımının güçlendirilmemiş, genel amaçlı bir platformda çalışması engellenmelidir. Güvenlik yazılımı servis yazzılımından ayrılmalıdır. DMZ'de bulunan sunucuların düzenli olarak yedeklemesi yap ılmalıdır

Vekil (Proxy) Sunucu

Kullanıcılar, dış dünya ile bağlantılarını uygulama programları üzerinden gerçekleştirirler. Bir sunucu tarafından sağlanan proxy servislerin temel kullanım amacı, sistem üzerindeki kayıtları tutmanın yanı sıra intern et'e bağlanan kullanıcıları da çok fazla sınırlamadan, uygulama temelli bir güvenlik kalkanı oluşturularak korunmasıdır.



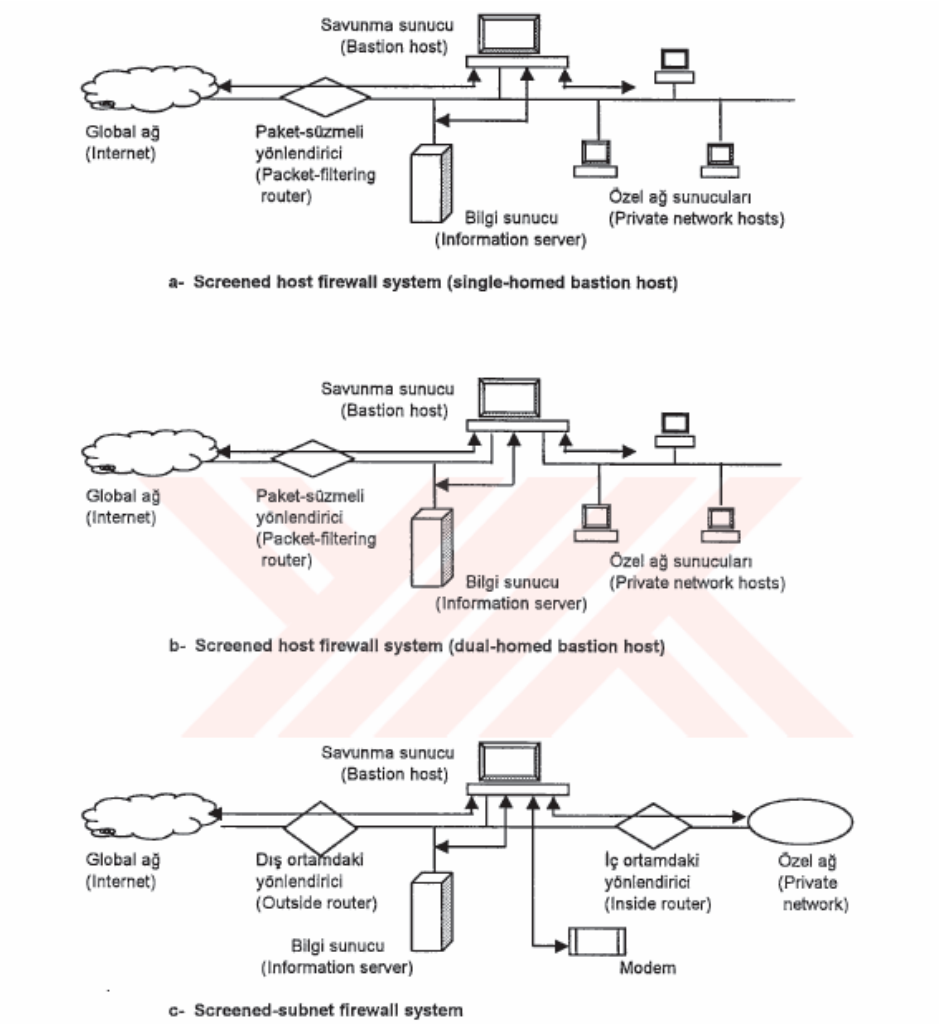
Şekil 8.20 Vekil Sunucuların Bağlantı Biçimi

Ağ üzerinde bulunan farklı istemciler, eğer aynı istekte bulunuyorlarsa bunlar, kullanılan proxy sunucu vasıtasıyla bir defaya indirgenir. Böylece hem sunucu hem de ağ trafik yükünde bir performans artışı sağlar. Ayrıca ağda izin verilen servislerin çalışması, yani izin politikasının oluşturulması bakımından da avantaj sağlar.

Bilgisayarımızın üzerinde çalıştığı ağda bulunan 50 bilgisayarın www.keskinstrateji.tr.cx sitesine bağlandığını varsayalım. Bir vekil sunucunun varlığı durumunda ilk isteğin yapıldığı anda bu sayfa vekil sunucu da depolanır ve geriye kalan 49 istek vekil sunucuda depol anan sayfa üzerinden yerel ağın sahip olduğu hız ile sağlanır. Böyle bir vekil sunucu kullanımında görüldüğü gibi internet trafiği de azaltılmış olacaktır.

Durum Koruması

Durum filtreler, paketler üzerinde değil bağlantılar üzerinden, bu bağlantıyı başlatanı takip ederek çift yönlü paket geçişlerine, karar verme prensibiyle çalışmaktadırlar. Böylece üstlerinden geçen bütün bağlantıları bilir ve takip ederler. Üzerlerinde depolanmış olan bağlantı parametrelerine göre kullanılmakta olan bağlantıların trafiğini, rasgele trafikten ya da zararlı bağlantı girişimlerinden ayırırlar. Yönetimlerinin kolay olması, yeni servislerin rahatlıkla eklenebilir olması, performanslarının çok yüksek olması ve paket filtrelerden daha güvenli bir yapıya sahip olmaları bakımından avantajlıyken, içeriğini analiz etmenin zorluğu ile uygulama düzeyinde çok fazla denetim yeteneği sağlamaması bakımından dezavantajlıdır.



Şekil 8.21 Firewall Türleri (Yusuf Saka, 2000, sy.54)

8.5.9 Güvenlik Politikaları

Kurumların internete de bağlı ağları üzerinde bulunan kaynaklar ve sahip oldukları varlıklarının korunmasıyla ilgili tüm kavramlarla ilgili kurallar, genel hatlar içerisinde belirlenip yazılı hale getirilerek ağ politikasını oluşturur.

Güvenlik politikasının en temel özelliği, en üst sistemden en alt olduğu düşünülen sisteme kadar, tüm ağı kapsayacak biçimde, güvenlik açısından tanımlanan tüm kural ve prosedürleri ifade etmesidir. İyi bir güvenlik politikası ağa herhangi bir biçimde erişebilecek tüm kişilerce ulaşılabilen, bu kişilerin görev ve sorumluluklarını belirleyen, kullanıcıların gizlilik seviyelerini tanımlayan, güvenlik hedeflerini sade ve açık bir biçimde anlatan, tanımlanan tüm konularda kurumun konumunu gösteren ve politikanın gerekliliklerıyle nasıl uygulanabileceğini açıklayan nitelikte, değişen teknolojilere karşı esnek ve belirli bir dönemi kapsayacak biçimde olmalıdır. Unutulmamalıdır ki " ideal güvenlik, ağ tasarımı, bilginin gizlilik derecesini ve kullanıcı hakları ile uygulama sınırlamalarını hesaba katan sağlam bir güvenlik politikası ile başlar."(Soğukpınar, Veri ve Ağ Güvenliği, syf.26)

Güvenlik politikası, uygulanabilirliği bakımından yöneticiler tarafından tüm çalışanlara imzalatılacak bir sözleşme ile de güvence altına alınabilir Ayrıca, personelin, performans değerlendirmesinin bir parçası olarak uygulanması da gerekmektedir. Güvenlik politikalarının daha kolay uygulanabilirliği bakımından sistem kurulmadan önce oluşturulması da önemlidir.

Aşağıda özetlenen izleme araçlarından gelen uyarılar ve bunların takibi politikanın uygulanabilirliği bakımından çok önemlidir.

Uygulama: Bu konuya güvenlik politikasının uygulanması konusunda ayrıntılı olarak değinilecektir.

Uygunluk: "Ayrıca güvenlik politikaları düzenli olarak gözden geçirilmeli, yeni gelişmeler, ihtiyaçlar ve tehditlerin ışığında gerekirse yenilenmelidir. Bu, güvenlik politikalarının, yaşayan sistemler haline gelmesini ve uygulamanın da kurumun günlük hayatının bir parçası haline gelmesini sağlamak için son derece önemlidir." (http://www.redbilisim.com)

Ağa giren ve çıkan trafiğin kontrolü bizim için olabilecek bir saldırının habercisi olarak değerlendirilebilir. Çünkü trafikte yaşanan olağandışı bir artış genellikle bir saldırıyı ifade eder. İzleme, çeşitli araçların kullanımıyla yapılabilir.

Tablo 8.3 İzleme Araçları

ARAÇ	İZLEME
Güvenlik Duvarı	**Aktivitelere ait logların kullanımı ve gerekli ayarlamaların yapılması**
IDS	**İçeriye ve dışarıya olan aktivitelere ait IDS loglarının takibi**
Hostlar	**Hostların düzenli biçimde açıklara karşı değerlendirilmesi**
Dosya Sistemleri	**Dosya sunucularının izlenmesi**
Uygulamalar	**Olağan olmayan hareketlerin izlenmesi**
Satın alma	**Bilinen zayıflıklara ve politikamıza karşı uygulamaların izlenmesi**
Eposta	**Uygun olmayan mail giriş ve çıkışlarının izlenmesi**
Fiziksel	**Fiziksel ve şifre güvenliğinin sağlanması**

8.5.9.1 Temel Politikalar

Güvenlik politikalarını oluşturan temel politikalar şunlardır:

- Geçerli kullanıcı politikası (acceptable use) politikası
- Erişim politikası

- Ağ güvenlik duvarı (firewall) politikası
- İnternet politikası
- Şifre yönetimi politikası
- Fiziksel güvenlik politikası
- Sosyal mühendislik politikası

Geçerli kullanıcı politikası (Acceptable Use) Politikası: Sistemin sahip olduğu olanakların kullanımı konusunda, kullanıcıların hak ve sorumluluklarını belirtir. Politika da temel olarak aşağıdaki konular belirlenmelidir:

- Kaynakların kullanım ve yönetim haklarına, kimlerin ne ölçüde yetkili, izinli ve öncelikli olduğu,
- Kaynakların uygun biçimde nasıl kullanılabileceği,
- Sistem yöneticilerinin kullanıcılar üzerindeki, kullanıcıların da sistem üzerindeki hak ve sorumluluklarının neler olduğu,
- Kritik bilgi ile nelere sahip olunduğu.

Erişim Politikaları: Kullanıcıların ağa bağlanma yetkilerini belirleyen bu politikalar, ağdaki en alt seviyede olarak tanımlanan kullanıcıda n, en üst seviyedeki sistem yöneticisine kadar tüm kullanıcılar için belirlenmelidir. Erişim kontrolü bir sınıflandırmaya tabi tutarsak sağduyuya dayalı erişim kontrolü (Discretionary Access Control-DAC), zorunlu erişim kontrollü (Mandatory - MAC) ve kaynak kontrollü erişim kontrolü (Ordinator Controlled Access Control - OCAC) olmak üzere üçe ayrılır.

DAC'da örneğin bir dosyanın sahibi, diğer kullanıcıların bu dosyaya erişim izinlerini de belirler.(http://www.hipaabasics.com)

MAC; erişim haklarının sistem tarafından belirlendiği ve kullanıcılara hiçbir değişiklik hakkının tanınmadığı erişim biçimini ifade etmektedir. OCAC ise Sadece bilginin yaratıcısının erişim haklarını belirlediği erişimdir. "Bilginin o anki sahibi aynı zamanda bilginin yaratıcısı değilse bu haklarda herhangi bir değişiklik yapamaz. " (Tosun, 2004, syf.5)

Yani bu erişim biçiminde bilginin herhangi bir zamandaki sahibi değil ilk sahibi erişim haklarının belirlenmesinde yetkilidir.

Bu bölümde kimlik belirleme, onaylama, şifrelerin belirlenmesi ve kullanılma kuralları, hesap yönetimi, şirket dışı personel tarafından (örneğin bayiler) şirket kaynaklarına ulaşım hakları gibi alanlar düzenlenir.(http://www.redbilisim.com)

Ağ Güvenlik Duvarı (Firewall) Politikası: Ayrıntılı olarak incelenen güvenlik duvarları, sadece dış saldırılara karşı sistemi koruma amaçlı değil, aynı zamanda performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılarak erişim politikalarını tanımlayabilmektedir. Güvenlik duvarlarının sahip olduğu vekil sunucular, anti virüs çözümleri, içerik filtreleme, özel sanal ağlar, Nüfuz tespit sistemleri gibi sahip olduğu tüm servislerin yapılandırmaları ve kuralları bu politika ile belirlenmektedir.

İnternet Politikası: Kurum içerisindeki tüm personelin internete bağlanması güvenlik açısından bazı sorunlara neden olabilir. Virüs ya da trojan gibi zararlı yazılımların sisteme girmesi, java ve ActiveX gibi kodların kullanımı ile sisteme yapılacak bazı saldırıların mümkün olması, film müzik gibi iş açısından kullanılmayacak dökümanların indirilmesinin ağa getireceği ilave külfet ve çalışanların internette iş amaçsız gezinmelerinin getireceği zaman kaybı gibi nedenler internet politikası ile belirlenen biçimde uygulanarak minimuma indirilebilir.(Şengonca vd. Teke, Karaarslan 2006, syf.2-3)

"Bu alanda Internet kullanım saatleri, kuralları, Internet'ten HTTP veya FTP protokolleri ile ile hangi dosya tiplerinin Internet'ten indirilebileceği gibi noktalar belirtilir. Ayrıca kurum elemanlarının VPN gibi bir teknoloji ile Internet üzerinden kurum sistemlerine nasıl ulaşacağı, şifreleme yöntemleri irdelenir.

Bu bölüm de buna ilave olarak, kurumun bilgisayarlarının ve bilgi işlem sistemlerinin kullanımı hakkında genel kullanım kuralları içerir. Örneğin Internet'e hangi kullanıcıların gireceği, Internet'ten hangi tür dosyaların indirilmesine izin

verilebileceği, kullanıcıların hangi durumlarda ne gibi sorumlulukları olduğu belirtilir."(http://www.redbilisim.com)

Şifre Yönetim Politikası: Kullanıcıların erişim izinlerinin denetildiği b ir araç olan şifreler yanlış ve kötü amaçlı kullanım durumunda doğuracakları problemler nedeniyle güvenlik politikalarında önemli yere sahiptirler. Bu bakımdan basit ve kolay tahmin edilebilir olmayan güçlü şifreler seçmek ve bunların da periyodik olarak değiştirilmeleri politikanın temelini oluşturur.

Kullanılacak şifrelerin uzunluğu en az 8 karakter olmalı ve karakter, rakam ve harflerin büyüklü küçüklü yazılmış karışık kombinasyonu biçiminde olmalıdır. Oluşturulan şifrelerden süresi dolanlar iptal ediler ek kullanıcıların yeni şifre almaya zorunlu bırakılması gerekmektedir. Ayrıca kullanıcılar, kendilerine tanımlanan tek şifre ile ağda kendilerinin erişimine izin verilen tüm uygulamalara erişebilmelidirler.

Fiziksel Güvenlik Politikası: Sistemlere fiziksel olarak erişebilen saldırganlar, sisteme kolaylıkla saldırabilirler. Ağ bağlantısına erişebilen bir saldırgan hattı dinleyebilir, trafik yaratabilir. Bu bakımdan fiziksel güvenlik politikası, dikkatle uyulması gereken bir güvenlik tedbiri olarak karşımıza çıkar. Binalara ve sistem odalarına erişimiyle, kullanıcıların zimmet kuralları, ağ alt yapısı gibi konular bu bölümde yer almaktadır. Şengonca vd. Teke, Karaarslan 2006, syf.4)

Sosyal Mühendislik Politikası: Yapılan saldırıların büyük bir kısmını oluştura n sosyal mühendislik yöntemlerine karşı alınacak önlemler bu politika ile belirlenir.

8.5.9.2 Politika İhtiyaçlarının Belirlenmesi

Güvenlik Politikalarının oluşturulması sırasındaki ilk adım olarak, bu politikanın kurumun hangi gereksinimlerine yönelik ol uşturulacağı belirlenmelidir. Politikanın oluşması için aşağıdaki aşamalar sırasıyla uygulanmalıdır:

1.Aşama: Bir güvenlik politikasının oluşturulmasında ilk temel adım; oluşturulacak politikanın hangi gereksinimler için yapılacağının belirlenmesidir.

2.Aşama: Korunacak nesnelerin belirlenmesi ise ikinci aşamayı oluşturmaktadır. Bu nesneler bir bilgisayar kaynakları, etkin iletişim cihazları, sunucular olabileceği gibi bilgiyi de ifade edebilir.

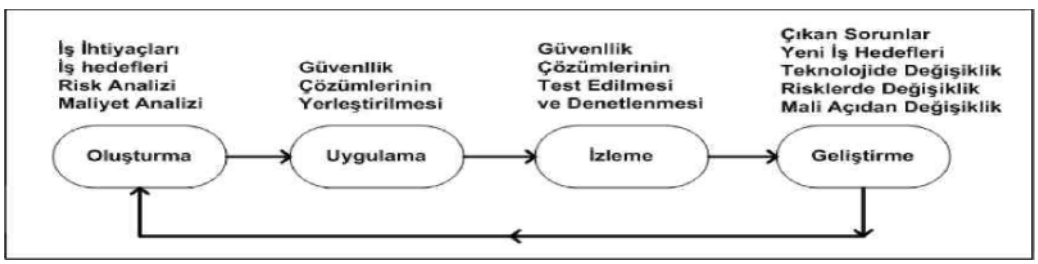
3.Aşama: Ağ üzerinde hizmet veren sunucuların hangi hizmetler i, hangi protokolleri kullanarak kimlere verdiği belirlenmelidir.

4.Aşama: Alınacak tedbirlerin kimlere karşı alındığının belirlenmesi olmalıdır. Alınacak önlemler dışarıdan ağa sızmaya çalışan bir saldırgana karşı olabileceği gibi, ağ içinden, dikkatsiz bir çalışanı da kötü niyetli olabilecek bir çalışanı da kapsamalıdır.

5.Aşama: Bilgileri saklama yöntemi, arşivleme ve yedeklenmelerinin nasıl yapılacağının belirlenmesidir. Bunların belirlenmesinde güvenlik, esneklik, erişilebilirlik ve bütünlük göz önüne alınmalıdır.

6.Aşama: Kurum içerisindeki tüm kişilerin görev ve sorumluluklarının ağ açısından yönetim, güvenlik bölümü ve kullanıcılar olmak üzere oluşturularak belirlenmesidir. Yönetim, güvenlik politikasını kuracağı güvenlik birimi vasıtasıyla oluştura rak uygulamakla, güvenlik birimi güvenlik politikasını bizzat oluşturarak, yayınlamak ve uygulamakla kullanıcılar ise bu politikaya uymakla sorumludur.

7.Aşama: Uygulanabilirlik açısından yaptırım gücünün belirlenmesi olmalıdır. Şengonca vd. Teke, Karaarsl an 2006, syf.5)



Şekil.8.22 Güvenlik Politikasının Hazırlanma ve Uygulanma Süreci (Akman ve ark. İnci, Erten, Kılıç, Bilir, Bilir, Tomur, Durgut, 2004)

8.5.9.3 Risk Analizi

Yapılacak risk analizleri, kurumun ağına, ağ kaynaklarına ya da varlıkların a yapılacak olası saldırılardaki riskleri tanımlamaktadır. Temel amaç değişik ağ bölümlerindeki tehdit tahminlerinin belirlenerek buna uygun güvenlik önlemlerinin alınması ve uygulanmasıdır. Oluşabilecek riskler, düşük, orta ve yüksek olarak derecelendirilebilir.

Riskler tanımlandıktan sonra, sistemin kullanıcıları sınıflandırılır. Bu sınıflandırma yöneticileri, daha öncelikli erişim hakkına sahip kullanıcıları, iş ortaklarını hatta müşterileri de kapsayacak biçimde ağda bulunan tüm kullanıcıları kapsamalıd ır. Güvenlik matrisi kullanıcılara karşılık gelen risk seviyelerini ifade eder ve ağ güvenliğinin başlangıç noktasını oluşturur.

Ayrıca bir kurumdaki alt ağ yapılandırmalarının yapılarak, bölümlerin hangi diğer bölümlere hangi protokoleri kullanarak erişim yapacağı da güvenlik matrisi ile belirlenmelidir. Çizelge'de hangi birimin (alt ağın) hangi birime erişim hakkı olduğu örnek olarak belirtilmektedir.

Tablo 8.4 Alt Ağların Erişim Hakları (Şengonca vd.Teke, Karaarslan 2006, syf.6)

	Bilgi İşlem	ArGe	Muhasebe	Satın Alma	İdari	İnternet
Bilgi İşlem	√	√	√	√	√	√
ArGe		√				√
Muhasebe			√			
Satın alma			√	√		
İdari	√	√	√	√	√	√

Bilgisayar ağlarında kritik önem taşıyan ve güvenli bir sistemin nasıl olması gerektiğini tanımlayan güvenlik politikaları, kurumsal güvenlik için öncelikle yazılı olarak planlanmalı, en alt sistemden en üst sisteme kadar tüm sistemi kapsamalı, kurumun tüm çalışanlarının katılımıyla oluşturulmalı ve çalışanların uygulama noktasında katılımı bazı değerlerle, ödüllendirme ve cezalandırmalarla sağlanmalıdır. Esnek yazılması gereken politikalar çeşitli koşullarda kendini yenileyebilmeli yani gerekli güncellemeler kolaylıkla yapılabilmelidir.

8.5.9.4 Politikanın Uygulanması

Güvenlik politikası uygulanmadan önce aşağıda belirtilen şartlar sağlanmalıdır.

- Kurumların yazılı bir güvenlik politikasına sahip olduktan sonra yapmaları gereken, bu güvenlik politikasının düzenli olarak kullanımını sağlayarak günlük hayatın bir parçası haline getirmektir. Güvenlik politikası, mümkün olduğunca çok kişinin katılımı ile oluşturulmalıdır.

- Kurumların güvenlik ortamlarının bazı nedenlerle birbirinden kopuk ve parçalı hale gelmesi ve bunun sonucunda herbir bölüm için ayrı politikaların oluşturulması, bir zorunluluk haline gelebilir. Farklı güvenlik politikalarının beraber çalışabilmeleri ise bu politikaların bazı standartlara sahip olma zorunluluğunu doğurur. Politika standartlarına "örnek olarak IETF'in "Security Policy Specification Language" (SPSL), Sun Systems'in "Generic Security Services API" (GSSAPI) ve "Pluggable Authentication Modules" (PAM) verilebilir(Şengonca vd.Teke, Karaarslan 2006, syf.7)

- Politikanın uygulanması noktasındaki dikkat edilmesi gereken bir diğer nokta da, güvenlik politikalarının yönetimce onaylanarak yürürlüğe sokulması ve bunun tüm birimlere duyurulmasıdır. Bu duyuru açıklayıcı nitelikte, net ve yönlendirici olmalıdır. Güvenlik politikalarına erişim ise, internetten erişimi de içine alacak biçimde çalışanların kolay erişimine olanak vermelidir.

Güvenlik matrisinde özellikle risk düzeyi yüksek tanımlanan sistemlerin, herhangi bir nedenle devre dışı kalması durumunda ne tür önlemlerin alınacağı, oluşturulacak acil durum planı ile belirlenmeli ve her türlü duruma karşı sistem yedeklemesi düzenli olarak yapılmalıdır. Politikaların uygulanması noktasında korunacak tüm nesneler için gerekli teknik yapılanma ve ayarlamalar yapılmalıdır. "Örneğin güvenlik matrisinde oluşturulan erişim kuralları ve hangi sunuculara hangi protokoller üzerinden erişilebileceği güvenlik duvarı veya erişim listeleri (access -list) yöntemleri kullanılarak oluşturulmalıdır. Fakat daha önemlisi ayarlanan güvenlik sistemleri sık sık sınanmalı, risk haritası çıkarılmalı, sistemin zayıf noktaları saptanıp gerekli önlemler alınmalıdır. Kayıtların incelenmesi ile güvenlik politikasının amacına ulaşıp ulaşmadığı anlaşılabilir(Şengonca vd.Teke, Karaarslan 2006, syf.8)

Şekil 8.23 Bilgi Güvenliği Politikasının Oluşturulması (Pekol, Kurumlarda Bilgi Güvenliği Politikaları, 2005)

8.5.9.5 Kurumsal Güvenlik Standartı

"BS 7799/ISO 17999, ürün ve hizmetlerin kalitesini geliştirmeye yönelik standartlar oluşturan ve bağımsız bir kuruluş olan İngiliz Standartlar Enstitüsü (BSI) tarafından belirlenmiş bir global bilgi güvenliği standardıdır. Bu standarda güre, bilgi güvenliğinin sağlanması için, gizlilik, bütünlük ve erişilebilirlik özelliklerini içinde barındıran bir sistem kurmak gerekir. BS 7799/ISO 17999, bilgi güvenliği yönetim standartlarının yanı sıra organizasyonda bilgi güvenliğini oluşturma ve uygulamada izlenecek yolları ortaya koyar."(http://www.innova.com.tr)

8.6 Ekonomik Bilgi Savaşı

Ekonomik savaş kavramı, bilgi sistemleri ile ekonomik unsurla rın bir bileşkesi olarak ortaya çıkmaktadır. Bilginin en önemli ekonomik güç olduğu günümüzde, bilginin satışı ve bilgiye erişim ülkelere yüklü miktarda ekonomik değer olarak yansımaktadır. Dolayısıyla herhangi bir ülkenin ekonomik bilgi sistemlerine erişiminin engellenmesi, ülkelerin ekonomik çöküntü içerisine girmelerine sebep olabilecektir.(Ünal ve Yarman, 2002, sy.217)

Ekonomik savaş öncelikle bilgi blokajı ve daha sonra da bilgi emparyalizmi ile yapılır. Ekonomik bilgi blokajı, önemli bilgi materyalini n aralıksız akışına dayanmaktadır. Bir bilgi barajı bir ülkenin uluslar arası haberleşmeye erişimini engeller. Örneğin o ülkenin uluslar arası finansal işlemleri mümkün olmaz.

Ekonomik bilgi blokajı etkinin şiddet olmadan yaratılmasıdır. Bilgi ve uzmanlığ ın internet içindeki ticareti, ekonomik bilgi blokajına günümüzde daha da farklı bir boyut getirmektedir. Bilgi emperyalizmi "ekonomi savaştır" fikrine dayanmaktadır.(Ahvenainen, 2000, sy.24-25)

Libicki'de kendi ifadesiyle "ekonomik savaşın bilgi savaşı il e olan evliliğini", daha önce bahsettiğim bilgi blokajı ile bilgi emperyalizmi olarak 2 şekilde tanımlamaktadır. Bunlar. Libicki, bilgi akışı ve erişimi kesilmiş devletlerin ayakları üzerinde duramayarak ağır tahribatlara uğrayacaklarını ifade etmektedir. (Libicki, 1995, Sy.67)

Ekonomik Bilgi savaşıyla ilgili bir diğer tanımda; "bilgi ticaretinin gerçekleşmesi için bilgi ekonomilerine karşı yapılan savaştır. Devlet politikasının bir aracı olarak ticarette kullanılan bilginin manipülasyonunu içerir."şeklinde dir. (Sağsan, 2002, sy.229)

Özetle; ekonomik bilgi savaşı ekonomide kullanılan bilgi girişinin kesintiye uğratılması ya da engellenmesi suretiyle karşı tarafın zarara uğratılmasını amaçlamaktadır. Bir ülkenin ekonomisinin lokomotifi olarak değerlendirilen sektörüne ait bilgiler o ülke için hayati, önem taşımaktadır. Dünyada birçok ülke dış ticaretini belirli kalemde malların satışı üzerine dayandırmaktadır. Bazı ülkeler sadece yer altı zenginliklerini bazıları ise sadece gıda, yas sebze ve meyve gibi ürünleri ihraç edebilmektedir. Bu ülkeler için belirli sektörlere ait bilgiler hayati önem taşımaktadır. "Dünyada o alanda doğru veya yanlış çıkan haberler, dedikodular, istatistikler, sağlığa veya diğer sektörlere etkileri gibi yayınlar ülke dış ticaretini ve dolayısı ile ekonomisini doğrudan etkileyebilmektedir."(Erdal, sy.9)

Batılıların, azgelişmiş ülkelerdeki ulusçu eğilim ve hareketlere karşı olmaları, ekonomik yapılarından kaynaklanan bir zorunluluktur. (Aydoğan, 2002, sy.303)

Ülkelerin, çağımızda yeniden şekillenen savunma ihtiyaçları, sadece askeri anlamda duyulan ihtiyaçlar olmaktan çıkarak, devletlerin faaliyet gösterdiği her alandaki yabancı girişimlere karşı, bu alanların savunulmasını gerektiren bir yapıya bürünmüştür.(Miman, 2007, sy.27)

Çağımızdaki hızlı değişim ve tehdit kavramının farklılaşması, ülkelerin ekonomik değerlerinin, küresel rekabet ortamında başka ülke şirketleri tarafından satın alınmasını, ulusal güvenliği tehdit eden girişimler olarak kabul edilmektedir.

Türkiye'de özellikle son dönemde Tüpraş, Ereğli Demir Çelik, Türk Telekom ve benzeri pek çok örnekte de olduğu gibi, stratejik düzeyde önemli olan kuruluşların özelleştirme süreçlerinin de, ulusal güvenlik boyutunda bazı tartışmalara yol açtığı görülmektedir. Burada tartışılan esas nokta Türkiye'nin bir biçimde bağımlılığının çok uluslu şirketlerin eline geçmesi ve bu yabancı güçlerin Türkiye ekonomisini yönlendirme, istedikleri gibi düzenleme yapabilme, kendi önceliklerini gerçekleştirme ihtimalleri bile milli güvenlik açısından ürkütücü olmasıdır.

Ekonomik yaptırımlar, finansal dengesizlikler, ham maddelerin akışı, yerel döviz kurlarındaki spekülasyonlar ve birçok değişik bağımlılıklar günümüzün potansiyel tehlikeleri olarak karşımıza çıkmaktadır. Komşu ülkeler tarafından bilinçsizce, istemeyerek bile olsa yapılan bir takım ekonomik suistimaller, pazar kayıplarına yol açabilmekte bu durum bazen ekonomik açıdan tehlikeli bir hal alabilmektedir. Bu nedenle ekonomi ile güvenlik arasındaki bağ daha güçlü bir hale gelmiştir. (Miman, 2007, sy.34)

Örneğin, son olarak yaşadığımız ekonomik krizle ilgili Umur Talu'nun 08.01.2000 tarihinde köşesinde belirttiği şu olaya değinmek istiyorum. Talu köşesinde, "Milattan sonra bir gün" adlı yazısında, Zekeriya Temizel'in, Ertuğrul Özkök'le yaptığı bir röportajında, krizin Amerika merkezli iki bilgisayar korsan fonunun bir milyar dolar çekmesi ile başladığını söylemesine dikkat çekmektedir. (Umur Talu, Milliyet Gazetesi, 08.01.2000)

Bu röportaja Emin Demirel'de dikkat çekmekte ve bu korsan fonların çektiği bir milyar doların yarattığı tedirgin hava ile, tetiklenen ikinci bir psikolojik dalganın, bunun da bankalar arasında ve sonra da borsada yarattığı etki ile de krizin yaşanmasına neden olduğuna değinmektedir.(Demirel, 2004, sy.115)

Bu durum aslında ekonomik bir saldırı niteliği taşımaktadır. Çünkü bu krizin ülkemizde yarattığı etkileri anımsamamak mümkün değildir.

Ekonomik ve askeri amaçlar dahil olmak üzere ulusal güvenlik gerekçesiyle bilgiye ulaşmanın ve saklamanın önemi, çağımızda bilgisayar ve uydular kanalıyla

ayrı bir değer kazanmış, belki de istihbari çalışmalar da yön değiştirmiştir. Teknolojiyi bilen uzmanlar eliyle istihbarat yapmak, klasik anlamdaki istihbarat elemanlarının da niteliği ve tanımını değiştirmiştir.(Demirel, 2 004, sy.36)

Jan Leijonhielm'in "Ekonomik İstihbarat İhtiyacı" makalesinde değindiği gibi "ekonomi günümüzde olduğu gibi gelecekte de güvenlik politikalarını etkilemeye devam edecektir. Gelişmiş ülkeler için ekonomik enstrümanları kullanarak güvenlik politikalarını sağlamlaştırma çabaları, bu şekilde daha verimli ve güvenli olacaktır. Bu durumun ekonomik istihbarat üzerindeki talebi arttıracağı söylenebilir. "(Miman, 2007, sy.34)

Ekonomik istihbaratla ilgili bir örnek, Almanya'da yaşanmıştır. 1999 yılı başla rında Alman istihbarat teşkilatı, geliştirmeye çalıştığı Eurofighter adlı uçağa ait sırların, son dönemde prestij kaybeden ancak yatırımlarının tamamını ekonomik istihbarata ayıran Rus istihbarat teşkilatınca çalındığı istihbaratıyla şok olmuştur. Olayın derinlemesine araştırıldığında Ruslar'ın bunu İsrail ile yaptıkları ortak bir çalışma sonucu gerçekleştirdiği anlaşılsa da, bu aslında teknoloji istihbaratı ile ekonomik bir saldırıya dikkat çekmektedir. Nitekim bu tür olaylar da Alman ekonomisine her yıl en az 21 milyar dolar zarar verdiği belirtilmektedir. (Demirel, 2004, sy.111 -112)

8.7 Siber Savaş

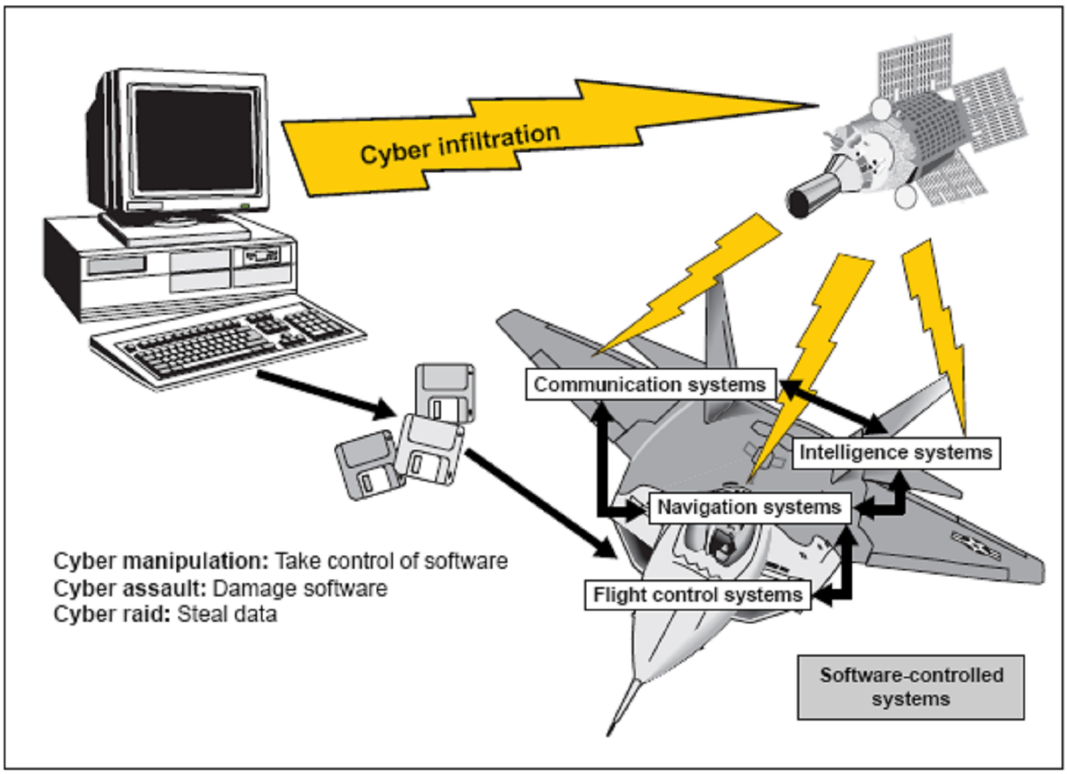
"Siber savaş, bilgi ile ilişkili ilkelere göre askeri operasyonların yürütülmesi anlamına gelmektedir. Siber savaş ile düşman birliklerinin bilgi ve il etişim sistemlerinin kesilmesi ve yıkılması amaçlanmaktadır. Başta komuta kontrol olmak üzere, istihbarat toplamak, işlemek ve dağıtmak; dost veya düşman birliklerini tanımak, pozisyonlarını saptamak gibi taktik iletişimlerini belirlemek ve akıllı silah sistemleri gibi farklı teknolojileri içermektedir. Siber savaşın mahiyetinde, düşmanın bilgi ve iletişim devreleri içerisine zorla veya izinsiz olarak girerek dezenformasyonun yayılmasını elektronik olarak çökertmek vardır." Saldırı amaçlı

yapılan bu savaşta, bilgi savaşçıları düşmanın bilgi merkezlerine (bilgisayar ağlarına, haber kanallarına) ani ve kesin saldırılar yaparlar."(Sağsan, 2002, sy.110)

Siber kelime olarak insan yerine mekanik ya da elektronik sistemlerin kullanılmasını ifade etmektedir. Burada kilit kontrol elemanı yazılımlardır. Siber savaşlar hedefe kansız, şiddetsiz uygulanarak ulaşılan yazılım yoğunluklu sistem savaşlarıdır. (Alford, 2000, sy.101)

Siber savaş, bilgisayarların askeri ve ya hükümet içerisinde artan kullanımıyla hem ulusal hassasiyetler hem de düşmana saldırı bakımından yeni bir savaşı ifade etmektedir. Siber savaş ateş açmadan bir butona basılması suretiyle düşmanın haberleşme sistemini yıkma ya da durdurmayı ifade etmektedir. Bu savaşta daha ucuz bir saldırı yöntem olan dizüstü bilgisayarlar kullanılmaktadır. (Coughlan, 2003, sy.7)

Örneğin aşağıdaki şekilde izah edildiği gibi siber anlamda yapılacak hile, baskın ve saldırı ile bir uçağın haberleşme, yönlendirme, kontrol ve istihbarat sistemleri etkisiz hale kolaylıkla getirilebilmektedir. Ancak siber saldırıların ulusal tüm değerlere, alt yapılara yapılabileceği unutulmamalıdır.



Şekil 8.24 Siber Savaş Örneği (Alford, 2000,sy.104)

Siber saldırılar "Bilgi terörizmi", "semantik saldırılar", "simüle edilmiş savaş stratejileri", "gelecek senaryoları" ve "sanal karakterlerin kullanımı" gibi temel referans kaynaklarıyla tanımlanır. (Murat Erdal, Teknoloji ve Ulusal Güvenlik, sy.10)

Terörizm bir yönetimi(devlet) veya bir topluluğu, korkutmak veya baskı amaçlı, sosyal ve siyasi amaçlara yönelik olarak insanlara veya mülkiyete karsı kanunsuz güç ve şiddet kullanımıdır (FBI). Siber terörizm ise klasik terörizm amaç ve hedeflerine ulaşmada bilişim teknolojilerinden faydalanılmasını ifade etmektedir. (Murat Erdal, Teknoloji ve Ulusal Güvenlik, sy.11)

“FBI, Siber terörizm‘i şu şekilde tanımlamaktadır;

- Gizli ajanlar yada ulus-altı gruplar tarafından,
- Muharip olmayan hedeflere karşı zor kullanma ile
- Kasıtlı ve politik amaçlı olarak,
- Bilgi, bilgisayar sistemleri, bilgisayar progr amları ve verilere yapılan saldırıdır.
- Siberterörizmin normal “hack” işlemi ile arasındaki fark “politik” bir amaç taşımasıdır.”(Baykal, Bilgi Teknolojisinin Ulusal Güvenlik ve Ulusal Güvenlik Stratejisi ile İlgili Boyutu, sy.9)

Semantik saldırıla rda güvenlik, ağı dinleyen bir saldırganın, aynı düz metnin birden fazla şifreli kopyasını aldığında dahi bunlardan düz metin hakkında herhangi bir bilgi edinememesini, alıcı ve gönderen arasında paylaşılan ve her mesaj alış-verişinde artırılan bir sayaç s ayesinde gerçekleştirilmektedir. (Nar ve Bilgin, Askeri İşbirlikli Nesne Ağlarında Güvenlik, sy.10)

“Simülasyon sözcüğü bir şeyin benzeri veya sahtesi anlamında kullanılır. Teknik anlamda simülasyon; deneyim kazandırma ve deney yapma amacıyla modell erin kullanımıdır. Gerçek sistemin olmadığı, gerçek sisteme erişimin kolay olmadığı, gerçek sistemle deneyin yüksek maliyetli, tehlikeli veya rahatsız edici olduğu, analitik çözüm tekniklerinin var olmadığı veya zor olduğu, sistemin çok yavaş veya hızlı olduğu durumlarda simülasyon gerekli olur. İhtiyaç duyulan simülasyonların gerçekleştirilmesi için modeller geliştirilir.

Stratejik savaş oyunlarının tarihi incelendiğinde Çin‘de geliştirilen Wei Hai adlı ilk stratejik oyundan Go‘ya, Hindistan‘da ortaya çıka n Chaturanga‘dan modern satranca, Koenigspiel‘den Kriegspiel‘e, Little War‘dan günümüz stratejik oyunlarına kadar gelen bir gelişim süreci karşımıza çıkar. Günümüz stratejik savaş oyunları artık yöneylem araştırması, analitik oyun teorisi, Monte Carlo simü lasyonu, Lagrange çarpanlar metodu, matematiksel programlama ve sistem analizi tekniklerinin bilimsel

uygulaması haline dönüşmüştür. Bu süreç modelleme ve simülasyon sistemlerinin de tarihi gelişimidir aynı zamanda. Çünkü savaş oyunu, gerçek askeri güçleri n faaliyet göstermediği, olay sırasının muhalif tarafları temsil eden oyuncuların kararlan ile belirlendiği bir savaş modeli veya simülasyonudur.

Simülasyon sözcüğü bir şeyin benzeri veya sahtesi anlamında kullanılır. Teknik anlamda simülasyon; deneyim ka zandırma ve deney yapma amacıyla modellerin kullanımıdır. Gerçek sistemin olmadığı, gerçek sisteme erişimin kolay olmadığı, gerçek sistemle deneyin yüksek maliyetli, tehlikeli veya rahatsız edici olduğu, analitik çözüm tekniklerinin var olmadığı veya zor o lduğu, sistemin çok yavaş veya hızlı olduğu durumlarda simülasyon gerekli olur. İhtiyaç duyulan simülasyonların gerçekleştirilmesi için modeller geliştirilir.

Simülasyonun merkezi olan model; bir sistemin, fenomenin ya da sürecin fiziksel, matematiksel ya da mantıksal temsilidir. Pek çok simülasyon modeli bilgisayar tabanlıdır, ama olmayabilir de. Örneğin; Miniaturk gibi parklar da birer simülasyondur, bu parklarda ziyaretçiler farklı yerleri görmenin yapay deneyimini yaşarlar.

İkinci Dünya Savaşı'n da ortaya çıkan Yöneylem Araştırması disiplini, askeri operasyon planlarının optimize edilmesi için kullanılan çeşitli tekniklerle yıllar içinde gelişmiştir. Bu süreçte simülasyon da temel bir araç haline gelmiştir. Bilgi teknolojisi daha gerçekçi, daha fa rklı alanlarda kullanılabilecek simülasyon araçlarının önünü açmıştır. Modelleme ve simülasyon sistemlerinin yaygın olarak kullanıldığı önemli alanlardan biri askeri uygulamalardır.

Simülasyon sistemleri silahlı kuvvetlerin kullandığı bilgi sistemleri içi nde önemli bir yere sahiptir. Savunma alanında simülasyon sistemleri operasyonel planlama, eğitim, tatbikat, stratejik analiz, ürün tasarımı, tedarik, test ve değerlendirme gibi faaliyetlere destek sağlar.

Simülasyon sistemleri kuvvet kompozisyonu, silah etkinliği, lojistik hususunda ortaya çıkan problemleri incelemede kullanılır. Askeri harekâtların planlamasında, harekât esnasında ve sonrasında oluşturulan değişik senaryoların sınanmasını sağlar.

Birçok eğitim artık simülatörler aracılığıyla yapılıyor. Simülasyonların etkinliği doğru zamanda, doğru yerde, doğru kişiye, doğru bilgiyi sağlamada sunduğu intikal kabiliyetiyle ilgilidir. " (Macit, 2007)

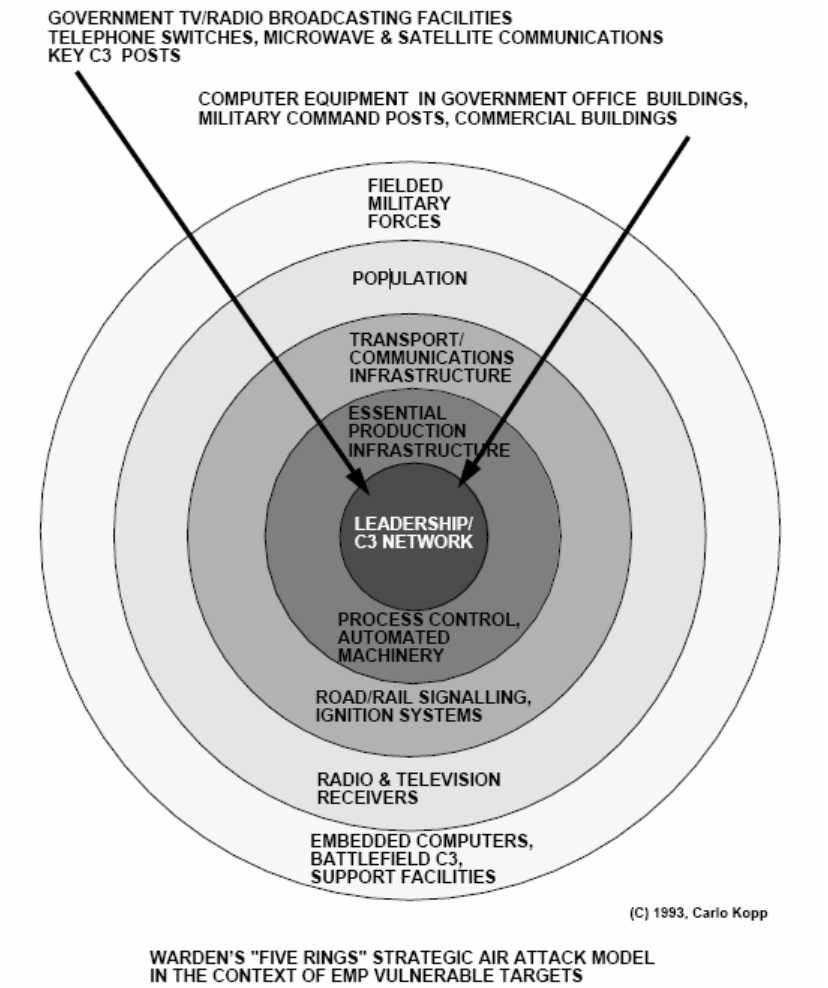
Gelecek senaryoları ise genel olarak içinde bulunan koşulların dengelere, zamana, ekonomik, istihbari, teknolojik, ekonomik, sosyal ve siyasi değişimlere göre planlanmasını ifade etmektedir. Devletler, stratejilerini oluşturma noktasında bu senaryolardan yararlanmaktadırlar.

8.8 Warden Modeli

Modern Stratejik hava saldırıları teorisi, Devletlerin savaşabilme yeteneklerini 5 merkezde tanımlayan Warden Modeline göre tanımlanmaktadır. Bunlar önem sırasına göre sırasıyla liderlik ve C3 destekleme yeteneği, hayati endüstrisi, taşıma ağı, nüfusu ve özellikleri ile askeri gücüdür.

Birinci halka ülkenin savaş mekanizmasını harekete geçirme ve savaşı sürdürebilme kabiliyetine sahip; hükümet, radyo-televizyon imkânları, telekomünikasyon sistemi, mikrodalga&uydu haberleşme sistemlerini ve hükümet binalarındaki bilgisayar donanımlarını, askeri yönetimi ve ticari binaları he def olarak göstermektedir.

İkinci halkada hedef düşman ülkenin hayati önem taşıyan ekonomik altyapısının tespitidir. Daha önce belirttiğim gibi bunların belirtilmesinde öncelikle bir liste oluşturulur.



Şekil.8.25 5 Halkalı Warden Modeli (Kopp, 1993, sy.9-10)

Özellikle yüksek seviyede otomasyon ve bilişim sistemlerince yönetilen ve bu sistemlerin kullanımının yoğun olduğu borsa, bankacılık sistemi gibi finansal yapılar enerji üretim dağıtım ve kontrol şebekeleri ile petro-kimya, metal işleme tesisleri oluşturulacak hedef listesinde öncelikli hedefler olarak değerlendirilmektedir. Bu listenin önceden yapılacak bir tespit ile yapılması önerilmektedir. (Özdemir tez!!!)

Üçüncü halkada özelikle bilgisayaralarca kontrol edilen hava, kara ve demiryolu sistemleri hedeftir.

Dördüncü halkada hedef ülkenin halkıdır. Yapılacak psikolojik harekâtlarla, daha önce bahsettiğim gibi özellikle medyanın kullanılmasıyla hedef halkın moralini azaltırken kendi kuvvetlerine moral sağlamaya çalışacaktır.

Son halkada ise savaş alanına sevk edilen askeri birliklerin komuta kontrol sistemleri ve taktik haberleşme sistemlerinin etkisiz hale getirilmesi ile aslında bir noktada elektronik harbide içine alacak biçimde yapılacak müdahaleleri içermektedir.

Elektromanyetik silahların Warden modeline uygun olarak kullanımı ilebilinen savaşlara göre daha az can kaybı ile savaşın icrası dünya kamuoyunda doğacak tepkileri azaltacaktır. Kuvvet tasarrufu sağlamasının yanında Stratejik Felç olarak adlandırılan etkisi ile düşmanın savaşma kabiliyetini olumsuz yönde etkileyecektir. Bilgi savaşının bu yöntemle kullanılmasıyla krizlerin sıcak savaş ortamına girilmeden çözümlenmesi daha kolay olacaktır.(Özdemir, 2003, sy.72)

Bu bakımdan stratejik felç de bilgi savaşının yöntemleri sınıfına girmek tedir.

8.9 Sayısal Bilgi Harekâtı

Sivil, askeri, politik, ekonomik yada kişisel amaçlarla, Kurum ve şahısların sahip oldukları tüm değer ve bilgilere izinsiz erişmek, zarar vermek, maddi/manevi kazanç sağlamak için bilişim sistemleri kullanılarak yapılan her türlü gizli hareket, "dijital saldırı" olarak tanımlanabilir.(Özavcı, Bilgi Sistemleri Güvenliğine Giriş, 2001)

Uluslararası konjüktürün uygun olmaması durumunda bilgi savaşının uygun hedefleri doğrultusunda belirli hedeflere üstü örtülü olarak kolaylıkla uygulanabilir. Devre dışı bırakma, zayıflatma, aldatma, istismar etme amaçlarına uygun olarak icra edilebilir.

Devre dışı bırakma; hedef alınan bilgi sistmeminin kullanımının yazılımsal veya donanımsal olarak kullanılacak zararlı yazılımlar vasıtasıyl a devre dışı bırakılmasıdır.(Özdemir, 2003, sy.73)

Zayıflatma; Örneğin, TCP Protokolüne Yönelik Saldırılarda anlattığım "İstek (Syn) Bombardımanı" konusunda bahsettiğim gibi, Sunucuya onun başedemeyeceği kadar taklit edilen sahte ip datagram istek paketler i gönderilmesi durumun da sunucu işlevlerini yerine getiremez ve yeni bir bağlantı da artık yapılamaz hale gelirdi. İşte bu ve daha önce anlattığım pek çok saldırı yönteminde olduğu gibi hedefin işlevleriniyerine getirilmesinin engellenmesi, performansının düşürülmesi "zayıflatma" amaçlı olarak yapılmaktadır.

Aldatma; Hedefe ya da düşmana ait bilginin değiştirilerek onu doğru bilgiymiş gibi işleme sokmasının sağlanması, bilginin yanlış yönlendirilmesi ya da geçersiz kılınması "aldatma" amaçlı olarak yapılan müdahalelerdir. Bu, rakip bir firmaya uygulanarak onu maddi ve manevi zararlara sokma amaçlı uygulanacağı gibi komuta kontrol ya da elektronik harp amaçlı olarak da kullanarak askeri olarak da değerlendirilebilir.

İstismar Etme; Yazılımsal saldırılar bölü münde değinildiği gibi bu zararlı yazılımların sisteme çalışması sırasında olabileceği gibi yapım aşamasında da sokularak sistemden bilgi sızdırılması "istismar etme" olarak adlandırılır.

Kimi zaman zevk için yazılmış birkaç satır kod, kimi zaman sistemini ze sızmak için fırsat arayan küçük bir program, ya da ustaca hazırlanmış bir elektronik postanın getireceği maddi ve manevi zararlar beklenmedik ölçülerde olabilmektedir. Kaybolan, bazen günlerce süren bir emek oluyor, bazen yılların arşivi, bazen bilgisayarınızda sakladığınız en mahrem sırlarınız, bazen de boşaltılmış bir banka hesabı hatta ve hatta ulusal güvenliği tehlikeye atabilecek riskler.(Daşkıran, 2005, syf.3)

Bir bilgisayara ya da sisteme sızma yöntemlerinden ilki, bu bilgisayarın kullandığı bir yazılımın içine konulan ve portlarında bir açık vererek bu bilgisayara sızmayı mümkün kılan programlardır.

Başka bir yöntem bilgisayarın şifresini ele geçirmek, bir diğer yöntemse kullanılan bilgisayara, belirli bir zamanda kullanılmak üzere, ürün ku llanıcının eline geçmeden hatta üretim aşamasında yerleştirilen, üzerindeki veriyi kopyalayan ya da belirtilen bir zamanda portlarını açan yazılımlardır.

Saldırı mimarilerinde değindiğim gibi sızma, genellikle keşif ve taramadan sonra yapılan, kalıcılığı sağlama yönünde yapılacak müdahalelerle daha ad etkin hale getirilebilecek saldırı yöntemidir.

Bu saldırılara karşı alınabilecek korunma yöntemleri daha önceki konularda ayrıntılı olarak anlatılmıştır. Ancak güvenlik noktasındaki can alıcı noktanın “siste min güvenliğinin en zayıf halkası kadar” olduğu ve sistemin korunmasının bir bütün içinde değerlendirilerek uygulanması gerekliliğidir.

9 ÖNEMLİ TEKNOLOJİ ve SİSTEMLER

9.1 Kriptografi

Şifreler özellikle çağımızda bilgilerin korunması, saklanm ası, iletilmesi ve değerlendirilmesi bakımından oldukça önemlidir. Şifreleme sistemleri önemleri bakımından, tarihin akışında bile çok önemli değişiklikler meydana getirmişlerdir. Bu değişiklikler ise, bazen çok önemli bir şifrenin çözülmesiyle bazen de bu şifrelerin çözülememesi neticesinde yaşanan yıkımlarla kendini göstermiştir.

Şifreleme için tarih boyunca çok çeşitli yöntemler denenmiştir. Kripto tarihçisi David Kahn'a göre ilk kriptografik belgeler yaklaşık M.Ö 1900 yılında yazıldığı tahmin edilen hiyerogliflerdir. Yine M.Ö 1500 yıllarında yaşayan Yeremya Peygamber'de atbash şifreleme yöntemini kullanmıştır.(Akyıldız ve ark. Çimen, Akleylek, 2007, sy.13–14)

"En basit tanımıyla kriptografi, mesajın harflerin değiştirilmesi ile içeriğinin gizlenmesi işlemidir. (Kalaycı, 2003, sy.19)

Şifrelemede kullanılan bazı tanımladeğinecek olursak;

- Orijinal mesaj "plaintext" olarak adlandırılırken kodlanmış mesaj "ciphertext" olarak adlandırılır.

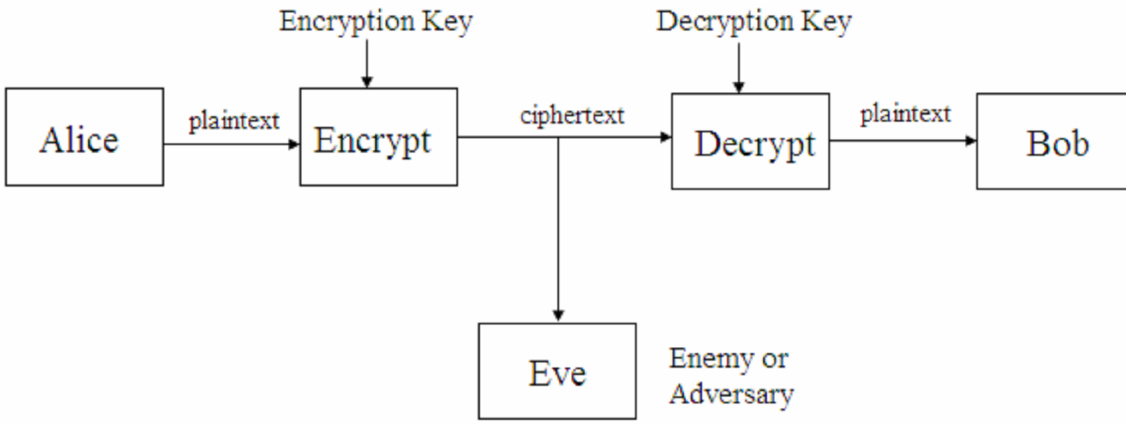
- Metnimizin şifreli metne dönüştrülmesi işlemine şifreleme ya d a "encryption", şifreli metnin tekrar tekrar normal metnimize dönüştürülmesi işlemine de deşifreleme ya da ingilizce'deki karşılığı olarak "decryption" denilir.

- Pekçok yöntemin kullanılmasıyla mesajların şifre ve deşifre edilmesiyle uğraşan bilim Kriptogr afidir.

- Bu yöntemlerin her biri ise Cipher ya da kriptosistem olarak adlandırılır.

- Şifreleme hakkında hiçbir bilgi olmadan şifrenin çözülmesi işlemine kriptoanaliz denilir.

- Kriptoanaliz ve kriptografi birlikte kriptoloji olarak adlandırılır.(Stallings, 2003, sy.24)



Şekil 9.1 Temel Haberleşme Senaryosu (Urhan ve ark. Zengin, Şanlı, sy.2-3)

Yukarıda gösterilen temel haberleşme sistemine göre Alice ile Bob arasındaki haberleşmeyi ele geçirmeye çalışan Eve, yalnızca şifrelenmiş mesaja ulaşabilecektir. Oysa şifreleme olmasaydı Eve direk olarak mesajı ele geçirebilecekti.

Kriptografi genel olarak daha önce anlattığım; gizlilik, bütünlük, reddedilemezlik ve kimlik belirleme (authentication) konularıyla ilgilenir.(Bektaş, 2006, sy.2)

Elektronik haberleşmedeki tehditlere karşı alınabilecek tedbirler, kullanılabilecek yöntem ve araçlar aşağıda görülmektedir.

Gizlilik sağlamak için veri şifreleme, Bütünlük sağlamak için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar, Kimlik doğrulaması için öz etleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar, sertifikalar, İnkâr

edememezlik için sayısal (elektronik) imzalar, işlem kayıtları, Süreklilik için yedek sistemler, bakım, yedekleme, alternatif haberleşme kanalları kullanılır.(http://www.kamusm.gov.tr/)

Şekil 9.2 Tehditlere Karşı Alınacak Tedbirler (Erol, 2004, sy.10)

M.Ö. 400 yıllarından başlayarak 1976 yılına kadar geçen yaklaşık 2500 yıllık bir süreçte; şifreleme ve deşifreleme işlemlerinde aynı anahtarın kullanıldığı Simetri k Kriptosistemler kullanılmıştır. Başlıca Simetrik Kriptosistemler; Yerine -koymalı (Substitution), Yer-değiştirmeli (Transposition), Yerine-koymalı ve Yer-değiştirmeli sistemlerin birleşiminden oluşan Ürün (Product), Akış (Stream) ve Blok (Block) kriptosistemler olarak sayılabilir (Koltuksuz, 1995)

Şifrelemeyle ilgili prensipleri ilk olarak, 1883 yılında Alman dil bilimci Kerckhoff, yayınladığı La Cryptographie Militarie adlı eserinde yazılı hale getirmiştir. Adıyla anılan prensibe göre; Bir sistemin güvenl iği kripto algoritmasına değil anahtara bağlı olmalıdır. Çünkü eğer algoritma ele geçirilirse anahtar olmadan bilgi ele geçirilemez,

anahtar ele geçirilirse bile bu anahtarın değiştirilmesine kadar işe yarar ki bu da uzun süreli olmaz.(Sight, Code Book)

Kerckhoff'un diğer prensipleri ise şunlardır:

1. Sistem pratik ve matematiksel bir temele dayanmalı
2. Sistem gizliliğe dayanmamalı. Yani sistem hakkındaki her şey herkes tarafından bilinmeli.
3. Sistemde kullanılan anahtarlar taraflar arasında kolayca, üçüncü kişini n değiştirilmesine izin verilmeden değiştirilebilmeli
4. Sistem telgraf uygulamasında kullanılmalı
5. Sistemin kullanılabilmesi için fazla sayıda insana ihtiyaç duyulmamalı(Akyıldız ve ark. Çimen, Akleylek, 2007, sy.44)

9.1.1 Şifrelemenin Tarihçesi

Kriptoloji çok eski çağlardan beri insanoğlu tarafından kullanılmaktadır. Bu tarihçeye kısaca şöyle özetlenebilir:

- MÖ.1900 dolaylarında bir Mısırlı kâtip yazdığı kitabelerde standart dışı hiyeroglif işaretleri kullandı.
- MÖ.60–50 Julius Caesar (MÖ 100–44) normal alfabedeki harflerin yerini değiştirerek oluşturduğu şifreleme yöntemini devlet haberleşmesinde kullandı. Bu yöntem açık metindeki her harfin alfabede kendisinden 3 harf sonraki harfle değiştirilmesine dayanıyordu.

- 725–790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, kriptografi hakkında bir kitap yazdı (Bu kitap kayıp durumdadır). Kitabı yazmasına ilham kaynağı olan, Bizans imparatoru için Yunanca yazılmış bir şifreli metni çözmesidir. Abu Abd al -Rahman, bu metni çözmek için ele geçirdiği şifreli mesajın başındaki açık metni tahmin etme yöntemini kullanmıştır

- 1000–1200 Gaznelilerden günümüze kalan bazı dokümanlarda şifreli metinlere rastlanmıştır. Bir tarihçinin dönemle ilgili yazdıklarına göre yüksek makamlardaki devlet görevlilerine yeni görev yerlerine giderken şahsa özel şifreleme bilgileri (belki şifreleme anahtarları) veriliyordu

- 1586 Blaise de Vigenère(1523–1596) şifreleme hakkında bir kitap yazdı. İlk kez bu kitapta açık metin ve şifreli metin için otomatik anaht arlama yönteminden bahsedildi. Günümüzde bu yöntem hala DES CBC ve CFB kiplerinde kullanılmaktadır

- 1623'de Sir Francis Bacon, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan stenografı buldu

- 1790'da Thomas Jefferson, Strip Cipher makinesini geli ştirdi. Bu makineyi temel alan M-138-A, ABD donanmasının 2.Dünya savaşında da kullandı

- 1917'de Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan "one-time pad"'i buldular

- 1920 ve 1930'larda FBI içki kaçakçılarının haberleşmesini çözebilmek bir araştırma ofisi kurdu

- William Frederick Friedman, Riverbank Laboratuarlarını kurdu, ABD için kriptoanaliz yaptı, 2. Dünya savaşında Japonlar'ın Purple Machine şifreleme sistemini çözdü

- 2. Dünya savaşında Almanlar Arthur Scherbius tarafından icat edilm iş olan Enigma makinasını kullandılar. Bu makine Alan Turing ve ekibi tarafından çözüldü.

- 1970'lerde Horst Feistel (IBM) DES'in temelini oluşturan Lucifer algoritmasını geliştirdi.

- 1976'da DES (Data Encryption Standard), ABD tarafından FIPS 46(Federal Information Processing Standard) standardı olarak açıklandı.

- 1976 Whitfield Diffie ve Martin Hellman Açık Anahtar sistemini anlattıkları makaleyi yayınladılar.

- 1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman: RSA algoritmasını buldular.

- 1985'de Neal Koblitz ve Victor S.Miller ayrı yaptıkları çalışmalarda eliptik eğri kriptografik (ECC) sistemlerini tarif ettiler

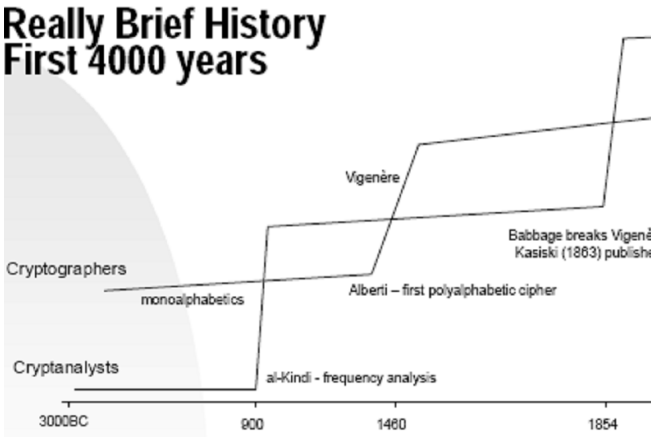
- 1990'da Xuejia Lai ve James Massey: IDEA algoritmasını buldular.

- 1991'de Phil Zimmerman: PGP sistemini geliştirdi ve yayınladı

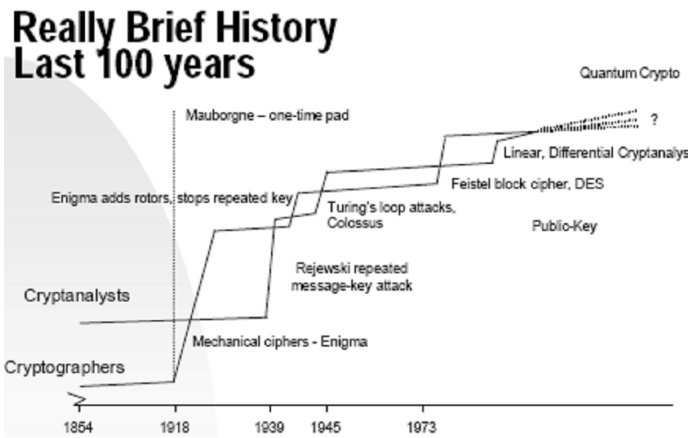
- 1995'de SHA–1 (Secure Hash Algorithm) özet algortiması NIST tarafından standart olarak yayınlandı.

- 1997'de ABD'nin NIST (National Institute of Standards and Technology) kurumu DES'in yerini alacak bir simetrik algoritma için yarışma açtı.

- 2001'de NIST'in yarışmasını k azanan Belçikalı Joan Daemen ve Vincent Rijmen'e ait Rijndael algoritması, AES (Advanced Encryption Standard) adıyla standart haline getirildi.(http://www.kamusm.gov.tr)



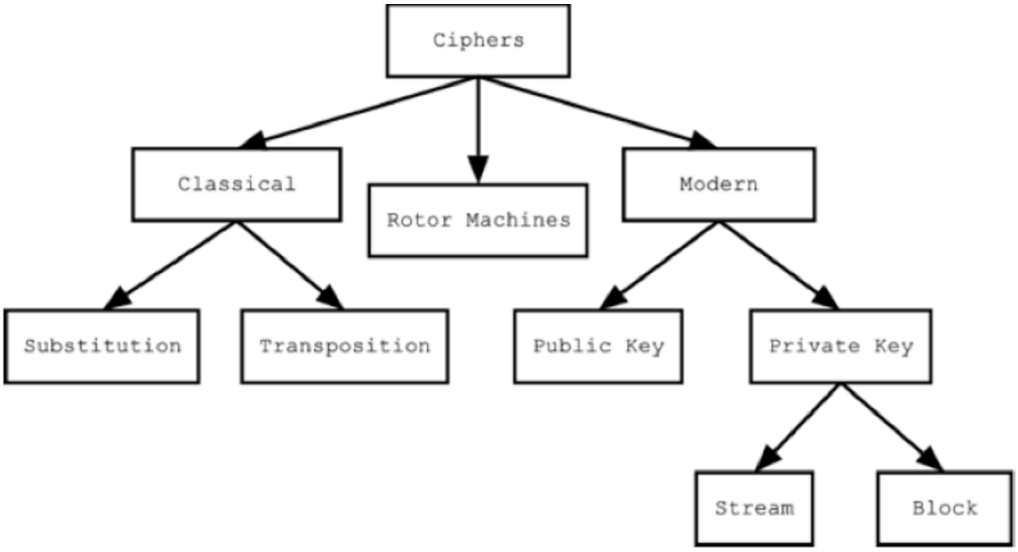
Şekil 9.3 İlk 4000 Yılında Kriptografi (Fleisch, 2001, sy.2)



Şekil 9.4 Son 100 Yıllık Süreç (Fleisch, 2001, sy.3)

9.1.2 Bazı Şifreleme Yöntemleri

Şifreleme yöntemlerini klasik, rotor makineli ve modern olmak üzere 3 başlık altında sınıflandırabiliriz. Klasik yöntemler yerine koyma ve yer değiştirme; Modern yöntemleri ise Açık anahtarlı sistemler ve özel anahtarlı sistemler olmak üzere sınıflandırabiliriz. Rotor makineler özellikle 2. Dünya Savaşında etkili olmuşlardır ve en önemli örneği de enigma makinesidir.



Şekil 9.5 Şifreleme Yöntemleri

Skytale: Skytale ilk askeri şifreleme sistemi olması bakımından önemlidir. Aşağıdaki şekilden de görüleceği gibi uzun bir parşömen ya da papirusa yazılı mesaj silindirik bir sopa etrafında sarılıyordu. Şerit açıkken hiçbir anlamı olmayan harf dizileri aslında o şeride sarılıyken her bir satırda var olan şifreli metinleri oluşturuyordu.(Akyıldız ve ark. Çimen, Akleylek, 2007, sy.16)

Şekil.9.6 Skytale (Sight, Code Book)

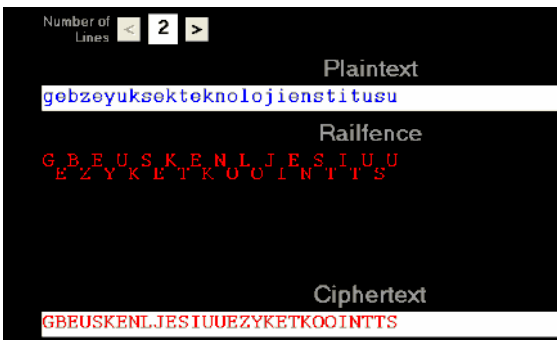
Polybius: Tablodan da anlaşılacağı gibi A=11, B=12, C=13, D=14, E=15, F=21....Z=55 şeklindedir. Burada yazılan her harf yerine bu harfin karşılığı olan iki rakamlı değeri yazılır. Yalnız unutulmaması gereken ilk rakamın satırı ikinci rakamın sütunu gösterdiğidir.(sy.20)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Şekil.9.7 Polybius

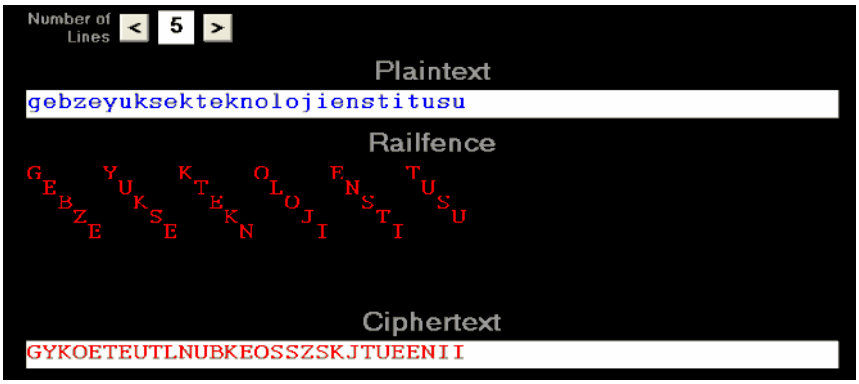
Railfence: Bir yer değiştirme şifreleme sistemi olan railfence'de; satır sayısının arttırılması şifreli metni daha güvenli hale getirir. (Sight, Code Book)

Örneğin iki satırlı sistemde "GEBZEYUKSEKTEKNOLOJIENSTITUSU" için yapılan kodlama aşağıdaki gibi olacaktır. Şifre metin ise "GBEUSKENLJESIUUEZYKETKOOINTTS" şeklindedir.



Şekil 9.8 2 Satırlı Railfence Uygulaması (Simon Sight, Code Book, 2004)

5 satırlı sistemde ise şifre metin aşağıda da gösterildiği gibi; GYKOETEUTLNUBKEOSSZSKJTUEENII biçimindedir.



Şekil 9.9 5 Satarlı Railfence Uygulaması (Sight, Code Book)

Görüldüğü gibi 2 satırlı metni çözmek diğerine göre daha kolaydır.

Örnek kelimemiz 29 harften oluşmaktadır. Eğer iki satırlı sistem kullanılmışsa bir satırda 15 diğerinde 14 harf olduğu kolaylıkla anlaşılacaktır. Yani, şifre metin GYKOETEUTLNUBKEOSSZSKJTUEENII olduğunda diğer denemeleri atlayarak şifre;

G Y K O E T

E U T L N U

B K E O S S

Z S K J T U

E E N I I şeklinde çözülmüş olacaktır.

Sezar Şifresi: "2000 yıl önce Julius Caesar ordusunun generalleri ile haberleşirken mesajlarında alfabedeki harflerin yerlerini değiştirmiştir. Caesar Cipher (Sezar

şifresi) olarak bilinen bu yöntemde harflerin yer değiştirme sayısının K=3 olduğunu duruma alfabedeki harfler aşağıda verilen şekilde şifrelenecektir. Dikkat edilirse harfler 3 kez sola kaydırılmıştır.” (Urhan ve ark. Zengin, Şanlı, sy.1)

1 4 3 5 6 2

Şifrelenecek harf (Plaintext) : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Şifrelenmiş harf (Ciphertext) : DEFGHIJKLMNOPQRSTUVWXYZABC

BULENT ↔ EXOHQW

Frekans Analizi: Dünya’da aynı alfabenin kullanıldığı bütün dillerde her harf aynı sıklıkla kullanılmamaktadır. Örneğin Latin alfabesini kullanan İngilizce ile Türkçe’yi düşündüğümüzde Türkçe’de en fazla kullanılan harf A iken İngilizce’de E’dir. Bu bakımdan frekans analizi yapılacak metnin dilinin belirlenmesi öncelikli iştir.(Akyıldız ve ark. Çimen, Akleylek, 2007, sy.30)

Ancak harflerin kullanım sıklıklarını kullanarak yapılan çözümler de her zaman doğru sonuç vermeyebilir. Bunun için harf ikilileri ya da üçlülerine bakılması işimizi kolalaştıracaktır. Türkçemizde en çok karşılaşılan harf ikilileri İN, AR, LA, AN, ER, İR,LE, DA, Bİ, DE, MA, KA, İL, AK, ME iken, üçlülerde DEN, NDA, RİN, ERİ, DAN, AMA, İNİ, ADA, NDE’dir. Bunun yanında dilin kendine özgü kuralları da şifreli bir metnin çözümünde kolaylık sağlayacaktır. Buna dilimizdeki büyük ve küçük ünlü uyumları örnek olarak verilebilir.(Akyıldız ve ark. Çim en, Akleylek, 2007, sy.32-33)

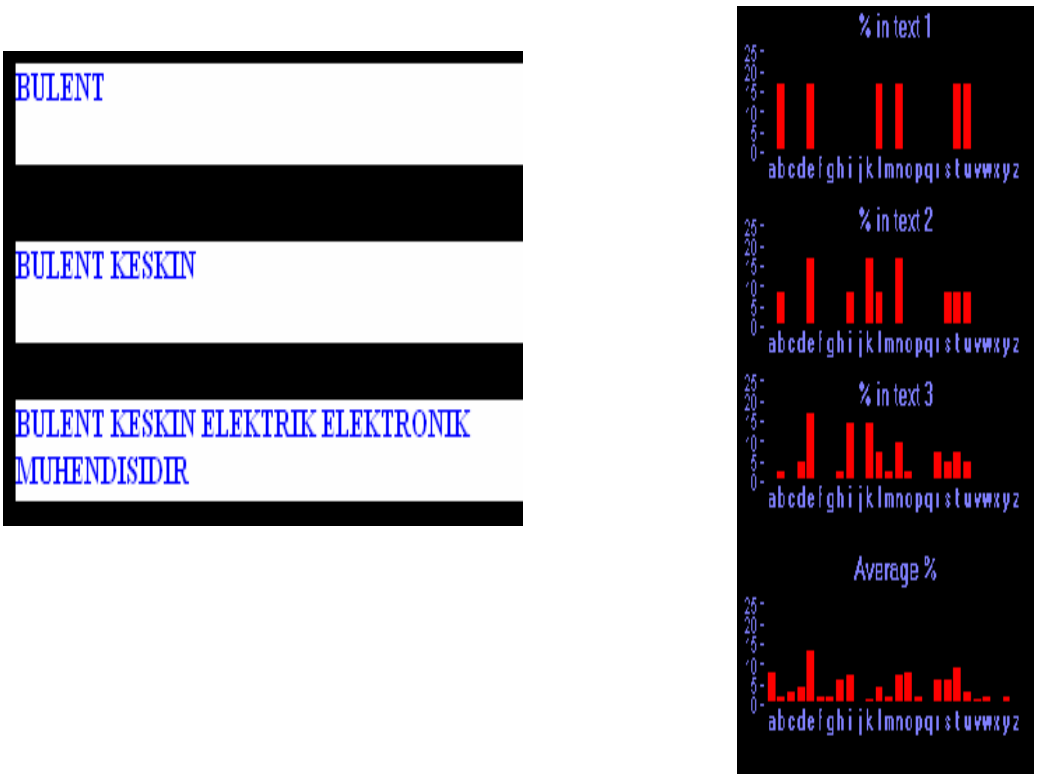
English:	ETAONIRSHLDCUPFMWYBGVKQXJZ	
Dutch:	ENIATORDLSGKHVUWBJMPZCFYXQ	*Xeno Handbook*
Esperanto:	AIEONLRSTKJUDMPVBGFCZH	*Xeno Handbook*
French:	EANRSITUOLDCMPVBFGHQJZXY	MA86, *Elcy*
German:	ENIRSADTUGHOLBMCWFKVZPJQXY	MA89, *Elcy*
Interlingua:	EAILNOSTRUDCMPVGBFHXQJWYZK	MJ75
Italian:	EAIOLNRTSCDMPUVGZFBHQ	MJ86, *Elcy*
Latin:	IEUTAMSNRODLVCPQBFGXHJKWYZ	ND50
Portuguese:	AEORSINDMTUCLPQVFGHBJZX	*Xeno Handbook*
Spanish:	EAOSRNIDLCTUMPGYBQVHFZ	JF86, *Elcy*
Swedish:	AENRTSIOMGKLDVFBCHPUYJXQWZ	JA81

Şekil 9.10 Dillere göre Frekans analizi(American Cryptogram Association, 2005, sy.18)

Harf	Olasılık(%)	Harf	Olasılık(%)
A	11.68	N	7.23
B	2.95	O	2.45
C	0.97	Ö	0.87
Ç	1.26	P	0.79
D	4.87	R	6.95
E	9.01	S	2.95
F	0.44	Ş	1.94
G	1.34	T	3.09
Ğ	1.13	U	3.43
H	1.14	Ü	1.99
I	5.20	V	0.98
İ	8.27	Y	3.37
J	0.01	Z	1.50
K	4.71		
L	5.75		
M	3.74		

Şekil 9.11 Harflerin Frekans Değerleri (Koltuksuz, 1995)

Dikkat edilmesi gereken bir diğer nokta da aşağıdaki metinde de görüldüğ ü gibi seçilen metnin uzunluğunun şifrelemenin çözümünde o kadar kolaylık sağladığıdır. Metin ne kadar uzunsa bize o kadar kolaylık sağlar. Nitekim sadece "BULENT" kelimesinin frekansı ile "BULENT ELEKTRİK ELEKTRONİK MUHENDİSİDİR" cümlesinin frekanslarının farklı olduğu görülmektedir. Seçilen metin ne kadar uzunsa yazıldığı dile ait frekans tablolarına da o kadar uyumlu olduğu görülecektir.



Şekil 9.12 Frekans Analizi Uygulaması (Sight, Codebook)

Vigenere Şifresi: İlk olarak 1553 yılında Giovan Ba tista Belasa tanıtılmış, 1586'da ise Blaise De Vigenere bu yöntemi düzenleyip kullanmıştır ve bu yöntemin adı "Vigenere şifresi" olarak kalmıştır.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Şekil 9.13 Vigenere Şifre Tablosu (http://www.koubk.org)

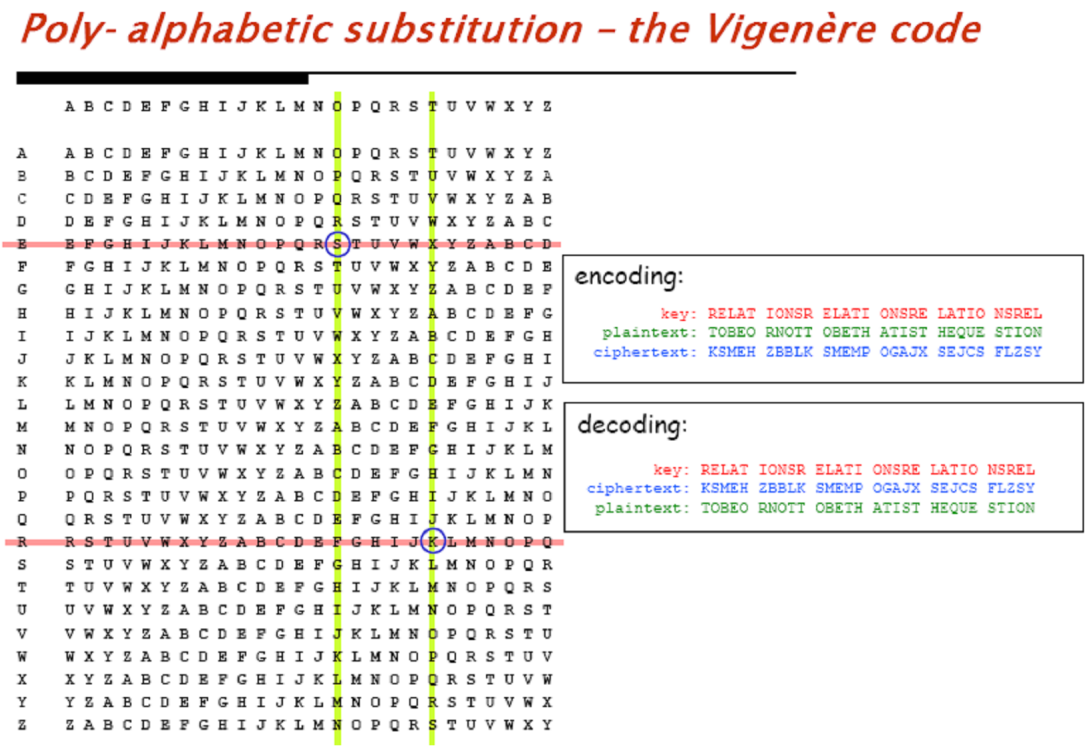
Açık Metin: BULENT KESKİN

Anahtar: MUHEND ISMUHE

Şifreli metin: NOPIAT SWEEPR

Açık metin harflerini ilk satırdan anahtar kelimenin harflerine ait alfabeyi de sol sütundan çıkartalım.

Deşifreleşmede ise şifrelemedeki işlemin tersine şifreli metindeki harfler anahtar kelimenin harfleri ile kesiştirilip açık metine ulaşılır. (Arda ve ark. Buluş, Yerlikaya, Türkiye Türkçesinin Bazı Dil Karakteristik Ölçütlerini Kullanarak Vigenere Şifresi İle Şifreleme ve Kriptanaliz)



Şekil 9.14 Vigenere Şifresi Örneği (Buttyáne, A Brief History of Cryptography, sy.11)

Jefferson diski: 1790–1793 yılları arasında George Washington'un teşviki ile mesajların şifreleme ve deşifresi amacıyla yapılmıştır. 26 silindirden oluşur ve her bir silindir numaralandırılmıştır. Her disk üzerind eki tüm alfabedeki harfler karışık yazılmıştır Jefferson Diski (Ott, 2007, sy.12 –15)

Şekil 9.15 Jefferson Diski (www.monticello.org)

Playfair Şifresi: 1854 yılında popüler olmuş bu şifrelemede, anahtar kelimenin harfleri 5*5'lik bir matrise tek sefer o lacak biçimde yazılır. Bu anahtar haricindeki harflerde yine bu matrise alfabetik sırayla yazılır.

Tablo 9.1 Playfair Matrisi

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Örneğin; "CRYPTOGRAPHY REQUIRES STRONG KEYS" anahtarı ile aşağıdaki gibi bir tablo ortaya çıkar.

Tablo 9.2 Örnek Matris

C	**R**	**Y**	**P**	**T**
O	**G**	**A**	**H**	**E**
O	**U**	**I/J**	**S**	**N**
K	**B**	**D**	**F**	**L**
M	**V**	**W**	**X**	**Z**

Bu matris oluşturulduktan sonra şifrelenecek metnimiz ikili harf gruplarına ayrılır. Örneğin;

“MEET ME AT THE SUBWAY” olan metnimiz ikili gruplar halinde;

“ME” “ET” “ME” “AT” “TH” “ES” “UB” “WA” “YX” şek linde ayrılır.

Şifreleme ikili harflerin aynı satırda, aynı sütunda ya da farklı satır ve sütunlarda olmasına göre farklı biçimlerde kurallara sahiptir.

Örneğin “AT” ikilisinde “A” ve “T” ikilisinden A harfi şifrelenirken A’nın bulunduğu satır ile T’nin bulunduğu sütunun kesişiminden “E” ve T harfi şifrelenirken de, T satırının A sütunuyla kesişiminde bulunan “Y” biçimine gelecektir.(Fischer, 2005)

Konuyla ilgili kurallar ise aşağıdaki biçimde özetlenebilir.

1. İkilideki harfler aynı satırda ise sağlarındaki harflerle yer değiştirirler.

2. İkilideki harfler aynı sütunda ise bir altlarında harflerle yer değiştirirler.

3. Her iki harfde aynı satırda ya da aynı sütunda değillerse, hangi harf şifrelenecekse ona ait satırın diğer harfin sütunuyla kesişiminde bulunan harfle yer değiştirilir. (Akyıldız ve ark. Çimen, Akleylek, 2007, sy.42)

Hill Şifresi: Hill Şifresi için alfabedeki her harf sıfırdan başlayarak bir rakama denk gelir.

A B C Ç D E F G Ğ H I İ J K L M N O Ö P R S Ş T U Ü V Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

Daha sonra anahtar olarak Z29’ da tersi olan bir matris seçilir. Matrisimiz

$S=\begin{matrix}\mathbf{23}\\\mathbf{45}\end{matrix}$ olsun.

Düzmetin olarak da GECE kelimesi ni seçelim ve bunu 2li matris şeklinde yazalım.

G:7 ve E:5’den; A: $\begin{matrix}7\\5\end{matrix}$

C:2 ve E:5’den de B: $\begin{matrix}2\\5\end{matrix}$ matrisleri elde edilir.

S*A matrislerin çarpmı bize; Mod 29’da $\begin{matrix}0\\24\end{matrix}$

S*B matrislerinin çarpımı da; Mod 29’da $\begin{matrix}19\\4\end{matrix}$ matrislerini yani GE=AU’yu CE=PD’yi verir.

1. Bu işlemin sonucunda GECE=AUPD elde edilir.(Akyıldıv ve ark. Çimen, Akleylek, 2007, sy.45-46)

Bu şifrelerin çözümü de S matrisinin tersini n AU ve PD matrislerinin çarpımıyla elde edilmiş olur.

Bu örneği Türkçemizin alfabesine göre verdim. Aşağıda İngiliz alfabesine göre verilmiş bir örnek bulunmaktadır.

İngiliz dilinde ise harflere karşılık gelen değerler harflerden kaynaklanan nedenle aşağıdaki gibi olur.

Tablo 9.3 İngilizce'de Rakamsal Sıralı Harfler (Sutherland,2005, sy.5)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Bu alfabede işlemler alfabedeki harf sayısından dolayı Mod26'ya göre yapılır. Aşağıdaki örnekte DO IT NOW kelimesi aynı yöntemler kullanılarak WVVYQTJO olarak şifrelenmiştir.

plaintext	do	it	no	wx
	$(3, 14)$	$(8, 19)$	$(13, 14)$	$(22, 23)$
(ax+by, cx+dy)	$(6+42=22$ $15+84=21)$	$(16+57=21,$ $40+114=24)$	$(26+42=16,$ $65+84=19)$	$(44+69=9,$ $110+138=14$
ciphertext	WV	VY	QT	JO

Şekil 9.16 Bir Örnek (Sutherland,2005, sy.13)

Vernam Şifresi: 1. Dünya savaşında Almanların çözmemesi için bir Amerikan Telefon ve Telgraf şirketinden bir çalışan olan Gilbert Vernam tarafından hazırlanan yöntem, savaş boyunca Amerika Birl eşik Devletleri'nin mesaj güvenliğini sağlamıştır. (Akyıldız ve ark. Çimen, Akleylek, 2007, sy.52)

1917 yılında Vernam tarafından geliştirilen bu yöntemle matematiğin de artık şifreleme sistemleri içine girdiğini görmekteyiz. Burada da Hill şifresinde oldu ğu gibi her harfe bir rakam verilir. Şifrelenecek metinle aynı uzunlukta olan seçilen anahtarda rakamsal olarak ifade edilir. Şifrelenecek metinle anahtar İngilizce de Mod26 Türkçe'de ise Mod29'a göre toplanır.

XOR ( ):

0 0 = 0; 1 0 = 1; 0 1 = 1; 1 1 = 0

a a = 0; a 0 = a; a b b = a

E(P, K) = P K (Fleisch, 2001, sy.7)

D(C, K) = C K = (P K) K = P

Metin :V E R N A M C I P H E R

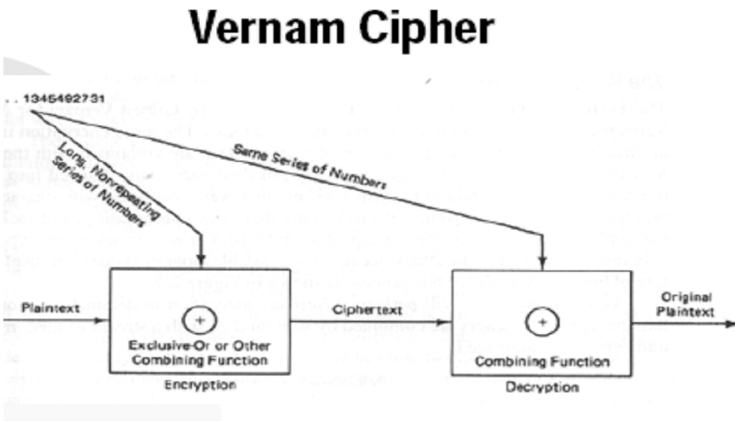
Rakamsal :21 4 17 13 0 12 2 8 15 7 4 17

Anahtar :76 48 16 82 44 03 58 11 60 05 48 88

=Toplam :97 52 33 95 44 15 60 19 75 12 52 105

=mod 26 :19 0 7 17 18 15 8 19 23 12 0 1

Şifre Metin :T A H R S P I T X M A B (Fleisch, 2001, sy.9)



Şekil 9.17 Vernam Şifre Blok Şeması (Fleisch, 2001, sy.8)

Bu şifrenin çözümünde de yine ters işlem uygulanır yani şifre metinden anahtar çıkarılır.(Akyıldız ve ark. Çimen, Akleylek, 2007, sy.54)

Orijinal şifrede her harfe karşılık gelen ikili karşılıkları kullanılmaktadır.

Örneğin;

Metin;1001001 1000110 ve anahtar 1010110 0110001 olsun.

Buna göre XOR işlemine göre şifre;

1001001 1000110 metin

1010110 0110001 anahtar

0011111 1110110 şeklinde olacaktır.

Deşifre ise; 0011111 1110110 şifre metin idi.

1001001 1000110 metin ile çözülerek metine ulaşılır. (Koç,sy.2)

Enigma

Şekil 9.18 Enigma Resimleri (http://www.iam.metu.edu.tr)

Enigma; 2. Dünya Savaşı sırasında Nazi Almanyası tarafından gizli mesajların şifrelenmesi ve tekrar çözülmesi amacı ile kullanılan şifre makinesidir. Daha açık bir ifade ile Rotor makineleri ailesi ile ilişkili bir Elektro-Mekanik aygıttı ve birçok değişik türü vardı.

Enigma makinesi, ticari olarak 1920 li yılların başında kullanılmaya başlandı. Birçok ülkede Ordu ve Devlet kurumları için özel modeller üretildi. Bunların en ünlüleri ikinci dünya savaşı öncesinde ve savaş sırasında Nazi Almanyası'nda kullanılan modellerdi. Alman ordu modeli olan Wehrmacht Enigma, en çok konuşulan modeldi.

Bu makine kötü bir üne sahip oldu çünkü Müttefik şifreciler (Polonya şifre bürosu, İngiltere-Bletchley Park vb.) tarafından geniş mesajları çözümlendi. Bazı tarihçiler, Alman Enigma kod sisteminin deşifre olması sayesinde Avrupa'da savaşın bir yıl daha önce bittiğini ileri sürmektedirler.

Enigma şifresinin bazı zayıf yanları olmakla birlikte, aslında diğer faktörler olan operatör hataları, prosedür açıkları ve nadir olarak ele geçen kod kitapları sayesinde çözümlenebildi.

İkinci dünya savaşında Bletchley Park-İngiltere'de üslenen Amerikalı ve İngiliz şifre çözücüler, o zamanın en yetenekli ve en değerli bilim adamı, matematikçi ve mühendis lerinden oluşmaktaydı. Bunlardan bazıları, daha sonra Bilgisayar biliminin kurucularından sayılacak Alan Matthison Turing ve dünyanın ilk dijital ve programlanabilir bilgisayarı olan Colossus'u yapan Thomas Harold Flowers'dır. Birçok Colossus bilgisayarı, 2.Dünya Savaşı sırasında Alman Lorenz SZ40/42 şifre sisteminin çözülmesi işleminde olasılık hesaplayıcı olarak kullanılmıştır.

2.İkinci Dünya Savaşı ve stratejik planların aktarılmasında kullanılan şifre sistemleri ve bunların çözülmesinde kullanılan algoritmalar, buluşlar, şifre çözücü makineler bir anlamda bilgisayar biliminin doğmasına neden olmuştur diyebiliriz. (http://tr.wikipedia.org)

Diğer Rotor makineleri gibi Enigma da Elektro-Mekanik bir sistemdir. Temel olarak, rotor mekanizması sayesinde olasılık üreten bir mekanizmadır. Daktilo klavyesine benzer herbir klavye tuşuna basıldığında, rotorlar döner. Belirgin olarak tüm Enigma sistemlerinde öncelikle en sağdaki rotor döner, daha sonra ona komşu olan rotorlar bir veya daha fazla adım atabilir. Rotorun dişli mekanizması her algoritma programlanmadan önce sökülür ve farklı bir konumda takılırdı. Ayrıca her mesaj çekiminden önce operatör tarafından alt bölümdeki elektrik soketlerini farklı şekilde dizerek şifrenin çözümünü daha da zorlaştırırdı. Mekanik sisteme bağlı elektrik sistemi, operatöre gösterge bölümünde hangi harfin basıldığını ışıklı olarak gösterdi.(http://tr.wikipedia.org)

Şekil 9.19 Alman Askerlerin Arazide Enigma'yı Kullanımını Gösteren Fotoğraf (Mowry, 2003,sy.3)

9.1.3 Günümüz Şifreleme Sistemleri

Günlük hayatta sürekli kullandığımız pek çok sistem için en gerekli özelliklerden birisi gizlilik, bunu sağlayan da kriptografi'dir.

Sayısal İmza gündelik yaşamda kullanılan örneklerden biridir. Sayısal imza özet olarak elektronik mesaja eklenmiş bilgidir. Çift anahtarlı bir kriptografik algoritmayla hazırlanan sayısal imza, hem gönderilen bilginin sayısal içeriğinin değiştirilmediğinin, hem de gönderen tarafın kimliğinin ispatlanması için kullanılır. Gönderilecek mesajdan üretilen "mesaj özetinin" sayısal içeriği, gönderen tarafın kendi gizli anahtarına bağlı olarak oluşturulur. Sayısal imzanın doğruluğunu kanıtlamak için mesajı alan taraf, kendisine gelen mesajın ve sayısal imzanın sayısal içeriği, gönderen tarafın açık anahtarını kullanır. (Kodaz, 2003, sy.6)

Örneğin bankaların verdiği bankamatik ya da kredi kartını bankamatiğe soktuğumuzda bankamatik bizden şifremizi ister. Bankamatikten girilen şifre ve kişisel bilgilerimiz genellikle DES algoritmalarının kullanıldığı, gizli anahtar şifreleme kriptografisini kullanılarak şifrelenerek sistem üzerinden merkezde bulunan bilgilerle karşılaştırılır.

Günlük hayatta sıkça kullandığımız cep telefonları da güvenliğe duyduğu ihtiyaçtan dolayı kriptografiyi kullanır. Çünkü cep telefonu kullanılmaya başlandığında güvenlik ve kimlik doğrulamasının yapılması gerekmektedir. Buradaki uygulamada cep telefonunda bulunan sim kartın şifreleme için kullandığı 128 bitlik anahtar içermesidir.

Bunlardan başka, şifreli televizyon kanalların yaptığı yayınlar, her an kullandığımız internet, bir okulun not sistemi ya da bir e-Devlet uygulaması, günlük hayatta karşılaştığımız ya da birebir kullandığımız yüzlerce örnekten sadece bir kaçıdır. (Akyıldız ve ark. Çimen, Akleylek, 2007, sy.91–95)

Şifreleme sistemleri anahtar yapısına göre temel olarak ikiye ayrılır. 20. yüzyılın son çeyreğine kadar bilginin şifre ve deşifresi için, tek anahtardan yararlanılan, anahtarın aynı olduğu simetrik veya gizli anahtarlı olarak bilinen (private key cryptosystem) şifreleme sistemleri kullanılırken daha sonra şifreleme ve şifre çözme anahtarının farklı olduğu asimetrik veya açık anahtarlı şifreleme adıyla da bilinen (public key cryptosystem) sistemleri de kullanılmaya başlandı. (Urhan ve ark. Zengin, Şanlı, sy.2–3)

Simetrik (Gizli Anahtarlı) Şifreleme

Simetrik algoritmalarda verinin kriptolanmasında kullanılan anahtar bilgisi ile kriptolanmış verinin kriptosunun çözülmesinde kull anılan anahtar aynıdır. Bu sebeple açık kullanılan anahtarın üçüncü kişilerden gizlenmesi gerekmektedir. Bu algoritmalara örnek olarak DES'i verebiliriz.(Yerlikaya ve ark. Buluş, Buluş, 2006, sy.3)

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Şekil 9.20 Bazı Simetrik Anahtarlı Algoritmalar (Steve Armstong, Network Security)

Simetrik sistemin avantajları;

- Algoritmalar hızlıdır
- Algoritmaların donanımla gerçeklenmesi kolaydır
- “Gizlilik” güvenlik hizmetini yerine getirir

Dezavantajları ise;

- Ölçeklenebilir değil
- Emniyetli anahtar dağıtımı zor
- “Bütünlük” ve “Kimlik Doğrulama” güvenlik hizmetlerini gerçeklemek zor

- Sayısal imza desteğinin olmamasıdır.

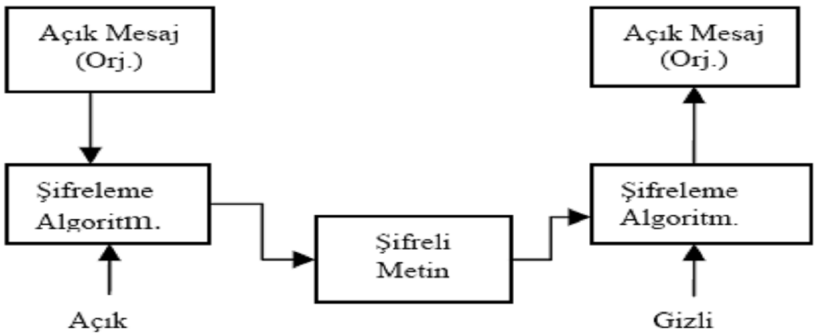
Bu şifreleme sisteminde kullanılan bazı yöntemler şunlardır;

- AES(AdvancedEncryptionStandard)
- DES(Data EncryptionStandard)
- IDEA(InternationalData Encryption Alg otirhm)
- Skipjack
- RC5,RC2,RC4 (Hüseyin, 2004, sy.18 –19)

Asimetrik (Açık anahtarlı) Şifreleme

Asimetrik kripto sistemlerde her kullanıcının biri gizli diğeri açık olmak üzere iki adet anahtarı mevcuttur. Açık anahtar bilgisi alıcı tarafa herhangi bir koruma yapılmadan iletilir ve alan taraf da bu bilgiden, kriptoyu çözmek amacı ile kullanacağı gizli anahtarı üretir. Açık anahtarın üçüncü bir kişinin eline geçmesi tek başına hiç bir şey ifade etmez. Her ne kadar bu yöntemin, anahtarların alıcı tarafa iletilmesi işlemini basitleştirdiği düşünülse de asimetrik algoritmaların işlem süresinin yüksek oluşu, veri kriptolamada yaygın olarak kullanılmalarını engellemektedir.” (Yerlikaya ve ark. Buluş, Buluş, 2006, sy.3)

Başka bir değişle asimetrik kripto sistemlerde, k ullanıcıların sahip olduğu anahtarlardan birisi sadece kendisinin bildiği ve güvenli bir şekilde saklanması gereken gizli anahtar, diğeri ise herkesin kullanabilmesi için dağıtılan açık anahtardır. Mesaj gönderen kişi ya da parti mesajı karşı tarafın açık anahtarıyla şifreleyerek gönderir. Bu mesaj ancak alıcının gizli anahtarıyla tekrar deşifre edilebilir. Şekilde asimetrik kripto sistemlerinde mesaj alışverişinin nasıl gerçekleştiği görülmektedir.



Şekil 9.21 Şifreleme Sistemi

Asimetrik kripto sistemlerin gücü gizli anahtarın açık anahtardan türetilme ihtimalinin yok denecek kadar az olmasından kaynaklanmaktadır. Bu sistemlere açık anahtarlı kripto sistemler de denilmektedir. (Kırımlı ve Erdem, 2007, sy.2)

Bu anahtarlar birbirine matematiksel bir ilişkiyle bağlanmıştır fakat anahtarlardan birini kullanarak diğerini elde etmek çok zor hatta imkânsızdır. Anahtarlardan açık olanıyla şifrelenen bir veri ancak, bu açık anahtara karşılık gelen özel anahtarla açılabilir.(Erol, 2004, sy.20)

Asimetrik sistemin avantajları;

- Anahtar yönetimi ölçeklenebilir
- Kripto-analize karşı dirençli (Kırılması zor)
- Bütünlük, Kimlik Doğrulama ve İnkâr Edememezlik güvenlik hizmetleri sağlanabilir
- Sayısal imza desteği mevcuttur.

Dezavantajları ise;

- Algoritmalar genel olarak yavaş (Simetrik kriptografi algoritmalarına göre ~1500 kat!)

- Anahtar uzunluğu bazı durumlar için kullanışlı değil

Bu şifreleme sisteminde kullanılan bazı yöntemler şunlardır;

- RSA (Rivest-Shamir-Adleman)
- El Gamal
- PGP (PrettyGoodPrivacy)
- Diffie-Hellman anahtar belirleme
- DSA (DigitalSignatureAlgorithm (Erol, 2004, sy.23 –24)

Bu bilgi selinde giderek daha da önemli hale gelen şifreleme biliminin önemini açıklayabileceğimiz en ilginç örneklerinden birisi de muhakkak 11 Eylül saldırılarıdır. Çünkü iddialara göre, NSA'nın s aldırı istihbaratını alamamasındaki en önemli neden olarak kriptolojidir. Çünkü şifreleme sistemleri artık terörist örgütler tarafından da etkin bir biçimde kullanılmaktadır.

Günümüzde daha da karmaşıklaşan şifreleme sistemlerine, parmaklarımızın ucundaki tıklamalarla eriştiğimiz internet üzerinden hem de ücretsiz biçimde ulaşmak mümkündür.(Dede, 2002)

9.2 Haarp (High Frequency Active Auroral Research Program)

Ülkelerin sahip oldukları uyduları yok edecek bir vuruş, anavatanımızın etrafında dışarıdan gelebilecek füzelere karşı oluşturulabilecek bir kalkan, Dünya'daki herhangi bir bölgedeki haberleşmeyi tamamen keserken bizim haberleşmemizi mümkün kılabilecek bir verici, hava kontrolünü mümkün kılacak bir silah, Dünya'nın derinliklerini tarayarak gizli üsleri depoları ya da madenleri bulabilecek bir tarayıcı, insanların zihinlerine kazıyacağı mağlubiyet hissiyle kazanılacak bir zaferin mimarı. Bu bahsedilen özellikler

özetle Haarp olarak bilinen “High Frequency Active Auroral Research” programın Dünya kamuoyunda tartışılan özelliklerini yansıtmaktadır.

Bu projenin en önemli prensibi; 1864 yılında İskoç Matematikçi, James Clark Maxwell tarafından yayınlanan, elektromanyetik dalgaların bir noktadan başka bir noktaya yayılabileceğini belirttiği “Elektro manyetik Alan Teorisi”’dir. Bu teorinin doğruluğu 1880’de laboratuar ortamında yaptığı titiz çalışmalar neticesinde Alman Fizikçi, Heinrich Hertz’in 1880'lerin sonlarındaki çalışmalarıyla doğrulanmıştır. (http://www.haarp.alaska.edu/haarp/ion2.html)

23 Mart 1983'de dönemin ABD başkanı Ronald Reagan'ın çağrısıyla, nükleer savaşı imkânsız kılacak bir savunma yaratma amacıyla başlatılan SDI (Stratejik Savunma İnisiyatifi) basın tarafından “Star Wars” olarak adlandırılacaktı. İşte Haarp'de aslında bu fikrin bir sonucu olarak ortaya çıkmıştır. Burada şundan da bahsetmek istiyorum ki; bu program çerçevesinde ortaya çıkarılan çalışmalar; Dünya devletleri tarafından ortak imzalanan pek çok anlaşma bakımından yasal yada yasal olmayan nitelikte olabilmektedir. Nitekim Haarp'in tartışılan yönleri, uluslararası bazı anlaşmaları da ihlal eder niteliktedir.

Bu süreçte ilk Haarp prototip çalışması 1993 yılının sonlarında yapıldı. 1995 yılında 1996 yılı için Harp harcamaları “Savunma İçin İleri Seviyede Araştırma” adı yla yer aldı. Bütçede Haarp’e ayrılan para yeraltının savunma amaçlı kontrolüyle Aurora aktarımlarının araştırılması olarak açıklanmaktaydı. Burada bahsedilen teknoloji “Toprak Delici Tomografi” (EPT) teknolojisidir. Kimine göre bu teknolojinin bütçelerde gösterilme nedeni, programın kamuoyu baskılarına karşı askeri değil sivil amaçlı olduğunu vurgulamaktır ve aslında bu teknolojinin adıyla Haarp projesine aktarılan bütçe, diğer çalışmaları da desteklemektedir.

Haarp projesi hava, deniz savunma bakanlığınc a yürütülen ve EXCEDE, RED AİR ve CHARGE4 kod adlarıyla bilinen bir projedir. (Smith, 1998)

Haarp ile ilgili Devlet kurumlarının yanında tiacri ya da özel kurulmada çalışmalar yapmaktadır. Bu kurumlar aşağıdaki tabloda belirtilmiştir.

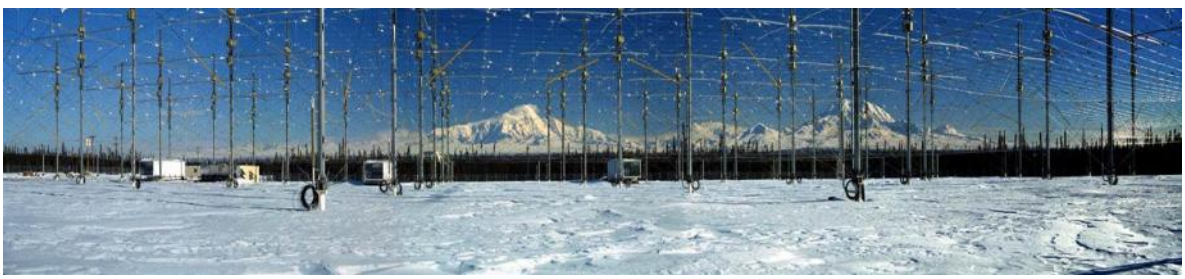
Tablo 9.4 Haarp'le İlgili Kurumlar(http://www.haarp.alaska.edu/haarp/osite.html)

Agency/Organizations	Level	Category
National Telecommunications & Information Administration	Federal	Transmitting Authority
Federal Aviation Administration	Federal	Transmitting (Aircraft Safety)
Environmental Protection Agency	Federal	Adherence to Safety Standards
Air Force	Federal	Transmitting(Elmendorf AFB Ops)/Environmental
Navy	Federal	Transmitting/Environmental
Army Corps of Engineers	Federal	Water Quality/Wetlands
National Park Service	Federal	Animal Tracking/Emerg. Comms
Fish & Wildlife Service	Federal	Wildlife and RFI
US Coast Guard	Federal	Emerg Comms/Rescue/Navig.
Bureau of Land Management	Federal	Land Use
Bureau of Indian Affairs	Federal	Native Concerns
Advisory Council on Historic Preservation	Federal	Archeological Resources
Alaska Deptartment of Environmental Conservation	State	Water Quality/Natural Resources Mining Plans/RFI/RFR
Historic Preservation Office	State	Archeological Resources
Alaska Fish & Game	State	Wildlife & RFI
Alaska Department of Natural Resources	State	Resource Conservation
Alaska Dept of Community and Regional Affairs	State	All categories
American Radio Relay League	Private	Amateur Radio Interests
Aircraft Owners & Pilots Association	Private	Aircraft Safety
Alyeska	Commercial	Pipeline Controls & Comms
ALASCOM	Commercial	Telephone Compatibility
Community Representative	Private	Community Interests

9.2.1. Haarp'in Teknik Özellikleri

Bernard Eastlund'un ileride bahsedeceğim ilk patentinde ort aya koyduğu; icadın çok büyük enerji ihtiyacı, projenin yürütüldüğü Alaska'daki kaynaklarla yakından ilişkilidir. Resmi olarak proje, Alaska'da Gakona askeri üssünde yürütülmektedir ancak Poker Flats olarak bilinen bölge de çalışmaların yürütüldüğüne iddia lar da mevcuttur. Çalışmalar Haarp'in kendi web sayfasında aynen "62 deg 23.5 min North Latitude,145 deg 8.8 min West Longitude " olarak verilmektedir. (http://www.haarp.alaska.edu/haarp/faq.html)

Haarp vericilerinin çalıştığı katman olan iyonosfere yönlendirilecek ışınlar, iyonosferi ve atmosferin birbiriyle etkileşimli diğer katmanlarını da ısıtacaktır. Bu nedenle bu vericilere iyonosfer ısıtıcıları denilmektedir.



Şekil.9.22 HF Antenler (http://www.haarp.alaska.edu/haarp/photos.html)

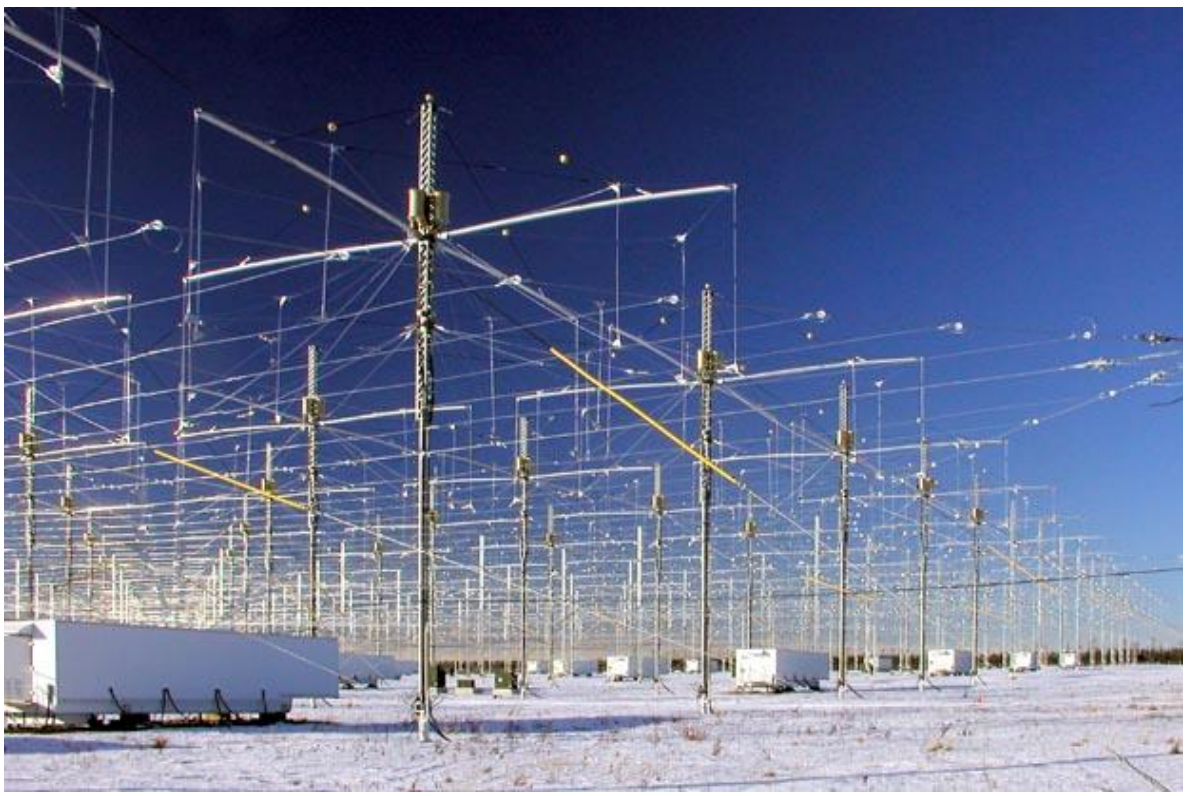
Programın özü, iyonosfer güçlendirme ve yönlendirme teknolojisinin Savunma Bakanlığı amaçları için potansiyel kullanımını değerlendirmek için gerekli öncü deneyleri yapabilecek şekilde eşsiz bir iyon osfer ısıtma becerisi geliştirmek olacaktır. (Smith, 1998, sy.32)

Ancak, Haarp'in içinde bulunan faz sıralı sistem bir radar değil, çok yüksek frekansların iyonosferdeki bazı noktalara odaklanmasında kullanılan sistemdir. Bu nedenle bazı Haarp karşıtları, bu teknolojinin kullanımının Dünya üzerindeki

herhangi bir noktada Gamma Patlamaları yaratabilecek güçte olduğunu savunmaktadırlar.

180 adet IRI denilen HF anteni ile tamamlanması planlanan tesisin sahibi ABD Savunma Bakanlığıdır. Sekiz sütun, altı sıradan oluşacak IRI vericilerinin bulunduğu kulelerin tepesinde, 2,8-7 MHZ ile 7-10 MHZ aralığında çalışacak biçimde ayarlı iki çift kutuplu anten, her kulenin tepesinde büyük bir X oluşturacak biçimde yerleştirilmiştir. Antenlerin yanında yerden 4,5 m. yükseğe yerleştirilen kafeslerle, RF dalgaların yere yansımaları tekrar yukarı doğru yönlendirilirken, aynı zamanda ışınların yoğunlaşması da sağlanmıştır. Temel olarak bu kafeslerle vericileri üzerlerinde bulunduran kuleler, birbirlerinden 25 m. uzaklığa sahiptirler. (Smith, 1998, sy.23)

HAARP Projesinin çekicisi olan IRI vericileri iyonosferin bir bölümünü geçici olarak tetiklemek amacıyla kullanılmaktadırlar.



Şekil.9.23 Sıralı Antenler (http://www.haarp.alaska.edu/haarp/photos.html)

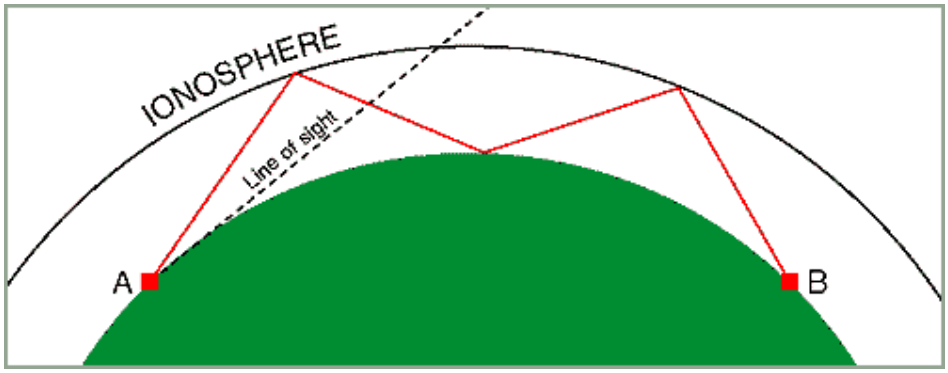
Resmi belgeler hükümetin Haarp için niyetini üst atmosferik ve güneş -dünya araştırmaları için önemli bir arktik tesis oluşturmak şeklinde açıklamaktadır.(Smith, 1998, syf.24)

HAARP, HF' da yüksek enerji çıkışları ile iyonosferin ısıtılması ve burada bir takım değişimler yapılarak etkilerinin incelenmesi için başlatılmış bir projedir.

9.2.2. İyonosferin Kullanımı

Yeryüzünden uzaya doğru sırasıyla troposfer, stratosfer, ozonosfer, mezosfer, termosfer, iyonosfer ve ekzosfer tabakaları bulunmaktadır. Her bir tabakanın önemli görevleri olmasına karşın iyonosfer, radyo haberleşmesinde kullanılan dalgaları, bünyesindeki elektrik yüklü gaz molekülleri ile yansıtarak uzak noktalar arasında haberleşmeyi mümkün kılması bakımından bizim için ayrı bir yere sahi ptir. Haarp bakımından bizi ilgilendiren kısımda aslında bu noktadır.

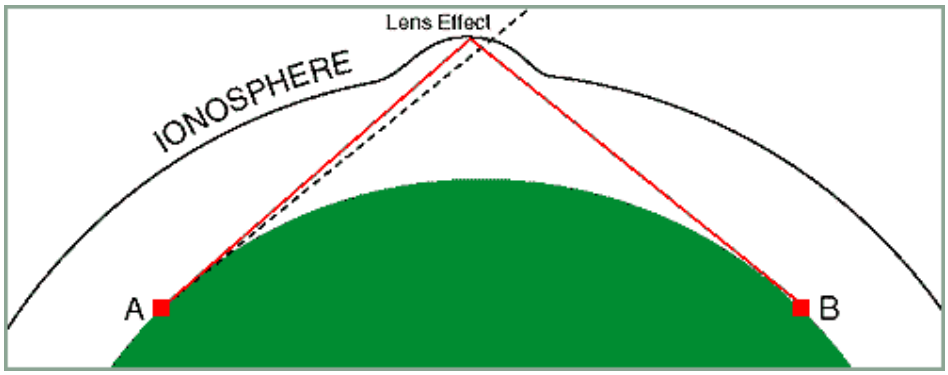
"İyonosfer tabakasının özelliği, içindeki gaz moleküllerinin iyon ve serbest elektronlara ayrılmış olmasıdır. Bu tabaka 60 –80 Km. yükseklikten başlayıp 1000 – 2000 Km.ye kadar çıkar. İyonlaşmanın nedeni ise güneşin morötesi ışınımıdır. İyonlaşma sonucu ortaya çıkan serbest elektronlar, iletkenlik yaratırlar. Bu elektronlar üzerlerine bir dalga geldiğinde salınmaya başlarlar ve sanki bir verici anten gibi yer yüzeyine dalga yayarlar. Böylece aşağıdan gelen dalga tekrar geri yansıtılmış olur. Elektron yoğunluğunun çok fazla olması ise dalganın yarattığı salınımın üst tarafa transfer olmasına neden olur. Absorbe edilmiş, yutulmuş gibi izlenim verir ve böylelikle yansıma engellenmiş olur."(Yaşar , 2005, syf.15–16)



Şekil 9.24 İyonosferde yansıma (Eden, Weapons of Total Destruction)

İyonosfer kısa dalga radyo yayınlarını yansıtan ve bu dalgaların, örneğin İstanbul'dan Ankara'ya gönderilmesine olanak tanıyan iletici bir katmandır. Kısa dalgalar herhangi bir radyo yayını için yeterli olabilirken, bu sinyaller uzun mesafelerde daha önce anlattığımız nedenlerden dolayı sinyal gücünde meydana gelen kayıplarla beraber hava şartlarından da olumsuz yönde etkilenirler. Kısa dalgaların aksine, aşırı yüksek frekans dalgaları çok daha kısa dalgalardır ve çevresel etmenlerden daha az etkilenerek sinyal kaybı bakımından da avantaj sağlarlar. Bu bakımdan noktadan noktaya uzak bağlantılarda daha çok tercih esilmektedirler. (Eden, Weapons of Total Destructio n)

Maalesef EHF dalgaları iyonosferden doğal olarak yansımayarak sıçrarlar. Bu nedenle HF dalgaların tek bir doğrultuda yayıldıkları söylenir. Kendi uydu antenimizin belirli doğrultuda yayınları almasının nedeni de budur.



Şekil 9.25 Lens Etkisi (Eden, Weapons of Total Destruction)

Eastlund HF ve EHF dalgaların iyonosferdeki bir nokta boyunca aşırı yüksek güç ihtiva ettiğini keşfetti. Bu olduğunda iyonosfer depolanan elektrik enerjisinden dolayı daha sıcak bir hal alıyordu. Bu durum atmosferin pişirildiği fikrini düşündürebilir.

Isınan iyonosfer aynen ısıtılan bir plastikteki gibi daha yukarda atmosferik bir çıkıntıya neden olur. Eastlund bu çıkıntının hem daha yukarda olmasından dolayı yatayda daha iyi bir iletime olanak tanıdığını hem de radyo dalgaların ı bu noktadan daha iyi yansıdığını keşfetti. Eastmund, normalde iyonosferi delerek uzaya geçen ELF ve mikrodalga sinyallerin güçlerini daha fazla kaybetmeden saptırılabilir olduklarını keşfetti ve buna lens etkisi adını verdi. (Eden, Weapons of Total Destruction)

9.2.3. Haarp'in Amaçları

Haarp'in amaçları noktasında sağlıklı verilere erişebilmek, yapılan bu çalışmaların çok gizli yürütülmesi nedeniyle çok mümkün gözükmemektedir. Ancak Uluslararası imzalanan bazı anlaşmaların doğa kontrolünü ima edilmesi, ra dyasyonun verebileceği zararların bu çalışmaları işaret edercesine açıklanması ve iyonosferik çalışmaların doğaya verebileceği zararlara dikkat çekmesi belki de bu çalışmaların en resmi belgeleri olduklarını düşündürebilir. Viewzone Dergisinde yayınlanan b ir makalede bu çalışmalar vasıtasıyla sahip olunacak yetenekler şöyle açıklanmaktadır:

"… yerkürenin atmosferdeki belirli stratejik yerlerde tahmin edilemeyecek miktarlarda enerji depolama ve güç enjeksiyon seviyesini kısmi seviyede yapabilme becerisi...

... Üçüncü parti haberleşmeleri engellemekle kalmaz, dünyanın kalan kısmında iletişim bozulsa dahi, bir iletişim ağını sağlamak amacıyla, bir veya daha çok ışının avantajını kullanabilir. Aynı zamanda diğerlerinin haberleşme ağını bozan sistem, bir haberleşme ağı olarak bu keşfini bilen biri tarafından kullanılabilir.

...Atmosferin geniş bölgeleri, beklenmedik yükseklikere, füzelerin, hiç beklenmedik bir şekilde ve plansız olarak gerideki kuvvetlerle karşı karşıya kalabilmeleri amacıyla taşınabilir..."

Ayrıca yapılan araştırmalar fonun, 1996 yılında tomografik bir tarama cihazını geliştirmek için onay verdiğini işaret etmektedir. Dünya'nın derinliklerindeki mağaraları, cephanelik ve potansiyel düşman sığınaklarını tarama kabiliyetine sahip bu cihazın yeteneği, fon anlaşmasının bir parçası olarak sıra dışı özellikteydi. Fakat tomografik taramalarda kullanılan dalga boyları, güçlü birer ELF radyasyonuydu. Ve bir kez yerleştirildikten sonra, yönlendirilmiş ışının gücü ve frekansı değiştirilerek stratejik hedefler yok edilebilirdi. (Eden, Weapons of Total Destruction)

Haarp projesinin kendi web sayfasında belirtilen amacında ise; Haarp'in iyonosferin özellikleri ve davranışları üzerinde inceleme yapmayı amaçlayan bilimsel bir girişim olduğuna ve özellikle, iyonosfer ile etkileşimli gelişmiş iletişim ve gözlem sistemlerinin geliştirilmesi ve güçlendirilmesi için kullanılmasına vurgu yapmaktadır. (http://www.haarp.alaska.edu/haarp/prpEis.html)

Haarp'in Dünya kamuoyunda tartışılan temel kullanım nedenleri ise şunlardır:

Savunma

Radarımızın ufuk üstünü görebilme yeteneği bize büyük savunma avantajı sağlayacaktır. Ya da iyonosferin yükseltilmesiyle ülkemize yönelen uçakların ya da

füzelerin sistemlerinin bozulması yoluyla saptırılmaları yada yok edilmeleri sağlanabilir. Yada, daha ilerideki bölümlerde anlatılan Zihin kontrol çalışmalarına uygulanabilirliği bakımından da Güvenlik açısından farklı bir risk içermekedir.

Doğa Kontrol

Örneğin geçen sene ABD'de meydana gelen kasırga binlerce zencinin ölümüne yol açmış ve bu durum ABD kamuoyunda büyük çalkantılara neden olmuştu. Hava durum kontrolünü yapabilen bir ülke benzer şekilde rakibine elbette ki böyle bir sıkıntıya sokma avantajını kullanmayı isteyecektir. Ya da bu çalışmayı kaleme alırken televizyondan duyduğum Çin'deki kötü hava şartlarının ülkede büyük bir enerji dar boğazına yol açtığı haberi bu yeteneğin sağlayabileceği avantajın boyutlarının nedenli büyük olduğunu göstermektedir.

Saldırı

Nötron Bombasının icat edilmesinin nedeninde de olduğu gibi canlılara azami zararı verirken eşyalara asgari zarar verecek bu silah, bir ışın biçiminde direkt olarak karşı ülke birliklerinin üzerine beyin kontrol aracı olarak da yönlendirilebi lir.

Toprak Delici Tomografi

Bu teknoloji aslında, iyonosfer çalışmaları ile bu katman hakkında elde edilen bilgilerin askeri amaçlı kullanımı bakımıyla Haarp ile benzerlik göstermektedir. EPT ile yer altında bulunan gizli tesislerin, kaynak ve maden yataklarının, zararlı atık sahalarının, arkeoloji bölgelerinin, mayınlar dahil gömülü tüm silah depolarının bulunması, deprem ve doğal felaket haritalarının çıkarılması gibi daha pek çok uygulamanın yapılması mümkündür. Bu yönünün kullanılması ve resmi b elgelerde daha çok bu uygulamaya yer verilmesinin en büyük nedeni aslında, uluslararası kamuoyunda oluşabilecek baskıları, çalışmaların sivil amaçlı olduğu noktasında ikna etme girişimidir.

9.2.4. Tesla ve Eastlund'un Çalışmaları

Elektriğin AC kullanımını ilk bulan kişi Tesla'dır. Tesla'nın RADAR ve toprak delici tomografi cihazlarına ait teorileri de bulunmaktadır. Yine Tesla'nın 1891 yılında icat ettiği Tesla Bobini günümüzde de başta radyo ve televizyon olmak üzere birçok elektronik alette kullanılmaktadır. Haarp ise aslında Eastlund'un icadı olarak kabul edilse de "Tesla kaynaklıdır" denilebilir.

Yaşadığı dönemde kimilerince bir deha, kimilerince de bir çılgın olarak görülen Tesla, belki de dehasını ticari amaçlı kullanamamasından dolayı yapabile ceklerini tam bitiremeden çok fakir bir biçimde hayatını tamamlamıştır. Bazı kaynaklarda da belirtildiği gibi belki de, elektriğin kablosuz ve ücretsiz verilebileceğini açıklamasıyla bu sonu hazırlamıştı. Bir gösterisinde 25 mil öteden 200 lambayı kablosuz olarak yakabilmesi belki de bunu doğrulamakta.

Kimine göre Eastlund' un patent kaynaklarından ilki de aslında 8 Aralık 1915'de The Newyork Times'da yayınlanmıştı." Bu makalenin bir kısmını aynen aktarıyorum;

"Mucit Nicola Tesla'nın patent başvurusunda bulunduğu planlar insanları hayal gücünü zorlayan olasılıkları temsil eden ve Thor'un tanrıları kızdıran insanları cezalandırmak için gökyüzünden gönderdiği yıldırımlara benzer bir gücü vaat eden bir makinenin esaslarını oluşturuyordu... İcadın uzayda saniyede 300 mil hızla yol alacak sinyallerle insansız kanatsız motorsuz bir aracı sadece elektrik gücüyle küre üzerinde istenen noktaya yöneltebileceğine, bu araç sayesinde istendiği takdirde büyük bir yıkım yaratılabileceğine söylemekle yetinelim. Dr. Te sla dün şöyle dedi:

Henüz böyle bir şeyin detaylarına girmenin zamanı gelmedi. Barış zamanında büyük şeyleri temsil eden bir prensibe dayanılarak ortaya çıkarıldı. Ama savaşta da çok büyük amaçlar için kullanılabilir. Yine de tekrarlıyorum henüz böyle şeyl eri konuşmanın zamanı gelmedi. Kablolar olmadan elektrik enerjisinin gönderilebilmesi ve uzaktan yıkıcı etkiler yaratılabilmesi mümkün. Bunu mümkün kılan kablosuz bir

vericiyi çoktan yaptım ve teknik yayınlarımda açıkladım; Aralarında 1,119,732 patent numarasıyla belirteceğim icadımda var. (Eden, Weapons of Total Destruction)

Bu türde bir vericiyle herhangi bir uzaklığa herhangi bir miktarda elektrik enerjisini yansıtabilir ve gerek savaşta gerekse barışta çok çeşitli amaçlarla kullanabiliriz. Bu sistemin evrensel uygulamaya konmasıyla, kanun ve düzenin korunması için ideal şartlar oluşturulabilir, çünkü bu şekilde enerjinin adalet için kullanılması verimli sonuçla getirecektir ama aynı şekilde saldırı ve savunma amaçlı da kullanılabilir. Yayılan gücün yıkıcı olması şart değildir, çünkü varoluşun kendisi buna dayandırılırsa enerjinin geri çekilmesi veya sağlanması, bugün silah gücüyle elde edilen sonuçları getirecektir.” .(Smith, 1998, sy.46–47)

Yine Eastlund'un belittiği 22 Eylül 1940'da The Newyork Times'da yayınlanan bir diğer makalede de Tesla'nın tele güç sırrını hükümete verebileceğinden bahsederken, bu gücün 250 mil uzaklıktan düşman uçaklarını yok edebileceğini yada ülkenin etrafında görünmez bir kalkan oluşturabileceğinin söylendiğini işaret ediyordu.

Bu makaleye göre Tesla bu sistemin bir ışın aracılığıyla işlevini yerine getireceğini ve bu ışının 4 yeni icadı kapsadığını belirtiyordu. “Bunlardan biri yüksek vakum gerekliliğini ortadan kaldırarak açık hava da ışınlar ve diğer enerji ifadelerini üreten bir yöntem ve araç, ikincisi çok büyük elektrik gücü üreten bir yöntem ve süreç, üçüncüsü bu gücü arttırmak için bir yöntem, dördüncüsü ise muazzam elektrik püskürtücü güç üretmek için bir yöntem. Bu, sistemin projektörü veya tabancası olacak. Işını hedefe yönlendirmek için gereken voltaj 50000000 volt gibi bir potansiyeli temsil ediyor. Bu inanılmaz voltajla, maddenin elektrik partikülleri yıkım amaçlı olarak hedefe fırlatılabilecek.” (Smith, 1998, sy.47–48)

Eastlund'un sahip olduğu en önemli 3 patentinin de ilk kayıtları Tesla'ya aittir, Eastlund bunları geliştirmiştir. Eastlund'un ilk patenti; Dünya'nın atmosferi, iyonosferi ve/veya manyetosferinde bir bölgenin değiştirilmesi için kullanılan method ve cihaz içindi. Bu ilk HAARP projesi patenti ABD Patent Dairesi'nde 4.686.605, numarası ile kayıtlıdır. Bundan sonra 4.712.158 ve 5. 038.664 no'lu kayıtlarla Bernard Eastlund tarafından 2 patent daha alındı.

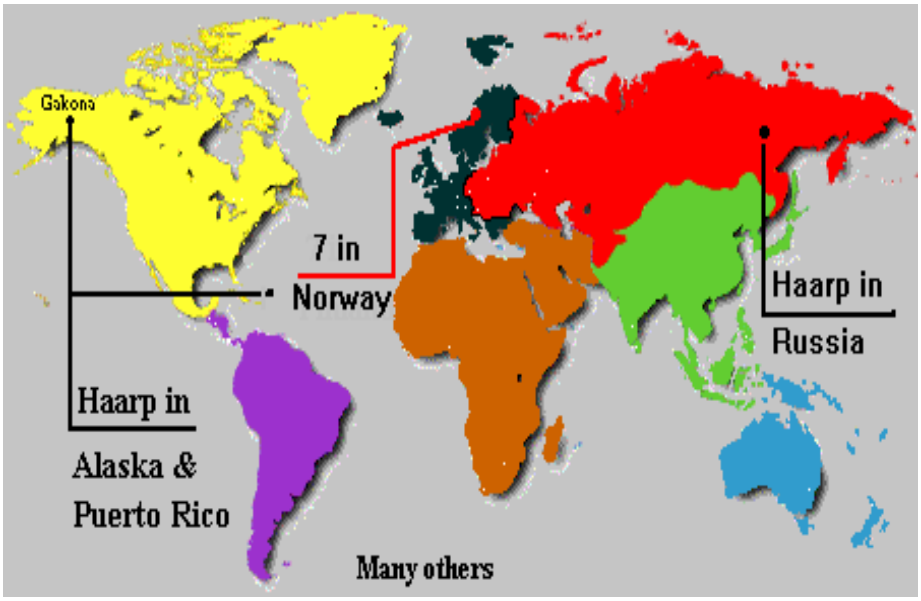
Alınan ikinci patent Dünya'nın farklı noktalarına iyonosferik çıkıntının kullanılmasıyla yansıtılmasını tanımlamaktadır.

5.038.664 kayıtlı üçüncü patentte temel olarak, dünya yüzeyinde rölativik partüküller oluşturma metodunu tanımlamaktadır.

Bugüne kadar Eastlund'un orijinal çalışmasından elde edilen on bir ayrı patent bulunmaktadır. Bu patentler, iyonosferin yansıtıcı değişkenliğinin, "radyasyonsuz nükleer ölçekli patlamalar", "güç yayan sistemler", "ufuk-ötesi radar sistemleri" ve "'nükleer füze bulma veya yok etme sistemleri" gibi kullanımlar için faydalanılabileceğini tanımlamaktadır. Bu patentler diğer askeri patentlerle birleştirilebilir ve savaş alanı uygulamaları için kullanılabilecek durumdadır. (Eden, Weapons of Total Destruction)

9.2.5. Diğer Çalışmalar

Bu iyonosferik ısıtıcılardan haberdar olan yalnızca ABD değildir. Nitekim Ruslar'da Eastlund'un teknolojisine dayalı araştırmalar yapmaktadır. Norveç, Brezilya ve Porto Riko'da da benzer üsler bulunmaktadır. Pek çok kaynakta değinilen bu üslerle ilgili olarak “cyberspaceorbit.com” adlı sitede bir harita yayınlanmaktadır.



Şekil 9.26 Haarp çalışmalarının yapıldığı yerler
(http://www.cyberspaceorbit.com/indexbck.html)

Bu teknolojiye sahip olma yarışındaki Ruslar'ın Moskova'daki ABD büyükelçiliği çalışanları üzerinde, özellikle de büyükelçinin odasına yönlerdirdikleri düşük frekans seviyeli bombardıman nedeniyle bazı kaynaklarda da değinildiği gibi "2 büyükelçilik çalışanı kanserden öldü." (http://www.tuncayozkan.com)

Hatta bazı kaynaklar, bu sinyalleri keşfeden CIA'nın yaklaşık 10 yıl boyunca bunu konsolosluk çalışanlarından da gizleyerek, bu bombardıman sonucunda olan durumları kontrol ettiği, bir noktada kendi çalışanlarını bir kobay gibi incelendiği yönündedir.

ABD'nin bu alandaki ilk kapsamlı projesi olan Pandora'nın nasıl başlatıldığı ABD Savunma Bakanlığında Bilim Danışmanı olarak görev yapan Dr. Stephen Possony tarafından şu sözlerle açıklanacaktır:

"Moskova'daki elçinin ve çalışanlardan bir çiftin lösemi nedeni yle ölmesinden sonra orada ne olduğunu çok dikkatli araştırmamız için ani bir emir geldi. Dev bir proje

yürürlüğe girdi. Bu tamamıyla Pandora Projesi olarak bilinen hale geldi ve bu Cia'yı, İleri Araştırma Projesi Ajansı ARPA'yı, ABD yönetimini, donanmayı ve orduyu içeren TUMS, MUTS ve BAZAR projeleri gibi çok sayıda paralel projeyi ihtiva etti." (Özkaya, 2003, sy.47)

ABD'nin elektromanyetik teknolojiler konusunda kısa zamanda ilerlemeler sağlaması başta NSA olmak üzere birçok haber alma teşkilatını da uzak tan beyin okuma ve yönlendirme konusunda çalışmalara yönlendirmiştir. (Özkaya, 2003, sy.49)

Bunun haricinde Dünyaca bilinen Rus Ağaçkakanı radyo sinyali çalışmaları da bir diğer kanıttır."Ağaçkakan sinyali, Tesla'nın büyütücü vericisini kullanan Har p benzeri bir aracın, ilkel bir modelini kullanıyor gibi görünüyordu. Savunma Bakanlığının resmi açıklaması, bunun düşman füze fırlatma operasyonlarını tespit eden bir ufuk çizgisi radar sistemi olduğu yönündeydi. Ufuk Çizgisi Üzerindeki Geri Dağılım (OTH-B) programının Harp tesisinin ilk sakininin yapmayı planladığı şey de tam olarak budur. Bu yayına müdahale edici Elektromanyetik sinyaller, 3 ila 30 MHz aralığındaydı ve genellikle saniyede 10 kez tekrarlanan atışlarla yayınlanıyordu." (Smith, 1998, syf93)

Sovyet Ağaçkakan sinyali 1975'in sonlarında keşfedildi. ABD'de "21 MHz.'de yayın yapan radyolarda toplanabilen bu yüksek frekanslı sinyaller, bir ağaçkakanın çıkardığı sesler gibi ' tak, tak, tak ' seslerine haizdi. Bunların kaynaklarının en sonunda Riga, Latvia'daki üç istasyonda izi bulundu. Yayılan sinyaller 7 –7,5 Hz. olan yerkürenin doğal zemin elektromanyetik alanından 25 –30 defa daha kuvvetli olabilmekteydi. Dünyadaki memelilerin beyni tabii olarak 7 –7,5 Hz.'lik frekansla yüklüdür. Fakat memelilerin %25'inin beyinleri Ağaçkakan sinyallerinin 10 Hz.'lik modülasyonlarıyla etkilenebilir. Sıra ile bu modülasyonlar doğrudan insan beynine yollanacak bir mesaj tipini taşımak için adapte edilebilirler. Yayın frekansında olduğu gibi yayınlanan pulsun karakteri stiğinde sık sık vuku bulan değişmeler birilerine bunun uzaktan kontrol veya telemetri için kullanılabildiği fikrini verdi."(Özkaya, 2003, sy.89)

Ancak hala bu sistemin tam olarak ne amaçla çalıştığı tespit edilememiştir. Bununla beraber Ağaçkakan sinyali ile ABD kuzeybatısının düşük frekanslı dalgalarla bombalandığının ve bu frekansın insan beyninin kontrol edilebilme aralığında olduğunun ABD kamuoyunca da tartışıldığı görülmektedir. Bu sinyallerin 60 Hz'lik enerji hatlarıyla emilerek tekrar yayınlanabildiği iddiası da ilginç olduğu kadar dikkat edilmesi gereken bir önem taşımaktadır.

Rusya'nın "büyük daha iyidir" adıyla bilinen programları, çok büyük miktardaki elektromanyetik enerjinin iyonosfere gönderilerek, tekrar dünyaya geri döndürülmesini başarmıştı. Bu yüksek güç seviyelerinde, enerjiyi yıkıcı bir biçimde depolayan yükselten ve boşaltan bir pil gibi davranan iyonosfer uzaktaki bir hedefi saniyeler içinde yok edebilirdi. Fakat bu dönemde Ruslar, bu enerji ışınını yönetip, kontrol edebilecek nitelikteki bilgisayarları kullanma imkânlarına sahip değildi.

ABD ise, CRAY ve EMASS bilgisayar sistemlerine sahip olmasına rağmen, Rus ısıtıcılarının güç çıktı yeteneklerine sahip değildi. Haarp bu durumu değiştirecekti.

9.2.6. Haarp Tehditi

New Mexico'daki Kirkland Hava Kuvvetleri Üssü'nde, Phillips Laboratuarı Elektromanyetik Etkiler Bölümü'nde, biyolojik etkiler grubu başkanı olan Dr. Cletus Kanavy, insan ve hayvanlar üzerinde yapılan klinik çalışmalarla elde edilen bilgilerinin; Haarp'lada yakından alakalı olan ELF sinyallerinin, davranış bozuklukları, sinir ağı rahatsızlıkları, embriyonik doku hasarları, katarakt, kan kimyasının bozulması, metabolizmanın değişime uğraması, salgı ve bağışıklık sisteminin sindirilmesini, beyin kimyasında ve yapısındaki normal olmayan değişikliklere neden olduğunu belirtmektedir. Hatta çalışmaların yapıldığı dönemde, denek amaçlı kullanılan kurbağalarda da ani ve açıklanamayan mutasyon örneklerine rastlanmıştı.

HAARP teknolojisi şu anda, dünya çapında birçok bilim adamı tarafından şüpheyle karşılanmaktadır. Haarp'in resmi yetkilileri ise HAARP'in ancak, Hawai'deki Keck Rasathanesi ya da New Mexico'daki Geniş Kompleks kadar öldürücü etkisi olduğunu ifade etmektedirler.

Gelecekte Dr. Eastlund'un teknolojileri g ezegenimizi değiştirecek. Elektrik enerjisi belki de iletim hatları kullanılmadan her yere iletilebilecek. Doğal felaketler minimize edilebilecek, iklimler daha yumuşak geçecek ve gıda üretimi düzenli yağışlar ve iklim etkisiyle daha artacak. Küresel haber leşme ucuzlayacak, kritik ozon yenilenebilecek. Daha da önemlisi nükleer silahlar, düşman tarama ve bulma sistemleriyle tamamıyla kullanılmaz hale getirilebilecek. Eastlund'un keşifleri ucuz enerjiyi sağlayacak ve sağladığı gıda avantajları ve benzer yarar larla insanlığın birbiri ile olan uyumunu sağlayacaktır.

Fakat bu insani uygulamalar hala gelecekte gözükmemektedir. Patentler askeri kontrol altında tutulmaktadır. Bu bakımdan aslında ölüm ışını ya da zihin kontrol mekanizmaları gezegenin daha yaşanır bir hal almasında kullanılmasından önce görülmesi daha olası gibidir.

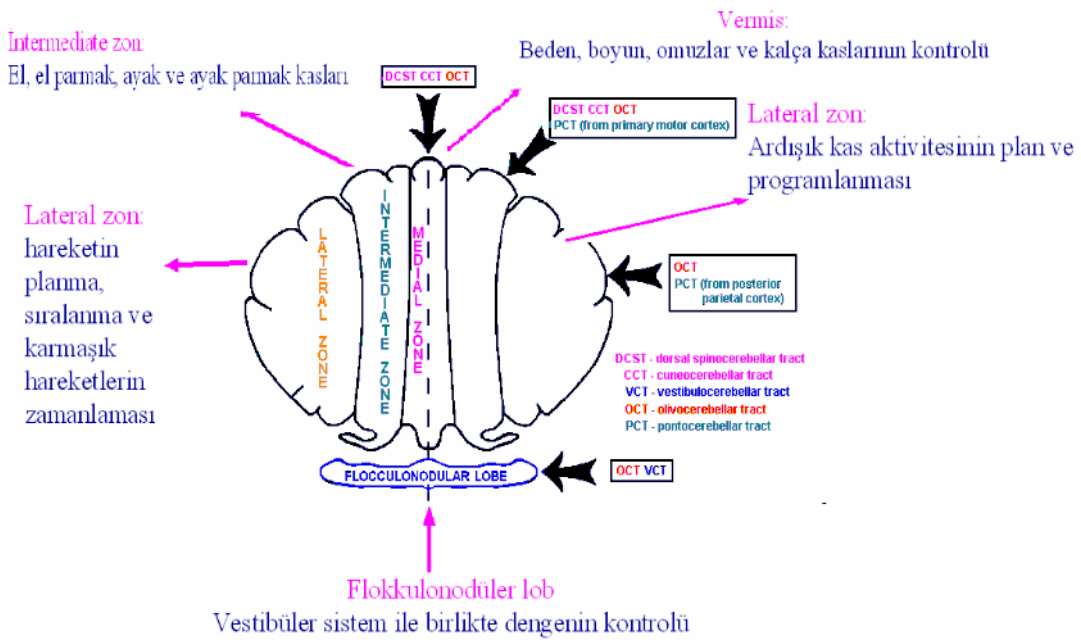
Ülkenin rejimi ne olursa olsun iktidarın en büyük destekçisi, çağlar boyunca hep silah olmuştur.

HAARP benzeri bir donanımın inşası, küçük bütçeli fakir ülkeler için bile mümkündür. Nükleer yakıt içermeyen ve gizlice yapılabilen bu teknolojilerin gücü çok yüksektir. Bu yeteneğe ilk olarak sahip olan ülke, diğer benzer donanımları bulup yok edebilir ve bununla Dünya üzerinde kendi güç dengesini istediği gibi sağlayabilir. Aslında bu noktada, bu tür ölümcül bir gücün, bir devlet ya da bir terör örgütünün elinde bulunması noktasında da çok fark bulunmamaktadır.

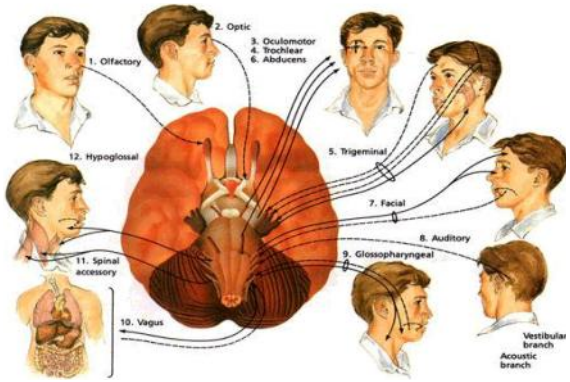
9.3 Beyin Kontrol

Beyin sürekli değişip, güncellenebilen, milyonlarca bilgiyi aynı anda işleme becerisine sahip yaşayan bir bilgisayar gibidir. Yapısını anlamak, kendimizi anlamaktır. Beyin pek çok biçimde bozulabilir ve bu bozukluk ruhsal hastalıklarla sonuçlanabilir. Dolayısıyla beyni oluşturan unsurları, nasıl çalıştığını, nasıl korunacağını, nasıl güncelleyip en az hasarla düzgün bir şekilde çalıştıracağımızı bilmek zorundayız. (http://www.beyinrehberi.com/ExPage3.asp)

Aşağıdaki şekillerde beyin bölgelerinin hangi işlevleri yerine getirdiğini Prof.Dr. Sacit Karamürsel'e ait iki çalışmadan şekilsel olarak derledim. Ancak beyin için sadece şekillerdeki işlevleri yerine getirdiğini söylemek yanlış olur. Beyin hala tam anlamıyla çözülemeyen bir organdır. Onu kontrol etmek bir insanı kontrol etmek demektir.



Şekil 9.27 Beyin Bölgeleri (Karamürsel, Serebellum)



Şekil 9.28 Fonksiyonlarının Yönetimi (Karamürsel, Beyin Sapı ve Orta Beyin, slayt 68)

Prof. Dr. Selim Şeker'e göre beyin, dışarıdan yapılabilecek elektromanyetik müdahalelerle yönlendirilebilecek, elektronik bir sistem olarak değerlendirilmelidir. (Özkaya, 2003, sy.75)

Beyin işlevlerini yerine getirirken pek çok etmene bağlı olarak çalışır. Dışarıdan gelen her türlü uyarım beyin fonksiyonlarının yerine getirilmesi bakımından oldukça önemlidir. Elektromanyetik müdahalelerde beyni olumsuz etkiler ve bu durumda farklı amaçlı kullanılabilir. Özellikle beynin kontrolü amacıyla Tesla'dan itibaren pek çok çalışmalar yapılmıştır ve yapılmaya da devam etmektedir.

Şeker, bu konuda yapılan çalışmaların eskilere dayandığının ancak modern anlamda bilinen çalışmaların 2.Dünya Savaşında yeni len Almanya'nın bilim adamlarının Rusya ve ABD'ye götürülmeleriyle başladığını ifade etmektedir.

Ancak, zihin kontrol deneyleri konusunda günümüz çalışmalarının ilham kaynağı, çalışmalarını 1969 yılında kitabında yayınlayan İspanyol Dr. Jose Delgado'dur. (Şimşek, 2005, sy.22)

Delgado yayınladığı kitabında; "Duygu ve ifadelerin elektronik olarak insan beynine nakledilmesi olanaklıdır ve insanların tek bir düğmeyle robotlar gibi kontrolü olanaklıdır" ifadesini kullanmaktadır. Delgado kafasındaki sistemi; "Ya kin bir gelecekte insanların insansız makinelerle bir radyo komünikasyon sistemi ve

elektronik devre ile takviye edilmiş bir beyin aracılığı ile yönetilmesi mümkün olacaktır" şeklinde fikirlerini açıklamaktadır. (Özkaya, 2003, sy.84 -85)

“Elektronik gözetim amacıyla, beynin konuşma merkezindeki elektrik faaliyetler, kurbanın sözlü düşüncelerine çevrilebilir. Kulağı devre dışı bırakarak, ses haberleşmesinin dogrudan beyne gitmesini sağlayarak, Uzaktan Nöral Denetim, şifrelenmiş işaretleri, beynin işitme korteksine gönderebilir. NSA ajanları bunu, paranoid şizofreninin karakteristiği olan işitsel halisünasyoları taklit ederek, kurbanların gizli olarak takatini kesmek için kullanabilirler. Kurbanla herhangi bir temas olmaksızın, Uzaktan Nöral Denetim, bir kurbanın beynindeki görsel korteksteki elektrik faaliyetlerini planlayabilir ve kurbanın beynindeki tasvirleri (görüntüleri) bir videonun monitöründe gösterebilir. NSA ajanları kurbanın gözlerinin gördüğü her şeyi görürler. Görsel hafıza da görülebilir. Uzaktan Nöral Denetim gözleri ve optik sinirleri atlayarak (devre dışı bırakarak), doğrudan görsel kortekse görüntü gönderebilir. NSA ajanları, beynin programlama gayesi için, gözetim altındaki kişi REM uykusunda iken, onun beynine gizlice görüntü yerleştirmek için bunu kullanabilirler.” (Özkaya, 2003, sy.95)

Bu konuda yapılan çalışmalar uzun bir süre, yapan ülkeler tarafından gizli tutulmuştur. Konu hakkındaki ilk belge ise, 1977 yılında İnsan Kaynakları Komitesi Sağlık ve Bilim Araştırmaları Alt Komitesi tarafından hazırlanan raporda, CIA zihin kontrol araştırmaları listesinde MKDELTA, MKULTRA, MKNAOMİ, MKCHKWIT ve MKOFTEN projelerinden bahsedilmesi gösterilebilir.(Keith, 2006, sy.71)

Beyinlere çok farklı biçimlerde müdahale etmek mümkündür. Yapılan çalışmalarda arenadaki bir boğa vücuduna yerleştirilen çipler vasıtasıyla beyninin öfke ve huzur merkezlerine elektrik verilmesi suretiyle, bir kumandanın tuşuna basılarak önce saldırgan daha sonra uysal bir hale sokulmuştur, ya da bir kedi, psiko -motor olarak adlandırılan gazlarla, beyninin korku bölgesinin aktif hale getirilmesi suretiyle bir fareden bile korkması sağlanmıştır.(Özkaya, 2003, sy.60 -62)

Bu çalışmalar elbette hayvanları kontrol etmek için yapılmamaktadır. Örneğin, bir savaş anında bu gazın insanlara verilmesindeki durumu hayal etmek bile bu tarz çalışmaların önemini ve diğer devletler için doğuracağı riskleri ortaya koymaktadır.

Çalışmaların olabilecek amaçlarından birini CIA eski başkanlarından Richard Helms'in, Watergate soruşturmalarında Warren Komisyonu`na verdiği bilgilerden anlayabiliriz.

"Helms Komisyona verdiği bilgilerde şöyle demiştir:

Yapılan araştırma göstermiştir ki SSCB kendi sisteminin isteklerine uygun politik görüşe bağlı olacak şekilde, halkının davranışlarını düzenleyebileceği bir kontrol teknolojisi geliştirmeye çalışmaktadır. Bundan böyle aynı teknolojiyi daha karışık bir yaklaşımla, bilgiler kodlanarak insan hedeflerine yöneltilebilecektir. Bu insan zihinleri harbi olacaktır." (Şimşek, 2005, sy.18)

Bu konuda yapılan çalışmalar yıllar içerisinde büyük bir hızla artmıştır.

Prof.Dr. Selim Şeker yapılan çalışmaları şöyle özetlemektedir;

- "CIA'nin desteklediği Dr.Ewen Cameron izinsiz olarak hastalarda hafızanın silinmesi ve yeni kimlik oluşturulması konusunda çalışmıştır.
- Dr.Rose Delgado'nun hayvan ve insanlar üzerinde yaptığı deneyler sonucunda elektronik simulasyon ile kızgınlık, şevhet, hırs, yorgunluk gibi, aşırı hisler oluşturulabileceğini göstermiştir. Ayrıca kişilik değişikliklere neden olan bölgeyi de bulmuştur. 1969'da yakında bilgisayarın beyinle iki yönlü radyo iletişimi kuracağını ifade etmiştir.
- 1974 yılında California, Stanford araştırma enstitüsünde elektronik mühendisi ve sinir fizyologu Dr.Lawrence Pinneo "bir kişinin aklını okuyabilecek bir bilgisayar sistemi geliştirdi". Time dergisinin temmuz,1974 sayısında akıl okuyan bilgisayar diye haber olmuştur. Bu çalışma Pentagon tarafından

desteklenmiştir. Dr.Pinneo ayrıca bilgisayardan doğrudan beyne bilgi aktarılması için gerekli teknoloji mevcuttur demiştir.

- Rus bilimadamı Dr.Ross Adey'in geliştirdiği Lida isimli makine insan ve hayvanların davranışlarını değiştiriyor, uyuşturuyor.(psychotronıc araştırmalar) associated press (82/83) göre Kuzey Kore benzer cihazı kore savaşında beyin yıkamak için kullanmıştır. Bu cihaz ABD'de denenmi ş ve patent almıştır.
- 1980 yılında ileri seviyede araştırma projeler ajansı (ARPA) senede 1 milyon ABD dolarını Illinois, Ucla, Stanford, MIT ve Rochester üniversitelerinde insan beyninin yaydığı dalgaları anlamak için harcamıştır. Hedef, bir makine geliştirerek insanların ne düşündüklerini beyin dalgaları sayesinde anlamak. Beyin dalgalarını şu an 1 m civarında bir mesafeden rahatlıkla alınabiliyor. Nihayi hedef uzaydaki uyduya yerleştirilmiş beyin okuyan makina ile dünyayı taramak…Bu anlatılanlar bilgisay arlar için tamamen çözülmüştür. Yani bilgisayarlarda yapılabilen bütün işlemler insan beyni içinde Kör olan insanlara yerleştirilen mikrocip sayesinde görmeleri sağlanıyor. 28 şubat hedeflenmektedir. Örnek uçak bilgisayarına yerden girilerek pilota rağmen uçak yere indirilebilinir veya istenilen herşey yapılır.
- Avusturalyalı bilimadamları beyin anahtarı "mind switch" dedikleri bir cihaz geliştirdiler. Cihaz insanların beyin dalgalarının kullanarak elektrikle çalışan cihazları , tv, lamba, müzikseti çalıştır maya yarıyor. İnsanın gözlerini bir saniyeden fazla zaman kapalı tuttuğunda oluşan alfa beyin dalgaları kullanılıyor. Sistemin güvenirliği %90'nın üstünde."(Şeker, 2004, sy.9 -10)

Beyin kontrolünün insan üzerinde kullanılmasıyla oluşan etkiler ise çok fark lı biçimlerde görülmektedir. Bunlardan bazıları ise şu biçimdedir;

- "Hafıza kaybı ve davranış bozuklukları
- Duyulan sesin yönü, şiddeti ve içeriğinin değişmesi
- Göz kapaklarını denetleyerek konuşmanın bozulması
- Şiddetli kalp çarpıntısı

- Zahmetli işler sırasında omuzları ve kolları zorlayarak kazalara neden olma
- Bir şey yaparken dirseklerin dürtüklenmesi ve işe engel olma
- Bacaklarda ağrı ve gereksiz hareketlenme, sağ ve sola sallanma ve aşırı sertleşme
- Ayağın zor ulaşılan yerlerinde kaşınma ve kızarmalar
- Sırttaki büyük kaslarda kasılmalar
- El hareketlerini kontrol edilmesi
- Düşüncelerin okunması veya dışarıdan düşünce iletilmesi
- Hareket eden hayali görüntüler görülmesi
- Göz kapaklarının sürekli açık tutulması
- Sürekli kulak çınlaması
- Çene ve dişlerin bir neden yokken titremesi”(Özkaya, 2003, sy.55-56)

Beyin kontrol yöntemleri tarihsel süreç içerisinde çok çeşitlilik göstermektedir.

Zihin kontrolü deneylerinde ilk kullanılan madde olan LSD, psikokimyasal bir maddedir. Bu maddeyi alan kişide, halüsinasyonlar görülür, bu kişi canlı ve neşeli olur, güçlü olma duygusu taşır, ardından farklı düşünce ve davranışlar içerisine girer. Bu maddeyi alan bir kişi, inandırıldığı konuda olağanüstü eylemler gerçekleştirebilmektedir. Bu kişiler birini ya da kendilerini öldürmeye meyilli bir hale gelmektedirler.

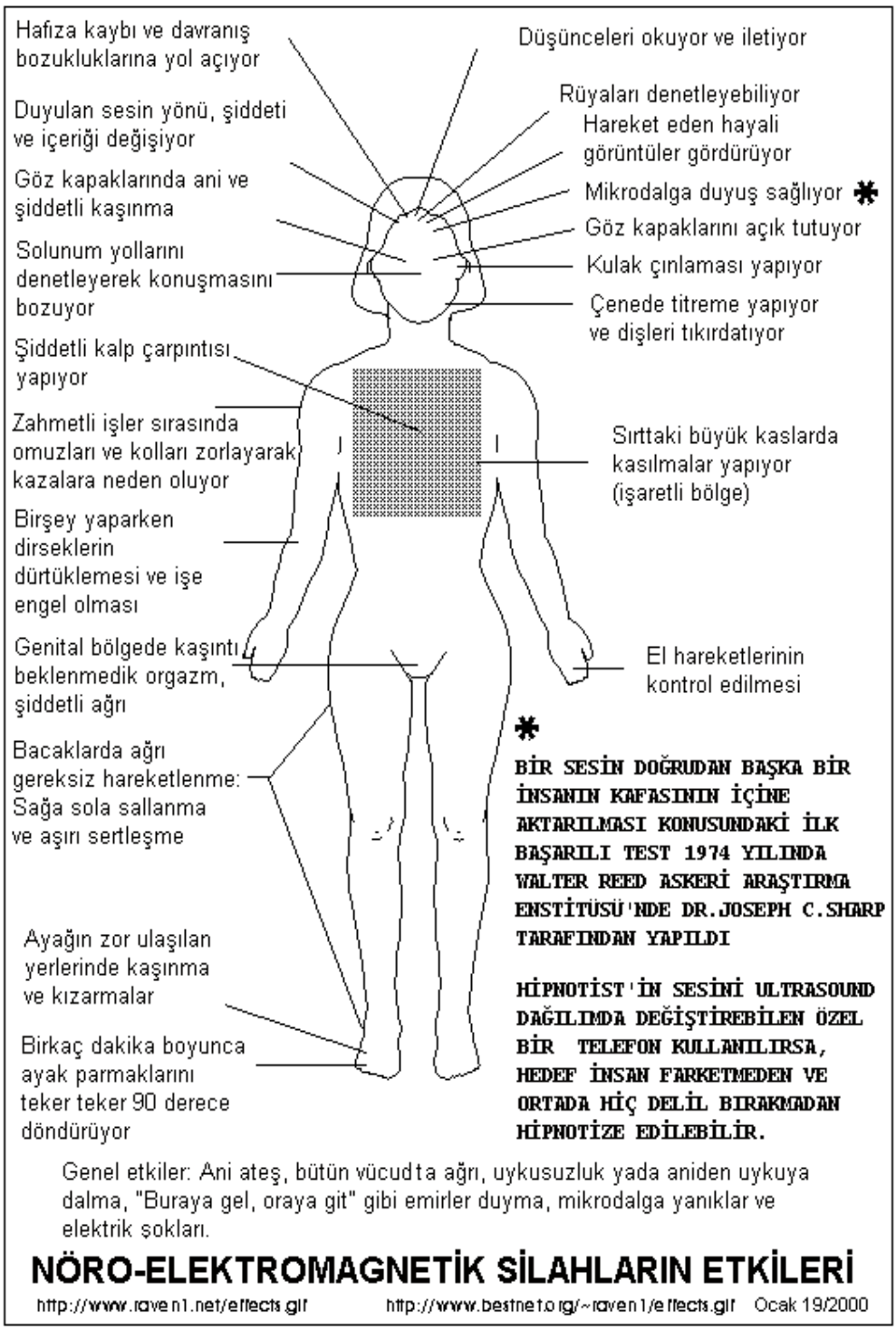
İkinci Dünya Savaşı'nda ise hem Hitler’in hem de Amerikan ordusunun "Amphetamin" isimli uyarıcı kimyasalı askerlere kullandırarak onların savaş gücünü arttırmayı hedefledikleri bilinmektedir.

Hipnoz ile hipnotik uykuya geçen kişinin, vücut ve beyin uyur, fakat terapistle, kişi arasında seçici bir algılama alışverişi kanalı açılır. Böylece kişi hipnoz yapan kişi tarafından yönlendirilebilir, düşünceleri ve duyguları değiştirilebilir. Bu tedavi amaçlı kullanılabildiği gibi siyasi amaçlı olarak da kullanılabilen bir yöntemdir. (Nevzat Tarhan, 2002, sy.30-31)

Kimyasal ve psikolojik yöntemlerin yanında insanların beyinlerine yerleştirilen elektronik implantlarla da insan beyini dolayısıyla insan yönetilmek istenmektedir.

Çağımızda yaşanan gelişmeler teknolojiye dayalı yeni savaş yöntemlerini devreye sokmaktadır. Bu yöntemler sadece virüsleri, kimyasal ve biyolojik silahları değil, biyoteknoloji ve elektroniği de içine almaktadır. Örneğin Körfez Savaşıyla, NATO'nun Yugoslavya'ya karşı gerçekleştirdiği müdahalede mikrodalga silahların denendiği biliyoruz. Bu müdahale sadece haberleşme sistemini bozma anlamında değil, aynı zamanda elektromanyetik dalga silahlarının kullanımıyla, hedeflenen insan kitlesi üzerinde kusma, baş ağrısı, sinir bozuklları gibi etkilerin yaratılmasıyla sonuçlanmıştır. (Özkaya, 2003, sy.82)

Kısmen kanıtlanan iddialara göre NSA, genel adıyla beyin kontrol işlemini, "Sinyal İstihbaratı" ile yapmaktadır ve bu sistem elektrik geçen her şeyin çevresinde oluşturduğu temel prensibe dayanarak çalışmaktadır. Sinyal istihbaratının ilk aşaması kontrol altına alınacak kişinin 3-50 Hz arasında değişen bir değere sahip ve herkes de farklı olan dalga boyunun tespit edilmesidir. Bu tespit edildikten sonra uydular ve çeşitli araçların kullanılmasıyla kişinin beyin beyin haritası çıkarılarak kişinin sözlerine hatta gördüklerine bile ulaşılabiliyor. Bizi esas ilgilendiren nokta da sinyal istihbaratının tersten uygulanabilmesiyle kişinin çok farklı biçimlerde yönlendirilebilmesidir. .(Özkaya, 2003, sy.45)



Şekil 9.29 Nöromanyetik silahların etkileri

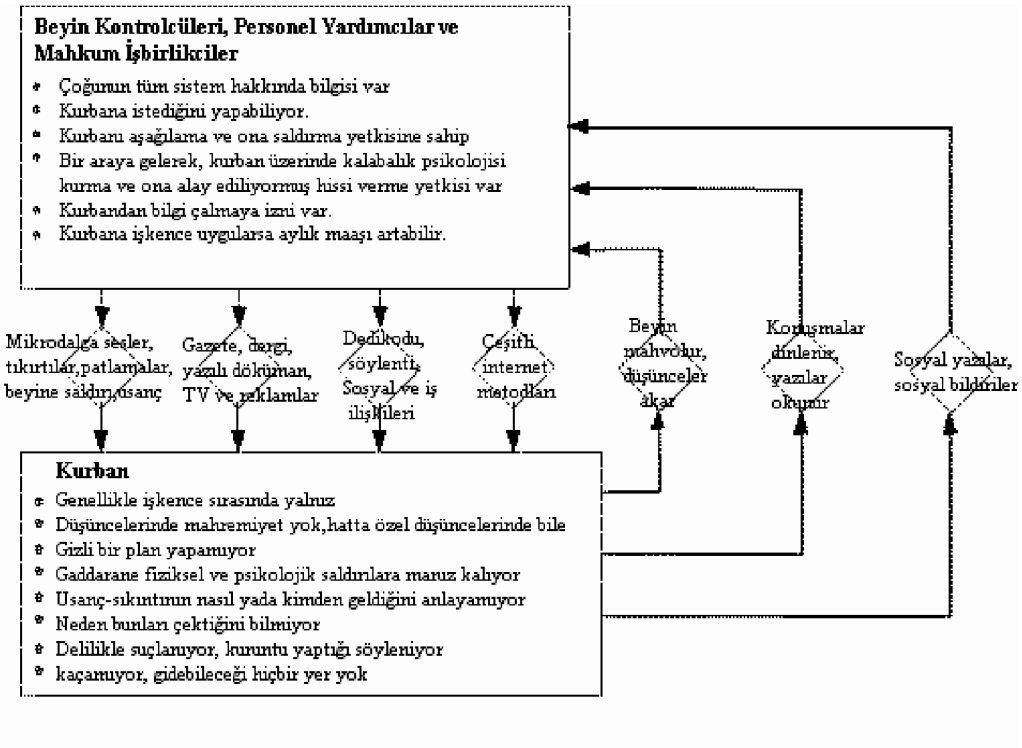
Mikrodalga silah endüstrisinin en son gelişmeleri konusunda öne sürülenler ise ürkütücüdür. Tüm internet ve cep telefonları ağının mikrodalga silah endüstrisinin etkisi altına girdiği söyleniyor. İddiaya göre, bu teknolojide meydana gelen yeni gelişmelerle artik insan beyni dalgalarının klonlanması söz konusu oluyor. EEG sinyallerinin içindeki kızgınlık, nefret, kıskançlık, depresyon korku gibi duyguların dalga boylarının tespit edilip bilgisayar aracılığıyla izolasyonu gerçekleştirildikten sonra, seçilen duygu dalgasının başka bir insan beynine klonlanmasının mümkün olabileceği söyleniyor.

Mikrodalga silahlarının geliştirilmesinin ilk aşaması beyne yerleştirilen mikro devreler aracılığıyla beynin kontrolü ve yönlendirilmesi olmuş, yani elektronik aracılığıyla beyne fiziksel müdahale yollarının araştırılması teknolojik olarak mikrodalga silahların geliştirilmesini sağlamıştır. (Özkaya, 2003, sy.84 -85)

1930'larda Hess'in kullandığı, beynin içine çok ince teller sokularak bunların dışarıda kalan uçlarına da, "uyarıcı-alıcı" (stimoceiver) denilen kibrit kutusu büyüklüğündeki cihazlar yerleştirilerek, beynin bu cihazlar yardımıyla uyarılması sağlanıyordu. Günümüz teknolojisinde ise bu iş, 1-2 santimetre boyundaki küçük çiplerle fazlasıyla yerine getirebilmektedir. (Şimşek, 2005, sy.22)

Hatta çağımızda teknolojinin, çip veya beyne sokulmuş elektrotlara ihtiyaç duymadan, belli merkezlerden beyine gönderilen elektromanyetik dalgalar sayesinde kurbanın beyin fonksiyonlarına müdahale edebilecek noktaya geldiği iddia edilmektedir.

Aşağıdaki şekil beyin kontrolünde kullanılan yöntemleri ve geri beslemeyi ifade etmektedir. Buna göre saldırgan bunu yapmak için genellikle kurban hakkında bilgiye sahiptir. Yöntemin uygulanması noktasında da yetki ve egrekli teknolojiye sahiptir. Görüldüğü gibi yöntemler elektronik, psikolojik ve sosyal bilimler tabanlıdır.



Şekil 9.30 Beyin Kontrol Geri Besleme Şeması

Bu çalışmalar artık eskisi kadar gizlenen, bilinmez kavramlar değildir. Beyinle ilgili çalışmalar çok farklı alanlarda kullanılmaktadır. Artık bir fuarda bile bu çalışmaların ipuçlarını görebiliriz.

Örneğin, bu sene Comdex Fuarı'nda tanıtılan bir gözlük zihin kontrolü gibi iddialı bir görevi işaret etmeketdir. Bu gözlüğü gözünüze taktığınızda oluşturduğu kimi renk, ses ve piksel şekilleriyle sizi yorucu bir günün ardından rahatlatabiliyor. (Radikal Gazetesi, Beyin kontrol gözlüğü, 09.04.2008)

Benzer bir örneği de 17.04.08'de Hürriyet gazetesinde yayınlanan bir yazıyı gösterebiliriz. Yazıya göre Pentagon, kullanacağı PCASS adlı, portatif yalan makinesi ile Afganistan'da aradığı kişilere ulaşmayı deneyecek Bu makinenin özelliği sorulan sorulara verilen cevaba göre yeşil, sarı ya da kırmızı ışıkların yanması suretiyle kişinin doğru söylediğini, makinenın kararsız kaldığını ya da kişinin yalan söylediğini belirtmesidir. Bu makinenin ilginç bir özelliği de 7500 dolar gibi düşük bir maliyetinin olmasıdır.

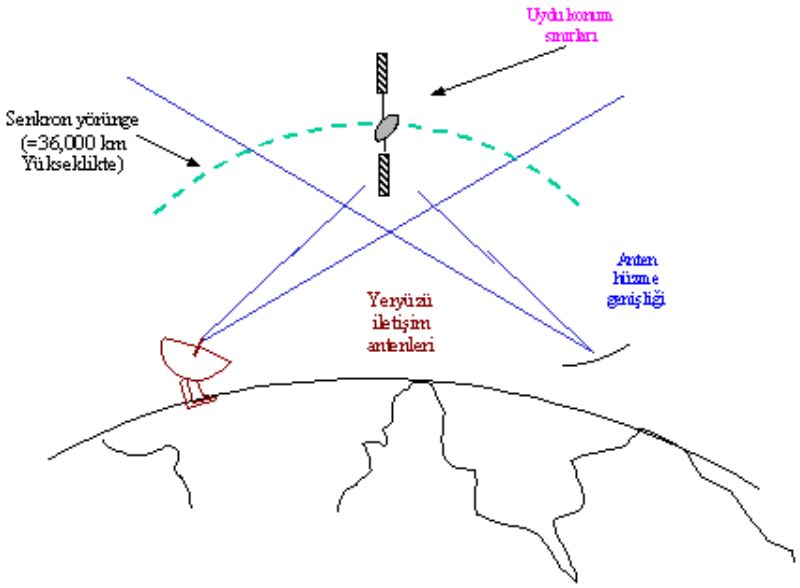
Ancak üzerinde çalışmalar yapılan ve bazı birimlerce de kull anılan karmaşık yalan makineleri, beyindeki hareketleri inceleyerek sonuca varmaya çalışıyor. Daha önce yapılan çalışmalar, yalan söylenirken beynin yedi, doğruyu söylerken de dört bölgesinde faaliyet olduğunu ortaya koymuştu. Ancak PCASS beyinle ilgili bi r analiz yapmıyor.

Zihin kontrol operasyonları çok çeşitli yöntem ve teknolojilerle uygulanabilmektedir. Bu yöntemlerle bir kişi robot haline getirilerek istenildiği gibi yönlendirilebilmekte, hatta kişi intihar ettirilebilmektedir ya da kişiye, ist emediği bir şey yaptırılabilmektedir.

Ülkemizde de bu çalışmaların üzerlerinde uygulandığını iddia eden kişiler bulunmaktadır.

9.4 Uydu Teknolojisi

İkinci Dünya Savaşı sayesinde büyük gelişme kaydedilen güdümlü füze ve mikrodalga haberleşme teknolojileri ve bunların beraber kullanımları Uydu Haberleşme Sisteminin doğmasına neden olmuştur. Uydu iletişim sistemleri; bir uydudan, uydunun yörüngesini, uzaydaki konumunu ve çalışmasını denetleyen bir yeryüzü istasyonundan ve uydu üzerindeki transponder (alma fre kansını, gönderme frekansına çevirici) aracığıyla gerçekleştirilen ve iletişim trafiğinin gönderilmesini (çıkarma hattı, uplink) ve alınmasını (indirme hattı, downlink) sağlayan yer terminalleri ağından oluşmaktadır.(Balık, 2005, sy.8)



Şekil 9.31 Uydu Haberleşmesi

9.4.1 Uydu Haberleşme Sistemi

Güvenli uydu iletişimi, bugünkü orduların öncelikli gerekliliklerinden biridir ve uydular, Irak operasyonu sirasinda komuta zincirinin savaş bölgesi ile ilgili gerekli bilgilerin alınmasında önemli rol oynamıştır. Uydu iletisiminin askeri anlamda önemini belirtmek amaciyla Koalisyon güçleri komutanlarından General David D.McKiernan "ordumuzda teknoloji gelişti... Savaş alanında yüzlerce mil öteyle uydular üzerinden konuşma imkânı bulabiliyoruz... Komutanlar nerede o lduklarını, bir sonraki kararları için nelere ihtiyaç duyduklarını konuşabiliyor ve bunları bir birliktelik içinde gerçekleştirebiliyorlar. Bu bize karar vermede ve kararımızı herhangi bir birime en hızlı şekilde iletme imkanı tanımıştır." demektedir.

Pentagon da General Buford Blount video telekonferans ile röportaj verirken taktik uydu haberlesmesinin (TACSAT) önemini ayrintili olarak belirtmistir. "TACSAT iletisimi bizim için çok uzak mesafelerle konusmada çok yeni bir sistemdi. Necef'te bir günde 230 km ileri gitmistik. Temel olarak saldiri ve çatisma seklinde iki ayri

durum mevcuttu. Kaynaklarin yönlendirilmesi, önceliklerin belirlenmesi, her bir komutanla konuşarak güçleri nerede, biz harekatı yürütürken savaş alanında neler yapacakları konularında komuta ve kontrol yetenegine sahiptik."(Köken, 2005, sy.9)

9.4.2 Uyduların Teknik Özellikleri

Daha uzun mesafelere iletişim gereksinimi sonucunda ortaya çıkan uydular günümüzde haberleşme ve güvenlik alanında hem sivil hem de askeri alanda büyük önem taşımaktadırlar. Askeri alanda istibarat amaçlı, sivil alanda da radyo -televizyon yayınları, meteoroloji gibi pek çok konuda kullanılmaktadır.

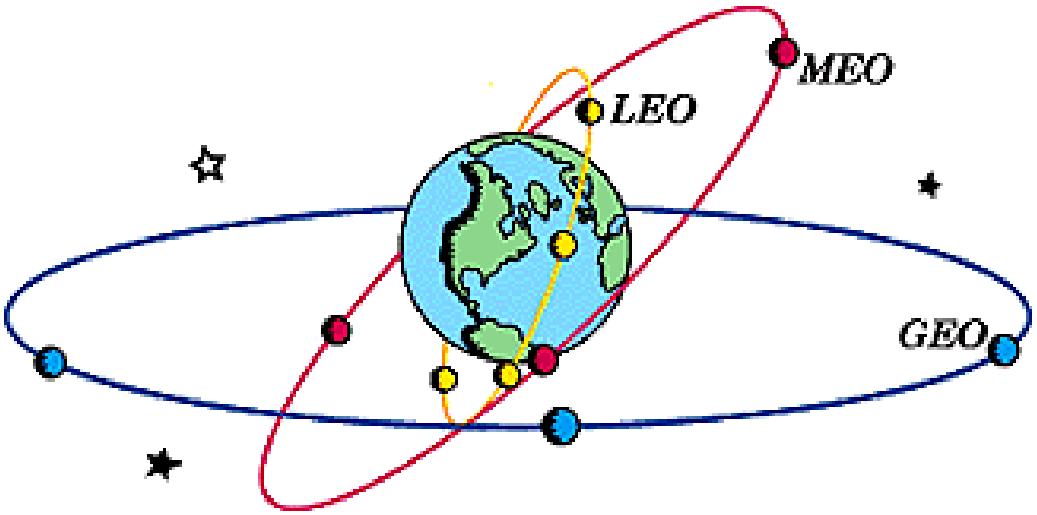
İlk uydular bugünküne uydulara oranla daha hafif ve elipsoyit bir şekil çizerek dünya etrafında dönüyorlardı. Ancak, uydunun yüksekliğine ve çizdiği yola bağlı olarak dünya etrafındaki turunun değişen süresi nedeniyle haberleşmenin dünya yüzeyindeki istasyonun uyduğu gördüğü süreyle kısıtlı kalması, sağlıklı bir iletişim açısından çok sayıda uyduya gereksinimi doğuruyordu. Bu durumda tabiî ki maliyetleri olumsuz etkiliyordu.

Bu olumsuz durumun ortadan kaldırılması amacıyla, uydunun ekvator etrafında dönmesine ve yüksekliğinin 22.300 mil(yaklaşık 35.800 km) olmasına karar verildi. Bu yükseklikte dünya yüzeyin görüş alanı yaklaşık, dünyanın 1/3 nü kaplıyordu. Böylece 3 uydu tüm dünyayı kapsayabiliyordu. (Yaşar, 2005, sy.7)

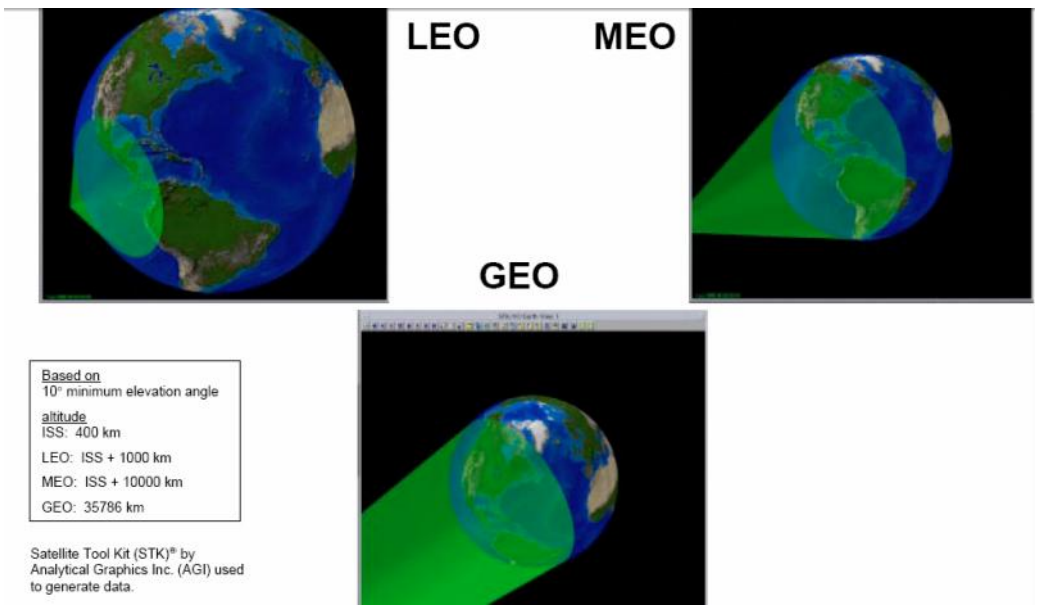
Uydular, yörüngelerinin şekillerine, ağırlıklarına, sağladıkları hizmetlere ve benzeri pek çok kritere göre sınıflandırılabilir ancak yaygın olarak kullanılan sınıflandırma türü uyduların yeryüzünden yüksekliklerine göredir. Yeryüzüne en yakın olan Alçak Yörünge Uyduları (Low Earth Orbit - LEO), Orta Yörünge Uyduları (Medium Earth Orbit- MEO) ve Yerdurağan Yörünge Uyduları (Geostationary Earth Orbit-GEO) uyduları bu sınıflandırmaya giren uydu türleridir. LEO ve MEO uydulara aynı zamanda Yerdurağan Olmayan Uydular (Non-Geostationary, NGEO) da denilmektedir. Uyduların özellikleri ve yörüngeler aşağıdaki tabloda gösterilmiştir."

Tablo 9.5 Uyduların Özellikleri (Bayhan ve Alagöz, 2007)

Özellikler	LEO	MEO	GEO
Yükseklik (km)	200-3000	5000-13000	36000
Kapsama Alanı(km)	Dar	Orta	Geniş
Gecikme (ms)	10-20	80-100	270
Yol kaybı	Az	Orta	Çok
Hareketlilik	Çok	Orta	Sabit
Ağ karmaşıklığı	Karmaşık	Orta	Az



Şekil 9.32 Yörünge Türleri(Derman, 2005)



Şekil 9.233 Geo, Leo ve Meo Uyduların Kapsama Alanları (Brackey et all Goldberg, Falk, Tappis, 1999)

Üyesi bulunduğumuz uydu sistemleri ise INTELSAT, EUTELSAT ve INMARSAT'tır. INTELSAT uzay kesimi Atlantik, Pasifik ve Hint Okyanuslarınınüzerinde bulunan uydulardan oluşmaktadır. 200'den fazla ülkede video, telefon ve veri hizmeti vermektedir. EUTELSAT ise Avrupa'nın sabit ve mobil haberleşmesini sağlamak amacıyla INMARSAT ise Uydular aracılığı ile denizde can ve mal güvenliğini sağlamak amacıyla kurulmuştur. (Gülşen, 2007, sy.16)

Uydu Haberleşmesinde temel kaynak radyo frekans (RF) spektrumudur. Frekans bandları ve yere göre durağan yörüngedeki boylamların tahsisi ITU tarafından yapılmaktadır. ITU dünyayı üç frekans bölgesine bölmüştür ve ülkemiz "1. Frekans Bölgesi"nde yer almaktadır. Frekans bandı seçimi, atmosferik iletim, anten kazançları, demet genişliği ve kullanılacak donanım gibi eknik özelliklere göre yapılmaktadır. (Selek, 2004, sy.7)

Tablo 9.6 Frekans Aralıklarının Harf Olarak Gösterimleri (Selek, 2004, sy.8)

Yaklaşık Frekans Aralığı (GHz)	**Harf**	**Tipik Kullanım**
1.5-.1.6	L	Mobil-uydu Hizmeti (MSS)
2.0-2.7	S	Yayın uydu Hizmeti (BSS)
3.7-7.25	C	Sabit uydu Hizmeti (FSS)
7.25-8.4	X	Devlet uyduları
10.7-18	K_u	Sabit uydu Hizmeti (FSS)
18-31	K_a	Sabit uydu Hizmeti (FSS)
44	Q	Devlet uyduları

Tablo 9.7 Uydu Haberleşme Sistemleri Tarafından Kullanılan Frekans Aralıkları (Selek-ITU 2002, 2004, sy.9)

Frekans Bandları			Tipik Kullanım
Band (GHz)	Yukarı bağlantı (GHz) (Band genişliği)	Aşağı bağlantı (GHz) (Band genişliği)	
6/4 (C-Bandı)	5.725-6.275 (550 MHz)	3.4-3.9 (550 MHz)	Ulusal uydular
	5.850-6.425 (575 MHz)	3.625-4.2 (575 MHz)	Uluslararası ve hizmetiçi uydular
	6.725-7.025 (300 MHz)	4.5-4.8 (300 MHz)	Ulusal uydular
8/7 (X-Bandı)	7.925-8.425 (500 MHz)	7.25-7.75 (500 MHz)	Devlet ve askeri uydular
13/11 (Ku-Bandı)	12.75-13.25 (500 MHz)	10.7-10.95 11.2-11.45 (500 MHz)	Ulusal uydular
13-14/11-12 (Ku-Bandı)	13.75-14.5 (750 MHz)	10.95-11.2 11.45-11.7 12.5-12.75 (1000 MHz)	Frekans bölgesi 1 ve 3'de uluslararası ve hizmetiçi uydular
		10.95-11.2 11.45-11.7 12.5-12.75 (750 MHz)	Frekans bölgesi 2'de uluslararası ve hizmetiçi uydular
18/12	17.3-18.1 (800 MHz)	11.7-12.5 12.5-12.75	Uydu yayın hizmetleri için besleme linkleri
30/20 (Ka-Bandı)	27.5-30.0 (2500 MHz)	17.7-20.2 (2500 MHz)	Uluslararası ve ulusal uydular
40/20 (Ka-Bandı)	42.5-45.5 (3000 MHz)	18.2-21.2 (3000 MHz)	Devlet ve askeri uydular

Günümüzde en çok kullanılanlar C bandı ve Ku bandıdır. Kullanılacak anten büyüklükleri de, yayılan dalganın taşıdığı enerji ve dalga boyu ile ters orantılı olarak değişmektedir. Yani en büyük anten C bandı için kullanılırken, en küçük antende Ku bandı için kullanılmaktadır. (Yaşar, 2005, sy.7)

Şekil 9.34 Uydunun Uzayda Fotoğrafı (Şahin, Uydular (Suni Peykler))

9.4.3 Uyduların Kullanım Alanları

- Uydularda mesafe önemli bir sorun değildir. Maliyet açısından 2000 km.lik bir link bağlantısının, 10 km.lik bir link bağlantısına göer farklılığı yoktu r.

- Uydular doğal genişbant araçlardır. Genişbandn tüm imkânları uydular vasıtasıyla her yere aktarılabilir.

- Bir uydu, antenlerinin gördüğü noktalarda bulunan tüm istasyonlarla çalışabilir

- Uydular, dağ, okyanus, şehirler vb. gibi doğal sınırlayıcılara bağlı olarak çalışmazlar. Bir Devlet, farklı noktalar arasındaki haberleşmesini uydular vasıtasıyla sağlıyarak bu noktalar arasında bütünlük sağlayabilir.

- Bir uydu sistemi tanımlanan servislerle küçük ve büyük şehirlere hizmet verebilir. Geleneksel karasal habe rleşme ağları büyük ve yoğun şehirlerde eski sistemler tercih edilmektedir. Bu nedenle endüstrinin akışı ve onun bilgi işleme imkânlarının çok kırsal yerlere aktarılması uydular vasıtasıyla sağlanabilmektedir.

- Uyduların getirdiği yetenekler yeni konseptle rin doğması sonucunu ortaya çıkarmaktadır. Eski uygulamaların kapsamları ydular vasıtasıyla genişletilebilirken, örneğin acil durumlarda da uyduların kullanımı oldukça kullanışlıdır.(Morgan and Gordon, 1989, sy.3 -4)

Elbert'te kitabında, uyduların 8 yararı başlığı altında özetle şu noktalara değinmektedir.

1. Lokasyondan bağımsız olarak mobil/kablosuz haberleşme imkânı,

2. Geniş alanlarda hizmet sağlayabilmesi,

3. Çok büyük band genişliği sağlaması,

4. Karasal Altyapıdan bağımsız olması,

5. Yer istasyonlarının hızlı kurula bilmesi ve yönetimde sağladığı avantajlar,

6. Düşük haberleşme maliyeti,

7. Tüm noktalar arasında eşdeğer servis karakteristikleri,

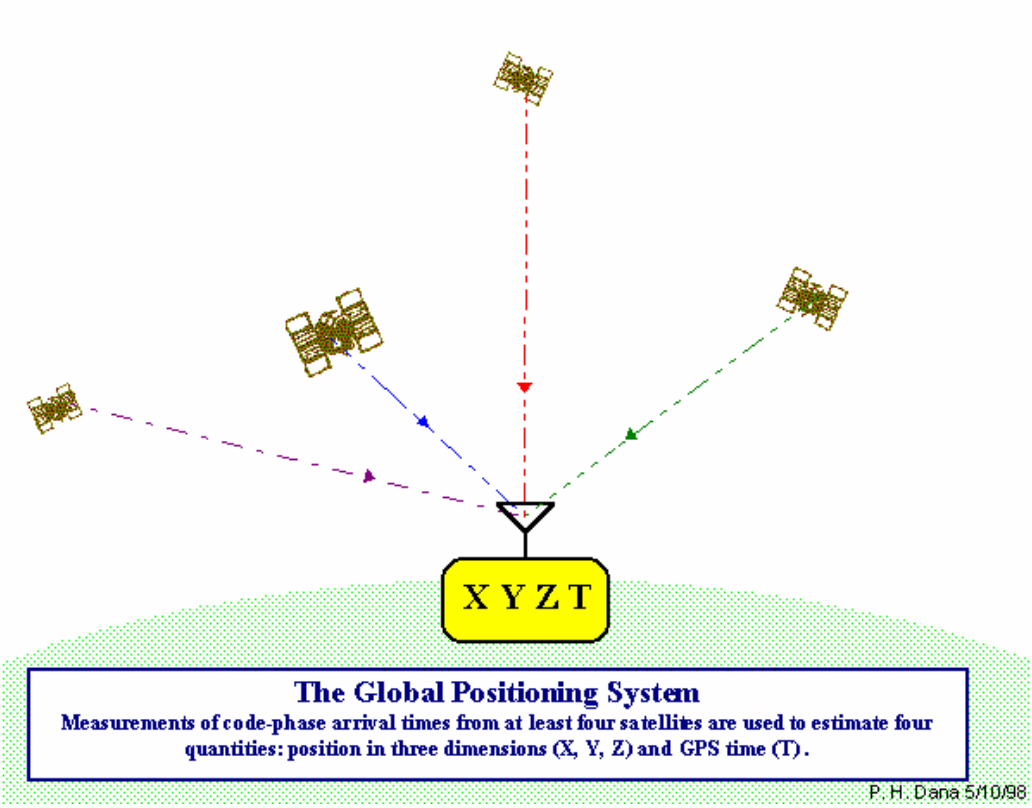
8. Tek bir elden yönetim ve tüm servislerin sağlanması.(Elbert Bruce, 1999, sy.8-12)

Uyduların kullanımı gün geçerek artmaktadır savaşlar artık uzay arenasına taşınmaktadır.

R.L. Haupt ve S.E. Haupt un "Practical Genetic Algorithms" çalışmasında 1991'deki Çöl Fırtınası Harekâtının, ilk uzay savaşı olduğu belirtilmektedir. Çöl Fırtınası Harekâtı, GPS sistemlerinin kara ve hava unsurları tarafından kullanılmasına sahne olmuştur. ABD Milli İstihbarat Ofisi tarafından yerleştirilen casus uydular savaş alanında istihbarat sağlayarak bilgi üstünlüğünün tesis edilmesine katkıda bulunmuş ve Savunma Destek Programı kapsamında yerleştirilen ihbar ikaz uyduları, balistik füzelerin fırlatılış anından itibaren tespit edilmesinde kullanılmıştır. (Savtek 2002 Savunma Teknolojileri Kongresi, Cilt II: Posterler, 2002, sy.196)

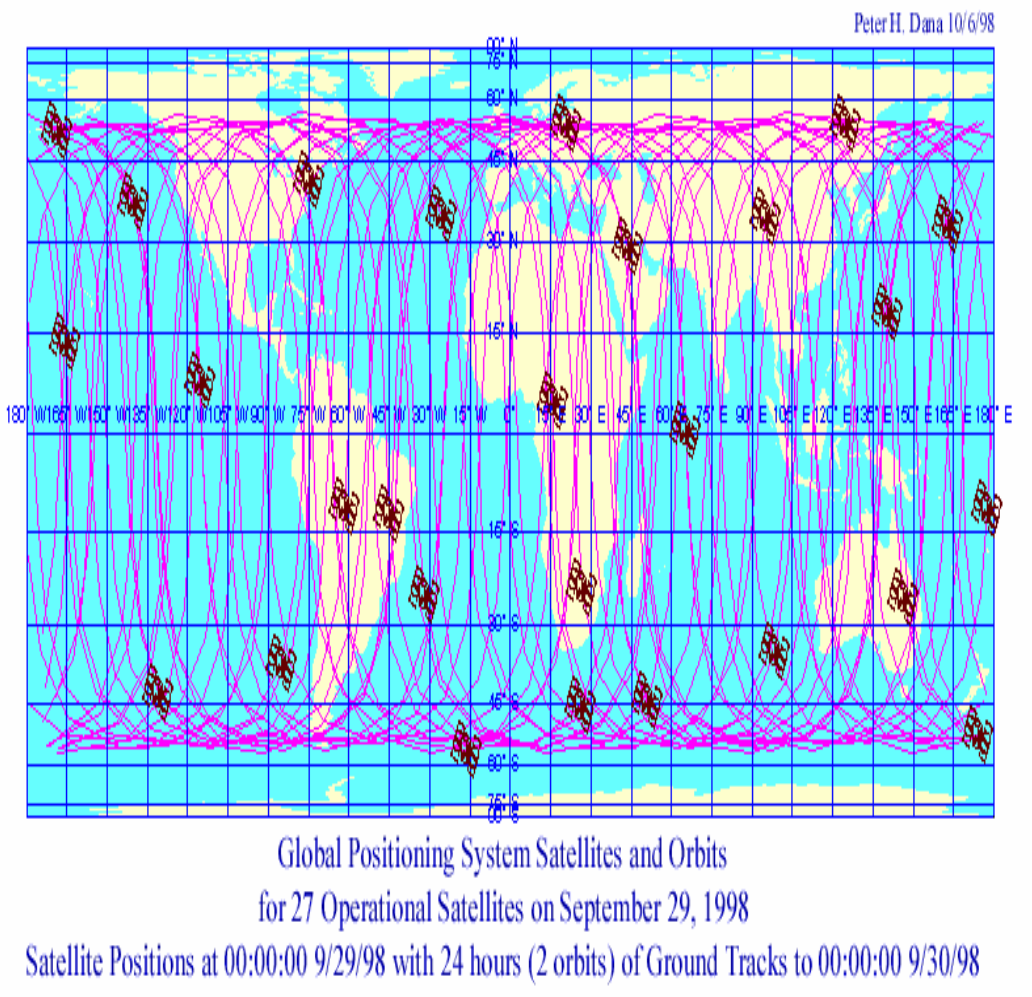
9.4.4 Küresel Konumlama Sistemi (Global Positioning System - GPS)

GPS, ABD Savunma bakanlığınca finanse ve kontrol edilen bir sistemdir. Sistemin Dünya genelinde sivil kullanımı olmasıyla beraber sistem askeri amaçlı olarak tasarlanmıştır. GPS, alıcısı içerisindeözel olarak kodlanmış sinyallerin işlenmesi ile pozisyon, vektörel hız ve doğrultunun hesaplanmasını sağlar.



Şekil 9.35 GPS (Dana, Global Positioning System Overview, 1999)

GPS sistemi, her birinde 4 GPS uydusu olmak üzere 6 dairesel düzlemden oluşmaktadır. Böylelikle 3 boyut ve zaman içerisinde pozisyonun hesaplanması nda kullanılan GPS sistemi, 24 adet uydudan oluşmaktadır. Her bir uydunun Dünya etrafındaki turu da 12 saatte tamamlanmaktadır.



Şekil 9.36 GPS Sistemi (Dana, Global Positioning System Overview, 1999)

GPS sistemleri de kullanım alanları hızla gelişmekte dir. Sistem sivil amaçlı pşarak tarım, belediyecilik, lojistik ve Haritacılıki gibi alanlarda kullanılabilmektedir. (Özdemir, 2003, sy.80)

Bunlar gibi sivil amaçlı kullanımlarının yanında, sistemin askeri kullanımı da yaygınlaşmaktadır. ÖrneğinAfganistan' da şimdiye kadar 5000'den fazla GPS güdümlü füze atılmıştır.

GPS, güdüm ve navigasyon desteğinin yanında senkronizasyon da sağlamaktadır. GPS'in gelecekte, GPS verilerini ve veri bağlantılarını kullanarak dost güçlerin ne zaman nerde olduğunu takip ederek, dost ateşi sonucu kayıpları önlemek amacıyla düşünülen 'Mavi Güç takibi' projeside yeni bir uygulama alanı olarak karşımıza çıkmaktadır. (Savtek 2002 Savunma Teknolojileri Kongresi, Cilt II: Posterler, 2002, sy.196)

"GPS sistemlerinin Askeri Alandaki Uygulamaları;

- Acil Durum Müdahaleleri
- Akıllı Füzelerin Yönelendirilmesi
- Askeri Birliklerin durumlarını belirlenmesi
- Düşman Kuvvetlerinin izlenmesi
- Kıtalararası füzelerin eşzamanlı yönlendirilmesi
- Uzaydan Balistik füzelerin imhası
- Helikopterle Mayın koordinatlarının tespiti olarak sayılabilir."(Özdemir, 2003, sy.80)

9.4.5 Echelon

1948 yılında NSA, Avustralya Savunma Bakanlığı, İngiltere, Kanada ve Yeni Zelanda İletişim Teşkilatları ile UKASA adıyla bilinen anlaşma çerçevesinde kurulan Echelon sistemine Almanya, Japonya, Norveç, Güney Kore ve Türkiye'nin de taraf olarak katıldığı öne sürülmektedir. (Çimen, 2006, sy.249)

Echelon 1998 yılı itibarıyla, dakikada 2 milyon, günde ise 3 milyar telefonu dinleyebilmektedir. Belirli anahtar kelimelere göre yer tespiti de yapabilen sistem özellikle ABD tarafından etkin bir biçimde kullanılmaktadır. Sistem; yeryüzünde kurulu 5 yer istasyonu, 5 ana stratejik ve 100'ün üzerinde irili ufaklı uydudan oluşmaktadır. (Özdemir, 2003, sy.78-79)

Ancak Rusya, Çin, Danimarka, Ho llanda, İsviçre, Fransa ve İsrail gibi devletlerin de benzer sistemler kullandığı bilinmektedir.

Echelon sisteminin verimliliği internetin yaygınlaşmasıyla daha da artmıştır. Ayrıca, ABD'nin okyanus tabanındaki telefon hatlarına da bu sistemin kontrolünü s ağlamak amacıyla dinleme cihazları yerleştirdiği bilinmektedir. Sistemi uyduların yanında, ABD'nin nükleer denizaltıları, okyanuslarda sürekli seyir halinde bulunan gemileri, özellikle RG-135 tipi uçakları sahip oldukları gelişmiş bilgisayar sistemleri il e beslemektedir.

İnternetin yaygınlaşması ve e-devlet projelerinin sistemi beslenmesi bakımından bu konular üzerinde daha da dikkatle durulması gerekmektedir. İnternette gezen, bu sisteme aişt e-postaları, haber gruplarını, sayfaları, sohbet odalarını kull anan herkes aslında arkasında iz bırakmaktadır. Hem bireysel hem de ticari olarak bunu ağlar üzerinde dolaşan bilgiler Echelon ve benzeri sistemler tarafından yakalanabilir özellik taşımaktadır.

Avrupa Parlementosu'nda 1998 yılında yayınlanan ilk ra pora göre ABD, Avrupa'daki telefon, faks ve e-posta haberleşmenin %90'ını Echelon sistemiyle denetliyebiliyordu. Echelon'un ayrıca, Amerikan şirketleri için rakiplerin sırlarını çalma suretiyle bu şirketlere milyarlarca dolar kazanç sağladığı da yapılan id dialar arasındadır.

Dünyanın gizli bir kulak tarafından dinlendiği aslında 6 Eylül1960'da, Rusya'ya iltica eden iki NSA görevlisinin basın toplantısında, NSA'nın 2000 dinleme istasyonuyla pekçok ülkeyi dinlediği şeklindeki iddialarına kadar uzanmak tadır.

Dünyadaki bütün telefon, faks, telsiz, SMS ve elektronik posta iletişimini dinleyen Echelon'un varlığı resmi olarak ilk kez, 23 Mayıs 1999'da Avustralya, Canberra'daki Savunma Sinyalleri Müdürlüğü (DSD) Başkanı Martin Brady'nin yaptığı açıklama ile ortaya çıkmıştır. 1999 yılında yapılan bu ilk resmi açıklamadan sonra Avrupa Birliği'de bu sistem üzerindeki çalışmalara, ABD'nin dünyayı dinleme faaliyetlerinin bir benzerini gerçekleştirmek amacıyla daha yoğun bir biçimde hız vermiştir.

“Avrupa Parlamentosu'na 1999'da elektronik istihbarat konusunda sunulan ikinci raporun yazarı olan Duncan Campbell'e göre Echelon, ABD'nin en büyük istihbarat örgütü olan Ulusal Güvenlik Dairesi (NSA) tarafından, ticari ve askeri iletişim uyduları aracılığıyla yapılan habe rleşmeyi zaptedip incelemek için geliştirilen bir araç. Sistemin öteki parçaları da internet, yeraltı ve denizaltı haberleşme kabloları, telsiz haberleşmesi ya da büyükelçiliklere yerleştirilen gizli aygıtlar aracılığıyla yapılan her türlü iletişimi zapted iyor ya da özel uydularla haberleşme sinyallerini topluyor.”

Amerika'da dinleme faaliyetlerini NSA (Ulusal Güvenlik Ajansı), FBI (Federal Araştırma Bürosu) yürütmektedir. (Dede, 2002)

9.5 Nanoteknoloji

Teknolojinin hızlı gelişimi 1900’lü yılların sonlarında nanoteknolojiyi doğurmuştur. Temel bilimlerin doğrudan uygulaması olarak nitelenebilecek teknolojilerin başında yarı iletken teknolojisi, biyoteknoloji ve nanoteknoloji gelmektedir. Bu teknolojiler aras ında ülkemiz için en önemli olanı, daha gelişim aşamasında olması nedeniyle nanoteknolojidir. Nanoteknoloji genel olarak atom ve moleküllerin bir araya getirilmesi ile fiziksel, kimyasal, biyolojik işlevli nanometrik ölçekli yapıların malzemelerini ve kend ilerini kontrollü biçimde üretme amaçlı bir teknolojidir. (Erkoç, 2007, sy.3–10)

Günümüzde nanoteknoloji ülkeler için stratejik bir önem taşımaktadır. Gelişmiş ülkeler öncelikli alanlarını belirleyip çalışma ve eğitim programlarını geliştirirken, ülkemizde nanoteknoloji araştırmaları daha çok bireysel ve kurumsal düzeydedir. Ancak nanoteknolojinin TÜBİTAK tarafından hazırlanan Vizyon 2023 Programı’na öncelikli alanlardan biri olarak alınması, ülkemiz açısından sevindirici bir gelişmedir.

Nanoteknolojinin önümüzdeki 10–15 yıl içinde yeni bir teknoloji devrimi olarak ortaya çıkacağına inanan teknolojide ilerlemiş ülkeler nanoteknolojiye odaklanarak, ciddi çalışmalar yapmaktadırlar. Bütün bu çabaların altında teknoloji yarışında geri

kalma endişesi dolayısıyla pek çok alandaki rekabet güçlerini korumayı amaçları yatmaktadır. (Çıracı, 2005, sy.4–7)

“Geleceğin teknolojilerinin atom, molekül ve nanoküme boyutlarında malzemenin şekillerinin kontrol edilmesi, aygıtlara dönüştürülmesi, malzemenin ve yüzeylerin tasarlanması öngörülmektedir. Nanoteknoloji önümüzdeki yıllarda sivil ve askerî stratejileri etkileyebilecek bir olgudur. Malzeme, elektronik, eczacılık yanında bugün düşünemediğimiz pek çok yeni uygulama, mühendislik ve tıp alanındaki birçok gelişme nanoteknolojideki ilerlemeler sonucunda mümkün olabilecektir.” (Bilim ve Teknoloji Stratejileri Çalıştayı Konuşma Özetleri, 2006, sy.63)

10. TÜRKİYE'NİN BİLGİ SAVAŞLARINA HAZIRLIK STRATEJİSİ

Türkiye'nin bilgi savaşına hazırlanması açısından, çağın teknoloj ik imkân ve yeteneklerinin belirlenerek, bunları elde etmek amacıyla, bunların temin metodlarının belirlenmesi oldukça önemlidir. Bunların elde edilmesi noktasında gerekli eğitim gereksiniminin ve kurumsallaşmanın nasıl ifade edildiği de büyük önem taşımaktadır.

Bu noktada Türkiye'nin bilgi savaşı stratejisinin belirlenmesinde;

1. Ekonomik, Politik, Sosyal ve Kültürel yapıdaki değişim ve gelişmeler
2. Jeopolitik Durum
3. Çağın gerekliliklerine göre değişen güvenlik anlayışlarının belirlenmesi
4. Türkiye'nin Bilim ve Teknoloji Politikalarının Belirlenmesi
5. Dünya Devletlerinin Bilgi Savaşı Potansiyelleri
6. Türkiye'de Bilgi Savaşı konusunda mevcut durumu

göz önüne alınması gereken noktalardır. (Özdemir, 2003, sy.86)

10.1.Ekonomik, Politik, Sosyal ve Kültürel yapıdaki Değişimler

Çağın getirdiği yeni politik anlayışların iyi analiz edilerek bunlara göre şekillenen kavramlar ve anlayışlar neticesinde ileride karşılaşılabilecek bir bilgi savaşı hazırlığı oldukça önemlidir. Bu bakımdan son dönemde yaşanan politik değişimler dikkatlice irdelenmelidir.

Dr. Şenol Kantarcı'nın TUSAM'da yayınlanan 01.08.2007 tarihli Rusya-ABD: "Koalisyonlar Dönemi mi"? Başlıklı yazısındaki bir bölümde son dönemde yaşanan gelişmeler şu şekilde özetlenmektedir.

ABD'nin 'Moskova'da üstlenmiş komünist tehditi, yaklaşık yarım yüzyıl boyunca hem Amerikan kamuoyunu hem de Batılı müttefikleri, Amerikanın istediği doğrultuda silahlanma yarışına destek vermeye yönlendirmiştir. Kantarcıya göre ABD aslında gerçekte varlığının sebebini ve ilerleyişini özellikle Soğuk Savaş süresince hep SSCB'ye borçluydu ve SSCB'nin aniden dağılması neticesinde de ABD'nin hem düşmanı, hem rakibi hem de emperyalist saldırılar için gerekçesi elinden alınmış olunuyordu.

Almanya'nın birleşmesi, Sovyet ekseninden çıkan Balkan ve Doğu Avrupa ülkelerinin Batı yörüngesine girişi ve sonucu olarak Varşova Paktı'nın dağılışı, NATO'nun yeni işlevini 20 Eylül 2002'de resmen ilan edilen Bush Doktrini gibi hadiseler aslında analizcilerin çoğu tarafından Sovyet İmparatorluğu'nun da tekrar toparlanamayacağı ilkesine dayanarak, Yeni Dünya Düzeni döneminin başlangıcı şeklinde tasvir edilmiştir. Askeri anlamda ABD'nin güçlü olmasına karşın, diğer pek çok alanda ABD'ninde Dünya arenasındaki devlet ve devlet dışı diğer aktörlere ihtiyaç duyduğunu söylemek yanlış olmayacaktır. Çünkü pekçok alanda farklı güçler, çok geniş bir alana dağılmış devlet ve devlet dışı aktörler arasında kullanılmaktadır. (Kantarcı, Rusya-ABD: Koalisyonlar Dönemi mi?, 2007)

Çağın en önemli olgularından olan küreselleşmenin en çok etkilediği konulardan birisi de muhakkak ekonomidir. Günümüzde, küreselleşme süreci üretimin uluslararası boyutunu öne çıkarmış, özellikle bilgi, bilişim, haberleşme ve nanoteknoloji gibi bazı teknolojiler daha da önemli hale gelerek, dünyada bölgeler boyutunda ekonomik bütünleşme hareketleri başlamıştır. Bu çerçevede, 1 Ocak 2007'teki son genişleme ile 27 üyesi bulunan Avrupa Birliği; Kanada, ABD ve Meksika'nın oluşturduğu NAFTA ve Pasifik Bölgesi üç ayrı ekonomik güç odağı olarak önem kazanmıştır.

Bunların yanında, ulusal ve uluslararası gelir dağılımının daha da bozulması değişen dönemin dikkat çeken olumsuzlukları arasındadır. 1995 yılında yapılan

Birleşmiş Milletler Dünya Sosyal Kalkınma Zirvesinde, yoksulluğun azaltılması, üretken istihdamın artırılması ve sosyal bütünleşme konularında acil kararlar alınmıştır. (Bircan, 2002, sy.12)

Dünya Bankası Başkanı Robert Zoellick, 15.04.08 tarihinde yaptığı son açıklamasında, artan gıda fiyatlarının yoksul ülkelerde 100 milyon kişiyi daha yoksulluğa itebileceği uyarısında bulunmuştur.

Nitekim Dünya'da geçtiğimiz yıl, buğday fiyatları yüzde 130, pirinç fiyatları yüzde 70'ten fazla yükselmiştir. Dünya Bankası rakamlarına göre temel gıda maddesi durumundaki bu ürünlerde yaşanan artış, genel olarak gıda fiyatlarının da son üç yılda yüzde 83 yükselmesine yol açmıştır. Bazı uzmanlar ise bu ve benzeri fiyat artışlarının birçok ülkede sosyal ve siyasi çalkantılar yaratabileceği uyarısında bulunmaktadır. Örneğin son dönemde Haiti, Filipinler ve Mısır'da 'gıda isyanları' görülmüştü. (Bircan, 2002, sy.12)

Benzer şekilde Mısır, Fildişi Sahili, Etiyopya, Filipinler ve Endonezya'da yüksek gıda fiyatları aleyhinde gösteriler düzenlenmiş hatta Haiti'de ise beş kişinin öldüğü olaylar sonrasında hükümet düşmüştür.(http://www.ntvmsnbc.com/news/442713.asp)

Yeni teknolojiler, özellikle bilgi, bilişim, haberleşme teknolojilerindeki hızlı gelişmeler, ekonomik ve sosyal yaşamı da önemli ölçüde değiştirmektedir.

Teknolojiyle beraber gelişen rekabet ortamı daha kaliteli mal ve hizmet üretimini hızlandırmış, ürün çeşitliliği artmış, Yabancı sermaye yatırımları dünya ölçeğinde artmıştır. Bilişim yoğun sanayilerin gelişmesi, teknolojinin baş döndürücü şekilde değişmesi, daha nitelikli insangücüne duyulan gereksinimi artmıştır.(Bircan, 2002, sy.12)

Ulusal politika belirleme çalışması yapılması için önerilen alanlar geleceğe yönelik kapsamlı bir kestirim ya da öngörü çalışmasına dayalı olmamakla birlikte konuyla ilgili uzmanların öngörülerine dayanarak Moleküler Biyoloji, Yeni Biyoteknoloji ve bu bağlamda Gen Mühendisliği, Deniz Bilimleri; Denizlerden ve Denizaltı

Zenginliklerinden Yararlanma Teknolojileri, Uzay Bilim ve Teknolojileri, Nükleer Teknoloji şeklindedir.(DPT, 2000, sy.34 -36)

Nanoteknoloji, Bilişim ve Haberleşme tek nolojileri de önümüzdeki döneme şekil vereceği düşünülen teknolojiler arasındadır.

İçinde bulunduğumuz dönemin en önemli hedeflerinden biri, üretim ve eğitim ilişkisinin güçlendirilmesi, eğitimin bu gelişmelere koşut olarak süreklilik kazanması olmalıdır. İşgücünün eğitimi ve niteliğinin sürekli olarak iyileştirilmesi ihtiyacı teknolojiyi üretme noktasında da oldukça önemlidir.

Yeni dönemin belirleyicisi olan bilim ve teknolojiden tam olarak yararlanabilmek, kurumsal ve tüm seviyelerdeki örgütlenmele rde değişikliklerin yapılması zorunluluğunu gelmiştir.

Türkiye'nin çağı yakalamak için köklü yapısal değişim ve toplumsal dönüşümleri gerçekleştirmesi, ülke stratejisi kadar, bu stratejinin hedeflerine odaklı kurumların da uzun dönemli stratejiler geliştir meleri ile olanaklıdır. Özel kuruluşların bunu kendi ve ülke çıkarlarını bağdaştırarak, kamu kuruluşları ise Türkiye'nin hedef ve kalkınma ilkeleri doğrultusunda koordine edilmek suretiyle başarıya ulaşabilirler.(Bircan, 2002, sy.13)

Teknolojik gelişmeyi s ağlamak, başka bir değişle Bilgi Toplumu olmak için 4 ana yapının dikkatle ele alınması ve şekillendirilmesi gerekmektedir:

- Bilginin serbestçe kullanımını ve dolaşımını, bilgi ve iletişim teknolojilerine yatırımı sağlayacak ve girişimciliği özendirecek kur umsal ve ekonomik altyapı (Bilgi ekonomisini sağlayacak çerçeve altyapı (müktesebat)
- Bilgiyi üretebilen, kullanabilen ve paylaşarak yayabilen, eğitimli ve donanımlı insan kaynakları (Bilgi ekonomisi insan sermayesi)
- Radyodan İnternet'e, Telefon'dan uydu si stemlerine kadar geniş bir dağılımda bilginin etkin bir şekilde işlenmesini, dağıtımını ve iletimini sağlayacak dinamik bir altyapı (Bilgi ve iletişim altyapısı)

- Küresel olarak biriken bilgilerden yararlanırken diğer taraftan yerel bilgiyi de değerlendirerek yeni buluşlar yaratacak bir yaklaşım içerisinde; araştırma kuruluşları, üniversiteler, fikir üretimi grupları, özel ilgi grupları tarafından oluşturulan ağlar (Ulusal inovasyon (yenilikçilik -buluşçuluk) sistemleri)

Bilgi Toplumuna Dönüşümün gerçekleştir ilmesinde, ulusal ölçekte işbirlikler ve ortaklıklarla kurulan, kamu, iş dünyası, sivil toplum kuruluşları ve giderek tüm yurttaşları kapsayacak, katılımcı bir bilgi toplumu ağının oluşturulması, bilgi ekonomisine geçişin sürekliliğini sağlayacak, dinamikl erini kalıcı kılacak asıl örgütlenme modeli olarak karşımıza çıkmktadır. Bilgi toplumuna geçişte karşımıza çıkan en temel alt sistem olan bilgi ekonomisi ancak böyle bir ağ yapılanması ile, toplumu gerçek bilgi temelli dönüşüme uğratacak, değer yaratımını güvence altına alacak nitelikte olabiecektir.(E -Dönüşüm Türkiye İcra Kurulu, 2004, sy.7)

10.2 Jeopolitik Değerlendirme

Türkiye, çevresindeki hemen hemen tüm ülkelerin kendilerine ait bazı sorunlarla boğuştuğu, yine aynı şekilde hemen hemen tamamının da Tü rkiye ile sorunlarının olduğu bir coğrafya'da bulunmaktadır.

Konuyla ilgili olarak Vecdi Gönül'e ait Milli Savunma Bakanlığına ait sitede yayınlanan makalenin bazı bölüölerine yer vermek istiyorum.

"Dünyanın güvenlik parametrelerinin değiştiği 21'inci yüzy ılda Türkiye; ulusal ve uluslararası güvenliği etkileyen çok boyutlu, çok yönlü, öngörülmesi güç ve sınır tanımayan asimetrik tehdit ve risklerin yaşandığı, istikrarsız bölgelerin merkezinde yer almaktadır. Başta terörizm olmak üzere, kitle imha silahların ın kontrolsüz olarak yayılması, organize suçlar, yasa dışı göç, uyuşturucu ve silah kaçakçılığı, din istismarcılığı ve etnik milliyetçilik hareketleri bu çerçevede güvenlik politikalarımızda dikkate alınması gereken tehdit ve riskler yaratmaktadır.

Bu gelişmeler; stratejik düşünce, uluslararası ilişkiler, ittifaklar, tehdit ve buna bağlı güvenlik algılamalarında büyük oranda değişime yol açmıştır. Küresel ve bölgesel güvenlik ortamı yeniden şekillenmeye başlamıştır. Şekillenme sonrasında nasıl bir güvenlik ortamının ortaya çıkacağı konusunda net öngörüler ortaya konulamamaktadır. Bu belirsizlik ortamının bir süre daha devam edeceği değerlendirilmektedir.

Günümüz güvenlik ortamının en önemli tehdit algılamalarından birisini, son derece organize bir yapıya sahip terörist örgütler oluşturmaktadır. Terör örgütleri, gelişen ve ulaşılması daha da kolay bir hale gelen teknolojiler sayesinde, herhangi bir zamanda, dünyanın herhangi bir yerinde ortaya çıkarak, saldırıda bulunabilme imkân ve kabiliyetine ulaşmışlardır. İstikrarsızlıkların merkezinde kalan ülkemizi, iç ve dış tehditlere karşı savunmakla yükümlü olan Türk Silahlı Kuvvetlerinin, caydırıcılık gücünü idame ettirmesi büyük önem taşımaktadır.

Türkiye'nin Savunma Stratejisinin temelini; caydırıcılık, kolektif güvenlik ve kriz yönetimi oluşturmaktadır. Bu kapsamda;

- Ülkenin bütünlüğüne, ulusal birliğine ve rejimin devamlılığına yönelik iç ve dış tehdit odaklarından kaynaklanan simetrik ve asimetrik tehditlerin mümkün olduğu kadar erken teşhis edilmesi ve özellikle terörün ülkemize zarar vermesinin önlenmesi,

- Bu tehditlere karşı, bütün millî güç unsurlarının koordineli olarak kullanılmasıyla oluşacak caydırıcı bir gücün vasıtasıyla, mevcut dengelerin ve millî menfaatimizin her hâl ve şart altında korunması,

- Meydana gelebilecek fiilî tecavüzlerin, sınır ötesinden itibaren karşılanarak, en kısa sürede ve asgari kayıpla bertaraf edilmesi,

- Birleşmiş Milletler, NATO, Avrupa Birliği ve Avrupa Güvenlik ve İşbirliği Teşkilatı başta olmak üzere, uluslararası kuruluşlarda ve bölgesel oluşumlarda aktif olarak yer alınması ve uluslararası yükümlülüklerin yerine getirilmesi,

- Türk Silahlı Kuvvetlerinin diplomatik, ekonomik ve diğer kriz yönetim tedbirlerine uygun olarak göreve hazır bulunmasının sağlanması,

- Türkiye'nin savunma stratejisinin esaslarını teşkil etmektedir.

Türkiye'nin Savunma Politikası, doğası itibarıyla savunmaya yönelik olması nedeniyle; ülkenin ulusal bağımsızlığını, egemenliğini, toprak bütünlüğünü ve hayati çıkarlarını korumak ve muhafaza etmek için düzenlenmiştir. Bu itibarla Türkiye, Millî Savunma Politikasında;

- Bölgede barış ve güvenliğe katkıda bulunmayı ve bunu geniş bölgelere yaymayı,

- Bulunduğu bölgeye ve ötesine yönelik tüm stratejileri etkileyebilecek, strateji ve güvenlik üreten bir ülke olmayı,

- Bölgesinde bir güç ve denge unsuru olmayı,

- Çevresinde bir "Barış ve Güvenlik Kuşağı" oluşturmayı,

- İşbirliği, yakınlaşma ve olumlu ilişkiler geliştirmek için, her türlü fırsattan istifade etmeyi ve girişimlerde bulunmayı, çağın gerektirdiği hedefler o larak görmektedir.

Bunun yanında; güçlü, istikrarlı, demokratik, laik ve çağdaş Türkiye'nin, öncelikle kendi bölgesinde olmak üzere, uluslararası alanda da barış, güvenlik ve istikrarın sağlanması yönünde, tarihten kaynaklanan sorumlulukları bulunmaktadır . 2000'li yılların yeni jeostratejik yapısı ve bölgemizdeki yansımaları dikkate alındığında; Türk Silahlı Kuvvetleri, içinde bulunduğu çağa uyum sağlayarak, yeni dünya düzeninde üzerine düşen her türlü görevi icra etme çabası içinde olmak durumundadır.

Türkiye Cumhuriyeti Devleti, başta "Yurtta Sulh, Cihanda Sulh." ilkesi olmak üzere, Ulu Önder Mustafa Kemal ATATÜRK'ün belirlediği inkılâp ve ilkeleri doğrultusunda,

Türk Vatanı ve Milletinin ebedî varlığını ve Türk Devletinin bölünmez bütünlüğünü muhafaza etmek, halkının refahı, maddî ve manevî mutluluğunu sağlamak, dünya uluslar ailesinin eşit haklara sahip onurlu bir üyesi olarak, çağdaş uygarlık düzeyine ulaşma yolunda, azim ve kararlılık sahibidir. Bu çerçevede, Devletimiz gerekli savunma ve güvenlik tedbirlerini uygulamaya ve geliştirmeye devam etmektedir.

Türkiye, geçen yüzyılın son 30 yılında, terörizm gibi asimetrik risk ve tehditlerle mücadeleye önemli imkân ve kabiliyetler hasrederken, aynı zamanda, insanlığa karşı işlenen bu suçlara karşı, tüm uluslararası toplumun seferber olması hususunda her platformda, başta müttefikleri olmak üzere, bütün dünya devletlerinin dikkatlerini çekmiştir.

Türkiye, günümüzün tehditleri ile mücadelede; yeni dünya düzeninin bilincinde, gelişen her yeni durum karşısında, millî menfaatleri doğrultusunda, uygun politikalara yönelmek ve jeopolitik imkânlarını etkin bir şekilde kullanmak suretiyle, küresel ortamdaki etkinliğini artırabilecek ve bölgesel inisiyatif sahibi ülke konumunu güçlendirebilecektir.

Türkiye, bölge ve dünya barışına katkıda bulunmak amacıyla; 11 Eylül 2001 öncesinde olduğu gibi, sonrasında da terörizme karşı savaşta edinmiş olduğu tecrübelerini, imkân ve kabiliyetlerini; uluslararası, bölgesel ve ikili platformlarda oluşturulan, ortak güvenlik sistemlerinde aktif olarak yer alarak paylaşmakta, barış ve güvenliğe katkıda bulunmakta ve insani yardımlarına aralıksız olarak devam etmektedir.

Başta bölge insanları olmak üzere, bütün dünyanın güvenlik ve refahını etkileyen Orta Doğu'daki istikrarsızlığın, 21'inci yüzyılın en büyük sorunlarından biri hâline geldiği görülmektedir. Tarihi ve kültürel varlığı, zengin petrol kaynakları ve dünya ulaştırma yollarının kesişme noktasında bulunması gibi özelliklerine rağmen, bitmeyen bir şiddetin merkezi hâline gelen Orta Doğu'da; barış, istikrar ve refahın sağlanması, dış politika önceliklerimiz arasında yer almaktadır. Bu çerçevede Türkiye, uluslararası toplumla birlikte bölge ülkelerinin karşılaştığı sorunların aşılması için her türlü desteği vermeye devam etmektedir.

Türkiye, demokratik, laik yapısı, hukukun üstünlüğünü esas alan yönetim biçimi, güçlü devlet geleneği, pazar ekonomisi, sosyal ve kültürel yapısı ile; Balkanlar, Kafkaslar ve Orta Doğu üçgeninin ortasında bir istikrar adasıdır ve böyle kalmaya da dev am edecektir. Askerî yönden güçlü ve kendi içinde de istikrarlı olan ülkemizden beklenen şekilde, bölgesinde barış ve istikrarın sağlanması ve sürdürülmesinde oynadığı etkin rolü devam ettirecektir.

Avrupa Birliği üyesi olma yolundaki vizyonunu sürdüren Türkiye için, Avrupa Güvenlik ve Savunma Politikası içerisinde yer alabilmek de, stratejik bir önem ve önceliğe sahiptir. Avrupa ile bütünleşmiş ve bulunduğu coğrafyanın avantajını da kullanan Türkiye, Avrupa Birliği'nin geliştirdiği Ortak Dış ve Güvenlik Politikasıyla, dünyanın sorunlu bölgelerinde küresel aktör olma gayretlerine önemli katkı sağlayabilecektir.

Gelinen aşamada; bir yanda NATO'nun Avrupa Birliğine desteği, diğer taraftan da Avrupa Birliği üyesi olmayan müttefiklerin, Avrupa Güvenlik ve Sav unma Politikası (AGSP)'na katılımı konusunda hassas bir denge kurulmuştur. Türkiye, bu hassas denge içerisinde yer alan ülkelerden biri olarak, Avrupa'nın savunma ve güvenliğiyle doğrudan veya dolaylı ilgisi bulunan, tüm çok uluslu operasyonlarda fiilen ve etkin olarak yer almaktadır. Bunlar, Birleşmiş Milletler, Avrupa Güvenlik ve İşbirliği Teşkilatı ve NATO çerçevesinde icra edilen operasyonlar olduğu gibi, Avrupa Birliği'nin NATO imkân ve yeteneklerini kullanarak, tek başına icra ettiği askerî operasyonl arı da içermektedir.

Türkiye, aynı anlayış içerisinde Avrupa Birliği tarafından geliştirilmekte olan, Muharebe Grupları Konseptini memnuniyetle karşılamaktadır. Bu projeyi Avrupa Güvenlik ve Savunma Politikası'nın, daimî yapılandırılmış işbirliği projesin in ilk örneği olarak görmektedir. İtalya'nın çerçeve ülke olacağı, Romanya'nın yanı sıra ülkemizin de katılımına açılan ve 2010 yılının ikinci yarısı için, operasyonel olması planlanan Kara Muharebe Grubu'nun teşkiline ilişkin çalışmalar devam etmektedir.

Türkiye, bölgesel ve küresel güvenlik ortamının iyileştirilmesi açısından, üzerine düşen sorumluluğun bilincinde olarak, Karadeniz'de güvenlik girişimine öncülük etmiştir. Bu

girişimlerinde, Karadeniz'in deniz güvenliğinin, öncelikle kıyıdaş ülkelerce alı nacak tedbirlerle karşılanması için işbirliğini savunmuştur.

Bölgesel ve küresel inisiyatiflerin yanı sıra, askerî anlamda ikili ilişkilerin geliştirilmesine, Türk Silahlı Kuvvetleri büyük önem atfetmektedir. Bugüne kadar 46 ülke ile Savunma Sanayii İşbir liği, 43 ülke ile Askerî Eğitim İşbirliği, 51 ülke ile Çerçeve Anlaşması imzalanmış durumdadır. Hâlen 9 ülke ile Askerî Eğitim İşbirliği, 22 ülke ile de Çerçeve Anlaşması yapma çalışmaları devam etmektedir. Bu anlaşmalar çerçevesinde, dost ülkelerin silahl ı kuvvetlerinin geliştirilmesi, savunma sanayii ürünlerimizin pazarlanması, dil öğretimi de dâhil olmak üzere, subay ve astsubaylar ile çeşitli birliklerinin eğitilmesi amacıyla birçok ülkeye destek verilmektedir.

Sovyetler Birliği ve Yugoslavya'nın dağıl masının ardından, Orta Asya, Kafkaslar ve Balkanlar'da bağımsızlığını kazanan ve çoğu ile tarih, kültür ve dil birliğimiz olan dost ve müttefik ülkelere, 1992 yılından itibaren yardım faaliyetlerimizi sürdürmekteyiz.

Fırsatların yanında sorunların da yoğu nlaştığı, ender görülen bir jeopolitik konumda bulunan Türkiye, bekasını ve ulusal menfaatlerini temin için, etkin dış ve güvenlik politikaları üretmek, kararlı ve duyarlı davranmak, muhtemel risk ve tehditleri zamanında ve doğru algılayarak gerekli önleml eri zamanında almak, maruz bulunduğu risk ve tehditler ile orantılı, caydırıcı ve dış politikasını desteklemeye yeterli ve etkili silahlı bir gücü elde bulundurmak zorundadır.

Bu kapsamda, Türk Silahlı Kuvvetlerinin içinde bulunduğumuz dönemin, güvenlik ihtiyaçlarına cevap verebilecek bir yapı içerisinde, kısa -orta-uzun vadeli tehdit/risk değerlendirmeleri ışığında, imkân ve kabiliyetleri, nitelik bakımından daha da geliştirilerek, daha küçük, ancak daha fazla etkinliğe ve yüksek teknolojiye sahip, daha modern, ateş gücü üstün ve manevra kabiliyeti yüksek bir güce kavuşması için gerekli çalışmalar devam etmektedir. "(Gönül Vecdi, Bakan Sunuşu, 2007)

Türkiye'nin içinde bulunduğu bölge itibarıyla Ortadoğu daha büyük bir önem taşımaktadır. Dr. Nadiye Mustafa'nın bir makalesinde, Özellikle Ortadoğu'nun, 11

Eylül'den sonra başlayan sürecin gölgesinde, ABD ve müttefiklerince dayatılan değişim ve yeniden yapılanma baskısıyla karşı karşıya kalmasının bölgesel dengeler üzerinde şiddetle etkili olduğuna ve olacağına değinilmektedir.

Makalede, önce Afganistan, ardından Irak derken, şimdi de 'Büyük Ortadoğu' için düğmeye basılması, 11 Eylül sonrası Amerikan stratejisinin üçüncü adımı olarak değerlendirilmektedir.

Böyle bir ortamda üzerinde durulması gereken konu ise, Çatışmaların ve gerginliklerin tırmanmasına katkıda bulunan jeostratejik unsurlar ile işbirliği ufuklarının belirmesine imkân tanıyan aynı kültürel ve tarihi bağlar arasındaki ilişki ve bunların değerlendirilmesidir.

Makale'de Türkiye'nin Ortadoğu Açısından karşı karşıya kaldığı diğer bölgesel etkiler ise İsrail'in 11 Eylül'den sonra ABD'nin yürüttüğü operasyonlardan istifade etmesi ve ABD ile ilişkilerinin derinlik kazanması ile bu çevrevede yeniden şekillenen Filistin Sorunu, Suriye'nin karşı karşıya bulunduğu baskılar, Amerikan işgali gölgesinde Körfez güvenliğinin ve bölgesel koalisyonun geleceği, Yeni Irak devletinin geleceği, İran ve Taliban sonrası Afganistan'a yönelik baskılar, ABD stratejisi gölgesinde Pakistan'ın rolü, Komşu Asya ülkeleriyle güvenlik sorunlarının sonuçları, Kitle imha silahları, su paylaşımı, azınlık hakları ve iç politik durum gibi sorunlar gösterilmektedir. (Radikal Gazetesi, Yeni Ortadoğu kurulurken, 30.06.2004)

Ortaasya'da tarihi bağlarımız olan önemli bölgelerden biridir. Bu bölge açısından önemli bir aktör olan ABD'nin, Rusya ve Çin ile olan rekabetinin artmaya başladığı bir ortamda 11 Eylül 2001 terör saldırılarına hedef olduğu görülmektedir. 11 Eylül sonrası oluşan ortamda bölge ülkelerinin ve Rusya'nın desteğini alan ABD, Afganistan harekâtı ile birlikte bölgeye askeri anlamda da yerleşmiş ve üslere sahip olmuştur. Yine aynı dönemde Sovyetler Birliği'nin dağılmasından sonra bağımsızlığını kazanan Cumhuriyetlerin, ABD'den gelen, demokratikleşme söylemini tehdit olarak algılamaları neticesinde yönlerini yeniden Rusya'ya çevirmeye başladıkları görülmektedir. (Kasım, ABD'nin Orta Asya Politikasındaki İkilem, 2007)

Nato açısından izlenecek politikalarda Ülkemizin Jeopolitik Değerlendirilmesi açısından diğer bir önemli konudur. Stanley R Sloan'a ait ilkbahar 2002 Nato Dergiside yayınlanan makalede, NATO'nun kendi içerisinde, Soğuk Savaş sırasında, 1966'da Fransa'nın İttifak'ın entegre askeri yapısından çekilmesi, 1979'da Müttefikler, Sovyetlerin Afganistan'ı işgal ine nasıl mukabele edecekleri konusunda anlaşmazlığa düşmesi, 1980'lerin başlarında Avrupa'da orta menzilli nükleer füzelerin konuşlandırılması, Bugün ise 11 Eylül'de Amerika Birleşik Devletleri'ne yapılan terörist saldırının getirdiği kriz ortamı gibi sor unlar yaşadığı belirtilmektedir. Makalede ayrıca, Nato'nun daha önce yaşadığı krizlerin güven krizi olarak görülürken bugün ki yaşadığı krizin güvenin yanında yeteneklerle de ilgili olduğu ifade edilmektedir. Bu örneklerde de görüldüğü gibi üyeler arasında hala farklı olaylar karşısında farklı bakış açıları mevcuttur. Bu farklı bakış açıları zaman zaman fikir birliğine ulaşmayı ve işbirliğini zorlaştıracaktır. (Sloan, 2002)

Özdemir kitabında Türkiye'nin önümüzdeki 10 yıl içerisinde temel dayanak alması gereken 3 konu olarak; üniter devlet yapısının korunarak ülkenin bütünlüğüne ve güvenliğine ilişkin tüm tehditlerin etkisiz hale getirilmesini, AB ile olan ilişkilerin ülkemize yararlar sağlayacak şekilde yürütülmesini ve modernleşme açısından yürütülecek toplumsal değişim çalışmalarına ivme kazandırılmasını göstermektedir. (Özdemir, 2003, sy.92)

10.2.1 Türkiye'nin Bazı Komşuları ile olan ilişkileri

Bu bölümde bilgi savaşı kapsamında değerlendirilmeyen, komşu devletler hakkında bilgiler verilmiştir.

10.2.1.1 Ermenistan

Türkiye'den tarihten gelen sorunları nedeniyle toprak talebinde bulunan Ermenistan, Türkiye'ye karşı Yunanistan ile benzer bir politika üretmektedir.

Azerbaycan'la yaşadığı sorunlar nedeniyle Rusya'ya yakın kalan ülke kontrol edemediği Diasporası ile uluslar arası arenada ülkemizi özellikle sözde ermeni iddiaları noktasında baskı altına almaya çalışmaktadır. Bu sorunun haricinde ülkemizdeki terör örgütlerini desteklemesi bakımından da ülkemizin güvenliği açısından bir risk teşkil etmektedir. (Özdemir, 2003, sy.)

10.2.1.2 Bulgaristan

Bulgaristan, Soğuk Savaş döneminde Sovyetler'in en yakın müttefiği olarak ülkemize ve topraklarında yaşayan soydaşlarımıza karşı hasmane bir tavır sergilemiş, bu dönemin sona ermesinden sonra, Türkiye açısından askeri bir tehdit olmaktan çıkmıştır.(Özdemir, 2003, sy.99-100)

Bilgi savaşı konusunda risk teşkil edecek yeterli altyapıya sahip değildir.

10.2.1.3 Suriye

Komşumuz olması nedeniyle yer verdiğim bir diğer ülkede Suriye'dir. 1946 yılında kurulan ve 1347 km uzunluğunda bir sınırı paylaştığımız ülkeyle ilişkilerimiz bu süre zarfında, normal diplomatik ilişkilerden, siyasi ve askeri tansiyonlara kadar uzanan düzensiz bir biçimde devam etmiştir.

Ülke İle Aramızdaki Temel Sorunların başında ise Hatay Sorunu, Sınır Aşan Sular Sorunu, Ülkenin Türkiye Aleyhine PKK'yı destekleyerek bunu Türkiye'ye karşı bir koz olarak kullanmak istemesi gelmektedir.

Bugün hala Suriye haritaları, Suriye-Türkiye sınırının İskenderun'dan geçen kısmını geçici bir sınır ya da İskenderun'u Suriye'nin bir parçası olarak göstermektedir. Ülke ile aramızdaki temel sorunların belki de en önemlisi olan su sorunu da, özellikle 1990 yılında Türkiye'nin Atatürk Barajı'nın rezervlerini doldurmaya başladığı sırada alevlenmiştir. Suriye'nin esas korKusu, Fırat'ın sularının Suriye'ye giden kısmının büyük ölçüde ve devamlı olarak azalacağı düşüncesidir.

Suriye, Türkiye'nin iç düzen ve dengelerini bozarak suyu silah olarak kullanmasını ve herhangi bir askeri çatışma ihtimalini engellemek amacıyla özellikle son dö neme kadar teröre destek vermiştir.(Yurdusev, 1998, sy.175 -178)

10.2.1.4 İran

Yüzyıllardan beri bulunduğu coğrafyada bir güç olan İran'la Osmanlı İmparatorluğu arasında hegomanya mücadelesi çerçevesinde 1473'den 1825'e kadar 22 savaş olmuştur. Sünni Müslüman Osmanlıların halifeliği İran tarafından kabul görmemiştir.. Bununla birlikte iki farklı kültüre sahip olan Türk ve İran halkı zaman içinde birbirlerinin bölgede varlığını kabul etmişlerdir. 1639 yılında Osmanlı İmparatorluğu ile İran arasında varılan Kasr-ı Şirin anlaşması ile çizilen sınır günümüze kadar değişmeden kalmıştır.

İran, Türkiye'ye yönelik olarak;

- Türkiye'deki kökten dinci akımları destekleme ve İslam devrimi için uygun bir ortam yaratma,

- Özellikle PKK terör örgütünü ve İran yanlısı Hizbulla h örgütünü destekleme,

- Türkiye'nin istikrarını bozmak ve zayıflatmak böylece bölgedeki dengeleri kendi lehine çevirme,

- İçinde bulunan Azeri, Türkmen, Kaşgar ve Avşar Türklerinin eritme ve onların kökleri ile ilgili bilinçlerini yok etmek ve Türkiye karşıtı terörist faaliyetleri destekleme,

- İran'da yaşayan Ermenilerin (yaklaşık 300.000) Türk karşıtı hareketlerine göz yumma, gibi politikalar izlemektedir.

Bu politikalar İran'ın tarafınca mümkün olduğunca gizli yürütülmektedir. Resmi olarak sergilemeye çalıştığı tavır ise Türkiye ile istikrarlı ve iyi komşuluk ilişkilerini

yürütme yönündedir. Çünkü Türkiye Irak'la eskiden beri var olan problemler karşısında tarafsızlığını korumuştur. Bununla birlikte Türkiye yakınlık ve düşük fiyatlar nedeniyle ekonomik olarak İran'ın ihitiyaçlarını karşılaması bakımından avantajlı bir ülkedir. Son nedense Türkiye'nin İran'ı batıya açan en direk yol olmasıdır.

Türkiye açısından İran ise Türkiye'nin Orta Asya ülkelerine açılan kapısı ve bu ülkelerle yaptığı ticaretin de geçiş alanını oluşturması bakımından önemlidir. (Yurdusev, 1998, sy.178-180)

Son dönemlerde füze sistemini geliştirmeye çalışan İran hem kendi iç üretimine hem de dış ülkelerle askeri-teknolojik işbirliğine önem vermekte, dış silah ortaklarından Rusya ile askeri imzaladığı askeri anlaşmalar ile dikkat çekmektedir. Rusya ile arasında, Kasım 2005'te, 700 milyon dolarlık kısmı sadece karadan havaya 29 Tor-M1 füzelerini kapsayan 1.3 milyar dolarlık askeri-teknoloji anlaşma imzalanmıştır. İran'ın askeri gücünün artması, İsrail ve ABD tarafından bölgesel askeri dengelerin bozulacağı şeklinde yorumlanmaktadır. İran, askeri gücünü artırarak hem bölgesel bir güç olarak kalmaya hem de ABD saldırısını önleme hazırlığı içerisindedir.

ABD'nin Kafkasya ve Orta Asya ile Orta Doğu' ya yerleşme çalışmaları bakımından Rusya ile müttefik gibi çalışmaktadır. İran ve Rusya arasındaki askeri-teknolojik işbirliği hacminin, on yıl içinde 10 milyar dolar olacağı tahmin edilmektedir. İran Askeri Gücünü Artırıyor, (Veliev, 2005)

10.2.1.5 Irak

Irak'ın ülkemiz açısından en öneli özelliği muhakkak, ABD'nin 2003 yılında Irak'ı işgalini müteakip kuzeyinde oluşan otorite boşluğunun PKK terör örgütünce kullanılarak onlara yaşama şansı tanımış olmasıdır. Örgüt bu rahatlık çerçevesinde, insan kaynağı, mali ve lojistik desteğini sağlayabilmiş, yeniden teşkilatlanmış, eğitim ve planlama ile terör eylemlerini gerçekleştirme fırsatını bulmuştur.

Bir diğer sorunda sahip olduğu petrol kaynakları, verimli toprak yapısı, geniş arazisi ve bu coğrafyadaki stratejik önemi olan Kerkük'ün, bir Türkmen şehri olmasına karşın Kürt vilayeti olarak mütalaa edilmesi ve Kürt bölgesine dahil edilmesi yönünde yapılan çalışmalardır. Bu durum Ülkemiz açısında kabul edilebilir bir durum değildir. Ayrıca Türkiye, bu bölgenin Kürt b ölgesine dahil olmasına, Kürt yönetiminin ekonomik ve politik gücünü arttıracağı nedeniyle de karşı çıkmaktadır. (Kuloğlu, Irak'taki Gelişmeler, Pkk Terör Örgütü, Abd -Türkiye İlişkileri Ve Kerkük, 2008)

10.3.Çağın gerekliliklerine göre değişen güvenlik anlayışlarının belirlenmesi

Hızla değişen dünyamızda gelecekle ilgili tahminlerde bulunmak ya da hesaplar yapmak, her türlü gelişmeye karşı çok yönlü projeksiyonlar ya da alternatif senaryolar hazırlama zorunluluğu bakımından oldukça risklidir. Gelece kte dünya'nın nasıl şekilleneceği sorusuna, ancak belirli öğelerden hareketle, bilimsel ve derinlemesine çözümleme ile bunu da ciddi bir kurumsallaşma ile sağlamak gerekmektedir. Gelecekte stratejik hedeflerin belirlenmesinde rol oynayacak faktörleri ana hatları ile şu şekilde sıralayabiliriz:

- Demografik eğilimler, Dünya nüfusundaki artış ve bu artışın %95'inin özellikle fakir ve gelişmekte olan bölgelerde olması önemli faktörlerin başında gelmektedir. Avrupa'daki yaşlı nüfusun ağırlık kazanmasına karşın, azgelişmiş ülkelerin çoğunda genç nüfusun ağırlık taşıyacağı tahmin edilmektedir. Bu durumu önemli yapan ise gelişmiş ülkelere olan göçün hızlanarak, bu durumunda yeni istikrarsızlık ortamları oluşturacak nitelikte olmasıdır. Bu durumun özellikle fakir ülk eler açısından da kaynakların kullanımı, altyapı ve liderlik korularında kriz yaratabileceği hatta suç örgütlerine zemin yaratabileceği öngörülmektedir.

- Dünya genelinde zengin yoksul kutuplaşması, aşırı milliyetçilik ve etnik, dinsel, siyasal, iktisadi çatışmalar nedeniyle birçok devlette kırılmaların yaşanması, insani operasyonların ölçeği ve sayısını artıracak, AGİT, NATO, AGSK ve BM gibi uluslararası örgütlerin işlevleri, rolleri ağırlık kazanacaktır.

- Yukarıdaki eğilimler dikkate alındığında, kaynakların eşitsiz dağılımı ve kıtlığı görülecek, su ve enerji sorunu neticesinde, bu kaynaklara sahip olma mücadelesi sertleşecektir. Diğer yandan yaşanacak çevresel sorunlar ülkeler açısından daha da önemli olacaktır.

- Kitle imha ve genetik silahlarının yaygınlaşması, siber saldırılar ve ülkelerin füze sitemlerine sahip olma eğilimleri, stratejinin şekli ve niteliğide değiştirmektedir.

- Değişimlerin yaşandığı başka bir alanda ideolojik/kültürel alandır. Bilginin hızlı yayılması ve paylaşılması çağa şekil veren en önemli unsurların başında gelmektedir.

- Bir başka gelişme ise uluslararası ve devlet destekli uluslararası terörizmin, düşük yoğunluklu savaş ve çatışmaların 21. yüzyılda artan boyutlarıyla varlığını sürdürecek olmasıdır.

- Başka bir nokta ise suç örgütlerinin ulusal ve uluslararası alanda yaratacağı kaostur.

- Dikkate alınması gereken diğer bir nokta da, özellikle SSCB'nin çökmesinden sonra ortaya çıkan güç boşluğu ve birçok bölgede etnik, dinsel, topraksal ve ekonomik tartışmalarda yaşanan belirsizlik ortamıdır. Bu noktadan bakıldığında değişen bu anlayışlara karşı yeni stratejilerin oluşturulması büyük bir gereklilik olarak karşımıza çıkmaktadır.

- Türkiye'nin önümüzdeki dönemlerde izleyeceği denge politikası ve stratejik ittifaklar içinde yer alması çıkarlar dengesine dayalı ilişkiler bakımından daha da önem kazanacaktır. AB'nin geleceği, Rusya ve Çin'in gelecekte uluslararası alandaki konumlarının ne olacağı, Kore'de yaşanan sorunlar; Basra Körfezi'ndeki sorunlar ve güç dengesi; Güney Çin denizindeki güç mücadelesi; Afrika'daki etnik, dinsel ve kabile çatışmaları ile bunların ortaya çıkmasındaki önemli uluslar arası faktörlerin değerlendirilmesi; Ortadoğu'da beklenen köklü değişiklikler; uzay çalışmaları; yeni silah sistemleri ve askeri teknolojinin yaygınlaşma düzeyi geleceğe yön verecek durumlar olarak karşımıza çıkmaktadır.

- Asimetrik tehditler ve terörizm gelecek senaryoları bakımından önemli kavramlardır. Bu ve yukarıda saydığımız diğer eğilimleri dikkate aldığımızda, karmaşık ilişkiler, krizler, belirsizlikler ve değişimin ne yönde olacağı sorunu, yeni olaylara ve durumlara yanıt verecek ya da hazırlıklı, aynı zamanda kapsamlı stratejik planlama gerekliliği karşımıza çıkmaktadır. Bu bağlamda operasyonel istihbarattan çok stratejik istihbaratın büyük önem taşıdığı açıktır.(Arslan, Tarihten Günümüze İç Ve Dış Tehditler, 2001)

10.4 Türkiye'nin Bilim ve Teknoloji Politikalarının Belirlenmesi

1998 yılında DPT'nca yapılan tanıma göre "Bilim ve teknoloji politikaları, bilim ve araştırma faaliyetlerinin ülkelerin iktisadi, sosyal, siyasal durum ve ihtiyaçları ile tutarlı bir şekilde geliştirilmesini sağlayacak önlem, faaliyet ve teşkilatlanmalar ile ilgili düzenlemeler olarak tanımlanmaktadır." Günümüzde, bilim ve teknoloji politikalarının ülkelerin refah düzeylerini etkileyen politikalar olmaları nedeniyle önemleri hızla artmaktadır. Bilim ve teknoloji politikalarını uygulayan ülkelerin üretim seviye ve çeşitliliklerinde artış görülürken, rekabet güçlerinin arttırılması ya da mevcut güçlerinin devamının sağlanması bakımından bu politikaların gerekliliği

ortaya çıkmaktadır. Nitekim gelişmiş tüm ülkelerin mevcut bilim ve teknoloji politikalarının olduğu görülmektedir. (Kaplan, 2004, sy.188)

Bilim Politikası açısından, alınması gereken bazı tedbirler ile plitikanın başarıy a ulaşması sağlanabilir. Alınması gereken önlemler aşağıdaki dört ana başlık altında toplanmıştır,

- Parasal kaynak yaratma amaçlı önlemler,
- İnsangücü kaynağı yaratma amaçlı önlemler,
- Özel kuruluşların A+G harcamalarındaki payının artırılması amaçlı önlemle r,
- Dünyadaki bilim ve teknolojiye katkı düzeyinin geliştirilmesini amaçlayan önlemler.(Türkiye Bilimsel ve Teknik Araştırma Kurumu, Türk Bilim ve Teknoloji Politikası, 1993-2003, sy.13)

Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK) 3 Şubat 1993'te karar alt ına aldığı "Türk Bilim ve Teknoloji Politikası: 1993-2003" dökümanı Türkiye'nin bugünkü, Bilim ve Teknoloji Politikası'nın temel dokümanı olma özelliğini taşımaktadır.

3 Şubat 1993 günü yapılan Bilim Ve Teknoloji Yüksek Kurulu Toplantısı Özet Kararları aşağıdaki gibidir.

"1. 1993–2003 yılları için Bilim ve Teknoloji Politikasının hedefleri olarak aşağıdaki değerler kabul edilmiştir:

a) Onbin nüfus başına mevcut % 7 olan araştırıcı sayısının %15'i aşması,

b) Araştırma-geliştirme harcamalarının, gayri sa fi milli hâsıla içerisinde bugün % 0.33 olan payının % 1'i aşması,

c) Ülkemizin evrensel bilime katkısı açısından, dünya sıralamasında halen kırkıncı sırada olan yerinin otuzunculuğa çıkarılması,

d) Ülke araştırma - geliştirme harcamaları içindeki özel s ektör payının % 18 olan mevcut durumdan % 30'a çıkarılması,

2. Bu hedeflere belirlenen sürede erişebilmek için ülkemizdeki mevcut potansiyel ve dünyadaki Bilim ve Teknolojinin gidişi de gözönünde bulundurularak, çağa damgasını vuran, ekonominin bütün sektörle rini ve yaşamın hemen tüm alanlarını etkileyen;

   - Bilişim (bilgisayar, mikroelektronik, telekomünikasyon teknolojilerinin bir birleşimi),
   - İleri teknoloji malzemeleri,
   - Biyoteknoloji ,
   - Nükleer teknoloji ,
   - Uzay teknolojisi

konularındaki çalışmalara öncelik ve rilmesi kararlaştırılmıştır.
Bilişim Sektörü ile ilgili olarak hazırlanan politika metni Kurul'ca onaylanmıştır.

Buna göre, Türkiye'nin bilişimden gerekli faydayı sağlayabilmesi için:

- İnsan gücü yetiştirilmesi,
- Kamu sektörünün öncülüğünde bilişim teknol ojilerinin yaygınlaştırılması,
- Yasal düzenlemelerin yapılması,
- Bilişim teknolojileri araştırma ve geliştirme projelerinin desteklenmesi ve hedeflerinin belirlenmesi konularında çalışmalar yapılması karara bağlanmıştır.
- Diğer alanlarda da benzer politika do kümanlarının ilgili kurum ve kuıuluşlarca hazırlanarak Kurul'a sunulması öngörülmüştür.

3. Kurulca onaylanan Bilim Politikası ana hedeflerine ulaşabilmek için alınması gereken önlemler aşağıda verilmiştir:

a) Parasal kaynak yaratmaya yönelik önlemler
1) Kamu alımları yoluyla iç piyasada rekabet ve talep yaratılması,

2) Ülkemizde yabancı ülke ortaklarıyla gerçekleştirilen büyük yatırımların offset'lerinin hedeflerin gerçekleştirilmesinde ek kaynak yaratmak amacıyla TÜBİTAK aracılığıyla ve/veya koordinatörlüğünde kullanılması,

3) Kamu araştırma - geliştirme projelerinin mümkün olduğunca tek elden, TÜBİTAK aracılığıyla desteklenmesi, bunun mümkün olmadığı hallerde saptanmış bulunan öncelikli alanlara uygunluğu açısından TÜBİTAK ile koordine edilmesi,

4) TÜBİTAK'ın rutin faaliyetleri dışında, taraf olduğu uluslararası mega projeleri yürütebilmesi için Geliştirme ve Destekleme Fonu'ndan ek kaynak aktarılması,

5) Türkiye'ye girecek teknoloji ve Know - How'ların seçiminin TÜBİTAK'ın aktif rol alacağı bir "Teknoloji Değerlendirme Merkezi"nce yapılması.

b) İnsan gücü kaynağı yaratmaya yönelik önlemler

1) Farklı kurumlar tarafından yürütülen yurt dışı doktora burs programlarının merkezi bir şemsiye altında koordine edilmesi,

2) Üniversitelerde lisans düzeyinde, fen dallarından kaçışı durduracak ve bu dallara yönelimi teşvik edecek önlemlerin alınması,

3) TÜBİTAK'ın 1992 yılında uygulamaya koyduğu ve büyük başarıyla sürdürdüğü eski Sovyetler Birliği'nden bilim adamı getirme programının kapsamının genişletilerek devam ettirilmesi,

c) Özel kuruluşlarının araştırma-geliştirme harcamalarındaki payının arttırılmasına yönelik önlemler

1) Küçük ve orta ölçekli işletmelerde araştırma geliştirme faaliyetlerinin özendirilmesi,

2) Türkiye'de yatırım yapan çok uluslu şirket lerin ülkemizde araştırma – geliştirme birimleri kurmalarının özendirilmesi,

3) Risk sermayesi piyasası kurulmasını temin için risk sermayesi şirketlerinin özel sektör eliyle geliştirilmesini teşvik edici yasal düzenlemeler konusundaki çalışmaların sonuçlandırılması,

4) Üniversiteler ve araştırma kurumları ile sanayi arasındaki işbirliğinin gelişmesinde önemli bir araç olan teknopark faaliyetlerinin TÜBİTAK ile koordine edilerek yürütülmesi,

5) Lisans anlaşmalarına dayalı üretimden özgün tasarıma geçişin özendirilmesi,

6) Patent ve Fikri Mülkiyet Mevzuatının güncelleştirilmesi ve özellikle bilişim sektörünün en önemli kesimini oluşturan yazılım sektörünün Fikri Mülkiyet Kanunu çerçevesi içine alınması,

d) Dünyadaki bilim ve teknolojiye katkı düzeyinin a rttırılmasına yönelik önlemler

1) İleri Araştırma Merkezleri (Centers of Excellence) kurulması,
Kurul bu amaçla, İstanbul'da Teorik Araştırmalar Merkezi kurulmasını ilke olarak benimsemiş ve kuruluş çalışmalarını sürdürme görevini TÜBİTAK'a vermiştir. Benzer bir Merkez'in de biyoteknoloji alanında çalışmalar yapmak üzere GAP bölgesinde kurulması yolunda prensip kararı alınmıştır.

2) Hem pozitif hem de sosyal bilimlerin tüm alanlarının kapsayacak Türkiye Bilimler Akademisi'nin kuıulması,

3) Uluslararası düzeyde bilimsel yayın faaliyetlerinin özendirilmesi..” (Türkiye Bilimsel ve Teknik Araştırma Kurumu, Türk Bilim ve Teknoloji Politikası, 1993 2003, sy.5-7) Ek2’de TÜRK BİLİM ve TEKNOLOJİ POLİTİKASI: 1993 -2003’de

yer verilen Türkiyenin Bilişim Politikaları Sorunlar, Hedefler ve Çözüm Önerileri bulunabilir.

10.5.Dünya Devletlerinin Bilgi Savaşı Potansiyelleri

10.5.1 Amerika Birleşik Devletleri

Bilgisayar teknolojisini toplumsal hayatın her alanında uygulamaya sokan ABD, bilgi savaşı kavramının ortaya çıktığı ilk ülkedir. ABD Savunma Bakanlığı bilgi savaşının tüm metodlarını uygulayarak, düşmanının kritik idari, askeri, ekonomik, sosyal sistemlerini etkisiz hale getirmeyi amaçlamaktadır.

ABD bu savaş çerçevesindeki tüm araçları mümkün olduğunca yoğun bir biçimde kullanma arzusundadır. Diğer savaşlara göre daha düşük maliyetli olan bu savaşda ABD nin en büyük handikapı; yeni dönemdeki düşman tanımının değişmesi, savaşın araçlarının herkesçe erişilebilir olması ve bu savaşın planlanması noktasında ülkeni n şeffaflık ilkesiyle savaşın planlaması ve icrası noktasındaki gizlilik gerekliliğinin çatışmasıdır.(Özdemir,2003,117-119)

ABD, Manevra yeteneği, iletişim teknolojilerinin etkin kullanımı, görünmez hava araçları, uzay sistemlerinin askeri kullanımı ve ye ni askeri araçlardan özellikle insansız hava araçları ve akıllı bombaları son 15 yıldaki çeşitli savaşlarda, özellikle Birinci ve İkinci Körfez Savaşlarında kullanmıştır. Körfez Savaşlarında, Bosna, Kosova, Afganistan operasyonlarında özellikle istihbarat sağlamada uydular, insansız hava keşif ve saldırı araçları ve görünmez özellikli hava bombardıman araçları kullanılmıştır.

Özellikle Birinci Körfez Savaşı ve sonra dönemlerdeki çatışmalar, ABD için elindeki sofistike silahları deneme fırsatı yaratmıştır. Birinci Körfez savaşı, ilk görünmez uçak olan F-117, ilk uzay savaşı teknolojileri olan GPS sistemlerinin kara birliklerince kullanılması ve gerçek zamanlı istihbarat desteği ile Cruise füzelerinin kullanımına tanıklık etmştir.

Bosna ve Kosova operasyonları ise ilk avcı insansız hava araçlarının denenmesi, B-2'lerin ilk kez savaşa sokulması ve ilk kez GPS yönlendirilmiş bombaların kullanılması bakımından dikkat çekicidir.

Son Irak savaşında da uzaktan hassas kumandalı füzelerin denenmesi ve ABD'ye ait tüm uçaklarının lazer yardımlı ve GPS güdümlü bombaları atma yeteneğine erişmeleri ABD'nin sahip olduğu teknolojinin göstermesi bakımından dikkat çekicidir. (Külebi, Geleceğin Savaşları 1-2, .2004)

10.5.2 Yunanistan

Yunanistan'ın Türkiye'ye karşı uyguladığı politikanın temeli " Türkiye'nin zararına olan her şey Yunanistan'ın yararınadır" ilkesine dayanmakta ve Yunanistan, Megola İdea emellerinin gerçekleşmesi noktasında da en büyük engel olarak Türkiye'yi görmektedir. (Özdemir, 2003, sy.99)

Yunanistan 1981'de Avrupa Birliği'ne üye olarak alındığında cumhurbaşkanı Karamanlis'in: "Artık Yunanistan At'ye tam üye oluyor. Böylece Türkiye, Asya'nın derinliklerinde kaybolacaktır" demesi, Yunanistan'ın her alanda Türkiye'yi en büyük rakip olarak gördüğünün ve kazandığı her avantajı Türkiye'ye karşı önemli bir koz olarak ele aldığının önemli bir kanıtıdır. 1986'da Yunanistan başbakanı Andreas Papandreou üye ülke devlet başkanlarına şu demeci verdiğinde de Yunanistan'ın "tehdit" tanımına bir açıklık getiriyordu: "Türkiye, Yunanistan'ı tehdit ediyor. Aramızda savaş çıkarsa siz de sorumlu olursunuz. Bize yönelen tehlike size de yönelmiştir."(Altınkaş, Türkiye Ve Yunanistan: Rakip Müttefikler, 2005, sy.3)
Türkiye üzerindeki emellerini AB'nin bünyesinde gerçekleştirmeyi hedefleyen Yunanistan'ın en önem verdiği husus Adalar Denizi'dir. Çünkü Yunanistan burada hedeflerine ulaşırsa deniz altındaki yeraltı kaynaklarına tamamen sahip olmanın yanında askeri, siyasi ve ulaştırma konusunda da kazanımlar elde edebilecektir. (Külebi, Yunan silahlanması ve olası savaş, 2006)

Yunanistan son yıllarda bilgi savaşının savunma stratejisini bilinçli bir biçimde hayata geçirmiş, yakın zamana kadar Dünya'da ele geçirilen 10 kadar kriptosistemin Yunanistan'a ait olduğu bilgisi ele geçirilmiştir. Savunma sanayi alanında özellikle Denizcilik faliyetleriyle, elektromanyetik alanda yatırımlar yapmaktadır. Bunun yanında Yunanistan'da ve adalarda fiber optik sisteme geçmesinin yanında sualtına geniş band data aktarımına uygun kablolar döşediği bilinmektedir.
Bütün bunlar Yunanistan'ın bilgi savaşı hazırlıkları çerçevesinde değerlendirilebilir.(Özdemir, 2003, sy.123-124)

10.5.3 Rusya

Sovyetler Birliği'nin yıkılması ile ortaya çıkan, Gürcistan, Ermenistan ve Azerbaycan tampon bölge oluşturarak 400 yıllık Türk-Rus ortak sınırının da ortadan kalkmasına neden olmuşlardır. Bu durum ise Türkiye açısından önemli bir ferahlama sağlamış, askeri imkan ve kabiliyetlerin ülkenin içeride ve dışarıda sorunlu olduğu bölgelere kaydırılabilmesine olanak sağlamıştır.

Ancak, AKKA hükümlerinin Rusya lehine iyileştirilmesi, Rusya'nın Gürcistan ve Ermenistan'da askeri üslerini yeniden teşkil etmesi, ve 1993 tarihli "yakın çevre doktirini" ile başlayan son askeri doktrin dahilinde de açıkca vurgulanan nükleer silaha başvurma tehditleri sebebiyle Türkiye açısından yenien daha yakın bir askeri tehdit kavramı olarakkarşımıza çıkmıştır.
Ülkeler arasında yaşanan güven sorunu olumlu yönde pek bir gelişme kaydedilmemesine neden olmuştur. Askeri açıdan bakıldığında da Rusya'nın AKKA hükümlerini delme girişimleri için ortaya koyduğu gerekçeleri inandırıcı bulmak zordur. Son Rus askeri doktirinin de bu yönde olumlu bir katkı yapması beklenemeyeceği açıktır. Oysa, gerek jeopolitik, gerek jeostratejik zorlamalar sebebiyle her iki ülkeye de avantaj sağlayabilecek ortak stratejiler mümkün gözükmektedir

Ulusal güvenlik konsepti çerçevesinde ortaya konulan yeni Rus askeri doktirini, Soğuk Savaş döneminin aksine, nükleer bir savaşı da içeren büyük ve kapsamlı bir

savaş tehditinin azalmakta olduğunu öngörmektedir. Buna karşın bölgesel çatışmaların ve silahlanma yarışının ise hızlanacağı yargısını ortaya koymaktadır. Özellikle kitle imha silahları ve balistik füzelerin hızla bazı bölgelerde yayılmakta olmasının yanı sıra bilgi teknolojilerinin hızlı aşamalar kaydetmesi ve geliştirilen iletişim araçlarının imkan ve kabiliyetleri sebebiyle "bilgi savaşları" yeni Rus askeri doktirini dahilinde artık ciddi tehdit olarak değerlendirilmektedir. (Kibaroğlu, 2001, sy.9-17)

Bilgi Savaşı konusunda tarih sürecindeki bazı dönemlerde en ön sırada bulunan Rusya, önümüzdeki dönemlerde nüfuz alanlarının kesişmesi neticesinde Türkiye açısından bir risk olarak değerlendirilebilir.

Sahip olduğu HERF silahı, nükleer gücü, füze sistemle ri ayrıca güvenilir askeri haberleşme sistemleri ile güçlü istihbarat toplama kapasitesi ülkenin önemli askeri güçleri arasındadır.(Özdemir, 2003, sy.122 -123)

10.5.4 İsrail

Doğal kaynakları hemen hiç olmayan, devamlı silahlı bir mücadele içinde o lup, yaklaşık 5 milyon olan nüfusunun %20'si ülkeye yeni göç edenlerden oluşan İsrail, bugün dünyanın en büyük savunma sistemleri ihracatçısı 7 ülke arasındadır. İsrail, uzay sistemleri geliştiren, üreten ve yörüngeye fırlatan ülkelerden biridir. Modern savunma sistemleri konusunda sahip olduğu gelişmiş teknoloji ve ürünleri, İsrail'i uluslararası savunma pazarının büyük bir oyuncusu yapmaktadır.

Uçak, tank, gemi, füze, insansız hava aracı (İHA), akıllı mühimmat, bazı son derece karmaşık uç teknolojilerin k ullanıldığı elektronik harp (EH), radar ve elektro -optik sistemler konularında olduğu kadar Bilgi svaşı konusunda da sahip olduğu güç İsrail'i uluslar arası arenada önemlibir güç unsuru olarak karşımıza çıkarmaktadır. (Ziylan, 2000, Çeviri: The Israel Air Force And The Defence Industry, Military Technology 5/99, Sy.10 -13)

Kaliteli eğitim sistemi, Arge'ye verdiği büyük önem İsrail'in dikkat çeken özellikleridir. (Özdemir, 2003, sy.124)

10.5.5 Almanya

2. Dünya savaşından yenilgiyle ayrılan Almanya, sa vaştan sonra girdiği yeniden yapılanma sürecinde sanayileşme açısından önemli adımlar atmıştır. Ancak bilgi çağını yakalama hedefleri bakımından sahip oldukları eğitim sistemi, özellikle Doğu Almanya ile birleşmelerinden sonra yaşadıkları ekonomik sorunlar ve artan işsizlik oranı ülkenin önündeki sorunlar olarak karşılarına çıkmaktadır.(Özdemir, 2003, sy.120-121)

Ancak, iki Almanya'nın getirdiği ağır sorumluluklara, küresel ekonomik krize, enerji darboğazına ve değişen küresel dengelere rağmen Almanya'nın yıllık enflasyonunun %1,5 civarında, kişi başına milli hasılatının ise yılda 35.650 € (2005) olması Almanya'nın ekonomik gücünü gösterir niteliktedir. Nitekim. Almanya ekonomisi Avrupanın en büyük, A.B.D ve Japonya'dan sonra dünyanın en büyük 3. ekonomisidir. Ayrıca Almanya en fazla silah üreten ve satan 3. ülkedir. Dünya ihracat (ABD´nin önünde) şampiyonudur.
(http://tr.wikipedia.org/wiki/Almanya#Ekonomi)

TürkiyeAlmanya ilişkileri bakımından önümüzdeki dönemde Türkiye'nin AB üyeliği konusunda anlaşmazlık yaşaması olasıdır.

10.5.6 Fransa

Sözde ermeni iddiaları ve Kıbrıs sorunu ülkemizle Fransa arasında yaşanan temel sorunların başında gelmektedir. Ermeni sorunu bakımından, Ermeni diasporasının Amerika ve Rusya ile beraber en güçlü olduğu üç ülkeden biri olması dikkat çekicidir.(Laçiner, Fransa–Türkiye İlişkileri ve Ermeni Sorunu (1980'e Kadar)

Fransa özellikle telekomünikasyon, uzay, nükleer ve bilgisayar teknolojilerine büyük ilgi göstermektedir. Özellikle kendisi ile tarihi bağları bulunan ülkele re bilgisayar, yeni nesil silah ve savunma sanayii ürünleri pazarlamaktadır.

Eğitimli toplum yapısı, yetişmiş personeli ve teknolojiye ilgi duyan halkı ile bilgi çağını yakalama noktasında oldukça avantajlıdır.(Özdemir, 2003, sy.120)

10.5.7 İngiltere

19.yy'da yaşadığı "güneş batmayan imparatorluk" hayali hiç bitmeyen İngiltere, 2.Dünya Savaşı yıllarında günümüz bilgi ve iletişim teknolojilerinin temelini atsa da diğer Avrupa Ülkeleri ile kıyaslandığında bilgi teknolojilerinde çok da ileri değildir. Ancak parlak geçmie duyulan özlem özellikle son dönemde İngiltere'yi bazı arayışlara itmiştir.

Ağır sanayi altyapısı, bilgi birikimi ve toplumsal tecrübesi bilgi toplumuna geçiş noktasında İngiltere'nin en büyük avantaj sağlamaktadır. (Özdemir, 2003, sy .120-121)

Günümüzde Ülkemizle İngiltere politikaları İngiltere'nin AB algılamalarıyla Türkiye'nin yaklaşımı arasındaki benzerliklerle, Soğuk Savaş sonrası dönemde uluslararası ilişkilere damgasını vuran uluslararası operasyonlardır

İngiltere cephesine bakıldığında son yıllardaki atılımları ve yaptığı yatırımlar ile yeni teknolojiler (bilgisayar, telekomünikasyon vb.) üzerinde yoğunlaşan ülke açısınadan Türkiye önemli bir pazar konumundadır. Türkiye pazarı, yüksek teknoloji danışmanlığı ve müteahhitliği, turizm ve diğer hizmet sektörleri (eğitim, sağlık, müzik vd.) konularında İngiltere açısından önem arzetmektedir. Bunun yanında doğalgaz ve petrol konusunda Türkiye'nin kilit bir ülke halini alması, Türkiye'de zaman zaman yaşanan enerji krizleri Özellikle İngiliz şirketlerinin dikkatini çekmektedir. İngiliz Hükümetinin ve İngiliz Şirketlerinin Turizm, Eğitim ve sağlık alanında da ülkemizde ilişkileri bulunmaktadır.(Laçiner, Türkiye –İngiltere İlişkileri ve İşbirliği İmkanları)

10.5.8 Çin

Çin-ABD arasındaki askerî gerginliğin önümüzdeki dönemlerdeki nedenleri arasında, Tayvan ve Kuzey Kore sorunu, Uydu teknolojileri ve silahlanma konusundaki rekabetin artması gösterilebilir.

Chatham House Rusya ve Avrasya Programı Direktörü Bobo Lo'ya göre, Rusya'nı n Çin ile ilişkilerini güçlendirmek istesinin temel nedeni ABD'ye karşı küresel bir manevra gücü kazanmakken, Çin ise, iki ülke arasındaki ilişkileri sadeece "ikili ilişkiler" şeklinde ele almaktadır. Bu ikili ilişki bakımından Rusya'nın Çin'e duyduğu ihtiyacın daha fazla olduğu değerlendirilmektedir. Ekonomik gücü daha fazla olan Çin'in, askeri gücü bakımından daha güçlü olan izole edilmiş Rusya tarafından Çin'i bir çıkış noktası olarak görmektedir.

Bu noktada Çin'in, ABD ilişkilerinde yaşadığı güven eksi kliğini ve Rusya ile olan ilişkileri gelecekte tam olarak kestirilemeyen senaryoları gündeme getirmektedir.(Hatipoğlu, Rusya-Çin İlişkilerinde Hassas Denge)

Son dönemde ekonomik alanda yaptığı hamleleri teknoloji alanına da yayan ve bilgi savaşı hazırlığının gerekliliğini bilen Çin'de, bilgi savaşı konusunda değişik konseptler tartışılmaktadır.(Özdemir, 2003, sy.117)

10.6.Türkiye'nin Bilgi Savaşı konusundaki Mevcut Durumu

20 Haziran 1998 tarihinde Bakanlar Kurulunca onaylanarak yürürlüğe giren Türk Savunma Sanayii Politikası ve Stratejisi Esasları Dokümanı, Türk Silâhlı Kuvvetlerinin ihtiyacı olan her türlü Silâh, araç, gereç ve mevzuatın, azamî ölçüde millî imkânlarla sağlanması hedeflerine ulaşılması amacıyla hazırlanmıştır.
Dökümanın, aşağıda bahsi geçen bölümleri savunma sanayinin olması gereken özelikleri nitelemesi bakımından önemlidir.

Türk Savunma Sanayii Stratejisi; Ülkemizin güvenliğini sağlama amacıyla, Silâhlı Kuvvetlerin ihtiyaçlarının, yüksek teknolojiye sahip silah ve araçların ülkemiz içerisinde üretilerek, üretim tesislerinin kurulmasını ve kurulu milli savunma sanayii tesislerinin de teşvik ve desteklenmesi içermektedir.

Bu konunun hayata geçirilebilmesi için gerekli olan yapılanma ve teşkilâtlanma; devlet, sanayi, üniversite ve diğer ilgili kuruluşlar arasındaki iş birliği ve koordinasyonun sağlanması, dış politika doğrultusunda ve Türkiye'nin taraf olduğu uluslar arası anlaşmalara uygun olarak yürütülmesi konularında Milli Savunma Bakanlığı ile Dışişleri Bakanlığı arasındaki koordinasyon öngörülmektedir.
Savunma Sanayii; Yüksek teknolojiye dayanan hassas üretim teknikleri, Özel kalite standartları, Yetişmiş insangücü, ARGE faaliyetleri ve yatırım, Tek alıcıya ve sınırlı ihtiyaca dayalı üretim, üretimde sürekliliğin sağlanması için dış pazara açılım, güvenlik ve gizlilik gerektirmesi gibi nedenlerle diğer sanayii kollarından ayrılmakta ve devlet desteğine ihtiyaç duymaktadır.

Türkiye'nin Savunma Sanayii Politikasının; Yerli ve yabancı özel sektöre açık, Dinamik bir yapıya kavuşmuş, Dünya piyasaları ile rekabet gücüne ve ihracat potansiyeline sahip, Yeni teknolojilere adapte olmakta güçlük çekmeyen ve teknoloji üretebilen, Teknolojisini yenileme kabiliyeti bulunan, Dost ve müttefik ülkeler ile iş birliğini mümkün kılan, Mevcut imkânları azamî ölçüde kullanan, entegre olmuş ve duplikasyonlardan arınmış, Alternatif iştigal sahalarına haiz, Alt yapısı oluşturulmuş özelliklerinde olması hedeflenmektedir.
(http://www.msb.gov.tr/birimler/arge/html/04A_savunmasanayi.htm)

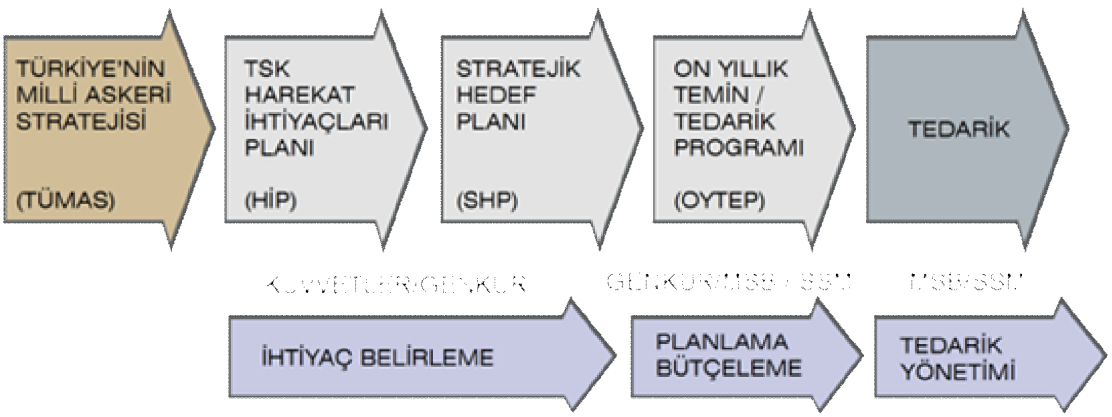
Türk Silahlı Kuvvetleri ile diğer güvenlik kurumlarının sistem ihtiyaçlarını karşılamakla görevli olan Savunma Sanayii Müsteşarlığı (SSM), ülkemizin savunma ve güvenlik ihtiyaçlarının karşılanmasına yönelik bugüne kadar 50'den fazla projeyi başarıyla tamamlamış hâlihazırda, yaklaşık 110 projeyi de yürütmektedir.

Gelişmiş ülkeler, savunma sanayii politikaları, savunma sistem tedariki, proje yönetimi, sanayileşme, finansman, Ar-Ge ve teknoloji yönetimi, projelere sanayinin

katılımı, kalite ve sanayi güvenliği, test ve değerlendirme, ihracat ve savunma sanayii gibi hizmetleri tek elden merkezi olarak, ancak günün değişen koşullarına ayak uydurabilen, dinamik ve proje yönetimine dayalı kurumsal y apılar eliyle yürütmektedir.

Ülkemizin, Milli Savunma Planlama Faaliyetleri, Türkiye'nin Milli Askeri Stratejisi (TÜMAS) ve sıralı konseptler ışığında, ihtiyaçlara yönelik olarak çok büyük önem arzeden Planlama, Programlama ve Bütçeleme Sistemi (PPBS) sür ecine uygun bir biçimde yürütülmektedir.

Bu çerçevede, Türk Silahlı Kuvvetlerimizin ihtiyaçlarının belirlenmesi ve karşılanmasına yönelik olarak Stratejik Hedef Planı (SHP), bu planda belirtilen öncelik sırası dikkate alınarak, mevcut kaynaklar çerç evesinde tedarik faaliyetlerinin bir takvime bağlanabilmesi için On Yıllık Tedarik Programı (OYTEP) ve bütçeleme döneminde de Program Bütçe hazırlanmaktadır.



Şekil 10.1 Strateji Oluşturma

3238 sayılı Kanunla Müsteşarlığa verilen ikinci önemli görev ise Güçlü bir savunma sanayii altyapısının ulusal güvenlik stratejisinin temel unsurlarından olduğu düşüncesiyle geliştirilmesidir. Caydırıcı lığın ve bağımsızlığın olmazsa olmaz koşulu olan, kendi kendine yeten bir savunma sanayii; askeri -stratejik, ekonomik ve politik

açılardan hayati önem taşımasına rağmen ülkemiz bu bakımdan ağırlıklı olarak dışa bağımlıdır.
Aslında bu bağımlılıkda ülkemizin bir savunma sanayi politikasını gerekli kılan en önemli nedenlerdendir. Bu konuda ayrıntılı bilgilere, “ http://www.ssm.gov.tr” adresinden erişilebilir.

Ülkemizde savunma sanayiini geliştirme çabaları, ağırlıkla 197 4 Kıbrıs ambargosundan sonra bir gereklilik olarak olarak şekillenmeye başlamış, Bu aşamada gerekli üretimin yapılması konusunda ağırlıklı olarak ön plana MKEK ve ASELSAN çıkmıştır.

Bu dönemde teknoloji açısından çok ileride olmayan sivil sektör özellikl e 2000’li yıllarda bir gelişim sağlanmış ve savunma sanayiine komşu sektörler olan otomotiv, gemi inşa, elektronik ve yazılım gibi sektörlerde dünya ile rekabet edebilen bir seviyeye ulaşılmış, artık kendi tasarımlarımızı yapma ve Silahlı Kuvvetlerimizin ihtiyaçlarını karşılama aşamasına gelmiş bulunmaktayız.

Artık, her türlü zırhlı araçlar, deniz araçlarının çoğunluğu, komuta kontrol sistemleri, elektronik harp sistemleri, atış kontrol sistemleri, haberleşme sistemleri, gözetleme sistemleri ve belirli güdümlü silahlar milli imkânlarla tasarlanıp Silahlı Kuvvetlerimizin kullanımına verilebilmekte, hatta bu ürünlerde ciddi ihracat başarıları da sağlanmaktadır.

2002 verilerine göre Türkiye, savunma ürünleri ithalatı açısından dünya ülkeleri arasında 3. iken, 2006 yılı verilerinde 11. sırada yer almış, 2002 verilerine göre savunma sanayii ürünü ihraç eden ülkeler arasında 31. sırayıda yer alırken de, 2006 verilerine göre 21.sırada yer almıştır. Gelinen aşama, savunma sanayiimizin derinlik kazandığını ve artık bu alanda üretime geçtiğimizi göstermektedir. (M.Vecdi Gönül, Millî Savunma Bakanı, 5018 Sayılı Kanunun 10'uncu Maddesi Gereğince Millî Savunma Bakanı'nın Kamuoyu Bilgilendirmesi)

Millî Savunma Bakanlığı tarafından yürütülen modernizasyon çalışmalarındak i temel öncelik olan Millî Savunma Sanayiinin geliştirilmesi ve TSK'nın modernizasyon ihtiyaçlarının, 21'inci Yüzyılın koşullarına uygun modern ve bilimsel metotlarla, azami ölçüde millî imkân ve kabiliyetler ile karşılanması amacı doğrultusunda bugüne kadar önemli adımlar atılmıştır. Modernizasyon projeleri, başta TUSAŞ, ASELSAN, ROKETSAN, HAVELSAN olmak üzere TÜBİTAK, üniversiteler ve sanayi kuruluşları ile müştereken yürütülmektedir.

“Bu temel yaklaşım ile TSK'nın modernizasyonu kapsamında;

(1) 2004 yılında çalışmaları başlatılan, ilk defa Millî İmkânlarla Modern Tank Geliştirilmesi Projesi ile ülkemizde ana muharebe tankının Otokar AŞ. ana yükleniciliğinde millî bir tasarım ile geliştirilmesi, azami ölçüde millî imkanların kullanılması öngörülmekte olu p, tankın kullanım ve ihracat dâhil bütün hakları Türkiye'ye ait olacaktır. Sözleşmenin 2008 yılı içerisinde imzalanması ve teslimatların Aralık 2014 tarihi itibarı ile tamamlanması planlanmıştır.

(2) Taarruz Taktik/Keşif Helikopteri (ATAK) Projesinin, yu rt içi sanayimizin maliyet-etkin şekilde kullanılacağı bir model çerçevesinde yürütülmesi amacıyla, helikopterlerin uluslararası işbirliği ile TAI tesislerinde üretimine karar verilmiştir. Görev bilgisayarı, yazılımları ve aviyonik mimarisinin tamamen Türk tasarımı olması planlanan helikopterler için, 2012 yılında seri üretime geçilmesi planlanmaktadır. Böylece ilk defa bir Türk Firması en gelişmiş helikopter ihalesini ve üretimini üstlenmiştir.

(3) Korvet sınıfında bir savaş gemisinin ülkemizde, sanayii ş irketlerimizin geniş katılımı ile ilk defa millî tasarımı ve üretimini öngören ve 2004 yılında başlatılan Millî Savaş Gemisi (MİLGEM) Projesinde, birinci gemi 2007 yılı Şubat ayında kızağa konulmuştur. Preveze Deniz Zaferinin yıl dönümü olan, 27 Eylül 2008 tarihinde, geminin denize indirilmesi planlanmaktadır. Geminin inşaatı; İstanbul Tersanesi Komutanlığı, savaş sistemleri; ASELSAN ve HAVELSAN, form

optimizasyonu; İstanbul Teknik Üniversitesi, tasarım hizmetleri ise; Savunma Teknolojileri Mühendislik ve Ticaret AŞ. (STM) tarafından yapılmaktadır.

(4) TÜBİTAK-TAI ortaklığı ile gerçekleştirilecek Yüksek Çözünürlüklü Görüntüleme Amaçlı Bilimsel Araştırma ve Teknoloji Uydusu Geliştirme Projesi (GÖKTÜRK-2); uydu sistemini millî olarak geliştirmek, üretmek ve yörüngeye yerleştirilmesini sağlamak, TSK'nın keşif ve gözetleme, diğer kamu kurum ve kuruluşlarının gözlem ve araştırma çalışmalarını desteklemek, Türkiye'de uydu ve uydu teknolojileri alt yapısını oluşturmak ve Türkiye'nin uzay alanında söz sahibi olan ülkeler arasında yer almasına katkı sağlamak üzere başlatılmıştır. Söz konusu proje, dünyadan 700 km yükseklikte, güneşe eş zamanlı yörüngede görev yapacak, gerçek zamanlı görüntüleme ve kriptolama kabiliyetine sahip olacaktır.

(5) ASELSAN tarafından özgün bir tasarımla, Türk Hava Kuvvetleri Komutanlığının vuruş gücünü artıracak, ASELPOD Hedefleme ve Seyrüsefer Podu, F-16 ve F-4E/2020 savaş uçaklarına takılacaktır. Sistem, pilotun yükünü asgariye indirirken, uçakların harekât kabiliyetini artıracak, termal ve gündüz kameralarla otomatik olarak çok sayıda hedefi izleyebilecektir. Benzer sistem, dünyada birkaç ülke tarafından üretilip, kullanılmaktadır.

(6) 3 yıllık çalışma sonucu teknolojik bakımdan en ileri ülkelerin sırlarını hassasiyetle sakladıkları Uçuş ve Atış İdare Görev Programları ile Görev Bilgisayarı Türk mühendislerince geliştirilmiştir.

(7) Kılıç II-A ve B Sınıfı Hücumbot Projeleri kapsamında yapılan 6 hücumbottan 3 adedi teslim edilmiş, diğer 3'ünün yapımına, Gölcük ve İstanbul Tersanelerinde devam edilmektedir.

(8) GÜR Sınıfı Denizaltı Projesi kapsamında; 3 adet denizaltı, Gölcük Tersanesinde inşa edilerek teslim edilmiş, 4'üncünün yapımı devam etmektedir.

(9) İlk defa gelişmiş Çift Pilotlu Temel Eğitim Uçağının tasarımı TAI'de yapılmaktadır. 2005 yılında başlatılan projede uçağın ilk uçuşunu 2009 yılında gerçekleştirmesi ve 2011 yılında teslim edilmesi planlanmaktadır.

(10) 2004 yılında ilk defa başlatılan, İnsansız Hava Aracı (İHA) Projeleri kapsamında, özel sektör şirketlerimizin desteğiyle geliştirilen, küçük sınıf bir İnsansız Hava Aracı 2008 yılı içinde kullanıma alınacaktır. Daha gelişmiş ve 24 saat havada kalabilen hava aracının ise TAI'de tasarımına başlanmış olup, ilk uçuşun 2009 yılında, teslimatların ise 2010 yılında gerçekleşmesi b eklenmektedir.

(11) Envanterimizdeki F-16 uçaklarının modern mühimmat, elektronik harp ve gelişmiş aviyonik sistemler ile modernize edilmesi için 2005 yılında imzalanan projelerin 2014 yılında tamamlanması planlanmıştır. Proje kapsamında test ve prototip uçaklarının modifikasyonu TAI'de gerçekleştirilecek, ayrıca ASELSAN ve MIKES firmalarınca geliştirilen Modern Elektronik Harp Sisteminin entegrasyonu TAI'de yapılacaktır.

(12) 2006 yılında nihai sözleşmesi imzalanan Yeni Nesil Savaş Uçağı (F-35) Projesinde, Şubat 2007 tarihinde üretim ve destek safhasının katılımına ilişkin 9 ülkenin yer aldığı konsorsiyuma iştirak edilmiştir. Proje için yapılacak harcamanın en az %50'sine tekabül eden yaklaşık 5 Milyar ABD Dolarlık bir iş payının, savunma sanayii sektörümüzün projeye ortak olan diğer 8 ülke sanayii ile birlikte üretim safhasında üstlenilmesi hedeflenmektedir.

(13) K.K.K.lığının Ara Nesil Tank Tedariki Projesi kapsamında Almanya'dan Leopard 2A4 Tankı alınmaktadır.

(14) Savunma Sanayii Müsteşarlığı ile Amerika Birleşik Devletleri Savunma Bakanlığı arasında imzalanan anlaşma ile; toplam 30 adet "F-16 Blok 50+" modeli uçak ve ilgili destek sistemleri, ABD Hükümeti'nden, Yabancı Askerî Satışlar yöntemiyle tedarik edilecektir. Alınacak Blok 50+ modeli uçakları n teslimatları, 2011 yılı ortasından başlayacak ve 2012 yılı sonunda 30 uçak da envantere girmiş olacaktır.

Uçakların üretim, montaj, uçuş test ve teslimat işlemleri TAI tarafından Ankara'da gerçekleştirilecektir. Uçaklara ASELSAN ve MIKES firmalarınca g eliştirilen elektronik harp sistemleri takılacak, yedekleriyle beraber 46 adet motorunun üretim ve montajı da TUSAŞ Motor Sanayii (TEI)'nin Eskişehir'deki fabrikasında yapılacaktır.

(15) 2003 yılında sözleşmesi imzalanan A400M Modern Ulaştırma Uçağı Geli ştirme Projesinde, konsorsiyum kapsamında üretilecek olan 180 uçağın tamamının orta gövde ve bazı alt sistemlerinin tasarım ve imalatından TAI sorumlu olup, ilk orta gövde teslimatını başarıyla tamamlamıştır. Proje kapsamında ilk uçak teslimatının 2009 yılında gerçekleştirilmesi planlanmaktadır.

(16) CN-235-CASA Nakliye Uçağı pilotlarına, gerçek ortamda uçuş eğitimleri, hava radar eğitimi ve acil durum eğitimleri sağlamak maksadıyla, HAVELSAN tarafından geliştirilen Tam Uçuş Simülatörünün tasarımı, yazılım ı, entegrasyonu ve testi tamamlanarak 30 Milyon ABD Dolarına Güney Kore'ye satılmıştır.

(17) 2005 yılında başlatılan ve HAVELSAN ana yükleniciliğinde yürütülen, Helikopter Simülatörleri Projesi ile tamamen yerli imkânlar ile geliştirilecek simülatörler üzerinde pilotların Sikorsky helikopterlerinde intibak, tazeleme, harbe hazırlık eğitimleri yapılacaktır.

(18) 2005 yılında başlatılan ve DEARSAN ana yükleniciliğinde gerçekleştirilmesi kararlaştırılan, Yeni Tip Karakol Botu Projesinde ilk kez 16 adet botu n, tamamen yerli imkânlarla tasarlanması ve inşa edilmesi planlanmakta olup sözleşme görüşmeleri devam etmektedir.

(19) 2004 yılında başlatılan Sahil Güvenlik Arama Kurtarma Gemisi Projesinde ilk kez askerî amaçlı bir gemi, özel sektör tersanesine (RMK Te rsanesi) sipariş edilmiş olup, geminin komuta kontrol sistemi, elektronik sistemlerinin geliştirilmesi ve gemiye entegrasyonu ASELSAN tarafından yapılacaktır.

(20) Orta ve Uzun Menzilli Silah Sistemlerinin millî olarak üretilmesi maksadıyla, 2003 yılında Orta Menzilli Modern Tanksavar ve Uzun Menzilli Tanksavar Projeleri başlatılmıştır. Söz konusu projeler ROKETSAN ana yükleniciliğinde gerçekleştirilmektedir.

(21) TSK'nın füze ihtiyacını karşılamak amacıyla başlatılan çalışmalar kapsamında ROKETSAN tarafından geliştirilen füze projeleri, ilk defa gerçekleştirilerek kadroya alınmıştır.

(22) Modern topçu silahlarına olan ihtiyacımızın özgün tasarımlarla karşılanması maksadıyla, 40 km menzilli PANTER ve FIRTINA Obüs Projeleri başlatılmış, proje kapsamında üretilen silah sistemleri K.K.K.lığı envanterine girmiştir. ”
(Gönül M.Vecdi, Millî Savunma Bakanı, 5018 Sayılı Kanunun 10'uncu Maddesi Gereğince Millî Savunma Bakanı'nın Kamuoyu Bilgilendirmesi)

11. SONUÇ ve ÖNERİLER

Bilim ve teknolojinin en temel güç ve üretici güce dönüştüğü çağımızda teknolojiyi üretmeden yarınları yakalamak mümkün görülmemektedir. Birbiriyle çok yakın ilişkisi olan bu iki kavram arasındaki açıklık da giderek daralmaktadır. Temel bilimlerdeki yeni gelişmelerin uygulamalı araştırmaların önünü açması ve yeni bilgilerle yeni teknolojilerin üretilmesine imkân sağlaması sonucunda bilim ve teknoloji birbirini tamamlayarak daha bütünleşik bir hal almakta ve yeni açılımları da beraberinde getirmektedir.

Bilgi kavramının geniş bir açıdan irdelenmesi, bilişim teknolojilerinin bilgi üzerindeki etkileri ve boyutlarının değerlendirilmesi, elde edilmesi zor olan bilginin korunması ihtiyacından doğan bilgi güvenliğinin sağlanması çağımızın olmazsa olmaz şartıdır. Küreselleşmenin yeni ve en önemli boyutu olan teknoloji çağımızda tehdit anlayışının değişmesinde de büyük etkiye sahiptir. Bu bakımdan bilgi, bilim ve teknoloji arasındaki ilişki açısından köprü görevini yürüten bilişim teknolojilerinin değerlendirilmesi ve milli bir altyapının kurulmasıda gitgide daha da büyük bir önem kazanmaktadır. Çağımızda teknolojinin de hızlı artışıyla paralel olarak bilgi güvenliğine yönelik saldırıların hem sayı hem de çeşitlilik açısından arttığı bir ortamda, etkin bir bilgi güvenliği oluşturabilmek için gerekli olan, güvenlik süreçleri ve bilişim güvenliğinin sağlanması açısından, ilgili uzmanlarca kullanılabilecek yaklaşımlar ve çeşitli teknolojilerin değerlendirilmesinin önemi giderek daha büyük bir önem taşımaktadır. Çünkü bulunduğumuz coğrafya güçsüz olan devletlere hiçbir zaman yaşama şansı vermemiştir. Güçlü kalabilmek de ilk şart da güçlü, çağı yakalamış sistemlerle donanımlı bir ordu ile sağlanabilir. Bu da gelişmiş ülkelerde olduğuı gibi teknoloji ile sağlanabilir.

İçinde yaşadığımız dünyada mali, askeri, sanatsal, bilimsel ve benzeri her türlü bilgiyi internet sağanağı altında yaşamımıza katarken, önemli olan kişisel ya da bir devlete ait bilgilerin bir kaynaktan diğerine; güvenli, hatasız ve hızlı bir biçimde iletilmesidir. Bu aynı zamanda milli güvenlik için de olmazsa olmaz şarttır.

Çağımızda, bilgisayar ağları ile taşınan her türlü bilgi, bilgi çağı olarak tanımladığımız çağın en değerli varlığıdır. Dolayısıyla bu veriler açısından bu sistemler de, bireyler ve ülkeler için hayati önem taşımaktadır.

Güvenli iletişimin sağlanması, çağın teknolojilerinin sağladığı avantajlar sayesinde hem çok kolay hem de çok zordur. Gelişmiş ülkelerin teknolojiyi istedikleri gibi kullanmaları durumunda, teknoloji yarışında geri kalmış ülkeler bir fanus içine alınabilir. Bunun önlenmesi içinse çağın güvenlik anlayışlarını göz önüne almak oldukça önemlidir.

Devletimizin güvenliği etkileyen milli güvenlik alt yapısının oluşturulması konusunda çalışmaları olmakla beraber, oluşturulan altyapının ihtiyaçları tam anlamıyla karşıladığı söylenemez. Milli bazda konu ile en alakalı oluşum olan Ulusal Bilgi Güvenlik Teşkilatı olup doküman seviyesinde yeterli altyapıya sahiptir. Bu konuda çalışmalarını sürdürmektedir.(Özdemir, 2003, 157 -158)

Bilgi Savaşı'nın Bölümleri Olan, Komuta Kontrol Savaşı, İstihbarat Temelli Savaş, Elektronik Harp, Psikolojik Harekât, Bilgisayar Korsan Savaşı, Ekonomik Bilgi Savaşı ve Siber Savaş kavramlarında da en önemli varlık ve silah teknoloji dir. Eğitimin, Bilişim, Kriptografi, Uydu, Enerji ve Nanoteknolojilerin önemi giderek artmaktadır. Bu savaş bakımdan ülkemizin hazırlanması çerçevesinde dikkate alması gereken; Ekonomik, Politik, Sosyal ve Kültürel, Jeopolitik Değerlendirmeler, Coğrafyamız aktörleri ile olan ilişkiler ve değişen güvenlik anlayışları, Türkiye'nin Bilgi Savaşı Konusundaki Mevcut Durumu ve diğer aktörlerin potansiyelleri bu çerçevede değerlendirilmelidir.

Savaş alanındaki birliklerin komuta ve kontrolunu sağlayan sistemler, emniyetli, süratli, en yakın gerçek zamanlı, güvenilir haberleşme ihtiyacı duymaktadırlar. Askeri haberleşme alt yapısı, birliklerden ve muhtelif sensörlerden gelen bilgilerin ve raporların, gerçek zamanda otomatik olarak toplanmasına, işlenmesine, değerlendirilmesine, harekat emirlerinin ilgili birliklere ve atış komutlarının silah sistemlerine gerçek zamanda ulaşmasına imkan sağlamalıdır.

Askeri Haberleşme alanında ASELSAN, günümüz modern ordularının taktik saha haberleşme ihtiyaçlarını karşılamaya yönelik, Bölge Muhabere Sistemleri, Telsiz Haberleşme Sistemleri, Telli Haberleşme Sistemleri ve Mobil Komuta Kontrol Haberleşme Sistemleri üretmektedir.

Konuyla ilgili özeti ASELSAN'ın belirlediği misyon çerçevesinde yapmak istiyorum.

"Kara, hava, deniz, uzay ve sivil uygulamalar kapsamında her nevi elektrik, elektronik, elektronik harp, haberleşme, mikrodalga, elektro-optik, güdüm, bilgisayar, bilişim, yazılım, kriptoloji ve güvenlik konularında Türk Silahlı Kuvvetleri'nin dışa bağımlılığını en aza indirecek; tüm müşterilerinin ihtiyaçlarını azami ölçüde karşılayacak; güncel ve gelişen teknolojilerle uyumlu, nitelikli ve maliyet etkin ürün ve sistem çözümleri tasarlamak, geliştirmek, üretmek ve her koşulda devamlılığını sağlamak yönünde öncü olmak" sadece ASELSAN'ın değil sayıları daha da arttırılan benzer kurumların da temel görevi olarak belirlenmelidir. Bu gibi kurumların sahip oldukları varlık ve kaynakları çoğaltmak ve değerlerini sürekli artırmak da ülkemizin misyonu olarak belirlenmelidir.

Eğitim

Her şeyin onun için olduğu varlık olan insanın eğitilmesi çok büyük bir gerekliliktir. Belirlenecek insan kaynakları stratejileri, toplumu eğiterek insanların öncelikli olarak bilinçli, şuurlu bireyler olmalarını, sonraki aşamalarda da bilim ve teknoloji araştırmalarına girmelerini teşvik edecek nitelikte olmalıdır. Bu stratejinin belirlenmesi ve hayata geçirilmesinde tecrübeyi de dikkate alarak konularında tecrübeli ve uzman kişilerden yararlanılmalıdır.

ARGE

Gelişmiş ülkeler incelendiğinde, bu ülkelerin bilim adamları sayısının ve ARGE yatırımlarının çok fazla olduğu görülmektedir. Ülkemizde beyin göçünü durdurarak geriye beyin göçü noktasında teşvikler arttırılmalı, projeleri değerlendirilen bilim

adamlarına her türlü maddi ve manevi destek sağlanmalıdır. Savunma Sanayi noktasında etkinliginin artırılması da Arge'ye yapılacak yatırımlarla mümkün olacaktır.

Bu bakımdan Milli savunma sistemlerinin geliştirildiği TSK, MSB,SSM, ASELSAN, TÜBİTAK vb. kurumların uzman sayıları arttırılmalı, üniversitelerin bu sistemlerin üretilmesinde geliştirici rol almaları sağlanmalıdır. Savunma Araştırmaları yapan birimler kurularak desteklenmeli, uzman kadrolar yetiştirilmeli ve koşullar ne kadar ağır olursa olsun bu kadrolar korunmalıdır. (Sevgi, 2002)

Kaynak Ayrılması ve İşbirliği

Araştırmalar konusunda yeterli kaynakların ayrılması ve devlet kurumları ile üniversiteler arasındaki işbirliği çok önemlidir. Bu noktada Üniversitelerinin sahip olduğu teknolojik altyapı ve bilgi birikimi ile üniversite -sanayii işbirliği çerçevesinde güdümlü projelerle teknolojik bilgi üretilerek sanayiye aktarılmalıdır. Bu bilgi de teknolojiye dönüştürerek, kazanç sağlayacak ürünlerin üretilmesiyle ekonomiye, dolayısıyla da uluslararası areneda ülkemize ekonomik rekabet gücüne büyük bir ivme kazandırılmış olacaktır.

Savunma Sanayii Müsteşarlığının görevlerinden olan savunma sanayimizin projelere katkısını sağlarken ordumuzun ihtiyaçlarını karşılama görevi ülkedeki mevcut durum çerçevesinde ordumuz ile işbirliği içerisinde yatırımların belirlenen bir strateji çerçevesinde arttırılması ile sağlanabilir. Bu noktada da en önemli konu bu strateji çerçevesinde çağın ihtiyaçlarının belirlenmesidir.

Çağın teknolojilerinin Belirlenmesi

Teknolojiye ya satın alarak, ya üreterek ya da transfer ederek ederek sahip olabiliriz. Bunlar arasında ülkemiz açısından en yararlısı muhakkaktır ki teknolojinin ülkemiz tarafından üretilmesidir. Üretim aşamasına geçme de, değerlendirilmesi gereken en önemli noktada verimlilik açısından çağın yeni teknolojilerinin belirlenerek özellikle bu konulara yatırım yapılmasıdır.

Mühendislik ve temel bilimler, nanoteknolojiler, enerji, bilişim ve haberleşme teknolojileri, her türlü güvenlik teknolojileri, sağlık, çevre ve uzay teknolojileri öncelik verilecek alanların başında gelmektedir.

Rekabet Gücünün Korunması

Çağımızda ülkeler, sahip oldukları teknolojilere ilave olarak, uluslar arası arenada rekabet güçlerini kaybetmemek adına yeni ve farklı teknojilere ihtiyaç duymaktadırlar. Bunun yanında gerekli araştırma ve geliştirme faliyetleriyle savunma sanayisinin planlanması da ülkeler açısından gereklilik olarak karşımıza çıkmaktadır.

Milli Bilgi Altyapısı

Ülkelerin güvenliğinin olmazsa olmaz şartlarında biri de toplumun her kesiminin bilgiye istediği zaman, istediği yerde, ekonomik ve güvenli bir biçimde ulaşabilmesini sağlayacak "Milli bilgi altyapısı"'na sahip olmalarından geçmektedir. Bu ise internete erişim kapasitesinin istenilen düzeye yükseltilmesi, elektronik ticaretin ve elektronik devlet uygulamalarının yaygınlaşması, bilgi güvenliğini sağlayacak uluslararası kural ve standartlar çerçevesinde hukuki ve kurumsal düzenlemeler yapılması gerekliliklerini ortaya koymaktadır.

Bilim Kentlerin Kurulması

Bilimkentlerin kurularak ve zaman içerisinde bunların sayılarını arttırarak büyük bir ekonomik gelişme sağlanabilir. Bu kentler bilim merkezleri kadar ticari özellikleri de taşıyarak Devlet'in ve özel sektörün desteğiyle ülkemizi teknoloji noktasında istenilen noktalara getirebilir.

Kontrollü Özelleştirme Politlkaları

ARGE 'ye ayrılan bütçelerin yüksek olmasının yanında belirlenmiş özel alanlarda devletin kontrolü elinde bulundurması çok önemlidir. Bu bakımdan ülkemizde son

dönemlerde yaşadığımız özelleştirmelerin ne kadar yararlı oldukları, önümüzdeki dönemlerde anlaşılabilecektir.

Yapılan özelleştirmeler, kamu yararına olması kaydıyla, gerçek anlamda ekonomik getirisi değerlendirildikten sonra, devletin sosyal yapısını da bozmayacak şekilde gerçekleşmelidir. Ayrıca, kamu kaynaklarının olumlu kullanılması ve beklide en önemlisi Milli Güvenliğimiz açısından tehdit oluşturmayacak biçimde o lmalıdır.

Dünya'da Meydana Gelen Değişimler

Global anlamda Dünyamızda meydana gelen gelişmeler ve değişimler değerlendirilerek, ülkemizin gelecekte karşılaşacağı tehditleri anlayarak tedbirler alabiliriz. Gelecekteki savaş eğilimlerinin tespiti bir ülkenin savunmasının teşkil edilmesinde büyük bir avantaj sağlayan öngörünün gelişmesini sağlayacaktır..

Deneyimlerden Yararlanma

Uluslararası organizasyonlar kapsamında faaliyet yürüten birimlerin çalışmaları milli bir bakış açısıyla gizli bir biçimde incelenmel i ve belki de geliştireceğimiz çok önemli bir teknolojiye kaynak teşkil edebileceği unutulmamalıdır. Yine aynı şekilde, Sanayi politikalarının ve teknolojinin geliştirilerek avantajlarından yararlanma sürecinde gelişmiş ülkelerin yaşadığı süreçlerde, ülkem izin şartları da değerlendirilerek göz önüne alınmalıdır.

Yabancı Ortaklıklar

Maliyet, zaman,ve imkanlar çerçevesinde yabancı kaynakların ülkemizin belirlediği, ülkeler arasında kurulacak denge politikaları ile kullanımı gerçekleştirilebilir.

İhtiyaçların bu tür ortaklıklar vasıtasıyla giderilmesi durumunda, bu sistemlerin üretimlerinin her aşamasının Milli Kuruluşlar tarafından denetlenmesinin ve üretilen ürünün de yine bu kurumlarca her türlü testlerinin yapılması hem güvenlik hem de bu teknolojilerin ülkemizce üretilmesini sağlama bakımından yararlı olacaktır.

Kaynakların Olumlu Kullanımı

Ülkemizin sahip olduğu üniversitelerdeki, firmalardaki, TÜBİTAK ve benzeri kuruluşlarındaki, üniversitelerindeki, araştırma kuruluşlarındaki bilgi kaynakları belirlenerek değerlendirilmelidir.

Ülkemizin coğrafi özelliklerinden gelen kaynakları da maalesef ülkemizce yeteri kadar değerlendirilmemektedir. Oysa dört tarafı denizlerle çevrili, farklı iklimlere ve su kaynaklarına sahip ülkemiz enerji ve biyolojik kaynaklar yönü nden zengindir. Bu kaynaklar enerji üretiminde daha verimli biçimde kullanılarak enerji ihtiyacının karşılanmasında özellikle orta vadede çözüm olabilir. Biyolojik kaynakların değerlendirilmesi de ilaç ve kozmetik sektöründe kullanılarak eoknomik değerlere dönüştürülebilir. Uzun vadede nükleer santraller enerji ihtiyacımızın karşılanması açısından düşünülebilir. Ancak nükleer enerjiye geçiş muhakkak kendi milli çalışmalarımız doğrultusunda ve alt yapı oluşturulduktan sonra yapılmalıdır. Aksi taktirde tarihte de görebileceğimiz bazı sıkıntılar ya da uzun vadede karşılaşabileceğimiz yüksek maliyetler ülkemizin karşısına çıkabilir.

Burada dikkat edilmesi gereken diğer nokta da Nükleer Denizaltılardır. Nükleer denizaltılar, enerjilerini su soğutmalı basınçlı nük leer reaktörlerden sağlarlar ve bu reaktörlerin çevresini saran basınçlı su devresi, diğer su kazanlarına girerek türbünlerde kullanılacak buharı üretir. Bu buhar hem pervane türbününü hem de elektrik jeneratör türbününü çevirir. Bu sistem, hiç hava gerekt irmez. Yalnız personele gerekli olan hava kimyasal yollarla temizlenir. Geminin su ve hava ihtiyâcı, deniz suyundan özel cihazlarla temin edilir. (http://tr.wikipedia.org)

Nükleer güçle kendi elektriğini üreten bu denizaltılarda, aracın içinde bir nükleer santral olması bulunmaktadır. Nükleer denizaltılar, "genel maksatlı nükleer denizaltılar" ve stratejik önemi yüksek "balistik füze taşıyabilen" nükleer denizaltılar olmak üzere taktik ve stratejik amaçlı olarak kullanılmaktadır. Uzun süre deniz altında su yüzüne çıkmadan seyretmesi, gizlenerek bilgi toplaması (görevsel veya elektronik), bazı özel operasyonlar için komando birliklerini taşıması bu denizaltıların en önemli özellikleridir.

Özellikle Soğuk Savaş'ta yoğun bir biçimde kullanılan bu savunma araçları, savaş yılları sürecinde, Amerikan ve Sovyetler arasında kamuya yansımayan pekçok çatışmanın aktörü olmuşlardır.

Özellikle Körfez Savaşı ve Balkan müdahalelerinde nükleer denizaltılar k ara hedeflerine yönelik füze saldırıları gerçekleştirerek birer su üstü gemisi rolü de üstlenmişlerdir.

Bu noktada ülkemizinde nükleer denizaltı konusuna daha da fazla önem vererek çalışmalar yapması, ya da mevcut çalışmaları geliştirmesi hem savunma hem haberleşme hem de düşmanlarımıza karşı caydırıcı bir güç olarak avantaj sağlayacaktır. (Atalan, 2001)

Rusya, 450 adet çift reaktörlü nükleer denizaltısı ile, sanki 900 adet nükleer santrali ile dünyanın çeşitli yerlerinde gezinmektedir. (Aksoy, 2007)

Milli Sistem ve Yazılımlar

Günümüz "Bilgi Savaşı" dünyasında, ileri teknoloji ürünlerin milli güvenlikteki yerleri de giderek önem kazanmaktadır. G izlilik esaslı çalışan ve daima ileri teknoloji kullanan Savunma sistemlerinin kontrolü ve transferleri de –eğer eskimiş değillerse- genellikle bu sistemlerin sahiplerinin yönetim ve iznine bağlıdır. Herhangi bir biçimde dışarıdan satın alınma suretiyle sahip olunan ve kullanılan sistemler, belki ilk etapta gayet güzel işliyor gibi görülse bile, çatışma ve savaş anlarında satın alındıkları ülkelerce sınırlandırılabilecek özelliklere sahip olabilmektedirler.

Bu durum, ülkeler arasında karşılıklı çıkar ilkesine uygun olarak kurulan ilişkilerin, çıkarların çatıştığı noktada bir süreklilik arzetmemesi durumunda, özel likle de geçmiş dönemlerde silah sistemlerini yurt dışından satın alma yoluyla temin eden ülkemiz açısından, bir risk teşkil etmektedir. Bu bakımdan, uzun dönemler müttefik olduğumuz bir ülke ile çıkarların uymadığı noktada, bu ülkeden satın alınmış savunma sistemlerinin, silah niteliğini kaybetme ihtimali de karşımıza çıkmaktadır.

Bunun en güzel örneklerinden birisi Körfez Savaşı'nda yaşanmıştır. Nitekim, elinde çok iyi silahlar bulunmasına karşın, sistemlerin teknolojilerine gerçek anlamda sahip olamamış Irak yenilmekten kurtulamamıştır. (Ziylan, 2003)

Bu konuda alınabilecek ilk tedbir, savunma sistemlerinin üretiminin hiçbir ülkeye bağlı olmayan, bağımsız olarak oluşturulacak milli sistemler çerçevesinde sağlanmasıdır. Hiçbir suretle hiçbir yabancı bir ülkeye ait sistem kritik yapılar içerisinde değerlendirilmemelidir. Bu amaçla ilk olarak milli yazılım ve donanım geliştirme faaliyetleri bir politika çerçevesinde tüm devlet birimleri ve özel katılımlarla sağlanmalıdır. Mevcut yazılımlar güçlendirile rek kullanımları yaygınlaştırılmalıdır.

Kritik noktalarda kullanılan tüm elektronik sistemlerin, milli ihtiyaçlar doğrultusunda milli olarak tanımlanması, geliştirilmesi, denenmesi ve kullanılması bir zorunluluktur. Milli sistemlere sahip olmayan ülkelerin , belki de kullandıkları teknolojiyi üreten ülkelere karşı yürütülecek bir savaş anında, kullandıkları silahların kendilerine dönmeyeceğini çağımız teknolojileri göz önüne alındığında kimse garanti edemez.

Örneğin F-16 uçaklarına milli yazılım yüklenmesi, uçağın bu yazılımlar sayesinde kimin dost kimin düşman olduğunu ayırt etmesini sağlaması bakımından önem kazanmaktadır. Mevcut durumları itibarıyla Türkiye ve Yunanistan'ın kullandığı uçaklar Nato'ya üyelikten kaynaklanan nedenlerle birbirlerini dost olara k görmektedir. Ege Denizi'nde yaşanan "it dalaşı" bundan kaynaklanmaktır.

"Özetlemek gerekirse, teknoloji gerek yüksek katma değer elde etmek, gerekse üretim sürecine hakim olmak, savunma sektöründe ise silah sistemlerinin güvenilirliğini sağlamak a çılarından çok önemlidir."

Ülkemizde genel olarak transfer edilen teknolojiler yaygın olarak kullanılmaktadır. Bu bakımdan Ülkemizde milli, özgün teknoloji üretiminin desteklenmesi ve özendirilmesi gereklidir. Bu aynı zamanda, Türk savunma sanayiinin ekono mik

anlamda rekabetçi olması ve yurtdışına satış yapabilmesi için de gereklidir.(Ziylan, 2003)

Savunma Sanayii Müsteşarı Murat Bayar'ında belirttiği gibi sıfırdan tank, helikopter, savaş uçağı, denizaltı ve daha da önemlisi bunların kendi yazılımlarını mil li bir çerçeve de üretmek en büyükl hedefimiz olmalıdır.

Bu gelişmeler çerçevesinde Milli Savunma Bakanlığı bütçesinin Milli Eğitim Bakanlığı bütçesinin ardından ikinci sıraya indiğini de söylemek de başka bir sevindirici gelişme olarak algılanabilir. (Ta hiroğlu, 2008)

Bilgi Savaşı Kavramının Anlatılması

Başta ekonomi, sağlık, savunma teknolojileri olmak üzere halka ve özellikle kamu sektöründe çalışanlara bilgi savaşı ve bu savaşa karşı alınabilecek savunma amaçlı tedbirler anlatılmalıdır.

Kritik Altyapının Belirlenmesi

Türkiye kendi ekonomik, siyasi, politik, coğrafi ve kültürel şartlarını göz önünde bulundurarak kritik alt yapılarını bir plan çerçevesinde tespit etmelidir. Bu tespit işleminin tüm Devlet kurumları ve üniversiteler arasında yürütülecek bir koordinasyon çerçevesinde özel sektöründe katılımıyla yapılmalıdır.(Özdemir, 2003, sy.141)

KAYNAKLAR

AHVENAİNEN Sakari, About İnformation Warfare, Finnish Defence Forces, 24th January 2000

AKIN H. Bahadır, Bilişim Teknolojilerinin Evrimi ve Bilişim Teknolojilerinin Çağdaş İşletmelerde Stratejik Yönetim Üzerindeki Etkileri, Çukurova Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Cilt:8 Sayı:1 Yıl:1998

AKMAN İbrahim, İNCİ Saadet, ERTEN Murat, KILIÇ Hürevren, BİLİR Aslı, İsmail Bilir, Emrah Tomur Meral Durgut, ,e-Devlet: BİLİŞİM GÜVENLİĞİ, Türkiye Bilişim Derneği, Kamu Bilgi İşlem Yöneticileri Birliği,2004

AKYILDIZ Ersan, ÇİMEN Canan, AKLEYLEK Sedat, , Şifrelerin Matematiği: Kriptografi, ODTÜ Yayıncılık, 2. Baskı, Ekim 2007

AKSOY Soner, Nükleer Enerji ile İlgili Konuşması, 10.05.2007, http://www.soneraksoy.net/icerik_detay.asp?id=308

ALBERTS David S. Director, Command and Control Research Program (CCRP),National Defense University, NDU Press Book,August 1996

ALBERTS David S. Garstka John J., Hayes Richard H., Signori David A., Understanding İnformation Age Warfare, Command and Control Research Program ,August 2001

ALBERTS David S. GARSTKA John J., STEİN Frederick P., Network Centric Warfare: Developing and Leveraging Information Superiori ty2nd Edition (Revised), CCRP publication series sy.15 August 1999)

ALFORD D. Jr, Cyber Warfare: Protecting Military System., USAF, Acquisition Review Quarterly—Spring 2000

ALKAN Mustafa, TEKEDERE Hakan, POLAT Ayşegül, Dsl Teknolojisinin İletişime Sunduğu Geniş Bant İmkânları, 2001

ALTINKAŞ Evren, Türkiye Ve Yunanistan: Rakip Müttefikler, Dokuz Eylül Üniversitesi, Uluslararası İlişkiler Bölümü, Araştırma Görevlisi, sy.3, 2005

AMERİCAN Cryptogram Association, A Handbook For The Members Of, 2005

ARDA Derya, BULUŞ Ercan, YERLİKAYA Tarık, Türkiye Türkçesinin Bazı Dil Karakteristik Ölçütlerini Kullanarak Vigenere Şifresi İle Şifreleme Ve Kriptanaliz, Bilgisayar Mühendisliği Bölümü Mühendislik - Mimarlık Fakültesi Trakya Üniversitesi, Edirne

ARI Tayyar, Geçmişten günümüze Ortadoğu: Siyaset, savaş ve diplomasi, Alfa yayınları, Ekim 2004, İstanbul

ARSLAN Feyzullah, Tarihten Günümüze İç Ve Dış Tehditler, Kamu Yönetim ve İdari Bilim Uzmanı, Polis Dergisi, 2001, Sayı:29

ARSLANOĞLU İbrahim, Misyonerlik, Batı Emperyalizminin Silahıdır

ARSLANOĞLU İbrahim, Ulusal eğitime neden gereksinim vardır?

ATABEY Osman, Temel saldırı teknikleri

ATALAN Sami, Nükleer denizaltılar, Military Science & Intelligence Magazine, MSI Dergisi, 01.09.2001

ATAY Mehmet, "Batıda Örgütlenmiş Casusluk ve Gizli istihbarat Savaşının - Öncüleri", Strateji Dergisi, , 2003, Sayı 9

AVCI Gültekin, İstihbarat Oyunları orduların karanlık senaryoları, Birey Yayınları, 1. Baskı, Şubat 2007

AYDOĞAN Metin, Türkiye'yi Bekleyen Tehlikeler Bitmeyen Oyun Kumsa ati Yayınları, 11. Baskı, Ağustos 2002

BAĞÇE H. Emre (1999), "Küreselleşme, devlet ve demokrasi", Amme İdaresi Dergisi 32 (4), Sy.9-10)

BALIK Hasan, Mikrodalgalar ve kullanım alanları, 2005

BANKS Darwyn O., Air Command and staff college air university information war crimes mitnick meets Milosevic, USAF, A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements Advisor: Lt Col Steven R. Hansen Maxwell Air Force Base, AlabamaApril 2001

BAŞTÜRK Rabi Psikolojik Harp ve Kültür Savaşları, IQ Kültür Sanat yayıncılık, 2005, İstanbul

BAYAZIT Hüseyin, Teknolojik Küreselleşmenin Güvenlik ve Strateji Alanındaki Gelişmelere, Uluslar Arası Güvenlik ve Strateji Kuruluşlarının İşlevine ve Yapılanmasına Etkisi

BAYHAN Suzan ve ALAGÖZ Fatih, Uydu Ağları Yönlendirme Protokolleri: Problemler Ve Bazı Çözümler, Akademik Bilişim 2007, Dumlupınar Üniversitesi, Kütahya, 2007, Boğaziçi Üniversitesi, Bilgisayar Mühendisliği, Uydu Ağları Araştırma Laboratuvarı (Satlab), İstanbul, 2007

BAYKAL Nazife, Bilgi Teknolojisinin Ulusal Güvenlik ve Ulusal Güvenlik Stratejisi ile İlgili Boyutu

BAYKAL Nazife, Bilgisayar Ağları veri İletişimi, Yerel Geniş Ağlar, İnterent Teknolojileri, SAS Bilişim Yayınları, Mart 2001

BEKTAŞ Atilla, Bilgi Güvenliği ve Kriptografi, SPK'da Geçen Ay Dergisi, Ocak 2006

BENGÜR Suat, ATMACA Fikri, ŞENER Oğuz, Türkiye'nin Özgün Elektronik Harp Sistemleri ve İşarete İşleme Teknolojisi, ASELSAN A.Ş. Mikrodalga ve Sistem Teknolojileri Grubu, Ankara

BERKAY Ahmet, Hack Teknikleri, G.Y.T.E. Bilgisayar Mühendisliği

BİCAN Can, Sosyal Mühendislik Saldırıları Sunu, Tübitak UAKAE

Bilim ve Teknoloji Stratejileri Çalıştayı, Konuşma Özetleri, Gazi Üniversitesi, 31 Mayıs-1Haziran 2006, Gazi Üniversitesi Bilim ve Teknoloji Stratejiler Araştırma ve Geliştirme Merkezi, Ankara

BİRCAN İsmail, Kamu Kesiminde Stratejik Yönetim ve Vizyon Planlama Dergisi, DPT'nin Kuruluşunun 42.yılı Özel Sayısı, Ankara, 2002

BOZKURT Veysel, Küreselleşme kavram, gelişim yaklaşımlar, mayıs 2005

BRACKEY Thomas A., Goldberg Eugene L., Falk Aaron D., Tappis Eugene C., and Les Yen Hughes Space and Communications Company, Commercial Communications for the ISS: System Considerations, Presented at Conference on International Space Station Utilization, Space Technology and Applications International Forum (STAIF-99), Albuquerque, New Mexico, February, 2, 1999

BRENTON Chris, HUNT Cameron, Network Security, SecondEdition, Sybex 2003

BUDANUR İsmail, Securıty Via Fırewalls

BUTTYÁN Levente, A Brief History of Cryptography, Laboratory of Cryptography and System Security (CrySyS) Department of Telecommunications, Budapest University of Technology and Ec onomics

BÜYÜKANIT Yaşar, Genelkurmay Başkanı Orgeneral Yaşar Büyükanıt'ın "Güvenliğin Yeni Boyutları ve Uluslararası Örgütler " Konulu Uluslararası Sempozyum Açış Konuşması, 31 Mayıs 2007

BYRD John T., Director,S&ategy and PolicyDivision(N51), Chief of Naval Operations, Departman of Defense, Departman of Navy Departman of Navy, OPNAVINST 3434.1, N515, 22 DEC 1997

CANBEK Gürol, Klavye Dinleme Ve Önleme Sistemleri Analiz, Tasarım Ve Geliştirme Yüksek Lisans Tezi, Bilgisayar Mühendisliği, Gazi Üniversitesi , Fen Bilimleri Enstitüsü, Eylül 2005, Ankara

CANBEK Gürol, SAĞIROĞLU Şeref, Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri:Bir İnceleme, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 23 (1-2) 1-12 (2007)

CEVİZOĞLU Hulki, Misyonerlik ve Siyasal Hristiyanlık Ceviz kabuğu yayınları, 1. Baskı Şubat 2005 Ankara)

COUGHLAN Shane M. The University of Birmingham School of Politics and İnetrnational Studies, Is there a common understanding of what constitutes cyber warfare?", Supervised by Dr. Terry Terrif, 2003

ÇALIŞIR İbrahim, Virüsler(sunu), Odtü Bilgi İşlem Dairesi Başkanlığı Bilişim Teknolojileri Güvenliği Ekibi Kullanıcı Destek Grubu,23 Aralık 2002

ÇANKAYA Seyit, ERTÜRK Servet, Optik İletim Kuramı, Ankara1999

ÇAVDAR Çiçek, Erişim Kontrol Me kanizmaları, Bilgisayar Ağlarında Güvenlik, Bilişim Enstitüsü, Bilgisayar Bilimleri, 20.04.2004

ÇIRACI Salim, Türkiye'de nanoteknoloji Ulusal Nanoteknoloji Araştırma Merkezi, Bilkent Üniversitesi, Fizik Bölümü, Bilim ve Teknik Dergisi, Ağustos 2005

ÇİMEN Ali, ECHELON, İstihbarat Dünyası'nın Perde Arkası, Timaş Yayınları, 5. Baskı, İstanbul, 2006

DANA Peter H., Global Positioning System Overview, The Geography Department, University of Colorado and Boulder, Revised: 05 /01/2000 (first published in September, 1994
http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html

DANIŞMAN Özgür, Güvenlik Riskleri trendler ve Bilgi Güvenliği Sertifikasyonu, 2007

DAŞKIRAN Levent, Bilim ve Teknik, Tübitak Yayınları, Sanal Tehdi t bilgisayar virüsleri, Mayıs 2005

DEDE Melih Bayram, 50 Yıldır Dinliyorlar, Mart 2002 , http://yenisafak.com.tr/diziler/echelon/index.html

DEMİR Hasan, Rehin Türklerin kurtuluşu, Yeniçağ Gazetesi, 03/12/2007

DEMİREL Emin, Teşkilat-ı Mahsusa'dan Günümüze Gizli Servisler, IQ Kültür Sanat Yayıncılık, 5.Baskı, İstanbul 2004

DEMİRKOL Zafer, İnternet Teknolojileri, Pusula Yayınları, 1. Baskı, Eylül 2001

DERMAN Ethem, Uydu Yörüngelerine Giriş, Ankara Üniversitesi, 20 05, http://derman.science.ankara.edu.tr/index.htm

DİNDAR İsmail, 21.yy'da teknoloji ve istiharat savaşları, IQ Kültür Sanat Yayıncılık,İstanbul, 1.Baskı, Temmuz 2004

DİRİCAN Can Okan, Teori ve Uygulamalar ille TCP/İP ve ağ güvenliği, Açık Akademi, Ekim 2005 İstanbul

DPT, Sekizinci Beş Yıllık Kalkınma Planı, Bilim Ve Teknoloji Özel İhtisas Komisyonu Raporu Ankara 2000, http://ekutup.dpt.gov.tr/

EDEN Dan, Weapons of Total Destruction viewzone http://www.viewzone.com/haarp00.html,http://www.viewzone.com/haarp11.html

E-Dönüşüm Türkiye İcra Kurulu, Bilgi T oplumu Stratejisi Taslağı, Yükleniciler: Türkiye Bilişim Vakfı, Bilişim Sanayicileri ve İşadamları Derneği; Katkı: Devlet Planlama Teşkilatı, Türkiye Bilişim Derneği, Bilgi Toplumu Stratejik Plan Hazırlığı, Dpt Kdep Eylem No 1, 8 Mart 2004

ELBERT Bruce R., İntroduction to Satellite Communication, Artech House Boston, London, Second Edition, 1999

ERDAL Murat, Teknoloji ve Ulusal Güvenlik, İstanbul Üniversitesi, Siyasal Bilgiler Fakültesi, İşletme Bölümü İstanbul

ERKOÇ Şakir, Nanobilim ve Nanoteknoloji, O DTÜ B ilim ve Toplum Kitapları Dizisi, Odtü Yayıncılık, 2. Baskı, Kasım 2007, Ankara

EROL Hüseyin, Sayısal (Elektronik) İmza ve Açık Anahtar Altyapısı, Bilgi ve Bilgisayar Güvenliği Dersi Araştırma Projesi, Aralık 2004 Ankara

ESLEN Nejat, Yeniçağın güvenlik sorunları, 17 Eylül 2001

FADİA Ankit, Network Security, A Hacker's Perspective, Second Edition, Thomson Course Technology, Boston, USA, 2006

FINDIK Oğuz, SADAY Taha, Bilgi Güvenliğinin Sağlanmasında Kullanılan Yöntemler Ve Bunların Etkin Kullanımı, Akademik Bilişim 2003, Çukurova Üniversitesi, Adana,3-5 Şubat 2003

FİSCHER M. J., CPSC 467b: Cryptography And Computer Security Week 2 (Rev. 2), Yale University Department of Computer Science., January 18 & 20, 2005

FLEİSCH Brett D. Cryptography and Data Security (2), College of Engineering University of California, Based on notes of Evans and Gemmell, 5/4/01

GÖNÜL M.Vecdi, Millî Savunma Bakanı, 5018 Sayılı Kanunun 10'uncu Maddesi Gereğince Millî Savunma Bakanı'nın Kamuoyu Bilgilendirmesi

GÖNÜL Vecdi, Bakan Sunuşu, Milli Savunma Bakanlığı, 2007
http://www.msb.gov.tr/Birimler/MALIYE/html/doc/BakanSunusu.pdf)

GÜLŞEN Azzet, Uydu Sistemleri, Telekomünikasyon Kurumu, Spektrum Yönetimi Dairesi Başkanlığı, 2007

GÜRAK Hasan, Küreselleşme nereye götürüyor? Doğrudan Yabancı Yatırımlar, Verimlilik ve Gelir Dağılımı,2003

HASANOĞLU Mürteza, Küreselleşmenin Devlet Yönetimine Etkileri, , Sayıştay Dergisi Sayı: 43 Ekim-Aralık 2001

HATİPOĞLU Esra, Rusya-Çin İlişkilerinde Hassas Denge, USAK, Uluslararası Stratejik Araştırmalar Kurumu,

http://www.usakgundem.com/uayazar.php?id=684

HEADQUARTERS Department of the Army Washingt on, DC, 31 May 1995, FM 100-16, Army Operatıonal Support, 9-I

HWEI P., Analog and Digital Communication, Analog ve Sayısal İletişim, Schaum's outlines, Nobel Yayın Dağıtım, Ankara 2003

JOİNT Chiefs of Staff, Department of Defense Dictionary of Mil itary and Associated Terms, as amended through December 7, 1998 ,Joint Publication 1 -02

JOİNT PUB 3-13 Joint Doctrine for Information Operations, 9 October 1998

KAHN David, İstihbaratın Tarihsel Teorisi, Avrasya Dosyası, Uluslar arası İlişkiler ve Stratejik Araştırmalar Dergisi, Yaz 2002 Fasikül: 23 Cilt: 8 Sayı: 2 (Bu makale, Intelligence and National Security Dergisi'nin 2001 yılı Sonbahar sayısındaki "An Historical Theory of Intelligence" başlıklı ingilizce orijinalinden çevrilmiştir.)

KALAYCI Tahir Emre, Bilgi Teknolojilerinde Güvenlik ve Kriptografi, İzmir, Haziran, 2003

KANTARCI Şenol, Rusya-ABD: "Koalisyonlar Dönemi mi?", TURKSAM, 01.08.2007, http://www.turksam.org/tr/yazdir1319.html

KAPLAN Zeynep, Avrupa Birliği'nde Bilim Ve Teknoloji Pol itikaları Ve Adaylık Sürecinde Türkiye'nin Uyumu, 3. Ulusal Bilgi, Ekonomi Ve Yönetim Kongresi Bildiri Kitabı, Yıldız Teknik Üniversitesi, İibf, İktisat Bölümü, 3. Ulusal Bilgi, Ekonomi Ve Yönetim Kongresi, Osmangazi Üniversitesi, İktisadi Ve İdari Bilimler Fakültesi 25-26 Kasım 2004, Eskişehir

KARA Berna, Doruk Yayımcılık 2004 Ankara Electronic Warfare in the İnformation Age-Bilgi Çağında Elektronik Harp D.Curtis Schleher, , sy.20

KARAMÜRSEL Sacit.Ü., Beyin Sapı ve Orta Beyin, İstanbul Tıp Fakültesi, Fizyoloji Anabilim Dalı, Sunu

KARAMÜRSEL Sacit.Ü.,Serebellum, İstanbul Tıp Fakültesi, Fizyoloji Anabilim Dalı, Sunu

KASIM Kamer, ABD'nin Orta Asya Politikasındaki İkilem, Abant İzzet Baysal Üniversitesi, Uluslar arası İlişkiler Bölümü Öğretim Üyesi ve USAK D anışmanı, 14 Eylül 2007

KAYNAK Mahir, Büyük Ortadoğu projesi ve Türkiye üzerine Stratejik Analizler, Truva Yayınları, 2005, İstanbul

KAYRAN Ahmet H., Analog Haberleşme, Birsen Yayınevi, İstanbul, 1999

KAYRAN Ahmet H., PANAYIRCI Erdal, AYGÜLÜ Ümit, Birsen Yayınları, 4.Baskı, İstanbul, 1998

KEİTH Jim, Amerikan Derin Devleti ve Beyin Yıkama Operasyonları, Nokta Kitap, Çeviri:Sibel San, Aralık 2006

KIRIMLI Meryem, ERDEM O. Ayhan, Açık Anahtar Kriptografisi İle Sayısal İmza Tasarımı Ve Uygulaması, Gazi Üniversitesi Teknik Eğitim Fakültesi Elektronik-Bilgisayar Eğitimi Bölümü, ANKARA, 2007

KİBAROĞLU Mustafa, Rusya'nın Yeni Ulusal Güvenlik Konsepti Ve Askeri Doktirini, Bilkent Üniversitesi, Uluslararası İlişkiler Bölümü Avrasya Dosyası - Rusya Özel Sayısı, Şubat 2001

KOÇ Çetin Kaya, One-Time Pad or Vernam Cipher School of EECS1148, Kelley Engineering Center, Oregon State University Corvallis, Oregon, USA

KODAZ Halife, RSA Şifreleme Algoritmasının Uygulaması, Bilgisayar Mühendisliği Bölümü, Selçuk Üniversitesi, Konya, 2003

KOLTUKSUZ A. " Simetrik Kriptosistemler için Türkiye Türkçesinin Kriptanalitik Ölçütleri ve Ulusal Kriptolojik Standart Geliştirimi", 1. Sistem Mühendisliği ve Savunma Uygulamaları Sempozyumu, Ekim 1995, Ankara

KOPP Carlo, A Doctrine for Use of Electromagnetic Pulse Bombs (Revised Draft of RAAF APSC Working Paper 15, July, 1993

KORKUT Refik, Psikolojik Savunma, Ankara, 1975, sy.1, ŞAHİN Hülya, Milli Mücadelede beyannameler ile Psikolojik Harp,(Atase arşivi belgelerine göre) Ankara 2003

KÖKEN Hayrettin, İkinci Körfez Savaşı ve Uzay Teknolojileri, 2005, H.H.O Havacılık ve Uzay Teknolojileri Enstitüsü

KULOĞLU Armağan, Global Strateji Enstitüsü, Irak'taki Gelişmeler, Pkk Terör Örgütü, Abd-Türkiye İlişkileri Ve Kerkük, Analiz, Global Strateji Enstitüsü (Gse), 19 Şubat 2008

KUMKALE Tahir Tamer Beynimizi kimler ve nasıl yönetiyorlar, Veysel Gani, küresel güçlerin psikolojik savaş yöntemleri, Pegasus yayınları, 2.Baskı, 2006

KÜLEBİ Ali, Geleceğin Savaşları (1-2), Tusam - Ulusal Güvenlik Stratejileri Araştırma Merkezi 23.11.2004

KÜLEBİ Ali, Yunan silahlanması ve olası savaş, TUSAM, 13.02.2006

LABRİS Teknoloji, Yazılımı Güvenliği Yaklaşımı, www.labristeknoloji.com/dosyalar/yazilim%20guvenlik%20denetimi%20ve%20risk%20analizi.doc

LAÇİNER Sedat, Fransa–Türkiye İlişkileri ve Ermeni Sorunu (1980'e Kadar), Ders Notları, USAK Stratejik Gündem, Yazarın TÜRKLER VE ERMENİLER, BİR ULUSLARARASI İLİŞKİLER ÇALIŞMASI adlı eserinden alınmıştır

LAÇİNER Sedat, USAK Stratejik Gündem, Türkiye –İngiltere İlişkileri ve İşbirliği İmkanları, http://www.usakgundem.com/makale.php?id=97

MACİT Betül, Savaşın Sanal Boyutu, Cumhuriyet Strateji, 26.11.2007

MAJ Paul JW, Electronic Warfare, MCS 08, Winter 2004

MARTİN Libicki, what is information warfare, National Def ense University, 1996

MARTİN Libicki, What Is Information Warfare? Strategic Forum Number 28, National Defense University,, First Printing, USA, Washinghton 1995

MCCLURE Stuart, SCRAMBRAY Joel, KURTZ George, Hacking Exposed, Fourth Edition, Mc Graw Hill Osborne, California, Usa

MİLLİYET Gazetesi, Bilgisayardaki Casus 19.03.2001

Milli İstihbarat Teşkilatı, 2007 Faaliyet Raporu

Milli Eğitim Bakanlığı, Megep (Mesleki Eğitim ve ÖğretimSisteminin Güçlendirilmesi Projesi), Elektrik Elekt ronik Teknolojisi, Analog ve Sayısal Haberleşme, Ankara, 2007

MİMAN Ahmet Tarık, Küreselleşmenin Ordusu Ekonomik İstihabarat, IQ Kültür Sanat yayıncılık, 1. Baskı, Mayıs 2007

MİTNİCK Kevin, D. William L. Simon Çeviri: Nejat Eralp Tezcan, Aldatma Sanatı, ODTÜ yayıncılık, Ocak 2006

MORGAN Walter L. and GORDON Garry D., Communications Satellite Handbook, A Wiley-İnterscience Publications, USA, 1989

MOWRY David P, German Cipher Machines of World War II. Center for Cryptologic History National Security Agen cy, 2003

NAR Pelin Çorak, Bilgin İbrahim, Askeri İşbirlikli Nesne Ağlarında Güvenlik, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı

Oktuğ Sema, İTÜ Bilgisayar Mühendisliği Bölümü, BLG433 -Bilgisayar Haberleşmesi ders notları,

OPPENHEİM, WİLLSKY, and NAWAB, Signals and Systems,2nd Edition 1996

OTT Katharine, Ciphers and Thomas Jefferson, Thomas Jefferson and Mathematics SeminarUniversity of Virginia, University of Virginia Department of Mathematics, January 30, 2007

ÖZAVCI Fatih, Bilgi Güvenliği – Temel Kavramlar sunu, Nisan 2002

ÖZAVCI Fatih, Bilgi Sistemleri Güvenliğine Giriş(sunu), Siyah Şapka Güvenlik Çözümleri, Ekim/2001

ÖZBİLEN Alper, Pusula Yayıncılık, Bilgisayar Ağları ve Güvenliği, İstanbul, Ocak 2005

ÖZDAĞ Ümit, Stratejik İstihbarat, Uluslararası İlişkiler ve Stratejik Araştırmalar Dergisi, Yaz 2002 Fasikül: 23 Cilt: 8 Sayı: 2,

ÖZDEMİR Eşref, Bilgi Savaşları, IQ Kültür Sanat yayıncılık, 2003, İstanbul

ÖZEREN Dilek, Güvenlik Yönetim Sistemleri , Ürün ve Hizmet Güvenliğinde TSE, TSE Bilgi İşlem Daire Başkanı

ÖZKAN Tuncay, Milli İstihbarat Teşkilatı, MİT, Dünden Bugüne Gizli Dünyanın Bilinmeyenleri, Alfa Yayınları, Aralık 2007

ÖZKAYA Ömer, CIA Belgeleriyle Zihin Kontrol Operasyonları, IQ Kültür S anat Yayıncılık, 4.Baskı, 2003, İstanbul

PEKOL Semih, Kurumlarda Bilgi Güvenliği Politikaları, Boğaziçi Üniversitesi, Yönetim Bilişim Sistemleri, 2005

PERRY William J., Annual Report to the president and the congress, Part 6: Command Control Communicati on Computer Intelligence secretary of defense, february 1995

PROAKİS John G.,SALEHİ Masoud, Communication System Engineering, Second Edition, Printice Hall, 2002

Pro-G Bilişim Güvenliği ve Araştırma Ltd., Bilişim Güvenliği, http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf, 2003

RADİKAL Gazetesi, Beyin kontrol gözlüğü, 09.04.2008

RADİKAL Gazetesi, Yeni Ortadoğu kurulurken, 30.06.2004, Dr. NADİYE MUSTAFA: Kahire Üniversitesi Uluslararası İlişkiler öğretim üyesi'ne ait İslamonline.net sitesinde ayyınlanan makalesinin çevirisi, 2004

ROECKL Chris, An overview of firewall technology and how Juniper Networks implements it, 1194 North Mathilda Avenue Sunnyvale, CA 94089 USA, 2004

RYAN Johnny, iSavaş: Yeni bir tehdit, uygulamadaki kolaylığı ve bu konuda giderek artan zayıflığımız Nato Dergisi: Güvenlik konusunda ortaya çıkan ve gelişen tehditler Kış 2007

SAĞSAN Mustafa, Bilgi Savaşı:Siperlerden Klavyelere Taşınan Savaşın Anatomisi, Psikolojik Harp İstihbaratı Avrasya Dosyası Ulus lararası İlişkiler ve Stratejik Araştırmalar Dergisi Yaz 2002 Fasikül: 23 Cilt: 8 Sayı: 2

SAKA Yusuf, Bilgisayar Ağ Güvenliği ve Şifreleme Muğla Üniversitesi Fen Bilimleri Enstitüsü İstatistik ve Bilgisayar Bilimleri Anabilim Dalı, , MUĞLA,2000

Savtek 2002 Savunma Teknolojileri Kongresi, Cilt II: Posterler, Editörler, Prof.Dr. R.Orhan Yıldırım, Prof.Dr. Mustafa İlhan Gökler, Doç.Dr.Öğ. Alb.A.Kadir Varoğlu, Prof.Dr. Bilgehan Ögel, Dr.Öğ.Bnb. Ahmet Uluşan, 24-25 Ekim 2002, Ankara

SELEK Yusuf Korhan, Dünyaya Göre Eş Zamanlı Hareket Eden İki Haberleşme Uydu Sisteminin Transponder Kanalının Girişim Etkilerinin İncelenmesi, Ankara Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Fizik Mühendisliği Anabilim Dalı, Ankara, 2004

SEVGİ Levent, Savunma Teknolojilerinde Ulusal Kaynaklar, Yetişmiş İnsan Gücü ve Eşgüdüm, SAVTEK 2002, Savunma Teknolojileri Kongresi, 24 -25 Ekim 2002, ODTÜ, Ankara

SHİMEALL Tim, Cyberterrorism, Carnegie Mellon Uni.,2002
www.cert.org/archive/ppt/cyberterror.ppt - 2005-10-11

SİNANOĞLU Oktay, Büyük Uyanış, Otopsi Yayınları,7. Baskı İstanbul, 2002)

SİNGH Simon, Code Book, designed by Nick Mee of Virtual İmage publishing Ltd. and Simon Singh, March 2004, Stockport, U.K

SLOAN Stanley R., Nato Dergisi, Genişlemeyi İncelerken, Düşünceler, Krize Mukabele, İlkbahar 2002,
http://www.nato.int/docu/review/2002/issue1/turkish/opinion.html

SMİTH JERRY The Ultimate Weapon Of The Conspiracy, 1998; Çeviri: Selim Yeniçeri Koridor Yayınları, 2007 İstanbul

SOĞUKPINAR İbrahim, Veri Güvenliği Ders Notları, G.Y.T.E.Bilgisayar Mühendisliği Bölümü

SPEER Robert, Searles Craig AIAA Team 5, www.aoe.vt.edu/~mason/Mason_f/ElectWarPres.ppt

STALLİNGS William, Cryptography and Network Security Preciples and Practise, Prentice Hall, Third Edition, USA, 2003

STALLİNGS William, Network Security Essential Applications and Standarts, Prentice Hall, Second Edition, New Jersey USA, 2001

STEİN George J., Enformasyon Savaşı-Siber Savaş-Net Savaşı 2002, sy.181) Avrasya Dosyası, Uluslar arası İlişkiler ve Stratejik Araştırmalar Dergisi, Yaz 2002 Fasikül: 23 Cilt: 8 Sayı: 2

STRASSBERG Keith E., GONDEK Richard, ROLLİE J. Gary, Firewalls, Mc Graw Hill Osborne, California, Usa, 2002

SUTHERLAND Scott, An İntroduction to Cryptography, Associate Professor of Mathematics Director of Undergraduate Studies in Mathematics State University of New York at Stony Brook October 26,2005

ŞAHİN Şenol, Uydular (Suni Peykler), Ankara Üniversitesi, Astronomi ve Uzay Bilimleri

ŞEKER Güven, Amerikan Örneklemi Işığında Kamu Alanında Bilginin İnternet İle Sunumu Ve Önündeki Tehlikeler, e-akademi aylık internet dergisi, Kasım 2002, Sayı 9

ŞEKER Selim, Bilgi Çağının Değerlendirilmesi, Boğaziçi Üniversitesi, Elektrik - Elektronik Mühendisliği Bölümü, İstanbul,2004

ŞEN Bilal, Elektronik Gözetim, Emniyet Genel Müdürlüğü Kaçakçılık ve Organize suçlarla mücadele Daire Başkanlığı

ŞENGONCA Halil KARAARSLAN Enis, TEKE Abdullah, , Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması Ege Üniv. Uluslararası Bilgisayar Enst., Ege Üniv. Bilgisayar Müh.,2006

ŞİMŞEK Erdal, İstihbarat Servislerinde Beyin Yıkama Operasyonları, Kum Saati Yayınları, Mayıs 2005, İstanbulTALU Umur, Milliyet Gazetesi, 08.01.2000

TARHAN Nevzat, Psikolojik Savaş, Timaş yayınları, 4. Baskı, 2002

TAYLOR Philip M., Institute of Communications Studies, University of Leeds, UK. Oslo, November 2006

TAYLOR Philip, Concepts of Information Warfare (Sunu), Institute of Communications Studies, University of Leeds, UK. Oslo, November 2006

TBD Kamu-BİB, Bilişim Sistemleri Güvenliği El Kitabı, Sürüm 1. 0, Türkiye Bilişim Derneği Yayınları, Abdurahman ULU, Adnan YILMAZ, Aslı Ayşe BİLİR, Ercan SOLAK, H. Erhan AYDINOĞLU, Emrah TOMUR, Eyüp YILDIRIM, İsmail BİLİR, Levent ÖZBEN, Mehmet YILMAZER, Murat

ERTEN, M. Nurettin KABADAYI, Üveyiz Ünal ZAİM, Yavuz ÖZİBA, Mayıs 2006

Telkoder,KabloTV komisyonu RaporuÖzeti,2003)

TOSUN Yalçın, , Güvenlik Politikaları, Ağ Güvenliği Proje Iıı 13.04.2004

TOSUN Yalçın, Vekil Sunucular Ve Güvenlik Duvarları Ağ Güvenliği Proje III, 13.04.2004

Türkiye Bilimsel ve Teknik Araştırma Kurumu, Türk Bilim ve Teknoloji Politikası, 1993-2003,

http://www.mu.edu.tr/t/universite/uluslararasi/TurkBilimTekPolitikasi_Tubitak.pdf

URHAN Oğuzhan, ZENGİN Fevzi, ŞANLI Musa, Des Algoritması Kullanılan Akıllı Kart İle Güvenlik Sistemi Tasarımı ve Uygulaması Elektonik ve Haberleşme Mühendisliği Bölümü Veziroluğu Yerleşkesi, Kocaeli Üniversitesi, 41040, Kocaeli

UZUNAY Yusuf, Bilişim Suçları, Orta Doğu Teknik Üniversitesi Enformatik Enstitüsü, Ekim 2005

ÜNAL Ahmet Naci, YARMAN Sıddık, Teknolojik Gelişmeler Işığında Yeni Savunma Kavramları ve Strateji Belirleme, SAVTEK 2002, Savunma Teknolojileri Kongresi, 24-25 Ekim 2002, ODTÜ, Ankara

VELİEV Cavid, Yakındoğu Ve Kafkasya Araştırmaları Masası, Tusam Değerlendirme, 06.12.2005

VURAL Fatoş Tünay Yarman, Bilgi Teknolojisindeki Gelişmenin Yarattığı Uluslar Arası Yeni Güvenlik Ortamı

VURMAY, H. Miray. "İslam'ın En Katı Yorumu: Vehhabilik", Cumhuriyet Strateji Eki, 12.10.2005

WİNKLER Ira S. and Dealy Brian Information Security technology?...Do n't Rely on It A Case Study in Social Engineering , Science Applications International Corporation, Proceedings of the Fifth USENIX UNIX Security Symposium Salt Lake City, Utah, June 1995

YAŞAR Sülbiye, COST -Bilimsel ve Teknik Araştırma Alanında Avrupa İşbirliği, Mobil Ağlar, 2005, ab.org.tr/ab05/tammetin/141.doc

YENİÇERİ Zuhal, Pivolka, Yıl 3 Sayı 13 03 / 2004

YERLİKAYA Tarık, Buluş Ercan, Buluş Nusret Kripto Algorıtmalarının Gelişimi Ve Önemi, Trakya Üniversitesi Bilgisayar Müh. Bölümü, 2006

YILDIZ Hayrullah, Milli Elektronik Harp Yaklaşımı ve Teknolojik Öncelikler, http://www.turkishdefense.net/reference/HY/hy0001.htm

YILMAZ Davut, Bilişim Korsanlığı ve Korunma Yöntemleri, Haya t Yayınları,3. Baskı, İstanbul 2005

YILMAZ Sait, 21.yy da Güvenlik ve İstihbarat, Alfa Yayınları, Haziran 2006

YILMAZ Sait, Ulusal Güvenlik ve İstihbarat: Türkiye ve ABD üzerine kavramsal bir çerçeve, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Uluslar arası İlişkiler Anabilim Dalı Doktora Tezi, Ankara, 200

YURDUSEV Esin, Dünyanın Ve Türkiye'nin Yakıntarihi, İlköğretim Öğretmenliği Lisans Tamamlama Programı, T.C. Anadolu Üniversitesi Yayınları No: 1019 Açıköğretim Fakültesi Yayınları No: 562, Eskişehir, Ekim 1998

YÜCEL Durdu, XDSL (Digital Subscriber Line) Sistemlerin Kıyaslanması, Kahramanmaras Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik - Elekronik Mühendisliği Anabilim Dalı, Kahramanmaraş, Eylül - 2005

YÜCEL İsmail Hakkı, Türkiye'de bili m teknoloji politikaları ve iktisadi gelişmenin yönü Dpt bilim, 2005

ZİCKUHR, Clare, Smith, Gar, Project HAARP: The military's plan to alter the ionosphere, Earth Island Journal, 10410406, Fall94, Cilt 9, Sayı 4

ZİYLAN Aytekin, Ankara, Hedef Ulusal Tekno loji Yeteneğinin Yükseltilmesi Olmalı, Aralık 2000, Hava Lojistik Dergisi, Ocak 2000, Aselsan Dergisi, Mart 2000, Kısaltılmış Çeviri: Aharon Lapıdot, The Israel Air Force And The Defence Industry, Military Technology 5/99

ZÜLFİKAR Hamza, Dünden Bugüne Tür kçe Türk Dili, 661. sayı Ocak 2007

İnernet Kaynakları:
http://beyazperde.mynet.com/film/3808
http://blog.milliyet.com.tr/Blog.aspx?Blog No=6733, 2006
http://en.wikipedia.org/wiki/Sherman_Kent)
http://hacivat.khas.edu.tr/~baskan/EH203%20Hab erle%feme%20Cihazlar%fd/tel efon1.pdf
http://img157.imageshack.us/img157/92/wanservicesfl9.jpg
http://inosci.blogspot.com/2007/12/elektronik -sava-nedir-ew-electronic.html
http://savassaygili.net/?m=200710
http://tr.wikipedia.org/wiki/ Almanya#Ekonomi
http://tr.wikipedia.org/wiki/Enigma_makinesi

http://tr.wikipedia.org/wiki/Kullan%C4%B1lan_Portlar%C4%B1n_numara_listesi

http://tr.wikipedia.org/wiki/Asker%C3% AE_denizalt%C4%B1lar#N.C3.BCkleer_Denizalt.C4.B1lar

http://webarsiv.hurriyet.com.tr/1998/04/09/37246.asp

http://www.atin.org/isthsair.asp

http://www.bid.ankara.edu.tr/yardim/inet-tr-HTML/bolum3.html

http://www.cert.org/stats/cert_stats.html

http://www.cyberspaceorbit.com/ indexbck.html

http://www.elkotek.com.tr/page.asp?PageID=67

http://www.haarp.alaska.edu/haarp

http://www.haarp.alaska.edu/haarp/photos.html

http://www.hipaabasics.com/glossary.htm

http://www.iam.metu.edu.tr/sempozyum/2005/sunumlar/051118_EAkyildiz.pdf

http://www.innova.com.tr/08Arsiv/download/bilgi_guvenligi.pdf

http://www.kamusm.gov.tr/tr/bilgideposu/belgeler/teknik/aaa/index.html?kriptolojinedir.htm

http://www.koubk.org/modules.php?name=Content&pa=showpage&pid=44

http://www.mgk.gov.tr/Turkce/sss.html#soru_13)

http://www.msb.gov.tr/birimler/arge/html/04A_savunmasanayi.htm

http://www.ntvmsnbc.com/news/442713.asp

http://www.redbilisim.com/sayfa.aspx?id=40

http://www.ssm.gov.tr/TR/kurumsal/Documents/SP/yazdir/yazdir7.html

http://www.tbd.org.tr

http://www.tcpsecurity.com/doc/genel/temelsaldiriteknikleri.html

http://www.tuncayozkan.com/yazi.php?yazi_id=56684)

http://www.turktelekom.com.tr/webtech/default.asp?sayfa_id=39

http://www.turktelekom.com.tr/webtech/default.asp?sayfa_id=445

http://www.turktelekom.com.tr/webtech/default.asp?sayfa_id=446

http://www.zonguldak.pol.tr/bilisim_sss.htm

https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/what-is-intelligence.html

www.bim.gazi.edu.tr/virus_nedir.doc

www.owlnet.rice.edu/~nava201/presentations/Lecture19.ppt , Naval Weapons System, C4ISR and Information Warfare

http://www.gym-tech.net/solutions/backbone.html

ÖZGEÇMİŞ

1978 yılında Sivas'ta doğan Bülent Keskin, Lise öğrenimini 1992 -1994 yılları arasında İstanbul Haydarpaşa Lisesi'nde tamamladıktan sonra, 1994 yılında Marmara Üniversitesi Fizik Öğretmenliği Bölümüne başlamıştır. Bölümden 1996 yılında ayrılan Keskin, yine aynı yıl, Dumlupınar Üniversitesi Elektrik Elektronik Mühendisliği Bölümüne başlamıştır. 2000 yılında mezun olduktan sonra Vatani görevini 2001-2002 yılları arasında Ankara'da yedek subay olarak tamamlayarak, 2002 yılında da Türk Telekom A.Ş'de Telek om Uzman Yardımcısı olarak çalışmaya başlamıştır. Kurumda sırasıyla Transmisyon Müdürlüğü, Bilişim Ağları Müdürlüğü ve Bilgi Güvenliği ve Strateji Planlama Müdürlüğünde görev alan Keskin, özelleştirme nedeniyle 2006 yılında kurumdan ayrılmıştır. Bu tarihte n itibaren de İstanbul Bayındırlık ve İskân Müdürlüğünde çalışmaktadır.

Uzm.Ecz. Zeliha Keskin ile evlidir. İngilizce ve Almanca bilmektedir.

EK:1 BİLGİ GÜVENLİĞİ TEŞKİLATI VE GÖREVLERİ HAKKINDA KANUN TASARISI

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

Madde 1- Bu Kanunun amacı; ulusal güvenliği ilgilendiren bilgilerin korunması, Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standar tlarının saptanması, ihracat ve ithalat izinlerinin ve sertifikalarının verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi kamu ve özel kurum ve kuruluşların arasında koordinasyonun sağlanması amacıyla bir teşkilatın kurulması ve görevlerine ilişkin esas ve usulleri düzenlemektir.

Kapsam

Madde 2- Bu Kanun, ulusal güvenliği ilgilendiren bilgiye işlem yapan kamu ve özel kurum ve kurulusları ile yerel yönetimleri, kamu kurumu niteliğindeki meslek kuruluslarını, üniversiteleri, bu yerlerde çalişan personeli, diğer tüzel ve gerçek kişileri, bilgi güvenliğinden faydalananları ve faydalanacak durumda olanları kapsar.

Tanımlar

Madde 3-

Bu kanunda geçen deyimlerden;

a**)** Ulusal Bilgi Güvenliği: Ulusal güvenliği ilgilendir en, yetkisiz ellere geçtiği taktirde devletin güvenliğini tehlikeye sokabilecek veya devlet aleyhine kullanılabilecek her türlü bilgiyi, üretim, kullanım, işlenme saklanma, nakledilme ve imha sırasında yetkisiz kişilerin erişimine ve olası her türlü fiziks el ve elektronik müdahaleye karşı korumaya; bilgiye erişim ve kullanıma ait usulleri açık şekilde belirlemeye ve bilgiyi gerektiğinde hazır bulundurmaya yönelik tedbirleri,

b) Haberleşme Güvenliği: Ulusal güvenliği ilgilendiren bilginin özellikle telekomünikasyon kanallarından gönderilmesi sırasında yetkisiz kişiler tarafından elde edilmesinde ve içeriğinin açığa çıkarılmasına ve diğer her türlü müdahaleye karşı alınan tüm tedbirleri,

c) Fiziki Güvenlik: Ulusal güvenliği ilgilendiren bilgiyi ihtiva eden ya da bu bilgiye işlem yapan cihaz, malzeme ve tesisi, yetkisiz kişilerin erişimine karşı korumak üzere alınan fiziksel tedbirleri,

d) Personel Güvenliği: Ulusal güvenliği ilgilendiren bilgiye yalnızca yetki verilen kişilerin, bilmeleri gerektiği oranda eri şebilmeleri için alınan tüm tedbirleri,

e) Teknik Güvenlik: Yurt içinde ve yurt dışında personel, araç, donanım ve binalarda dinleme ve gözetleme amacıyla yapılan teknik yerleşmelere karşı alınan tüm güvenlik tedbirlerini,

f) TEMPEST: Tüm elektronik teçh izattan ve bunların kuruluşundan iletkenlik ve ışıma yoluyla istem dışı yayılan bilginin önlenmesine ilişkin alınan tedbirleri,

g) Güvenlik hali: Bilginin güvenliğinin bilerek veya istenmeyerek yapılan herhangi bir işlem nedeni ile tamamen ya da kısmen ort adan kaldırılmasını,

h) Kripto: Birbirleriyle haberleşen iki tarafın, haberleşmesi esnasında üçüncü tarafa bilgi sızdırmamak amacıyla bilginin gizlenmesini sağlayan sistemleri,

i) Kriptoloji: Kriptografi ve kripto analiz konuları ile ilgilenen bir bilim d alını,

j) Kripto Sistemleri: Şifreleme ve şifre çözme etkinliklerinden birisini veya ikisini birden yerine getirmeye yarayan, bu sistemler kapsamında veri iletişimi de dahil olmak üzere her türlü iletişim sistemlerinde kullanılan sistemleri,

k) Kriptografik Algoritma: Bir bilginin gizlenmesi için yapılan matematiksel bir islemi,

l) Ulusal Bilgi Aği: Kamu ve özel kuruluşlarda ulusal güvenliği ilgilendiren bilgiye işlem yapan mevcut terminalleri, bilgi teatisi maksadıyla birbirine bağlayan ağı,

m) Üst Kurul: Ulusal Bilgi Güvenliği Üst Kurulunu,

n) Kurum: Ulusal Bilgi Güvenliği Kurumu Başkanlığını, ifade eder.

İKİNCİ BÖLÜM

Kuruluş ve Görevler

Kuruluş

Madde 4- Ulusal bilgi güvenliğinin sağlanması amacıyla başbakanlığa bağlı Ulusal Bilgi Güvenliği Üst Kurulu ile tüzel kişiliğe sahip katma bütçeli Ulusal Bilgi Güvenliği Kurumu Başkanlığı kurulmuştur.

Ulusal Bilgi Güvenliği Üst Kurulu

Madde 5- Ulusal Bilgi Güvenliği Üst Kurulu; Ulusal bilgi güvenliği alaninda genel direktif organı olup, başbakanın başkanlığında; Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu genel sekreteri, Genel Kurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Milli Istihbarat Teşkilatı Müsteşarı, Türkiye Bilimsel Ve Teknik Araştırma Kurumu ile kurum başkanından oluşur. Başbakanın katılmadığı hallerde üst kurula, Adalet Bakanı başkanlık eder.

Üst kurulun daimi üyeleri tarafından ihtiyaç duyulduğu hallerde, diğer bakanlar ile kamu ve özel kurum ve kuruluşlarının temsilcileri de üst kurul toplantılarına katılabilir.

Üst Kurulun toplantı yeter sayısı daima üyelerin üçte ikisidir. Kararlar, toplantıya katılan daimi üyelerin oy çokluğu ile alınır. Toplantılara katılmaları uygun görülen diğer kişilerin oy hakkı yoktur.

Üst Kurul, Nisan ve Ekim aylarında olmak üzere, yılda iki defa olağan olarak toplanır. Üst Kurulun gündemi, Başbakan tarafından belirlenir.

Başbakan, daimi üyelerden birisinin talebi üzerine, Üst Kurulu olağanüstü toplantıya çağırabilir.

Üst Kurulun sekreterya hizmetleri, kurum tarafından sağlanır.

Ulusal bilgi güvenliği kurumu başkanlığı

Madde 6- Ulusal Bilgi Güvenliği Kurumu Başkanlığının teşkilatı, aşağıda isimleri belirtilen ana hizmet birimlerinden oluşur:

a) Plan Program ve Koordinasyon Daire Başkanlığı,

b) Bilgi Güvenliği Daire Başkanlığı,

c) Kriptoloji Daire Başkanlığı,

d)Bilgi Destek Daire Başkanlığı,

e)Denetleme ve Bilgilendirme Daire Başkanlığı,

Kurumun danışma birimi, Uluslararası İlişkiler ve Hukuk Müşavirliği; yardımcı birimleri ise, Ulusal Bilgisayar Güvenliği Merkezi Müdürlüğü ve Genel Sekreterliktir.

Kurumun teşkilatı Ek'li cetvelde gösterilmiştir.

Ulusal bilgi güvenliği üst kurulunun görevleri

Madde 7- Ulusal Bilgi Güvenliği Üst Kurulunun görevleri aşağıda belirtilmiştir:

a)Ulusal bilgi güvenliğine yönelik tehdidi değerlendirmek, ulusal bilgi güvenliği siyasetinin tayini, tespiti ve uygulamasıyla ilgili kararları almak ve kuruma bu konuda direktif vermek,

b)Tespit edilen ulusal bilgi güvenliği siyasetine ilişkin kararlar doğrultusunda yapılan uygulamaları incelemek, değerlendirmek ve yönlendirmek,

c)Ulusal bilgi güvenliğine ilişkin mevzuat değişikliği tekliflerini değerlendirmek.

Ulusal Bilgi Güvenliği Kurumu Başkanlığının Görevleri

Madde 8- Ulusal Bilgi Güvenliği kurumu Başkanlığının görevler i aşağıda belirtilmiştir:

a) Ulusal bilgi güvenliğine karşı yurt içi ve yurt dışı tehdidin tespit edilmesini sağlamak, gerekli tedbirleri almak ve alınmasını sağlamak,

b) Ulusal bilgi güvenliği sistemini oluşturmak için politika, konsept, ilke, standart ve usulleri tespit etmek ve geliştirmek,

c) Ulusal bilgi güvenliğinin sağlanmasına esas olarak bilginin gizlilik, bütünlük ve kullanıma hazır olmasını sağlayacak tedbirleri belirlemek, uygulamak, uygulanmasını sağlamak ve kontrol etmek,

ç) Ulusal bilgi güvenliği risk yönetimi ve değerlendirmesini yapmak ve yapılmasını sağlamak,

d) Ulusal bilgi güvenliği alt yapısını korumak amacıyla gerekli görülecek ulusal bilgi güvenliği sistemi esaslarını tespit ederek kurmak ve geliştirmek,

e) Ulusal bilgi güvenliği siste minin mimarisinin oluşturulmasında caydırma, koruma, ikaz, tespit, onarım ve tedbir unsurlarını belirlemek,

f) Ulusal bilgi güvenliği ile ilgili uluslararası mevzuat ve teknolojideki gelişmeleri takip etmek,

g) Güvenlik hassasiyeti gösteren personel, yazı lım, donanım, kripto, iletişim ortamlarını ve iletişim ağlarını her türlü tehdit kaynağına karşı maliyet etkin tedbirlerle koruma altına alınmasını sağlamak, bu tedbirleri uygulamaya sokmak ve kontrol etmek,

h) Ulusal bilgi güvenliğine ilişkin güvenlik kategorilerini ve sistemin minimum güvenlik ihtiyaçlarını belirlemek, uygulamasını sağlamak,

i) Tüm gizlilik dereceli ve tasnif dışı hassas bilgiye işlem yapacak birimler ve şebekeler için onay vermek,

i) Ulusal güvenliği ilgilendiren bilgiye işlem yapacak donanım ve yazılım ihtiyaçlarına ait güvenlik değerlendirmesini yapmak ve değerlendirilmiş ürün listelerini hazırlamak ve yayımlamak,

j) Haberleşme güvenliği sistemlerinin tehdit analizi ve hassasiyet değerlendirmelerini yapmak,

k) Hassas ve gizlilik dereceli bilgiyi korumak üzere, anahtarlama materyali üretim esaslarını belirlemek,

l) TEMPEST standartlarını hazırlamak ve onay işlemlerini gerçekleştirmek,

m) Kripto sistemlerinde kullanılacak materyal ve anahtarları üretecek teçhizatı onaylamak, kripto anahtarlarının dağıtılmasına ilişkin standartları ve yöntemleri belirlemek ve denetlemek,

n) Ulusal bilgi güvenliği gerekleri, ihtiyaçlar, ticaret ve gizlilik arasında uygun bir denge kurarak kriptolojik malzemelerin ihracat ve ithalatıyla ilgili Genelkurmay Başkanlığı ve Dışişleri Bakanlığı'nın uygun görüşleri alınarak gerekli lisansları vermek,

o) Ulusal bilgi güvenliği ile ilgili mevzuat değişikliklerine ilişkin teklifleri Üst Kurula sunmak,

ö) Bilgi çağının gerektirdiği çağdaş güvenlik tedbirlerini belirleyerek Üst Kurula teklif etmek,

p) Üst Kurulun almış olduğu karar ve direktifleri uygulamak,

r) Ulusal bilgi güvenliği amacıyla, Genelkurmay Başkanlığı ve Dışişleri Bakanlığı ile koordineli olarak diğer ülkelerle ve uluslararası kuruluşlarla işbirliği yapm ak, Sistemlerin, nihai sistem güvenlik kriterlerini belirlemek ve onay işlemlerini yapmak

s) Ulusal bilgi güvenliği konusunda eğitim standartlarını belirlemek, plan ve programları yapmak,

t) Ulusal bilgi güvenliği konusunda araştırma ve geliştirme faaliye tlerini sağlamak,

u) Kamu ve özel kurum ve kuruluşlar için gizlilik dereceli bilgi veya kripto cihazlarına ilişkin her türlü yetki belgesi (klerans) düzenlemek ve onay yöntem ve usullerini belirlemek, uygulanmasını sağlamak,

ü) Ulusal bilgi güvenliği konus unda üretim yapan kamu ve özel kurum ve kuruluşlarını bir program çerçevesinde denetlemek ve üretilen ürünleri onaylamak.

Uluslararası İlişkiler ve Hukuk Müşavirliği

Madde 9- Uluslararası İlişkiler ve Hukuk Müşavirliği, Kurum Başkanına doğrudan bağlı olup görevleri aşağıda belirtilmiştir:

a) Uluslararası Bilgi Güvenliği politikasının oluşturulmasında uluslararası ilişkileri ve gelişmeleri takip etmek, değerlendirmek, koordine etmek ve önerilerde bulunmak, gerekli kanun tasarısı taslaklarını hazırlamak,

b) Ulusal bilgi güvenliği konusunda Kurum tarafından hazırlanan veya Başbakanlık, Bakanlıklar ve kuruluşlardan gönderilen kanun, tüzük ve yönetmelik taslaklarını hukuki açıdan inceleyerek, görüş bildirmek,

c) Ulusal Bilgi Güvenliğine ilişkin konularda altya pı temini modelinin oluşturulması ve altyapının güvenirliğinin sağlanarak kullanıma hazır tutulması için gerekli yasal düzenlemeleri ve sözleşmeleri hazırlamak,

d) Bireysel mahremiyeti koruma ve birey için gerekli kamu bilgisine erişimi sağlayıcı yasal düzenlemeleri belirlemek,

e) Uluslararası Bilişim güvenliğine ilişkin suçların mevzuatımızda yer alması için gerekli kanun tasarısı taslaklarını hazırlamak,

f) 4353 sayılı kanun hükümlerine göre adli ve idari davalara ilişkin gerekli bilgileri hazırlamak, Maliye Bakanlığı Başhukuk Müşavirliği ve Muhakemat Genel Müdürlüğünü ilgilendirmeyen idari davalarda kurumu temsill etmek,

g) Uluslararası Bilgi Güvenliği tehdide uğradığı hallerde ekonomik kısıtlama, diplomatik yanıt gibi tedbirlerin kullanımını Dışişleri Bakanlığı ve ilgili Bakanlıklarla koordine etmek ve önerilerde bulunmak,

h) Kurum tarafından verilen diğer görevleri yapmaktır.

Ulusal Bilgi Güvenliği Merkezi

Madde 10- Ulusal Bilgi güvenliği merkezinin görevleri aşağıda belirtilmistir :

a) Güvenli bilgi sistemlerinin geniş bir şekilde, kullanımını teşvik etmek,

b) Endüstri ve Kamu tarafından geliştirilmiş sistemlerin, teknik koruma yeteneklerini değerlendirmek,

c) Bilgi güvenliği konusunda faaliyet gösteren, kamu ve endüstri Gruplarının teknik desteğini sağlamak,

d) Bilgi sistemlerinin değerlendirilmesi için, gerekli teknik kriterleri geliştirmek,

e) Ticari Sistemleri değerlendirmek,

f) Bilgisayar ve Ağ Güvenlik teknoloji araştırmalarını icra ve yönlendirmek,

g) Güvenli Bilgi Sistemlerini geliştirme ve test etmede kullanmak için, gerekli modifikasyon ve analiz teçhizatını geliştirmek ve bilişim emniyetini sağlamak,

h) Bilgi güvenliği sahasında eğitim vermek,

i) Kamu ve Endüstrinin diğer bölümlerine bilgi güvenlik bilgisini dağıtmak,

j)Tehdidin türüne göre geliştirilen karşı tedbirleri gerektiğinde uygulamaya koymak,

Genel Sekreterlik

Madde 11- Genel Sekreterliğin Görevleri Aşağıda Belirtilmiştir

a) Kurum Başkanının resmi ve özel yazışmalarını yürütmek,

b) Kurumun idari, bakım-onarım ve idame hizmetlerine ilişkin görevlerini yürütmek,

c) Kurumun maliye ve satın alma hizmetlerini sağlamak,

d) Kurumun güvenlikle ilgili hizmetlerini yürütmek,

e) Üst Kurulun sekreteryasını yapmak,

ÜÇÜNCÜ BÖLÜM

ANA HİZMET BİRİMLERİ VE GÖREVLERİ

Plan, Program ve Koordinasyon D airesi Başkanlığı

Madde 12- Plan, Program ve Koordinasyon Dairesi Başkanlığının Görevleri aşağıda belirtilmiştir:

a) Telekomünikasyon ve Bilgi sistemleri ortamındaki değişimlere uyum sağlayacak Ulusal bilgi güvenliği politikasının oluşturulması için gerek li verileri hazırlamak, prensipleri belirlemek,

b) Ulusal Bilgi güvenliği ile ilgili olarak görev alanına ilişkin planlama ve programlama faaliyetlerinde bulunmak, gerekli mevzuatı düzenlemek,

c) Ulusal Bilgi güvenliği altyapı esaslarını ortaya koymak yapı lmış olan risk analizleri neticelerine göre altyapıyı iyileştirici tedbirleri belirlemek

d) Uyuşum standartları ve kriterlerini ortaya koymak,

e) Ulusal Bilgi güvenliği konusunda bilgilendirme ve eğitim faaliyetlerini planlamak,

f) Kamu ve özel sektöre Ulu sal bilgi güvenliğine ilişkin danışmanlık ve teknik yardım sağlamak,

g) Kurumun personel faaliyetlerini yürütmek ve koordine etmek,

h) Ulusal Bilgi Güvenliği Başkanlığının bütçe düzenleme faaliyetlerini yürütmektir.

Bilgi Güvenlik Dairesi Başkanlığı

Madde 13- Bilgi Güvenlik Dairesi Başkanlığının Görevleri aşağıda belirtilmiştir :

a) Ulusal bilgi Güvenliği ihlallerine karşı alınacak tedbirleri belirlemek, ihlallere karşı gerekli tedbirleri almak ve ilgili makamlarla koordineli olarak uygulanmasını sağlamak,

b) Ulusal Bilgi güvenliği açısından Personel güvenliğine, fiziki güvenliğe ve donanım ve yazılım güvenliğine ilişkin usul, kriter ve prensipleri belirleyerek dökümantasyonunu hazirlamak,

c) Kurumun, ulusal bilgi ağı TEMPEST, haberleşme güvenliği ve teknik güvenliğine ilişkin usul, kriter ve prensiplerini belirleyerek dökümantasyonunu hazırlamak,

d) Elektronik kripto dışında ihtiyaç duyulacak kod ve parola sistemlerini belirlemek, geliştirmek ve üretmek,

e) İletişim ortamları, donanım ve ağlar için tehdidi ve zafiyeti dikkate alarak risk analizleri yapmak, ve risk yönetim usullerini belirlemek, risk analizleri sonucunda belirlenmiş koruyucu tedbirleri uygulamaya koymak,

f) Yazılım Güvenlik, kriter ve standartlarını belirlemek,

g) Ulusal ve uluslararası iletişim ağlarına ilişkin olarak ulusal bilgi güvenliği açısından güvenlik, usul, kriter ve prensipleri belirlemek, dökümantasyonunu sağlamak,

h) Güvenlik denetimlerine ilgi alanı itibariyle katılmak, alt kurulara sekreterya hizmeti vermek ve görev alanına ilişkin mevzuat değişikliklerine ilişkin teklifleri hazırlamaktır.

Kriptoloji Dairesi Başkanlığı

Madde 14- Kriptoloji Dairesi Başkanlığının görevleri aşağıda belirtilmistir :

a) Kriptografik algoritma, ihtiyaçlarini belirlemek, üretiminin denetimini yapmak ve kütüphanesini oluşturmak,

b) Kripto cihaz ve kriptografik bilginin ihracat ve ithalatında Genel Kurmay Başkanlığı, Dışişleri Bakanlığı ve gerektiğinde ilgili diğer bakanlıklarla koordineli olarak esas ve usulleri belirlemek, lisans belgesi vermek,

c) Risk analizleri ve risk azaltma planları yapmak , kabul edilebilir riski tespit etmek,

d) Kripto merkezlerinin sağlaması gereken kriterlerini ve denetleme usul ve esaslarını belirlemek, denetleme raporlarını değerlendirerek onay vermek, kripto anahtar üretimi ve dağıtımını yapmak, gerektiğinde kurum ve kuruluşlara kendi kripto anahtar üretimi ve dağıtımı konusunda yetki vermek,

e) Gizlilik derecesiz uygulamalarda da kripto kullanım esaslarını belirlemek, uygulamaları teşvik etmek ve denetlemek,

f) Kripto cihaz ve dökümantasyonu için, kripto saymanlık, işletme, bakım ve onarım usullerini belirlemek,

g) Kripto ihlallerine karşı alınacak tedbirleri belirlemek ve gerekli tedbirleri almak,

h) Her tür kriptografik yöntem ve teçhizata ilişkin sertifikasyon ve onay usul lerini belirlemek,

I) Kripto hizmetlerinde çalıştırılacak personele kripto yetki belgesi verilmesi esas ve usullerini belirlemektir.

Bilgi destek dairesi başkanlığı

Madde 15- Bilgi Destek Dairesi Başkanlığının görevleri asağıda belirtilmiştir;

a) Ulusal bilgi güvenliği altyapısına karşı iç ve dış tehdidi teşhis etmek, tanımlamak, genel tehdit değerlendirilmesi yapmak ve Üst Kurula sunmak,

b) Ulusal bilgi güvenliğine karşı tehdidin teknik özelliklerini ve muhtemel etkilerini belirlemek, karşı tedbirleri geli ştirmek,

c) İstihbarat üreten kurum ve kuruluşlar ile bilgi güvenliğine ilişkin istihbarat bilgisi değişimi için protokoller yapmak,

d) Mevcut ve tasarlanan iletişim ortamları, donanım ve ağlar için tehdidi ve zafiyeti dikkate alarak risk analizleri yapmak tır.

Denetleme ve değerlendirme dairesi başkanlığı

Madde 16- Denetleme ve Değerlendirme Dairesi Başkanlığının görevleri aşağıda belirtilmiştir;

a) Ulusal bilgi güvenliği açısından kripto, bilgi güvenlik ve TEMPEST denetleme kriter ve usullerini belirlemek ve geliştirmek,

b) Kripto denetleme programlarını hazırlamak, kripto merkezlerinin kriterlere uygunluğunun denetlemesini sağlamak, gerektiğinde denetlemek ve denetleme raporlarını değerlendirmek,

c) Ulusal bilgi güvenliği sistemlerine karşı yapılan saldır ıları ve güvenlik ihlallerini değerlendirmek,

d) Eğitim, öğretim ve biçimlendirme ihtiyaçlarını tespit etmek,

e) Genel değerlendirme raporu hazırlayarak Üst Kurula sunmak,

f) İletişim ortamları, şebeke, yazılımlara ait güvenlik sistemleri ile ilgili denet leme usul ve kriterlerini belirlemek, geliştirmek, denetleme yapılmasını sağlamak, gerektiğinde denetlemek ve denetleme raporlarını değerlendirmek,

g) TEMPEST standartlarını hazırlamak ve onay işlemlerini gerçekleştirmek,

h) Ulusal bilgi güvenlik alt yapısına ait sistemlerin nihai sistem güvenlik kriterlerini belirlemek ve onay işlemlerini yapmak.

DÖRDÜNCÜ BÖLÜM

Çesitli Hükümler

Gizlilik dereceleri

Madde 17- Bilgi güvenliğinin sağlanmasından kullanılacak gizlilik dereceleri ile hangi makam tarafından ne şekilde verileceği hususları Kurum tarafından çıkartılacak yönetmelikte düzenlenir.

Kamu ve özel kurum ve kuruluşlarının yükümlülüğü

Madde 18- Tüm kamu ve özel kurum ve kuruluşları, ulusal güvenliği ilgilendiren bilginin korunması için kendi i dari yapıları içerisinde gereken organizasyonu kurmak veya değişiklikleri yapmak ve gerekli tedbirleri almak konusunda sorumludurlar.

Ulusal bilgi güvenliği, tüm kamu ve özel kurum ve kuruluşlarda bir bütün olarak değerlendirilir ve gerekli koordinasyon Ku rum tarafından sağlanır. Bu amaca yönelik tüm kaynaklar yerinde, zamanında ve en etkin bir şekilde kullanılır.

Kamu ve özel kurum ve kuruluşları, Kurum tarafından bu Kanunun uygulanmasına ilişkin olarak yayımlanan esas ve usullere uymak zorundadır.

Kurum, gerekli gördüğü ulusal bilgi güvenliğinin sağlamaya iliskin bilgileri, bu Kanun kapsamına giren kamu ve özel kurum ve kuruluşlardan doğrudan istemeye yetkilidir. Bu konuda istenen gizlilik dereceli her türlü bilgi, makam onayı ile en kısa zamanda verilir.

Özel kanunlardaki hükümler saklıdır.

Kişi ve kurumların hizmetlerinden yararlanma

Madde-19- Genel ve katma bütçeli idareler, kamu iktisadi teşebbüsleri ile bunlara bağlı kuruluşlar ve müesseselerde çalışanlar, Kurumda sözlesmeli olarak istihdam edilebilirler. Bu personel kurumundan aylıksız izinli sayılır. İzinli oldukları sürece memuriyetleri ile ilgili özlük hakları devam ettiği gibi bu süreler terfi ve emekliliklerinde hesaba katılır. Kurumda çalıştıkları sürece bunların sicilleri Kurum tarafından verilir ve bu sicillere göre kendi kurum ve kuruluşlarınca terfileri yapılır. Bu personelin, çalışma usul, esas, ücret ve sayılarına ilişkin hususlar, Bakanlar Kurulu Kararıyla tespit edilir. Ancak bu personelin aylıkları, hiç bir halde kendi kurum ve kuruluşlarında aldıkları aylıklardan az olamaz.

Birinci fıkrada belirtilen kurum ve kuruluşlarda görevli personel, gerektiği hallerde aylık, ek gösterge, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kendi kurumlarınca ödenmek tab i oldukları kanun hükümleri çerçevesinde geçici olarak Kurumda görevlendirilebilirler.

Kadrolar ve personel

Madde 20- Kadroların tespit, ihdas, kullanım ve iptali ile kadrolara ait diğer hususlar, 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kar arname hükümlerine göre düzenlenir.

Kurumda başkan, başkan yardımcıları, hukuk müşavirleri, daire başkanları, şube müdürleri, mühendisler ve yüksek öğrenim görmüş olanlar, kadro karşılık gösterilmek kaydıyla 657 sayılı Devlet Memurları Kanunu ve diğer kanu nların sözleşmeli personel hakkındaki hükümlerine bağlı olmaksızın sözleşmeli olarak çalıştırılabilir. Kurumda başkan, başkan yardımcıları ve daire başkanları olarak atanacak personelde bu sahada en az lisans düzeyinde eğitim yapmaları ve kamu kurum ve kuruluşlarında Kurumun ilgi alanını oluşturan görevlerde en az 10 yıl görev yapmış olmaları şartı aranır.

Bu şekilde çalıştırılacak sözleşmeli personelin sayısı, sözleşme usul ve esasları Başbakanlıkça tespit edilir. Sözleşme ile çalıştırılacak personel, iste kleri üzerine Türkiye Cumhuriyeti Emekli Sandığı ile ilgilendirilir.

Atama

Madde 21- Kurum Başkanı, başkan yardımcıları, birinci hukuk müşaviri ve daire başkanları sözleşmeli olarak çalıştırılmadıkları takdirde, haklarında 657 sayılı Devlet Memurları Kanununun istisnai memuriyete ilişkin hükümleri uygulanır. Bunlardan Başkan, Başbakan'ın onayı ile diğer personel ise, Başkanın onayı ile atanır.

Sözleşme ile araştırma, etüd, proje ve program yaptırma

Madde 22- Kurumun hizmetlerine ilişkin araştırma, etüd, pr oje ve program işleri, üniversiteler ile gerçek ve tüzel kişilere sözleşme ile yaptırılabilir.

Kurumun gelirleri

Madde 23 - Kurumun gelirleri aşağıda belirtilmistir;

a) Genel bütçeden yapılacak hazine yardımı

b) Döner sermaye gelirleri

Döner Sermaye İşletmesi

Madde 24- Kurumda, bu Kanunda öngörülen faaliyet temel ve sürekli görevlere bağlı olarak ortaya çıkan üretim ve hizmet fazlasının değerlendirilmesi amacıyla döner sermaye işletmesi kurulabilir.

Döner sermaye işletmesinin sermaye limiti 2.5 trilyon Türk Lirasıdır. Tahsis edilen sermaye miktarı, Maliye Bakanlığının uygun görüşü üzerine Bakanlar Kurulunca on katına kadar artırılabilir. Bu suretle artırılan sermaye, elde edilen gelirle karşılanır.

Döner sermaye, Başbakanlık bütçesine konulan ödenekle, Hazin ece verilecek ayni yardımlar, döner sermaye gelirinden elde edilecek karlar, bağış ve yardımlardan oluşur.

Ödenmiş sermaye tutarı, tahsis edilen sermaye tutarına ulaştıktan sonra elde edilen karlar, hesap dönemini izleyen yılın Şubat ayı sonuna kadar Hazin eye gelir kaydedilmek üzere Kurum saymanlığına yatırılır.

Döner sermaye faaliyetlerinin gerektirdiği giderler ile Bütçedeki ödenekten karşılanamayan kiralama, satın alma, araç, gereç, araştırma ve benzeri diğer ihtiyaçlar döner sermayeden karşılanır.

Döner sermaye işletmesinin faaliyet alanları, gelir kaynakları, mali ve idari işlemlerine ilişkin usul ve esaslar Maliye Bakanlığı ile Sayıştay'ın görüşleri alınarak hazırlanacak yönetmelikle düzenlenir.

Döner sermaye işleri 1050 ve 832 sayılı Kanunların vizeye ilişkin hükümlerine tabi değildir. Ancak gelir ve giderler için bütçe yılı sonundan itibaren 3 ay içinde düzenlenecek yıllık bilançolar ve ekleri gelir ve gider belgeleri ile birlikte Sayıştay Başkanlığına, tasdikli birer sureti de Maliye Bakanlığına gönd erilir.

Ceza Hükmü

Madde 25- Kamu ve özel Kurum kuruluşların yöneticisi durumunda olan personelden, bu kanunun 18.maddesinde belirtilen yükümlülükleri yerine getirmeyenler, bu fiilleri başka bir suça vücut verse bile ayrıca bir yıldan beş yıla kadar hapis cezası ile cezalandırılırlar. Failin bu fiilden kendisi veya bir başkası yararına bir menfaat temin etmesi veya fiilin bir zarara sebebiyet vermesi halinde hapis cezasi iki yıldan az olamaz.

Geçici Madde- 1- Üst Kurul ile Kurumun çalışma usul ve esasları dairelerin alt birimlerinin kuruluş ve görevlerine ilişkin usul ve esaslar, Döner sermaye işletmesine ilişkin usul ve esaslar ile Kanunun uygulanmasında ihtiyaç duyulacak usul ve esaslar,

Kanunun yürürlüğe girdiği tarihten itibaren bir yil içinde Kurum tar afından hazırlanacak ve Bakanlar Kurulu kararıyla yürürlüğe konulacak yönetmeliklerde gösterilecektir.

Geçici madde 2- Ekli (1) sayılı listede belirtilen kadrolar ihtas edilerek 190 sayılı Kanun hükmünde Karanamenin (1) sayılı cetveline " Ulusal Bilgi Güve nliği Üstkurulu ile Ulusal Bilgi güvenliği Kurumu Başkanlığı" bölümü olarak eklenmiştir.

Geçici Madde 3- Bu Kanunun kabulu ile asgari ihtiyaçları karşılayacak çekirdek kadro ile faaliyete geçirilecek kendi ihtiyaçları doğrultusunda azami üç yıl içinde nihai teşkilatını kuracaktır.

Yürürlük

Madde 26- Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 27- Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

EK-A DEVAMI

EK (1) SAYILI CETVEL

ULUSAL BİLGİ GÜVENLİĞİ KURUMU BAŞKANLIĞI TEŞKİLATI

i)BAŞKANLIK

Başkan

ii)DANIŞMA BİRİMLERİ luslararası İlişkiler ve Hukuk Müşavirliği

iii) ANA HİZMET BİRİMLERİ

1.Plan Program ve Koord. D.Bşk.lığı

2.Bilgi Güvenlik D.Bşk.lığı

3.Kriptoloji D.Bşk.lığı

4.Bilgi Destek D.Bşk.lığı

5.Denetleme ve Değerlendirme D.Bşk.lığı

iv) YARDIMCI BİRİMLER

1.Ulusal Bilgisayar Güvenlik Merkezi Müdürlüğü

2.Genel Sekreterlik

GENEL GEREKÇE

Günümüzde bilgi; tarih boyunca olduğundan süratle iletilmekte, buna bağlı olarak da üretilen bilginin saklanması, kullanılması, bir yerden diğer bir yere nakledilmesi ve imhası için klasik usullerin dışında, gelişen teknolojiden sonuna kadar yararlanma gereği ortaya çıkmıştır. Teknolojiye ve bilgiye olan bu bağımlılık, ülkeleri, bilginin korunması için yeni usuller geliştirmeye ve yasal düzenlemeler yapmaya mecbur bırakmıştır.

Bilgi teknolojisine giderek artan bağımlılığın sonucu olarak, merkezi kontrol, devlet yönetimi, ekonomik ve toplumsal hayatın her yönünün ortak bileşeni bilgi altyapısının kötü niyetli kişilere, terörist faaliyetlere ve doğal afetlere karşı korunması önem kazanmıştır. Kamu ve özel kurum ve kuruluşların kendi yapılarına uygun farklı bir güvenlik önlemleri almaları ve bu konuda ulusal bir politikanın olmayışı, Ülkemizin ulusal güvenliğini hassas hale getirmektedir. Bilgi güvenliği konusundaki ulusal politika ile; motivasyonları ve görev alanları farklı olan kamu ve özel sektörün, gerek kendi işlerinde, gerekse karşılıklı ilişkilerinde her türlü tehdit ve hassasiyete karşı bilgi güvenliğini tam olarak sağlayacak ilke ve önceliklerin tespiti gerekmektedir.

Ulusal bilgi güvenliğine yönelik tehdidin ulusal bilgi altyapımızı etkilemek, zarar vermek ve taarruz etmek için birçok farklı seçeneği vardir. Altyapıya karşı saldırılar teknik yeteneklerden, motivasyona kadar birçok değişiklik arz ederek, veri tabanını karıştirması veya programların uygulamalarını bozma yada fiziksel olarak yok edecek biçimde çatışma seviyesine (baris, kriz ve savas) uygun olarak yapılır. Nispi barış periyodu sırasında dahi tehdidin, değişik seviyelerde devamlı olarak mevc ut olduğunu unutmamak gerekir. Tehdidin kaynakları bireylerden (muhbir ve yetkisiz kullanıcılar) karmaşık ulusal organizasyonlara (yabancı istihbarat servisleri ve askeri istihbarat unsurları) kadar geniş bir yelpaze olarak ortaya çıkmaktadır. Bu gruplar arasındaki sınırlar belirsiz olduğundan, genellikle olayın kaynağını tespit etmek oldukça zordur.

Türkiye Cumhuriyeti Devleti‘nin ulusal ve ekonomik güvenliğini etkileyen ulusal bilgi altyapısının bugünkü haliyle güvenirlik ve hizmete hazır olma kriterleri açısından ihtiyaçları tam olarak karşılamadığı değerlendirilmektedir. Altyapının tehdite ve hassasiyetlere karşı yetersiz oluşu, altyapıda muhtemel kesintilere ve olabilecek kötü niyetli saldırılara karşı hassasiyeti arttırmaktadır. Bu nedenle, bu tür tehditleri ortaya çıkarmak ve gerekli önlemleri almak üzere merkezi bir yönetim birimine ihtiyaç duyulmaktadır.

Bu çerçevede, Devletin kamu ve özel tüm kurum ve kuruluşlarının endüstriyel, politik, ekonomik ve sosyal alanlarda kaçınılmaz olarak etkileşim için de olduğu hususu dikkate alınarak, ortak olarak kullandıkları altyapının, Devletin ulusal ve ekonomik çıkarları için güvence altına alınması amaçlanmıştır. Öngörülen ana esaslar çerçevesinde sorunun; ulusal güvenlik politikasından sorumlu üst organın direktiflerine uygun olarak, gecikmeksizin çözümlenmesi için merkezi bir ulusal bilgi güvenliği yönetim yapısının oluşturulması ihtiyacı ortaya çıkmıştır. Bu bağlamda, Hükümet seviyesinde ulusal güvenlik ihtiyaçları doğrultusunda genel prensipleri vazeden bir üst organ; direktifleri ve yasalarda verilen görevleri uygulayacak ve ulusal bilgi güvenlik sistemini işletecek bir yönetim birimi teşkili yoluna gidilmektedir. Taslak ile; ulusal güvenliği ilgilendiren bilgilerin korunması ve devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli stratejilerin (politikaların) üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartların saptanması, ihracat ve ithalat izinlerinin ve sertifikaların verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi, kamu ve özel kurum ve kuruluşları arasında koordinasyonun sağlanması amaçlarını gerçekleştirmek üzere oluşturulan teşkilatın görevlerine ilişkin esas ve usuller ile bunlara ilave olarak, bu yasal düzenleme ile kamu ve özel bütün kurum ve kuruluşlarda, bilgi güvenliğini sağlayacak gerekli yapılanmaya geçilmesi hususu düzenlenmektedir.

MADDE GEREKÇELERİ

Madde 1- Madde ile, Kanunun düzenlenme amacı belirtilmektedir.

Madde 2 - Madde ile, Kanunun kapsamı belirtilmektedir.

Madde 3 - Madde ile, Kanunda yer verilen deyimlerden ulusal bilgi güvenliği, haberleşme güvenliği, fiziki güvenlik, personel güvenliği, teknik güvenlik, TEMPEST, güvenlik ihlali, kripto, kriptoloji, kripto sistemleri, algoritma, ulusal bilgi ağı, üst kurul, kurum terimleri açiklanmaktadir.

Madde 4 - Madde ile Ulusal Bilgi Güvenliği Üst Kurulu ile Başbakanlığa bağlı olarak Ulusal Bilgi Güvenliği Kurumu Başkanlığının kuruluşu düzenlenmektedir.

Madde 5 - Madde ile, Ulusal Bilgi Güvenliği Üst Kurulunun asil üyelerinin kimlerden oluştuğu, Üst Kurula başkanlık usulü, diğer kamu ve özel kurum ve kuruluşların temsilcilerinin katılım durumu, oy verme ve karar yeter sayısı, olağan toplantılı tarihleri, gündem, olağanüstü toplantıya çağrı usulü, sekreterya hizmetleri düzenlenmekte ve üst Kurulun çalışma usul ve esaslarının daha sonra çıkarılacak Yönetmelikle düzenleneceği belirtilmektedir.

Madde 6- Madde ile, Ulusal Bilgi Güvenliği Kurumu Başkanlığının alt birimlerini oluşturan daire başkanlıkları ile uluslar arası ilişkiler ve hukuk müşavirliği, ulusal bilgisayar güvenlik merkezi ve genel sekreterliğin kuruluşu düzenlenmekte ve dairelerin alt birimlerinin kuruluş şekillerinin ve görevlerinin çıkarılacak Yönetmelikle düzenleneceği belirtilmektedir.

Madde 7-Madde ile, Ulusal Bilgi Güvenliği Üst Kurulunun görevleri düzenlenmekte.

Madde 8- Madde ile, Ulusal Bilgi Güvenliği Üst Kurumu Başkanlığının görevleri düzenlenmektedir.

Madde 9 - Madde ile, Uluslararası İlişkiler ve Hukuk Müşavirliğinin görevleri düzenlenmektedir.

Madde 10 -Madde ile, Ulusal Bilgisayar Güvenliği Merkezinin görevleri düzenlenmektedir.

Madde 11 -Madde ile, Genel Sekreterliğin görevleri düzenlenmektedir.

Madde 12- Madde ile, Plan Program ve Koordinasyon Başkanlığının görevleri düzenlenmektedir.

Madde 13-Madde ile, Bilgi Güvenliği Dairesi Başkanlığının görevleri düzenlenmektedir.

Madde 14- Madde ile, Kriptoloji Dairesi Başkanlığının görevleri düzenlenmektedir.

Madde 15- Madde ile Bilgi Destek Dairesi Başkanlığının görevleri düzenlenmektedir.

Madde 16- Madde ile, Denetleme ve Değerlendirme Dairesi Başkanlığının görevleri düzenlenmektedir.

Madde 17- Madde ile, bilgi güvenliğinde kullanılacak gizlilik dereceleri ile hangi makam tarafından ne şekilde verebileceğinin Kurum tarafından çıkarılacak bir Yönetmelikle düzenleneceği belirtilmektedir.

Madde 18- Madde ile, ulusal bilgi güvenliği, tüm kamu ve özel kurum ve kuruluşlarda bir bütün olarak değerlendirildiğinden, her kurum ve kuruluşun kendi bünyesinde gereken organizasyonu oluşturması ve ulusal bilgi güvenliği konusunda belirtilen önlemleri alınması için yükümlülük düzenlenmektedir. Belirtilen hükümlülüklerin yerine getirilmesinde özel kanunlara tabi kurum ve kuruluşlara ilişkin hükümler saklı tutulmaktadır.

Madde 19- Madde ile, oluşturulan teşkilatın görevlerinin yerine getirilmesinde, diğer kurum ve kuruluşlarının ihtiyaç duyulan hizmetlerinden ve personelinden yararlanma esasları ile söz konusu personelin mali ve sosyal hakları saklidir.

Madde 20- Madde ile, oluşturulan teşkilatın kadroları ve bu kadrolarda görevlendirilecek personelin yasal dayanağı, sözleşmeli olarak çalıştırılacak

personel, Emekli Sandığı ile ilgilendirilme ve özel uzmanlık gerektiren işlerde uzman personel çalıştırabilmesi hususları düzenlenmektedir.

Madde 21- Kurum Başkanı, daire başkanları ve birinci başhukuk müşavirleri hakkında istisnai memurluk statüsünün uygulanması ve personelin atama onay usulü düzenlenmektedir.

Madde 22- Madde ile, oluşturulan teşkilatın yaptıracağı araştırma, etüt, program ve proje işlerinin sözleşmeyle yaptırabilmesi hususu ve ihaleyle ilgili esaslar düzenlenmektedir.

Madde 23- Madde ile, Ulusal Bilgi Güvenliği Kurumu Başkanlığının gelirleri düzenlenmektedir.

Madde 24- Ulusal Bilgi Güvenliği Kurumu Başkanlığının faaliyet alanına giren konularda gerçek ve tüzel kişilere verilecek hizmetlerin yerine getirilmesine araştırma-geliştirme faaliyetleri için gerekli olan kaynağın elde edilmesine yönelik olarak bir döner sermaye işletmesi kurulması ve bunun işletilmesi esasları düzenlenmektedir.

Madde 25- Ceza hükmü düzenlenmektedir ve kanunda belirtilen yükümlülükleri yerine getirmeyenler hakkında caydırıcı nitelikte hükümler düzenlenmektedir.

Madde 26- Yürürlük maddesidir.

Madde 27- Yürütme maddesidir

(Kaynak: http://www.tbd.org.tr)

EK:2 TÜRK BİLİM ve TEKNOLOJİ POLİTİKASI: 1993-2003Türkiyenin Bilişim Politikaları Sorunlar, Hedefler ve Çözüm Önerileri

l. GİRİŞ

Gelecekte uluslararası pazarda rekabet gücünü belirleyecek en önemli unsurlardan birisi de bilişim sektörü olacaktır.

Ülkemizde bilişim sektörü son yıllarda önemli gelişmeler kaydetmiş ve gösterdiği büyüme oranı yüzde otuzlara ulaşmıştır. Bununla birlikte, ülkemizde kişi başına bilgi işlem tüketimi (donanım, yazılım ve hizmet) 10 $ düzeyinde iken bu rakam Frans a ve Almanya'da 600 $ düzeyini bulmaktadır.

Değişen dünya koşulları altında, giderek artan yoğunlukta ekonomik ve politik sorumluluklar üstlenen Türkiye'nin bu sorumluluklarının üstesinden gelebilmesinin bir önkoşulu da, çağdaş bilim ve teknolojiyi bilip k ullanmanın ötesinde, bunları üretip geliştirebilmesi, başka ülkelere satabilmesidir.

Sanayi ötesi toplum, ya da bilgi toplumu diye adlandırılan yarın'ın gelişmiş toplumları için, tarım ve sanayide ileri konumda bulunmak yeterli olmayacak, kısaca bilişim diye adlandırılan iletişim, bilgisayar ve bilginin birleşmesinden doğan ve her tür bilginin işlendiği, dağıtıldığı ve kullanıma sunulduğu bir yapıyı da kurabilmiş olmaları gerekecektir.

Bilişim sektörünün önemi ve ülke içindeki gelişme potansiyeli, konuyu Tü rkiye'de güncel hale getirmiş ve konu iki ayrı platformda derinlemesine tartışılmıştır. Bu platformlardan biri 1992 yılında gerçekleştirilen 3. İzmir İktisat Kongresi'dir. Diğeri ise, Dünya Bankası raporunun, 1991 ve 1992 yılları içindeki hazırlık aşamasın da oluşturulmuş olan tartışma platformudur.

Dünya Bankası (DB) tarafından hazırlanan 17 Temmuz 1992 tarih ve 10759 -TU numaralı "Bilişim Tabanlı Ekonomiye Doğru Türkiye" isimli rapor Türkiye'nin bilişim alanındaki durumunu ve sorunlarını iyi değerlendiren k apsamlı bir çalışmadır. Raporun adından da anlaşılacağı üzere "eylem planının" ana hedefi bilişim teknolojilerinin yaygın olarak kullanıldığı toplumsal bir ortam yaratmaktır. Bu nedenle de raporda bilişim teknolojilerinin kullanılmasına bu teknolojilerin geliştirilmesinden daha fazla önem verilmiştir. Raporun hedefleri göz önüne alındığında bu normal sayılabilirse de bu teknolojileri ülkemizde geliştirebilmenin hayati önemini de hatırlatmakta yarar vardır.

2. SORUNLAR, HEDEFLER VE ÇÖZÜM ÖNERİLER İ

Türkiye'nin bilişimden gerekli faydayı sağlayabilmesi için aşağıdaki konularda çalışma yapılması gerekmektedir:

İnsan gücü yetiştirilmesi,

Yasal düzenlemelerin yapılması,

Kamu sektörünün öncülüğünde bilişim teknolojilerinin yaygınlaştırılması,

Bilişim teknolojileri A+G projelerinin desteklenmesi ve hedeflerinin belirlenmesi.

2.1. İnsan Gücü Yetiştirilmesi

Bilgisayar alanında teknoloji üretmek ve uygulamalar geliştirmek için önemli ön şartlardan bir tanesi bu alanda eğitilmiş kalifiye elemanlar ın bulunmasıdır. Ülkemizde halen bilgisayar mühendisliği konusunda lisans eğitimi veren üniversitelerin bir sene içinde mezun ettikleri bilgisayar mühendisi sayısı bir kaç yüz ile sınırlıdır. Bu ülke nüfusuna oranla son derece az bir

rakamdır ve talebin çok altındadır. Önümüzdeki 5 yıl içinde 21000 yetişmiş insana gereksinim duyulacağı sanılmaktadır (DB3.45). Eğitilmiş insan gücü üretimini arttırmak için alınması gereken önlemler:

a) Öncelikle talebin bir çözümlemesi yapılıp hangi özelliklerde insanların yetiştirilmesi gerektiği saptanmalıdır. Bu konuda şöyle bir sınıflandırma yapabilir.

1. Bilgisayar bilimleri ve mühendisliği araştırmacıları (doktora veya yüksek lisans eğitimi almış)

2. Yazılım mühendisleri, uygulama geliştiriciler (yüksek lisans veya lisan s eğitimi almış)

3. Sistem çözümleyicileri/uzmanları (yüksek lisans veya lisans eğitimi almış)

4. Programcılar (lisans eğitimi, 2 senelik meslek yüksek okulu eğitimi almış)

5. Hazır (paket) program kullanıcıları (2 senelik meslek yüksek okulu eğitim, kurs eğitimi almış)

6. Sistem işletim personeli (lise eğitimi, kurs eğitimi almış)

7. Veri girişi, vb. personeli (lise eğitimi, kurs eğitimi almış)

b) Öncelikle ilk iki gruptaki personelden çok daha fazla sayıda yetiştirmeyi amaçlayan bir eğitim politikası benimsenmelidir. Böyle bir yaklaşım orta vadede ülkenin kendi pazar ihtiyaçları doğrultusunda problem çözücü ve yazılım sistemleri geliştirici adımların atılmasını kolaylaştıracaktır. Bu tip eğitimi veren özel Enstitülerin kurulması desteklenmeli ve halen kurulu bulunan bilgisayar mühendisliği bölümlerinin bilgisayar bilimlerinde araştırma ve geliştirme yapması özendirilmelidir.

c) Özellikle dört ve beşinci gruplardaki tipten personeli eğitecek kısa süreli (1 -2 sene) eğitim programlarına ağırlık verilmelidir. Bu özellikteki eğitimin amacı temel bir ön hazırlıktan sonra, piyasada kullanılan ve ihtiyaç duyulan programlama dillerini veya paket programları (örneğin DBase, AutoCAD, Word, vb.) kullanmasını bilen teknik eleman yetiştirmek olmalıdır.

d) Yukarıda açıklanan amaçlara ulaşmayı hedefleyen bir başka plan da Dünya Bankası tarafından önerilen "Özel Bilişim Enstitüsü"dür. Banka böyle bir çalışmayı destekleyebileceğini belirtmektedir.

e) Bilişim sektöründe kendini yetiştirmiş insanların belirlenip, belgelendirilmesi için bir kurum (TÜBİTAK, YÖK, Enstitü...) sınav düzenleyip belge vermelidir. Bu belgenin amacı mesleki bağnazlığa yol açıp, bu dalda çalışanların sayısını sınırlamak

değil, aksine insanları kendilerini yetiştirmeye teşvik edip sektöre üniversitelerin başka bölümlerinden insan gücü aktarılmasını sağlamak olmalıdır.

f) Ülkemiz açısından önemli eksikliklerinden biri de kuramsal araştırmalar yapan ve öğrencilerine yazılıma yönelik "formal" eğitim veren bölümlerin yokluğudur. ABD ve İngiltere'de oldukça yaygın olan bu bölümlerin öğrencileri program gereksinimlerinin nasıl yazılacağını, programların nasıl doğrulanacağını, hızlı bir şekilde program prototiplerinin nasıl geliştirileceğini iyi öğrenmektedirler. Yine bu bölümlerde program tasarımı ve algoritmaların analizi konularına önem verilmekte, öğrencilerin matematik bilgileri program geliştirme sürecinin her safhasında yararlı olacak tarzda motive edilmektedir.

Ülkemizde bilgisayar eğitimi alan tüm öğrenciler için geçerli bir genelleme büyük bir çoğunluğu ciddi (10 4î-5î mertebesinde satır ve yüksek seviyeli bir dilde yazılmış) bir program yazmadan veya varolan bir programın yaşam çevriminin bir evresiyle ilgili çalışmalar yapmadan (örneğin kullanıcı el kitabı yazmak, yazılım kütüphanesi yaratmak, programa önemli ve orijinal bir parça eklemek gibi) mezun olduğudur. Programlar bilgisayar biliminin doğal ve ayrılmaz parçalarıdır ama bu basit gerçek varolan eğitim sistemi içerisinde gözden kaçmaktadır. Bilgisayar biliminin temel dersleri olan "Programların Doğrulanması" ya da "Veri Yapıları" gibi derslerin verilmediği üniversitelerimizde bilgisayar bilimiyle ilgisi tartışmaya açık dersler okutulmaktadır.

Sonuç olarak bilgisayar bölümlerinde (ya da kurulması düşünülen Bilişim Enstitüsünde) endüstriyle işbirliği yaparak oluşturulacak kadrolara çok başarılı, aktif ve uluslararası tanınmış Türk ya da yabancı bilim adamlarının beş sene gibi uzunca sürelerle getirilerek güçlü bir altyapının oluşturulması gerekir. ABD'de bilgisayar bilimine damgalarını vurmuş birçok araştırmacı böyle pozisyonlara sahiptirler ve etraflarına toplanmış geniş kadrolara liderlik etmektedirler. Bu kadrolarla sürekli olarak yeni ve iz bırakan kavram ve fikirler oluşturulmaktadır.Sistem kaliteli araştırmaları neredeyse sonsuz özgürlük veren bir doğaya sahiptir.

2.2. Yasal Düzenlemelerin Yapılması

Türkiye'de yazılım sektörünün gelişmesi önündeki en büyük engel uygulanabilir bir fikri mülkiyet kanununun olmamasıdır. Bu boşluğun olumsuz bir yan etkisi de yabancı yazılım şirketlerinin ortak yazılım proj elerine girmekte çekimser kalmalarına neden olmasıdır. Kültür Bakanlığında bu konudaki çalışmalar halen sürmekle birlikte yazılımın kendine özgü özelliğinden dolayı kesinlikle normal yazılı basın fikri mülkiyet kanunu ile birlikte ele alınmamalıdır. Hazırl anmakta olan fikri mülkiyet kanununun bilgisayar yazılımlarıyla ilgili kısmının hazırlanması, ilgili tüm özel ve kamu kurumlarınında görüşleri alınarak, TÜBİTAK tarafından yapılmalıdır.

Sektörün ve ağların gelişmesi ile birlikte bilgisayarla işlenen suçlar da artış olacaktır. Verilerin gizliliği, bilginin insan haklarına aykırı biçimde kullanılması, bilgisayar sistemlerine izinsiz girme, virüsler ve izinsiz yazılım kopyalama gibi suçlar 1991'de çıkarılan yasaya rağmen halen kanunlarımızda açık değildir. Türk iye, OECD'nin "Verinin Korunması" ve "Sınır Ötesi Veri Akışı" belgelerini imzaladığı halde, kanunlarında bu belgelerin gerektirdiği değişiklikleri yapmamıştır.

Eğer bu yasal düzenlemeler yapılmazsa, Türkiye "veri cenneti" denilen ülkeler grubuna girebilir ki, bu da sınır ötesi ülkelerle veri alışverişimizin engellenmesiyle sonuçlanabilir. Bu nedenle dünyadaki durumu izlemek ve yasalardaki gerekli değişiklik önerilerini yapmakla TÜBİTAK görevlendirilmelidir.

2.3. Kamu Sektörününün Rolü

Kamu sektörü son on yılda bilgisayar alımlarına 500 milyon Dolar'dan daha fazla yatırım yapmakla birlikte (DB, sayfa 205) bu konuda bir standardı ve politikası yoktur.

Bilgisayarlar bir ağa bağlı olmadan bağımsız olarak çalışmaktadırlar,

Kapasitesi kurumların gereksinimle rinin üstünde oldukları için çoğunlukla boş durmaktadırlar,

Birçok kamu kuruluşunda bu bilgisayarları etkin çalıştıracak yeterli sayıda yetişmiş eleman yoktur.

Bunun yanında son on yılda Türkiye GSMH 'sının % 1'ini telekominikasyon ağını geliştirmeye harcamıştır.

Haberleşme altyapısının ülke ekonomisi için önemi açıktır. Ekonominin verimli işlemesi, rekabet gücü, giderek haberleşme altyapısına daha bağımlı hale gelmektedir. Mikroelektronik, fiber-optik ve yazılım teknolojilerinde son yirmi yılda meydana gelen ilerlemeler sayesinde, haberleşme altyapısı kurmak süratle ucuzlamıştır. Türkiye de bu teknolojik gelişmelerden yararlanmayı başarmış ve telefon şebekesini son on yılda önemli ölçüde büyütmüştür.

Teknolojik gelişmeler, klasik haberleşme hizmetlerinin verilmesini ucuzlatmanın yanında, yeni bir takım hizmetlerin verilmesini de mümkün kılmıştır. Mobil telefon, çağrı cihazı, paket anahtarlamalı veri iletişimi, yüksek hızlı veri iletişimi, telekonferans bu yeni hizmetler arasında sayılabilir.

Haberleşme sektörü hızlı bir teknolojik değişim süreci içindedir. Haberleşme altyapısının yeni hizmetleri verecek şekilde sürekli yenilenmesi gerekmektedir. Haberleşme hizmetlerinin verilmesinde meydana gelecek darboğazlar, ülke ekonomisinde darboğazlar yaratacaktır.

Haberleşme şebekesini genişletmek konusunda örnek bir başarı göstermiş olan Türkiye'nin önümüzdeki dönemdeki hedefleri şu başlıklar altında toplanabilir:

a) Hizmet arzında tıkanıklıklar olmamalıdır. Telefon, mobil telefon, veri iletişimi gibi temel kabul edilebilecek hizmetlerin verilmesinde tıkanıklık ortaya çıkmaması için gerekli yatırımlar zamanında yapılmalıdır. Örneğin, mobil telefon konusunda Türkiye geç kalmıştır. Acilen bu hizmetin temini yoluna gidilmelidir.

b) Abone ekipmanı piyasası rekabete açılmalıdır. Bürokratik engelleri kaldırarak, tüketicinin daha ucuza terminal cihazları edinebilmesi sağlanmalıdır. PTT'nin standart dışı altyapı

yatırımlarından kaçınması tüketiciyi korumak açısından özellikle önemlidir. Kötü bir örnek, Türkiye'deki araç telefon sistemidir; standart dışı bu sistemle, araç telefonu pazarı uzun süre rekabete kapalı tutulmuştur.

c) Hizmetler ucuzlatılmalı, kullanım yaygınlaştırılmalıdır. PTT yeni hizmet sunumunda ve fiyatlandırılmasında yalnızca ticari kaygılarla hareket etmemelidir; PTT bir tekel durumundadır ve topluma karşı yükümlülükleri vardır. Hizmetlerin ucuzlaması ve kullanımın azami sosyo/ekonomik yarar sağlayacak düzeye çıkarılması hedeflenmelidir. Örneğin, veri hizmetlerinin yaygınlaşmasını önleyen faktörlerin birisi telefon ağından veri taşıma masrafının yüksek olmasıdır. Bu hizmetin ucuzlatılması genel olarak telefon ücretlerinin düşürülmesi dışında, kısa vadede, kilit kullanıcılara (üniversiteler gibi) PTT'nin bu hizmeti sübvanse ederek vermesiyle mümkün olabilir. Veri iletişimi hizmetlerinin ucuzlatılmasının "telecommuting" gibi olanaklara kapı açarak iş sahalarını genişleteceği açıktır. Bunun olanaklı olması için ise telefon konuşmalarında "flat rate" tarifeye gidilmesi, ya da modem haberleşmesinde "flat rate" tarife uygulanması gerekmektedir. Ayrıca PTT'nin kamu yararı olan konularda şu andaki düşük sürüm nedeniyle yüksek ücret politikası izlemesini engelleyici yaptırımlar olmalıdır.

Devletin, böylesine büyük yatırımlara giriştiği bilişim sektöründe koordinasyon ve yönlendirme için liderliğine ihtiyaç vardır. Son zamanlarda çok tartışılan devletin öncü rolü ile ilgili olarak yeni ABD Başkan Yardımcısı Al Gore tarafından (Scientific American, Eylül 1991 sayfa 150) açıklanan görüşler konunun önemini bir kez daha ortaya koymaktadır. Devletin, aşağıda sıralanan hedeflere yönelik bir eylem planını uygulamaya koyması gerekir. Bu hedefler şöyle sıralanabilir:

Kamuda kaynak israfını önlemek;

Standardizasyonu sağlamak;

Bilginin kullanıcısının eline daha çabuk geçmesini sağlamak;

Bilgiyi daha hızlı toplamak ve işlemek;

Doğru bilgiye çabuk ulaşılan bir ortam yaratmak;

Araştırmaları desteklemek;

İnsanların evlerine bilgiyi götürmek (Fransız MINITEL gibi);

Telekominikasyon altyapısının optimum kullanımını sağl amak;

Sonuç olarak bilişim tabanlı toplum yapısı yaratmak.

Yukarıda açıklanan hedeflere varmak için aşağıda açıklanan adımların atılması zorunludur.

a) Kamu kurumlarında bilgisayarlaşmayı denetleyen ve otomasyona geçiş için gerekli hazırlıkları yapan bir ofis, bürokrasiden etkilenmeyecek bir idari yapıya sahip olacak şekilde kurulmalıdır. Bu ofiste TÜBİTAK, TSE, YÖK, DİE, PTT, MPM temsilcileri bulunabilir.

b) Uluslararası düzeyde bilgisayar ağlarının dayandığı platform, Açık sistemler ara bağlantı (OSI: Open Systems Interconnection) katmanlı yapısıdır. Devletler bu katmanların teknik özelliklerini belirleyerek Devlet Açık Sistemler Ara Bağlantı Kesitini belirlemekte (GOSIP: Government Open Systems Interconnection Profile) böylelikle de bilgisayar bağlantılarını standardize etmektedirler. TÜBİTAK tarafından desteklenen bir proje kapsamında çeşitli ülkelerin GOSIP'leri incelenmekte olup 1993 yılı sonuna kadar Türk Kanunlarına uygun bir GOSIP önerisi hazırlanacaktır. Bu çalışmanın ilgili kuruluşlar tarafında n da incelendikten sonra kabul edilmesi gerekir. Halen bazı kamu kuruluşlarının teknik şartnamelerine koydukları OSI standartlarına uygunluk şartı ancak bundan sonra sağlanabilecektir.

c) Ülkemizdeki tüm üniversiteleri, araştırma kuruluşlarını, özel sektör deki bilgisayar şirketlerini ve diğer kurumların (bankalar, finans kuruluşları, hastaneler, vb.) bilgisayar merkezlerini kapsayan bir bilgisayar ağı kurulmalıdır. Bu ağın temel özellikleri şunlar olmalıdır:

1. Ağın ana düğümleri arasında çok yüksek bir ile tişim kapasitesi sağlanmalıdır. (Örneğin 10 Mbit/Sn.) Bu kapasite fıber -optik teknolojisiyle rahatlıkla sağlanabilir.

2. Sistem en azından bugünkü INTERNET ağının sağladığı kütük gönderimi (file transfer) elektronik mesaj ve uzaktaki bir sisteme kullanıcı olarak bağlanma (remotelogin) işlevlerini yerine getirmelidir. Bu işlevlerin üzerine, gizli ve güvenilir haberleşme, vb. gibi daha üst katmanlar eklenebilir.

3. Sisteme bağlanmayı özendirecek tanıtımlar yapılmalı ve bağlantı ücretleri belli bir süre için de olsa makul düzeyde tutulmalıdır.

4. Birbirleriyle bilgi alış verişi olan devlet kurumları böyle bir ağ vasıtası ile bilgi iletişim gereksinimlerini giderebilirler. (Örneğin devlet kurumları arasında istatistiki, mali ve finansal bilgilerin toplanması ve paylaşılması, özel kurumlardan (banka, aracı kurum v.b.) bu gibi bilgilerin alınması böyle bir ağ vasıtası ile olabilir.

5. Sistem birbirine coğrafi olarak yakın noktalar arasında (örneğin şehir içinde) çok daha yüksek kapasitede (örneğin 100 Mbitlsn) bilg i iletişimini sağlayabilmelidir. Böyle bir altyapı varsa örneğin hastaneler arası radyolojik görüntü transferi yapacak sistemler kurularak sağlık hizmetlerine katkıda bulunulabilir.

6. Bilgisayar ağı teknolojisine ek olarak halen tüketici konumundaki birey lerin rahatça erişmekte olduğu telefon ağı daha basit bir takım işlevler için kullanılabilir. Elinde bir terminal veya bir kişisel bilgisayar artı -modem olan her birey bir bilgisayar servisine bağlanıp çeşitli bilgileri alabilmelidir. Fransa'da MINITEL sistemi ve ABD'de yaygın olan (BBS diye bilinen) sistemler buna bir örnektir. Bu sistemlerde kişiler bilgisayar vasıtası ile banka işlemlerini gerçekleştirebilmekte borsa işlemlerini aktif olarak izlemekte, alış veriş yapabilmekte, uçak, tiyatro v.b.

için yer ayırtabilmektedir. Bu sistemin özendirilmesi ile temel ürünü "bilgi" olan yepyeni bir endüstri doğacaktır. (Olumlu bir yan etki olarak ise kullanıcılara ucuza ulaştırılacak modem, terminal v.b. donanımların ülke içinde üretilmesi ve böylelikle ulusal donanım sektörüne katkı sayılabilir.) Dünya Bankası tarafından BİLGİTEL adıyla benzeri bir sistem önerilmiştir. PTT altyapısı böyle bir sisteme uygun olmakla birlikte uç birimlerinin Dünya Bankası raporunda belirtildiği gibi sübvanse edilmesine ihtiyatla yaklaşmak gerekir.

d) Bütün kamu kuruluşları zaman içinde bu ağa bağlanmalı ve kurulacak ofis vasıtası ile kamuda bilgisayarların efektif kullanımı sağlanmalıdır.

e) Kamu kuruluşlarında otomasyona geçilerek verim ve hız artırılmalı, personel giderlerinde tasarruf sağlanmalıdır. Otomasyona geçerken gereken yazılımların yerel yazılım şirketlerine verilerek yazılım sektörümüzün güçlendirilmesi hedeflenmelidir. HDTM'de Dünya Bankası'ndan alınan kredi ile böyle bir otomasyona gidilmektedir. Benzer çalışmaların DPT'de yapıldığı göz önüne alınırsa, otomasyona Başbakanlık ve bağlı kuruluşları kapsayacak şekilde başlanabilir.

f) Kurulacak ağ üzerinde bilgi bankalarının kurulması, var olanların bu ağa bağlanması, bu projenin en önemli uygulamalarından biridir. Proje DİE ve TÜBİTAK tarafından yürütülebilir.

g) Ağ, bilgisayar destekli eğitim amacıylada kullanılabilir. Milli Eğitim Bakanlığı'nda bu konuda çalışmalar yapıldığı bilinmektedir.

2.4. Bilişim Teknolojileri A+G Projelerinin desteklenmesi ve hedeflerin belirlenmesi TÜBİTAK, bilişim teknolojilerini öncelikli alan olarak belirlemiştir ve bu konuda kuruma verilen A+G projeleri öncelikli olarak desteklenmektedir. Bununla birlikte, konunun önemi nedeniyle daha geniş kapsamlı bir desteğe ihtiyaç vardır, çalışmalar ilgili tüm sektörlerin katılımıyla sürdürülmektedir.

Genç eğitimli nüfusumuzun üretime katılması sağlanmalıdır. Bu noktada bu özel ve çoğu ülkenin ihtiyacını hissettiği kesimi psikolojik ve kültürel yönden de kimliğimize uygun biçimde eğitmek en önemli görevlerimizd en biri olmalıdır.