Siber Savaş

kıyametin ilk halkası

MUTLU ÇÖLGEÇEN



arşiv KİTAPLARI

Mutlu ÇÖLGEÇEN

1971 Denizli doğumlu. Denizli- Tavas -Çağırgan İlkokulu, Denizli- Yeşilköy Ortaokulu, Muğla -Turgut Reis Lisesi ve İstanbul Üniversitesi Edebiyat Fakültesi'ni bitirdi. Gazetecilik hayatına lise yıllarında başlayan Çölgeçen, şimdiye kadar çeşitli gazete, televizyon ve ajanslarda çalıştı. "SİBER SAVAŞ- Kıyametin İlk Halkası" yazarın ikinci kitabı. Yazar daha önce 11 Eylül saldırılarını konu alan "ŞÜPHE- Sorular ve Senaryolar" adlı çalışmasını kitaplaştırdı. Çölgeçen, güncel konulara ilişkin araştırmalarının yanında kitap çalışmalarını da sürdürmekte.

Arşiv Kitapları: 3
İnceleme Araştırma: 2

Siber Savaş
Yazan: Mutlu Çölgeçen
Editör: Nasuhi Güngör

1. Basım: Mayıs 2002
Ofset Hazırlık: Ankara Dizgi Evi
Kapak: Ahmet Mayalı
Baskı-Cilt: Barışcan Ofset

Arşiv Kitapları
Serkon Sitesi E-4 Blok No: 17
25 Mart Mah. Yenimahalle/ANKARA
Tel: 0-312-336 78 90 0-542- 747 90 44
e-mail: arsivkitaplari@yahoo.com

Siber Savaş

Kıyametin İlk Halkası

Mutlu Çölgeçen

Arşiv
Ankara/2002

Eşime...

İÇİNDEKİLER

BÖLÜM 1
SİBER YÜZYIL 15
Teröristler 'BİLGİ'liydi 16
Korkunun nedenleri 17
Felaket tablosu 18
Siber savaşa hazırlık 19
Virüs yazarları da düşman! 20
"Sessiz Savaş" 20
ABD, sanal teröre savaş açtı ! 22
Clinton'un politikası 24
Nixon'u hack'lediler 25
Nixon olayı 26
GELECEĞİN SİBER SAVAŞLARI 27

BÖLÜM 2
BİLGİ SAVAŞI NEDİR? 35
Bilgi Savaşı Türleri 35
Tüzel Bilgi Savaşı 37
Global Bilgi Savaşı 38
VAROLAN ve OLASI BİLGİ SAVAŞI SİLAHLARI 38
Bilgisayar Virüsleri 38
Kurtlar(Worms) 38
Truva Atları (Trojan horses) 39
Mantık Bombası (Logic Bombs) 39
Tuzak Kapıları (Trap doors) 40
Mikroçipler (Chipping) 40
Nano Makineleri 41
Elektronik Sıkışıklık 41
HERF Silahları ve EMP Bombaları 41

BÖLÜM 3
ABD'NİN SİBER RÜYASI 43
Siber saldırı beklentisi 43
Bilgi Savasları ile İlgili Kurumsal Altyapı 48
Kritik Altyapılar 55

BÖLÜM 4
ENFORMASYON SAVAŞININ AŞAMALARI 57
Sanal saldırıya gerçek mermi 57
Sanal dünyayla bütünleşen saldırganlık 58
Müttefiklerin de canı yanacak 59
I. Merkezi Kuruluşlar 59
II. Kuvvet Komutanlıklarına Bağlı Kuruluşlar 63
III. Eğitim ve Geliştirme Amaçlı Kuruluşlar 67
ELEKTRONİK HARP VE SENARYOLAR 69

BÖLÜM 5
ULUSAL BİLGİ GÜVENLİĞİ 73
Teknolojik Gelişmeler 73
ABD 76
İngiltere ve Almanya 80
Norveç 81
Fransa 82
Türkiye'de Durum 83

BÖLÜM 6
ECHELON 85
Echelon 11 Eylül'ün şifresini çözemedi 85
Echelon'un çözemediği şifre 85
"Arka kapı" tehlikesi 86
Echelon'u örseleme günü: Jam Echelon Day! 87
50 yıldır dinliyorlar 87
Avrupa'nın yüzde 90'ını dinliyor 88
AB'nin 'Echelon'u Enfopol 88
Ticarî sırları da çalıyorlar 89
Kökleri Enigma'ya kadar uzanıyor 89

Dünyanın En Büyük Kulağı : NSA 90
'Umbra Gamma' gizlilik! 91
Gelişmiş bilgisayarlar kullanılıyor 92
Elektronik sinyal istihbaratı 93
Havada, Karada ve Denizde ECHELON 94
İnternetin yaygınlaşması bu planın bir parçası mı? 95
Echelon üsleri kapatılacak 95

EKLER 97
Notlar 143

Savaş, politikanın uzantısıdır.

Clausewitz

ÖNSÖZ

"Çinli bilgisayar korsanları, ABD Çalışma ve Sağlık Bakanlıklarının Internet sayfalarına saldırarak, bu sayfaların geçici olarak kullanılamaz duruma gelmesine neden oldu. New York Times Gazetesi, korsanların, Çalışma Bakanlığı'nın Internet sayfalarından birine, Güney Çin Denizi üzerinde 1 Nisan'da Amerikan casus uçağıyla çarpıştıktan sonra düşen Çin savaş uçağının ölen pilotunun fotoğrafını yerleştirdiğini ve sayfada 'Tüm ülke, en iyi evlatlarından biri olan Wang Wei'yi kaybetmenin üzüntüsünü yaşamaktadır' şeklinde bir mesajın yer aldığını yazdı. Gazete, bu olay yüzünden bakanlığın Internet sayfasının birkaç saatliğine kullanılamaz duruma geldiğini kaydetti. Çalışma Bakanlığı'ndan bir yetkili, gazeteye yaptığı açıklamada, soruşturmalar sonucunda, Çinli korsanların güvenlik sistemlerine girmeyi başaramadıklarını ve hiçbir bilginin kaybolmadığını belirtti.

Çinli hacker'lar ateşkes ilan etti

Çinli bilgisayar korsanları amaçlarına ulaştıklarını belirterek, bundan sonra ABD sitelerine saldırmayacaklarını duyurdu. Çinli hacker'ların Honker Union of China adlı resmi olmayan birliğinden yapılan açıklamada, ABD'ye karşı açılan online savaşa son verdikleri belirtildi. Yakın zamanda binden fazla Amerikan sitesine saldırdıklarını söyleyen hacker'lar amaçlarına ulaştıklarını vurguladı. Çinliler, bundan sonra ABD sitelerine yönelik saldırılandan Honker Union'un sorumlu tutulmamasını istedi. Çin'li hacker'lar ile Amerikalılar arasındaki siber savaş, ABD'ye ait casus uçağının Çin'de düş-

mesi üzerine iki ülke arasındaki ilişkilerin gerginleşmesiyle başlamıştı. Çin sitelerine saldıran Amerikalı bilgisayar korsanları Çinlilere duydukları 'nefreti' dile getiren mesajlar bırakmıştı. Bu saldırılara seyirci kalmayan Çinli hacker'lar da çok sayıda ABD sitesini hakladı. Aralarında Beyaz Saray gibi üst düzey kurumlara ait sitelere girenler Çinli'lerin mesajlarıyla karşılaştı

FBI Rus hacker'ları 'hakladı'

Amerikalı güvenlik yetkilileri kanıt toplamak için ilk defa sınır ötesi bilgisayarlara sızdı.Siber suçla mücadele konusunda yabancı hükümetlerden gerekli yardımı alamadığından yakınan FBI ilk defa 'sınır ötesi' bir operasyon gerçekleştirdi. Operasyon kapsamında iki Rusun bilgisayarı hack'lendi. Yetkililerin verdiği bilgiye göre, FBI Rus şüphelileri yakalamak için bir güvenlik firması adına iş teklifi yaptı. Görüşmeye gelen şüpheliler güvenlik güçlerince tutuklanarak mahkemeye çıkarıldı. FBI kanıt toplamak için Alexey Ivanov ve Vasily Gorşikov adlı şüphelilerin Rusya'daki bilgisayarlarına sızdı. Bilgisayar korsanlarını hack'leme fikrinin, Moskova'nın işbirliği teklifini reddetmesinin ardından alındığı belirtildi. Halen ABD'de tutuklu bulunan Ivanov ve Gorşikov ile işbirlikçileri 40 banka ve e-ticaret sitesinin bilgisayarlarına girmekle suçlanıyor. Güvenlik uzmanları, hacker'ların bu saldırılarda Microsoft'un Windows NT işletim sistemindeki bilinen bir açıktan yararlandığını söyledi. Microsoft söz konusu açıkla ilgili gerekli yamayı çıkarmış olmasına rağmen saldırıya uğrayan şirketler sistemlerini güncellememişti

Binlerce haber arasından aldığımız yukarıdaki üç haber 21.yy'ın önceki yüzyıllardan çok daha farklı olacağının işaretini veriyor. İnsanlık tarihi boyunca beden gücünü hep ön planda tutan insanoğlu için artık beyin gücü her yönüyle bir

adım öne geçmiş bulunmakta. Sanayi Devrimi ile birlikte önü alınmaz bir değişim içine giren dünya, bir bakıma kendini yok etmek için yeni buluşlara ev sahipliği yaparken, insan bedenini yönlendiren beyin, bedenin arkasına sığınmaktan çıkmış, artık her platformda kendi varlığını bütün yönüyle ispatlama telaşına girmişti.

"Dünya artık eski dünya olmayacaktı" ABD Başkanı Franklin D. Roosevelt'in 2. Dünya savaşı sırasında Japonya'ya atılan atam bombası sonrası söylediği bu sözler, 21. yy'la hazırlığın bir miladıydı adeta.. İnsanoğlu, eski çağın ok ve yaylarından, mızrak ve kılıçlarından kurtulmuş, şimdi daha güçlü ve daha mükemmel silahlarla kendisini donatmıştı. "Savaş özgürlük için gereklidir" sözlerinin doğruluğunu ispatlamaya çalışan dünya artık geri dönülmez bir yola girmişti. Adını 'Bilgi ve teknoloji" çağı olarak yazdıran 21. yy aslında dünyanın yeniden yapılanma senaryosunun yazıldığı bir başka tarih dilimi olacak. İşte "SİBER SAVAŞ-Kıyametin İlk Halkası" bu senaryonun hazırlık aşamasını kısmen aralamaya çalıştı...

Teşekkür...

Kitabın hazırlanması sırasında yazılarından fazlasıyla istifade ettiğim Nihat Halıcı ile Melih Bayram Dede ve moral desteklerini esirgemeyen sevgili dostlarım İsmail Zenginer ile Mahmut Filizer'e şükranlarını sunarım. Her zaman olduğu gibi en büyük teşekkür ise beni her ortamda destekleyen eşim ve çocuklarıma...

Mutlu ÇÖLGEÇEN
Mayıs 2002-A.Paşa-Ankara

"1969'dan bu yana yaratılan World Wide Web ağlarının siber-uzay atlası hazırlandı...İngiltere'deki London College'de görevli bilim adamı Dr.Martin Dodge, siber-uzay atlasını çıkarmayı başardı. Böyle bir atlası hazırlamak için tam 4 yıl boyunca 1969 yılından bu yana oluşturulan World Wide Web ağlarını tek tek inceledi. İlk kez 1969 yılında ABD'deki UCLA Üniversitesi'nin yarattığı World Wide Web ağından başlayarak bu zamana dek oluşturulan tüm siber ağları tek tek elden geçiren Dr.Dodge, bu incelemenin sonucunda 40 kadar harita ve grafik ortaya çıkardı. Dr.Dodge'un çıkardığı grafik haritalar sayesinde artık servis sağlayıcılarının uzay dağılımını görmek mümkün olacak. Dijital alanların tümünü grafik ve haritalarla görüntülü hale getiren Dr.Dodge, siber alemde bir ilke imza atmış oldu. Bilgisayar yardımıyla çıkardığı siberuzay atlası ile tarihe geçen Dr.Dodge, bu çalışmasının ileriki tarihlerde siber çalışmalarına ışık tutacağını söyledi. Coğrafya bilimi ile uzak mesafeleri birbirine eklemlemeyi başaran Dr.Dodge, 40 kadar harita ve grafik sayesinde yeni uzay coğrafyasının daha iyi anlaşılacağını bildirdi."

BÖLÜM 1

SİBER YÜZYIL

Dünya Ticaret Merkezi (New York) ve ABD Savunma Bakanlığı Pentegon'a (Washington) 11 Eylül 2001 tarihinde yapılan saldırılar dünyada yeni bir milat olarak tanımlandı. 1945 yılından bu yana dünyanın süper gücü ABD'yi yörüngesinden oynatan 11 Eylül'ü farklı kılan bir başka olgu ise dünyanın SİBER yüzyıla girdiğinin belirginleşmesiydi. 11 Eylül'ü her kim yapmış olursa olsun 'Bilgi'den yararlandığı ve Enformasyon'u en ince detayına kadar kullandığı bir gerçekti.Böylesi kapsamlı bir eylemin belki de aylarca sürmüş hazırlık çalışmalarının, en başta CIA gibi milyarlarca dolar bütçesi olan bir istihbarat örgütüne fark ettirilmeden sürdürülmesi dikkate değer. CIA, dünyanın çalışma ağı en geniş ve teknik imkanları en yüksek istihbarat teşkilatı olarak kabul edilir. Ayrıca dünyanın diğer etkili haber alma teşkilatlarının da ABD'yle ve CIA ile sağlam ilişkiler içerisinde olduğu görüşü de yaygındır. Echelon ve yüksek teknolojili istihbarat sistemlerine rağmen böylesi büyük bir terör eyleminin planlanması ve kusursuzca uygulanması çok şaşırtıcı. ABD'nin tüm askeri, savunma ve istihbarat birimlerinin kullandığı bilgisayar sayısının yüz binlerle ifade edilen sayılarda olduğu biliniyor. Bu bilgisayarların oluşturduğu yerel ağlara sızmalar olduğu da bir çok defa yazıldı. Özellikle Pentagon'un ve CIA'in "çok gizli" enformasyon ambarlarına girilmesi ve ciddi hasarlar verilmesi, hackerlar için çok iyi bir referans sayılır. Dünyanın en iyi hackerları arasına girebilmek için, ABD'nin savunma ve istihbarat teşkilatının bilgisayar sistemlerine sızmak birinci kuraldır.

Devletler, elektronik istihbarat tekniklerini elbette yoğun olarak kullanmaktadır. Örneğin ABD Ulusal Güvenlik Ajansı (NSA)'nın bu konuda çok kapsamlı ve sistemli operasyonlar yürüttüğüne değişik kaynaklarda rastlamak mümkün. Dünyanın bir numaralı yazılım üreticisi Microsof'un ürettiği yazılımların, NSA'nın haber alma çalışmalarına hizmet ettiğine dair komplo teorileri de çok yaygındır. Microsoft'un, kuruluşundan itibaren NSA tarafından desteklendiği ve üretilen işletim sistemlerinde bulunan "gizli kapı" sayesinde NSA'nın bu işletim sistemlerini kullanan tüm bilgisayarlara hükmettiği de iddialar arasında bulunuyor.

Viladimir Putin'in Rusya Devlet Başkanı olur olmaz verdiği ilk talimatlardan birinin, tüm askeri ve savunma birimlerinde Microsoft ürünlerinin kullanımını yasaklaması, bu iddiaları destekler nitelikte. Microsoft'un gizli kaynak kodlarından şüphelenen Putin, Linux gibi kaynak kodları açık olan işletim sistemlerinin kullanımını tavsiye etmişti. Hatta 2000 yılında, Alman savunma ve uluslararası ilişkiler teşkilatlarına ait bilgisayarlardaki gizli bilgilerin, Microsoft bünyesinde çalışan NSA birimi tarafından ele geçirildiği haberleri Der Spiegel Dergisi'nde çıkmıştı.

Teröristler 'BİLGİ'liydi

Bilgisayar ve iletişim teknolojilerindeki gelişmeler hem devletlerin, hem de devletlere zarar vermek isteyen odakların işine yaradı. Mesele, kimin bir adım önde olduğudur. Yani bütün espri, kimin tedbir almak ve sürekli savunmada kalmak zorunda olmasında; kimin saldırmakta ve açıklardan sızarak kaynaklara ulaşmak pozisyonuna yerleşmesindedir. ABD'nin maruz kaldığı bu büyük terör eylemleri zincirinin bütün halkalarının birbirine bağlı olduğu aşikar. Bu halkaların ne şekilde ve hangi araçların kullanılmasıyla birleştirildiğinin

cevabını belki hiç öğrenemeyeceğiz. Bunun cevabını vereceklerden bir kısmı düşen uçaklarda öldü, koordinatif ve operasyonel düzeydekilerin de kim ve nerede olduğu bilinmiyor. ABD gibi, teknolojiyi her alanda maksimum düzeyde kullanan bir ülkenin böylesi bir organize terör faaliyetiyle karşılaşması hiç şaşırtıcı değil. Dünya Ticaret Merkezi bina yönetimi bilgisayar sisteminin, Pentagon'un yerel bilgisayar ağlarının, Amerikan Hava Yolları'nın bilgi ve yönetim organizasyonunu sağlayan bilgisayar sisteminin ne düzeyde korunduğu ve bu sistemlerin profesyonel "hacker"lara ne kadar direnebileceği konusunda şüpheler var.

Uçağı kontrol edenin, ikiz kulelerin neresine çarpacağını çok iyi bildiğini söyleyebiliriz. Koskoca binaların çökmesi için çok kritik mimari bilgilere sahip olmak gerekir. Bu eylemi yapanlar ABD'nin güvenlik zaaflarını öğrenmek, eylemin tüm organizasyonunu ve uygulamasını gerçekleştirmek için büyük olasılıkla yoğun bir "siber istihbarat" faaliyeti yürüttüler. Teröristlerin birebir istihbarat yöntemlerini kullanarak, ajanları gerekli birimlere sızdırarak bu denli bilgiye ulaşması ve pratik güce ulaşması bana çok uzak bir ihtimal olarak görünüyor. [1]

Korkunun nedenleri

ABD Hükümeti son yıllarda yoğun şekilde "ikinci Pearl Harbour'u" yaşamamak için hazırlıklar yürütüyor. Bu kez baskın havadan değil kablolar, bilgisayar sistemleri ve telefon hatları üzerinden bekleniyor. Washington'u tedirgin eden tehlikenin adı "dijital Pearl Harbour".

Bu korku nedensiz ve saçma mı? 11 Eylül olayından sonra oluşturulan Anavatan Güvenlik Ofisi'nin (Homeland Security Office) "siber güvenlikten sorumlu" danışmanı Richard Clarke bakın ne diyor: "Geride bıraktığımız son 20 yıl içinde,

Kongre gerekli yasaları çıkarmaksızın ya da bu konuda somut idari kararlar alınmaksızın Amerika tamamen yeniden yapılandırıldı. Bir anlamda kendiliğinden bir gelişme oldu. Bugün ülke altyapısının önemli bir bölümü, bilgisayarların yönlendirdiği sistemlere bağımlı. Buna ordu ve ekonomi de dahil. Bunun geç farkına varıldı. Diyebiliriz ki, bilgisayarlardaki 2000 yılı sorunu, uyanmamıza neden oldu. Birdenbire daha önce hiç farkına varmadığımız bir sorunla yüz yüze gelirken, konunun daha derin ve kapsamlı boyutlarını algılama fırsatı bulduk..."Daha önce Ulusal Aniterör Koordinatörlüğü ve 1998'de kurulan Yaşamsal Altyapı Güvenliği Ofisi'nin (Critical Infrastructure Assurance Office) yöneticiliğini de yapan Clarke, uzun yıllardır "dijital Pearl Harbour" tehlikesinin ABD'yi tehdit ettiğini ısrarla savunanlardan...Clarke'a göre 11 Eylül onun tezlerini haklı çıkarmış durumda: "New York saldırısına kadar insanlar, 'teröristler hep bildikleri eylemleri tekrar eder durur' diye düşünüyorlardı. Oysa ne oldu? Hiç akıllara gelmeyen bir faciaya imza attılar."

Felaket tablosu

Havaalanı kontrol kulelerinde radarlar çalışmaz. New York Borsası'nda bilgisayarlar çöker. ATM'lerden para çekilemez... Hastanelerde hayat bağışlayan makineler çalışmaz olur... Telefonlar susar...İşte Richard Clarke'ın resmettiği olası bir siber saldırı sonrası İmpartorluk'un hali; dijital Pearl Harbour önlenememiştir.

Clarke'ın önlem olarak önerdiği projenin adı GovNet. Aslında GovNet, eski Başkan Bill Clinton döneminde FIDNet adıyla gündeme gelmiş, ancak sivil toplum örgütlerinin yoğun tepkisi sonucu uygulamaya konmamış bir proje. Sivil toplum örgütlerinin bir zamanlar "hükümet herkesin internet trafiğini denetleyecek" diye karşı çıktığı FIDNet, şimdiki adıyla GovNet için artık ortam uygun. Ilımlı Clinton'un yerinde, savaş

naraları atmasını pek iyi beceren Bush oturuyor...Ve 11 Eylül pek çok taşın yerinden oynamasına neden oldu. Ulusal Güvenlik Ajansı'nın (National Security Agency-NSA) danışmanlarından James Adams'ın ifadesiyle, "füze savunma sistemi kadar pahalı, yaklaşık 50 milyar dolar bütçeli bir proje"ye start verilmesi için uygun zemin oluşmuş durumda.

Siber savaşa hazırlık

Böylesine büyük bir rakamın siber savaşa hazırlık amacıyla kullanılacak olması mümkün mü? Bazı uzmanlar bu rakamların abartılı olduğunu ifade ederken, bazıları da şu somut olgulara dikkat çekiyor: ABD Savunma Bakanlığı'nın (Pentagon) yalnızca enformasyon üretme, toplama ve dağıtma işlemleri için harcadığı yıllık miktar yaklaşık 43 milyar doları buluyor. ABD Deniz Kuvvetleri'nin önümüzdeki 6 yıl içinde "enformasyon savaşına" ayırdığı bütçe ise 10 milyar dolar tutarında. Bu yalnızca Deniz Kuvvetleri'nin bütçesi. ABD Ordusu'nun diğer birimlerinin de benzer miktarları kullandıklarını düşündüğümüzde İmparatorluk'un GovNet projesi için 50 milyar doları gözden çıkarmaması için bir neden görünmüyor.

ECHELON sistemi ile İkinci Dünya Savaşı'ndan bu yana, dünyadaki her türlü veri iletişimini "dinlediği" ortaya çıkan ABD'nin GovNet'i, internetten ayrı bir iletişim ağı olacak. Ağ sürekli denetlenecek, virüs ve saldırı gibi durumlara anında müdahale edilecek. GovNet'te yaşamsal önemdeki tüm kamu birimleri yer alacak. ABD'nin siber savaş hazırlıkları GovNet'le sınırlı değil. 2002 Ocak ayından bu yana ABD Federal Adalet Bakanlığı, kadrolarında istihdam etmek üzere "Bilgi Teknolojisi (IT) deneyim ve birikimi olan" hukukçular arıyor.

Newsbytes internet dergisinin haberine göre, bakanlık "birkaç düzine avukat, aynı sayıda yardımcı personel ve sek-

reter ile hukuk deneyimi olmayan bazı IT uzmanlarını" oluşturulacak yeni departmanda görevlendirecek. Bu departmanın görevi, bilgisayar suçlarına ve "siber teröre" karşı hazırlanacak her yasanın biçimlendirilmesinden "copyright haklarına" kadar geniş bir alana uzanacak.

Virüs yazarları da düşman!

ABD'nin "dijital Pearl Harbour" korkusunun yalnızca ağ üzerinden sistemlere sızan ve "hacker" diye adlandırılan "siber terörist"lerle sınırlı olmadığını Demokrat Parti senatörü John Edwards yine Ocak (2002)ayı içinde Senato'da yaptığı bir konuşmada şöyle ortaya koyuyor: "Nimda ve Code Red virüsleri, Amerikan ekonomisine tam 3 milyar dolara mal olmuştur. Öyle bir çağda yaşıyoruz ki, bir siber terörist bir modem ve bir klavye aracılığıyla bir bombanın yapabileceğini yapabilir."

Virüslerin yalnızca maddi kayıplara yol açmadığını NATO'nun Kosova müdahalesi sırasında ABD bizzat yaşamıştı. 1999 Nisan ayı öncesi Belgrad merkezli bir bilgisayardan müttefik birliklerin e-posta adreslerine binlerce e-posta gönderilmiş ve bu "e-posta saldırısı" söz konusu adresleri uzun süre kullanılamaz hale getirmişti. Sistem güvenliği alanında kendini sorumlu ilan eden ve Avrupa'nın önde gelen hacker kuruluşlarından biri olarak nitelendirilen Chaos Computer Club'un (CCC) sözcüsü Frank Rieger'e göre: "e-posta saldırısı Melissa virüsü destekli yürütülmüş. Melissa, Pentagon'un e-posta listesini 1999 Mart ayından itibaren teslim almıştı. Yine Körfez Savaşı sırasında, Irak bilgisayar sistemine ABD tarafından bir virüsün bulaştırıldığı iddia edilmişti." [2]

"Sessiz Savaş"

Gelinen noktada, "Yeni dünya düzeni" söylemi bünyesinde sıkça dile getirilen "soğuk savaş sona erdi" tezi hızla çü-

rümektedir. Sovyet Rusya'nın çökmesinden sonra, ABD kaynaklı olarak dünya literatürüne sokulan bu tez, en son gelişmeler doğrultusunda, ABD ve müttefiklerine karşı yeni oluşmaya başlayan bloklaşmalarla birlikte iyice geçerliliğini yitirmektedir. Bu şartlar altında "savaş" kavramı en son ihtimal olarak başvurulan,zaman olarak sınırlı, silahlı kuvvetlerin silahlı kuvvetlere ve onların destek unsurlarına karşı yürüttüğü gürültülü bir eylem olmaktan çıkıp; sızma mantığı ile, sürekli ve toplumun bütün katmanlarına yönelik, her türlü araç kullanılarak sürdürülen "sessiz" bir eyleme dönüşmüştür. ABD'nin 42. Başkanı Bill Clinton'un "Boeing için iyi olan ABD için de iyidir" sözleri ile sinyalini verdiği ve en son olarak küresel Echelon casusluk sistemi ile ABD'nin Alman şirketleri üzerinde aktif casusluk faaliyetleri yürüttüğünün ortaya çıkması ile somutlaşan bu anlayış, girilecek işbirliklerinin aynı zamanda sağlıklı bir şüphecilik ile dengelenmesi gerektiğini açıkça ortaya koymaktadır. Artık savaşlar kan dökmek yolu ile cephelerde değil, toplumu kontrol etmek yolu ile o topluma ait "bilgi alanları" üzerinde kazanılmaktadır ki, bu değişim topraklarını kanlarının son damlasına kadar korumaya and içmiş uluslar için büyük tehlike arz etmektedir.

Son olarak Çinlilerin ABD'nin Los Alamos Nükleer Laboratuvarları'ndan en son nükleer silah başlıklarına yönelik bilgileri çaldığının ortaya çıkması bu açıdan güzel bir örnek teşkil etmektedir. Akademik bir havanın hakim olduğu bu laboratuvarlar, akademik kültür nedeniyle bilginin serbestçe dolaşacağı bir ortam yaratmış ve Çinliler bu ortamdan kendi çıkarları doğrultusunda faydalanmayı bilmişlerdir. Şüpheciliğin, akademik özgürlüğü boğacağı nokta ile, güvenin, güvenliği tehdit edeceği nokta arasında ki çizgiyi tutturamayan bu kurum, son yıllarda ABD'nin karşı karşıya kaldığı en büyük güvenlik skandallarından birinin merkezine oturmuştur. Bu ör-

nek; eğitim sistemlerini sanayii, sanayisini ulaşım altyapısı, ulaşım altyapısını uydu sistemleri,elektrik altyapısını telekomünikasyon sistemi ile entegre etmek zorunda olan bir ulusun, ulusal güvenlik politikasının ne gibi tehlikelerle maruz kalacağını göstermesi açısından büyük önem teşkil etmektedir.

ABD, sanal teröre savaş açtı !

ABD 42. Başkanı Bill Clinton 21. yüzyılda terör tehlikesinin ülkenin ulusal bilgisayar ağlarını hedef alan siber saldırılara odaklanacağını görevi bırakmadan kısa bir süre önce öne sürdü. Clinton, 2000 yılında Deniz Harp Akademisi'nde yaptığı konuşmada bu tehditlerin adı sanal bile olsa gerçek olduklarını ve yeni nesil Amerikalıların şimdiden bu gibi saldırılara hazırlanmaları gerektiğini belirtti. Bilgisayar korsanlarının günümüzde bankaları talan ettiklerini, askeri bilgisayarların kontrolünü ellerine geçirdiklerini ve bilgisayar virüsleri yayma tehdidiyle para sızdırdıklarını hatırlatan Clinton "Gelecek savaşa hazırlıklı olmalıyız. Yeteri kadar sert tepki veremezsek, teröristler, suçlular ve düşman rejimler, hayati bilgisayar sistemlerimize girebilir, ticari yeteneğimizi felç edebilir, sağlık ağımızı çökertebilir ve kriz anında tepki hızımızı düşürebilir" yorumu ile bu konudaki olası gelişmelere dikkat çekti.

Nitekim 10 Aralık 2000'li tarihine gelindiğinde işin Clinton'un söyledi kadar ciddi olduğu ortaya çıktı. Aynı tarihlerde son derece hassas bilgilerini internette tutmaktan gayet huzursuz olan ABD yönetimi yeni bir yapılanma için düğmeye basıyordu. Clinton'un Deniz Harp Akademisi'nde yaptığı konuşma sonrası Başkanlık Siber Güvenlik Danışmanı Richard Clarke, internetin en azından bir bölümünün mutlak güvenlikli olmasının gerektiğini vurguladı. Clarke göre kimsenin anonim olarak kullanamayacağı, giriş ve çıkışların sıkı kurallarla

denetleneceği yeni internette bu sebeple kişisel haklar ve özgürlüklerden de söz etmek söz konusu olmayacak. Zira bütün kullanıcılar tek tek izlenecek, yaptıkları kayda alınacaktı.

ABD'nin siber teröre karşı bu kadar duyarlı olmasını sağlayacak belki haklı sebepler vardı. Ancak ne ilginçtir ki dünyayı siber terör gerekçesi ile kontrol eden ABD, kendisine yönelik siber terörden korkuyordu. 4 Eylül 1999 tarihli ABD gazeteleri siber terör senaryolarına yer verirken dijital soğuk savaş sendromunun olası etkilerini de gündeme taşıyorlardı. Haberlerde, "ABD hükümeti siber uzaydan gelecek saldırılardan korkuyor. ABD'ye muhalif pek çok ülkenin, hedefinin ABD'nin çeşitli devlet örgütlerinin bilgisayarlarına sızarak zarar vermesi paranoyası giderek güçleniyor. Üstelik siber terörizm münferit ve kaynağını tespit etmek de çok zor. Yeni soğuk savaş siber uzay paranoyası nedeniyle yaşanabilir."yorumları yapılırken aynı dönemde Amerikan Bilim Adamları Federasyonu güvenlik analisti John Pike, hacker'ların izlerini sürmenin çok zor olduğunu söyledi: "Hidrojen bombası imal eden birinin kendisini gizlemesi zordur, ancak bilişim saldırısı yapabilecek nitelikte birini keşfetmek samanlıkta iğne aramak gibidir. Potansiyel siber terörist herhangi bir yerde Internet bağlantısına sahip bir bilgisayarı olan kişidir."

Clinton dönemi Beyaz Saray'ın Kritik Altyapılar Müdürü Jeffrey Hunker bakın ne diyor: "ABD'ye düşman gelişmekte olan birçok ülke var ve siber saldırı yetkinliklerini sürekli geliştiriyorlar; birçoğunun ilk hedeflerinin ABD olduğunu biliyoruz."Hunker bu iddiasını, özelikle Rusya ve Çin'de birçok yetkilinin, kendi ülkelerinde gelişmekte olan hacker gruplarının yeterince engellenmediğini dile getirmeleriyle destekliyor. ABD eski Başkanı Clinton da zaten sık sık ülkelerin siber saldırılar karşısında korunmasız durumda olduğunu belirtiyor. Başkan'a göre bunun nedeni artık tüm dünya ülkelerinin yük-

sek teknolojiye muhtaç olmaları. Çünkü bu bağımlılık, beraberinde ülke kapılarının sanal aleme açılışını getiriyor.

Clinton'un politikası

ABD'de 1990'lı yıllardan sonra gelişen süreç ve ABD'de yaşanan dijital soğuk savaş sendromunu bir hayli arttırdı. ABD Hazine Bürosu, Milli Gelir Servisi ve Savunma Enformasyon Bürosu gibi devlet sektörünün önemli networklerinin güvenliğini sağlayan Axent Technologies'in sahibi Drew Williams, halen kullanılan bilgisayar sistemlerinin siber uzaydan gelecek sabotajlara karşı korunmasız olduğunu dahi söyledi. Williams'a göre ise, "Bilgisayar sistemlerine dışarıdan yapılan her müdahalenin arkasında organize bir hareket yok. Zaten Beyaz Saray ve FBI'ın Ulusal Altyapı Koruma Merkezi (NIPC) kazaen girişler için endişe duymuyor. Çünkü bu tür kanunsuz girişler kasti saldırılara göre düşük bir yüzdeye sahip."

Clinton'dan sonra göreve gelen 43.Başkan George W.Bush ise ülke güvenliğini sağlamak ve terörle mücadele etmek için, 11 Eylül saldırısından bir süre sonra, Eylül (2001) ayının son günlerinde İç Güvenlik Konseyi'ni kurdu. Yapılan atama ile bir ara adı başkan adayları arasında geçen Tom Ridge başkanlığa, emekli orgeneral Wayne Downing ise terörizmle mücadelede Bush'un başdanışmanlığına getirildi. Clinton dönemi siber terör uzmanı Richard Clarke ise ülkeyi siber saldırılara karşı koruyacaktı. Her biri alanında deneyimli olan uzmanlardan Tom Ridge; 11 Eylül'den sonra oluşturulan İçişleri Güvenlik Konseyi, ekim (2001) ayı başlarında işbaşı yaptı. Konsey, Adalet Bakanı, Savunma Bakanı, Hazine, Sağlık ve İnsani Hizmetler, Tarım Bakanlığı ve FBI ile Federal Acil Yönetim Bürosu Başkanları'ndan oluşturulurken Konseye Pennsylvania Valisi Tom Ridge başkanlık etti. Ridge'in

bürosu Beyaz Saray'ın Bati Kanadı'nda Bush'un makamına yakın bir yerde oluşturulurken ABD medyasında Ridge'nin de en az Ulusal Güvenlik Danışmanı Condoleezza Rice kadar etkin bir güce sahip olacağı haberleri yer aldı. Ridge, kendisine verilen yetki ve bütçe çerçevesinde 100 kişilik bir ekiple FBI, CIA dahil 46 istihbarat dairesinin faaliyetlerinin koordinasyonundan sorumlu olacak. Doğrudan ABD Başkanı'na bağlı olarak çalışacak olan Konsey, ABD'ye yönelik her çeşit saldırıyı önleme ve korumayla sorumlu olacak ve masraflarını Beyaz Saray ödeyecek.

Emekli general Wayne Downing ise ; İç Güvenlik Konseyi'nde istihbarat ve askeri kaynakların koordinasyonunda görev aldı. Downing, 1996 yılında Suudi Arabistan'da 19 ABD'li askerin öldüğü saldırıyla ilgili soruşturmayı yürütmüştü. Terörle mücadelede uzman olan Drowning, daha önce terörizmin sürekli bir tehdit olduğunu ve hükümetin 'ilan edilmemiş olan bu savaşla' baş etmesi gerektiğini söylemişti. 10.8 milyar dolarlık bir bütçeye sahip olacak olan Downing, savunma ve diplomasiyle işbirliği yapıp ülkenin terörle mücadele planlarını oluşturacak.

Bill Clinton zamanında Ulusal Güvenlik Konseyi'nde terörle mücadele şefi olarak görev alan Richard Clarke, yeni kurulun Siber Güvenlik Bürosu'na başkanlık edecek. Clarke'ın görevi ülkenin telekomünikasyon ve enformasyon yapısını terör saldırılara karşı korumak olacak. Richard Clarke'ın bürosu, sanal alemdeki terörist faaliyetleri de sıkı takibe alarak, muhtemel tehditleri ortaya çıkaracak.

Nixon'u hack'lediler

Başkan Bill Clinton döneminde artık tam anlamıyla korku sınırını aşan Siber Terör ve Hack olayları aslına bakılırsa epey gerilere gidiyor. Başkan George W.Bush'un 11 Eylül

saldırıları sonrası oluşturduğu özel birlik daha önce kurulmuş olsaydı belki eski Başkan Richard Nixon'un karşı karşıya kaldığı o tatsız şakayı önleyebilirdi. Nixon'un başkanlığından uzun süre sonra ajanslara düşen bir haber herkesi adeta şaşkına çevirdi. Çünkü ajans haberine göre Ünlü hacker John Draper, eski başkan Nixon'u işletmişti.

Hacking dünyasında yaşayan efsane olarak anılan ve ücretsiz şehirlerarası konuşma yapabilen 'Blue Box'un mucidi olarak tanınan John Draper ve arkadaşlarının ABD eski Başkanlarından Richard M. Nixon'u, Merkezi Haber Alma Teşkilati (CIA) ile irtibat kurdugu özel hattan arayip "işlettikleri" ortaya çıktı. Hackerler, telefona çıkan Nixon'a ulusal bir krizin varlığını haber verip, Nixon'un problemin ne olduğunu sorması üzerine ise tuvalet kağıtlarının bittiğini söylemiş.

Nixon olayı

2-3 gün sonra tekrar aynı numarayı arayıp sosyal mühendislik yapmak istediğini anlatan Draper, olayı şöyle anlatıyor : "Karşımdakine kim olduklarını sorduğum zaman, CIA'nın Beyaz Saray hattına girdiğimi anladım. Acil durumlarda Başkan ile görüşmek için direk kullandıkları gizli bir hattı. Daha sonra Olimpus diye bir kod duydum ve aynı numarayı arayıp "Olimpus" dediğimde karşıma Başkan Nixon çıkmıştı ve ben hemen telefonu kapattım."

O dönemlerde hackerlerin numaraları aralarında değiş tokuş yaptıklarını bildiren Draper, Apple'nin kurucusu Steve Wozniak'a kendisinde ABD Başkanı Richard Nixon'un numarası olduğunu söylediğini, arkadaşlarının ise onlarla dalga geçtiğini sandıklarını anlattı. Draper, "Steve numarayı çevirdi ve "Olimpos" deyince Başkan'ı karşısında bulmuştu. O da Nixon'a "Ciddi bir ulusal kriz var" dedi. Başkan da nedir diye sorunca tuvalet kağıdının bittiğini söyledi" diye konuştu. Los Angeles telefon santralına girip, dışarıdan gelen tüm arama-

ları operatör gibi karşıladıklarını da anlatan Draper, "Herkese Los Angeles'ta nükleer bir sorun olduğunu söylüyorduk ve bir süre sonra basın hücum etti, ordu arayıp birlik göndereceğini söyledi" diye konuştu. Olayların Los Angeles Times gazetesinde "Nükleer şaka" diye yer aldığını kaydeden Draper, Steve Wozniak'ın, hattına ulaştığı Papa'yı sabahın 3'ünde arayıp görüşmek istediğini de kaydetti. [3]

Geleceğin Siber Savaşları (Onward Cyber Soldiers)

Çağımıza damgasını vuran teknolojik buluşlar, özellikle bilgisayar alanında inanılmaz boyutlara ulaşmıştır. Bilgisayar teknolojisini bütün birimlerine yerleştiren Amerikan Ordusu, klasik savaş anlayışını kökünden değiştirmiştir. Amerikan Savunma Bakanlığı(Pentagon), yeni enformasyon savaş teknolojisinden (INFOWAR) yararlanarak düşmanın haberleşme komuta kontrol merkezlerini : askeri, sosyal, ekonomik sistemini tek bir kurşun sıkmadan, belki de kan akıtmadan, işlemez hale getirme planları yapıyor. Bilgisayar teknolojisinin sağladığı bütün olanakları kullanan Amerikan ordusu, her hangi bir savaşı sadece video ekran, klavye ve fare (mouse) ile kazanmayı hedefliyor. Pentagon yetkilileri, bilgisayar -savaşlarının en büyük zaafının, kendi sistemlerinin de başka ülkeler tarafından yok edilebilmesi ihtimali olduğunu belirtiyorlar. Enformasyon Savaş Teknolojisi (İNFOWAR)'nin imkan ve kabiliyetlerini şöyle sıralayabiliriz;

1. Elektromanyetik Çarpma : Delta gücü komandoları düşman ülkenin başkentine sızıyorlar. Bir çanta içerisindeki nükleer olmayan, elektromanyetik dalga (EMP) bombasını patlatıyorlar. Dalgalar Merkez Bankası ve haberleşme sisteminin ana bilgisayarını felç ediyor, finansal işlemler duruyor.

2. Akıllı Bomba : Hasım ülkenin hava, demir, kara yolları, trafik kontrol sistemleri devre dışı bırakılıyor. Uçaklar yan-

lış havaalanlarına iniş yaparken, askeri teçhizat taşıyan trenler ülke içinde kayboluyor.

3. Bilgisayar Virüsü : CIA, haberleşme ağına virüs koyuyor. Telefonlar arapsaçına dönüyor. Daha uzun süreli tahribat için, elektronik malzeme yiyen mikroplar sistemlere yerleştiriliyor.

4. Hayali Telsiz Bağlantıları : Özel donanımlı uçaklar TV yayınlarını bozuyor, hükümet programları yerine Amerikan yapımı olanlar giriyor. iletişim sistemlerinde parazit üreten Amerikan uçakları devreye giriyor. Cephedeki birliklere sahte komutlar gönderiliyor.

Kuzey Virginya'daki A.B.D. Kara Kuvveleri gizli istihbarat ve Güvenlik Teşkilatından Albay Mike Tanksley, bilgi çağının getirdiği yeni teknolojik silah sistemlerinden kısaca bahsetmiş ve bu silahların detaylarına girmeksizin kabaca ana hatlarına değinmiştir. Yeni senaryo; gelecekte bir gün Amerikanın müttefiki olan (Suudi Arabistan, Mısır, İsrail), Babil ülkelerinin (örneğin Irak, İran ve hatta Libya, v,d.) ani saldırıları üzerine A.B.D.nin derhal ani müdahale kuvvetini, harp gemilerini, uçaklarını göndermesi yerine yüksek teknoloji ürünü bilgisayar yazılımları, bilgisayar ekranı, fare (mouse) ve klavyelerin oluşturduğu sistemi savaş alanına sürmesi üzerine kurulmuştur.

Buna göre; bilgisayar virüsü, önce hasmın telefon santral şebekesi içine yerleştiriliyor, ülkenin telefon şebekesi felce uğratılıyor. Daha sonra (zaman ayarlı) akıllı bombalar patlatılarak demir yollarının, kara yollarının, elektronik beyin merkezleri sabote ediliyor seyir halinde olan trenler yanlış yerlere yönlendiriliyor, bir seri kazalar ve kaoslar meydana getiriliyor. Arazideki birlik komutanlarının haberleşme şebekelerine girilerek komutanların ses tonları taklit edilerek kasıtlı

yanlış, emirler alınması sağlanıyor. Psikolojik sansasyon yaratmak için elektronik harp teçhizatlı Amerikan uçaklarıyla, hasım ülke TV yayınlarına girilerek menfi propaganda yapılıyor ve halkın diktatörleriyle olan güven bağları koparılıyor. Ülke liderleri İsviçre bankalarına kaçırdıkları milyonlarca dolar kıymetindeki servetlerine kendi PC'leri ile ulaştıklarında, hesaplarının sıfırlanmış olduğunu hayretle görüyorlar. Bütün bu yapılanlar için Amerika tek bir kurşun atmamıştır. Albay Tanksley'in "Bu yeni sistemle harpleri daha başlamadan sona erdirebiliriz." demiştir.

Bu bilgisayar teknolojisindeki büyük devrim, Amerika için de geçerli bazı sosyolojik sorunlar gündeme getirmektedir. Bunlar ise ;

*Döviz piyasası ve borsayı alaşağı edecektir.

*Ucuz teknoloji kullanan ülkelerin yöneticileri, kötü niyetlerinin tezahürü olarak, NASDAQ gibi borsaları kilitleyebilirler.

*Daha önemlisi ; Terörist ve korsan bilgisayar programcılarını satın alıp, batı ülkelerinin önemli havaalanlarının bilgisayar iletişimine girerek, hava seyrüseferlerini tehlikeye sokabilirler.

Bilgisayar teknolojisindeki bu değişimler, Amerika Birleşik Devletleri Askeri birliklerinin her kademesine yansımaktadır. Körfez savaşının ilk günlerinde, güdümlü füzeler taşıyan STEALTH jet tayyareleri, Bağdat'ın elektrik güç kaynakları ile haberleşme şebekelerini kullanılamaz hale getirmişlerdi. Ayrıca, Pentagon iktidardan uzaklaştırılan Cumhurbaşkanı Jean Bertrand Aristide' yi tekrar iktidara getirmek üzere HAİTİ askeri rejimine karşı çağdaş bir psikolojik baskı kampanyasını da başlatmıştı. ABD Kara Kuvvetlerinin 4'ncü Psikolojik Harekat Grubu, yaptığı araştırmasına göre Haitilileri 20 ayrı

gruba bölerek, her birine Aristide lehinde havadan binlerce bildiri attı. Amerikanın müdahalesinden önce, CIA, çok sayıda isimsiz telefonlar etmiş bilgisayarı olanlara isimsiz E-mail mesajlar göndererek halkı Aristide etrafında toplamaya çalıştı. Teknolojik bilgisayar harbi, bilgisayar mikro prosesörlerinde ve iletişimde, modern sensör ve role devrelerinin üretilmesiyle fiilen başladı.

Teknolojik bilgisayar, ABD Kara, Deniz ve Hava Kuvvetleri'nde kullanılmaya başlamıştır. Washington'daki Ulusal Savunma Üniversitesi 2000 yılında teknolojik bilgi eğitimi almış 16 subay mezun etti.

Zaman zaman ortaya bilgisayar yazılımlarında kötü amaçlı korsan kişiler çıkmaktadır. Bu amaçla Ulusal Güvenlik Teşkilatı, gizli ajanlarıyla, Kara, Hava ve Deniz Kuvvetlerinin çeşitli kuruluşlarında faaliyet gösteren bilgisayar birimlerine böyle kişilerin muhtemel sızmalarına ve virüs bulaştırmalarına karşı önlemler almaya çalışmaktadır. Virüsün diğer bir çeşidi, "Akıllı Bomba"dır. Zaman ayarlı olarak bilgisayar donanımına sokulan bu virüs, bilgileri yok eder. Ulusal Hava Savunma Bilgisayar sistemine veya Merkez Bankası ana şebekesine girdiği zaman tüm sistemi etkisiz hale getirmektedir. CIA yaptığı son gizli çalışmalarında; yabancı ülke silah üreticilerine satılan silah sistemlerinin bilgisayarına bubi tuzak tipi chipsleri gizlice takarak, silahların istenmeyen ülkelerin ellerine geçmesini önleyici çalışmalar yaptı.

Ayrıca; Ulusal Güvenlik Teşkilatı; silah yapım firmalarının kiraladıkları bilgisayar programcılarını satın alarak, yazdıkları programlara virüs sokmalarını sağlayıcı faaliyetler içindedir.

Teknolojik bilgiye dayalı silahlardan bazıları bilgisayar virüslerinden daha yeni ve daha ilginçtir. New Meksiko'daki

Los Alamos Ulusal Laboratuaru bir bavul büyüklüğünde ve yüksek enerjili elektromanyetik dalgalar üreten bir silah üretmiştir. Örneğin, bir buhran durumunda komandolar hasım ülke başkentine sızma yapmış olsunlar, akıllı bomba bir bankanın yanına konup patlatılsın, sonuçta yayılan dalgalar binanın tüm elektronik donanımını yakıp işlemez hale getirecektir Pentagon kurmaylarının üzerinde durduğu diğer bir silah türü ise elektronik virüstür Tıpkı çöplükte mikroorganizmaların ürediği gibi, bilgisayar içindeki elektronik devreleri ve yalıtkanları yok eden bir mikrop üretmektir.

Teknolojik bilgi harbi yeni yeni istihbarat bilgilerini elde edecek sistemleri bünyesinde toplayacaktır. Bunlar uydular, casus uçakları ve gövdesine kamera takılmış insansız hava araçlarıdır. Gelecekte, gök yüzünde sayısız ufak sensörler doğacak ve ya bu sensörler düşman derinliklerine atılacak. "Massachusett Institute of Technology"nin Lincoln laboratuarı, fotoğraf çekebilir, sigara kutusu büyüklüğünde, insansız hava araçlarını üretme aşamasındadır. Bu küçük hava aracideki askerleri saptayabilmektedir. Şöyle ki düşman askerleri üzerine aerosol sprey fışkırtılır veya yiyecek maddelerinin üzerine kimyasal bir madde gizlice bulaştırılır.

Sonra bu birlik üzerinde uçan biyosensör araçlar, insanların nefeslerinden ve ter kokularından yerleri saptanarak yok edilmelerini sağlar. Pentagon'un, Silahlı Kuvvetler harcamalarına önemli kısıtlamalar getirmesi ve kara kuvvetlerinin sayısal olarak 1.1 milyon kişiye (dünyada sayı olarak 8 nci) düşmesi üzerine Ordunun üst düzey komutanları "Gelecekteki muharebelerden zaferlerle çıkmak istiyorsak Amerika, liderliğini bilgi, işlem ve iletişim teknolojisinde de göstermelidir" demişlerdir. Fort Leavenworth, Kansas'ta (2000) Mart ayında Yapılan Simülasyon Muharebe oyunlarında, 2010 yılında muhtemel bir senaryoda kendisinden sayıca 3 kat faz-

la Kuzey Kore Ordusuna karşı 20.000 kişilik olarak bir piyade tümeni tam teçhizatlı modern bilgi- işlem- iletişim cihazlarıyla donatılmıştır. John Hopkins Üniversitesi Uygulamalı Fizik Laboratuarındaki bilim adamları "Süper Elit Bilgisayarı" üzerindeki çalışmalarını yoğunlaştırmışlardır. Bu bilgisayar Donanma muharebe grubunun radar sinyallerini alır, işler ve ekranda üç boyutlu muharebe sahası modeline dönüştürür. Donanma komutanı tahtada semboller yerine, ekranda üç boyutlu model üzerinde dost ve düşman gemilerinin grafik resimlerini görerek yerleri ve hareketleri hakkında muhakeme yapabilir. Bilgisayar, ekran başında kimse olmaksızın taarruz edilecek hedefi seçip ikaz edebilir, hatta hava sahasını da gözleyebilir. Bilgisayar bir tehdit sinyali aldığında, flash ve sis düzeniyle komutanı ekran başına çağırır. Teknolojik bilgiye dayalı yeni sistemler ordunun aşağı kademelerinde de kullanılmaya başlayacaktır. 2010 yılından önce ABD Kara Kuvvetleri Muharebe Sahasını elektronikleştirecektir. Her asker ve her silah sistemi elektronik iletişim şebekesine bağlanacaktır.

Natick, Massachusett'teki Ordu Araştırma ve Geliştirme Laboratuarı 21.Yüzyıl sahra erinin giysisini tasarlamıştı. Helmette mikrofon ve kulaklık olacak, gece görüş dürbünü ve termal görüntüleme sensörü ile, arazi üzerinde nerede bulunduğunu gösteren ve devamlı istihbarat bilgilerini içeren göz visörü takacaktır. Mikroprosesörlerdeki yenilikler silah sistemlerini daha küçük boyutta üretilebilirliğini ve uzaktan kontrollü insansız hava araçlarının, yer hedeflerini hatta uçak gemilerinin yerlerinin saptanmasında büyük katkıları olacaktır. Geleceğin savaşlarında jet tayyareleri yerlerini insansız hava araçlarına bırakacaktır.

Bu teknolojinin devreye girmesiyle emrin en üst komutandan sahradaki en ast birlik elemanına ulaşması mümkün olacaktır. Düşey hiyerarşi kalkacaktır. Kara Kuvvetleri harekat

merkezinden bir general "Bu enformasyon savaş teknolojisinin tümenlerin ve donanma görev kuvvetinin yerine geçeceğini zannediyorsanız yanılıyorsunuz, böyle bir bombardımana maruz kalmış bir ülke gene de arkasında kesin yumruğu vuracak bir kuvvetin bulunup bulunmadığına bakacaktır" demiştir. Ulusal Savunma Teşkilatından Martin LIBICKI'nin de söylediği gibi, eğer elektromanyetik harp Irak savaşında başarılı olsaydı, Saddam ve hükümeti hemen görevde olmayacaktı. Amerika bu savaşta, elektronik karıştırmadan mikro bilgisayarlara kadar en modern iletişim tekniklerini kullanmış, Irak'ın telefon şebekesini ve elektrik güç kaynaklarını saf dışı bırakmıştı. Modern bilgi teknolojisine uygun bilgisayar donanımları oldukça pahalıya mal olmasına rağmen, kötü niyetli bir programcının bu donanımları sabote etmek için bir bilgisayar ve bir modem cihazına sahip olması yeterlidir. Bunun maliyeti ise oldukça düşüktür.

Bilgi iletişim ağına son günlerde korsan müdahaleler gözlenmektedir. Örneğin, Washington'da konuşlandırılmış Askeri Otomasyon İşlemleri Güvenlik ve Destek Şubesi vardır. Görevi Pentagonun bilgisayar şebekesine olası bir müdahalede devreye girerek, işlemleri aksatmadan çalışır halde tutmaktır. 1 Temmuz'a kadar18 aylık süre içerisinde, dünya genelinde ABD Askeri bilgisayar ağına ait operatörlerde 28 bin defa yardım çağrısı alınmıştır. Bu ise; devrelere korsan müdahale olduğunu göstermektedir. Bundan sonra, ABD'nin askeri intikallerini, kargo uçak, tren ve gemi seyrüseferlerini saptırarak geciktirmek, dolayısıyla dünyanın Jandarmalığına soyunmuş Amerikanın askeri imajını sabote etmektir.

Amerikan silah ve komuta kontrol sistemlerine dönük bilgisayarlar dışındaki (örneğin personel kimlik bilgisi, maaş, özlük hakları, ulaştırma, levazım, ordu donatım gibi) işlemler için kullanılan bilgisayarlar Pentagon'dakilerle çevrim içinde

olup, ciddi bir korunma içerisinde de değildir. Böyle bilgisayarlara günde 500 defa müdahale girişiminde bulunulmakta, bunlardan sadece 25' i saptanabilmektedir. Hatta bu konuda Beyaz Saray yetkilileri de Enformasyon Savaş Teknolojisinin geleceğinden kaygı duymaktadırlar. 42. Başkan Clinton bu yeni teknolojik harbe karşı güvenli bir korunma stratejisinin saptanmasını ve hangi kurumun bu amaç doğrultusunda görevlendirileceğinin bilinmesi ve hatta bu faaliyetlerin 1996 başkanlık seçimlerinin yara almasına meydan vermeyecek şekilde önceden başlatılmasını istemiştir.

Bu yeni teknolojik bilgi savaşı beraberinde bazı önemli sorunları da getirmiştir. Ordudaki din görevlileri Cyber savaşlarını, düşmana klasik çatışmalarda olduğu gibi teslimiyet bayrağını çekme fırsatı tanımayacağını ve sonuç tüm ülke imkanlarının perişanlığa yönelik olduğu için ahlaki bulmamışlardır. Sonuç olarak enformasyon savaş teknolojisi II. Dünya Harbinde Tokyo ve Dresden nehirlerinin bombalanmasından, Bosna'daki etnik temizlik harekatı gibi modern savaş tekniklerine yönelmiştir. Fakat, geride bir ülkenin hava trafik kontrol veya telefon sistemlerinin beyni olan bilgisayarları kullanılamaz hale getirirken, diğer taraftan o ülkenin insanlarına zarar vermektedir. Ambargoda olduğu gibi, bir ülke için ekonomik kaos da bir felakettir. Fakat, şu gerçeği de unutmamak lazım ki, bu teknoloji sayesinde muharebe sahalarının kanlı bilançosundan kurtulmuş olmaktayız. Amerikan iç harbi komutanlarından General Willam Sherman'in sözü bu gün halen geçerliliğini korumaktadır. "Savaş gaddarlıktır, fakat onu hiç bir zaman zarifleştiremezsiniz." [4]

BÖLÜM 2

BİLGİ SAVAŞI NEDİR?

Peki Bilgi Savaşı nedir ? Günümüzde sıklıkla kullanılan "Bilgi Savaşı" deyimi çoğunlukla yanlış anlaşılmakta ve daha çok üstün teknoloji silahları ile yapılan savaşları çağrıştırmaktadır. Oysa Bilgi Savaşı; "karşı tarafa ait, bilgi tabanlı işlemcileri, bilgi sistemlerini, bilgisayar tabanlı network sistemlerini etkileyecek bir hareket gerçekleştirmek ve kendi sistemlerini korumak" anlamına gelmektedir. Kısaca, Bilgi Savaşı'nın askeri bir boyutu olmasıyla beraber daha çok bilgi sistemlerini çökertmeye yönelik, internet savaşlarını tanımlayan bir deyimdir. Bilgi Sitemlerinin tanımı ise, bilgi yaymak, göstermek, iletmek, yedeklemek için gerekli makine, personel ve ekipmanı kullanarak oluşturmuş altyapı, organizasyon ve işlemci" şeklinde yapılmaktadır.

Bilgi Savaşı Türleri

Bireysel Bilgi Savaşı

Bu grupta yer alan saldırılar bir bireyin elektronik mahremiyetini hedef almaktadır. Bir kişiye ait tüm, dijital kayıtları ve veri tabanlı girişleri tehdit eden bu saldırılar; bilgi nerede saklı olursa olsun onu bulup zarar vermeye yöneliktir. Ortalama bir bilgisayar kullanıcısının sakladığı bilgi üzerindeki kontrolü ne yazık ki çok fazla değildir. Biz kendimize ait bilgilerinin tamamını kontrol edememekteyiz. ABD'de yapılan bir araştırmaya göre, bilgisayar kullanıcılarının yüzde 78'i böyle bir sal-

dırı sonucu bilgi kaybına uğramıştır. Geçmişte, bir kişi hakkında bilgi almak için çalışan bir ajan, minyatür kamera ya da mikrofon kullanmak zorundaydı. Günümüz ajanları ise, o cihazların daha da küçülmüş modellerini kullanmakla beraber, çoğunlukla zaten varolan verilere ulaşarak, her türlü bilgiyi edinmektedir. Birisine şantaj yapmak için artık onu aylar boyu takip etmek gerekmiyor, telefon hatlarının ucunda bulunan bir bilgisayardan pek çok şey öğrenmek mümkün. Hakkımızdaki bilgilerin, çevreye yayılmasından endişe duyuyor muyuz? Tabii ki hiçbirimiz kredi kartı borçlarımızın, banka hesap numaralarımızın, finans yatırımlarımızın, tıbbi kayıtlarımızın, sabıka kaydımızın, mahkeme kayıtlarımızın ya da herhangi bir kişisel bilgimizin gazetede, internette yayınlaması istemeyiz. Bunu bırakın, arkadaş ya da aile çevremiz tarafından bile öğrenilmesinden rahatsız oluruz. Daha da kötüsü ya birisi hakkımızda bir bilgi yaratıp, bunun doğru olduğunu söylerse, bütün ömrümüzü bunu temizlemek için harcasak da, yapıştırılmış suçlamadan kurtulamayız. Örneklemek gerekirse, birisi suç unsuru olan bir veriyi, bizim kaydımıza işlerse, kendimizi temize çıkartmamız yıllar alabilir. Kendinize ait kredi kartının çalıntı, pasaportunuzun sahte olmadığını ya da kimseyi öldürmediğinizi, bir polise anlatmak zorunda kaldığınızı düşünün. Bir gün kapınızın çalınıp, interpol tarafından aranan azılı bir terörist olduğuz söylenirse, ne yaparsınız? Ya da siz tatildeyken birisi evinizi satarsa... Bu örnekler çoğaltılabilir.Kısaca;

Hayatımız hakkındaki pek çok bilgi dijital ortamda saklanmaktadır.

Hakkımızdaki bilgiler sürekli bilgisayarlar arasında gidip gelmektedir.

Bilgisayarda kayıtlı olan bilgiler %100 doğru değildir.

Yanlış bir yasal kaydı düzeltmek oldukça zordur.

İlk başta çok da tehlikeli görünmeyen bu gibi saldırılar, bir insanı hayatını mahvedebilir.

Tüzel Bilgi Savaşı

Bu grup savaşlarda rekabet ana öğedir. Rakip kuruluşların birbirlerine yaptıkları saldırılar bu gruba girmektedir. Bir milyon dolarlık yatırım yapacak olan bir şirketin, rakibinin sistemini kırarak, on beş milyon değerindeki projesini ele geçirmesi ve rakibini ortadan kaldırması mümkündür. Ayrıca, rakibinin projesini ele geçirmekle kalmayıp, kaza ya da virüs süsü vererek, rakip şirketin konuyla ilgili tüm verilerini de yok edebilir. Bu tarz savaş aslında yeni değil, geçmişi Amerika-Rusya arasındaki soğuk savaş dönemine uzanmaktadır. O dönemki ajanların bilgi toplama çalışmalarına benzemektedir. Ancak günümüzde rekabet için bilgi saldırıları yeni bir boyut kazanmıştır. Sadece şirketler arasında değil, devletler arasında da bu gibi saldırılar yapılmaktadır. Örneğin, bazı devletler yurtdışında eğitim gören öğrencilerinden sadece derslere devam etmekle kalmayıp, bulundukları ülkedeki şirket ya da kuruluşlara stajyer olarak girip, bilgi toplayıp, bu bilgileri devletlerine aktarmalarını istemektedirler. Bu grupta yer alan savaş sadece bilgi edinmek üzerine değil bilgi yaymak üzerine de kurgulanmaktadır. Yayılacak bilgi gerçek ya da gerçek dişi olabilir. Örneğin, bir ilaç şirketi, başka bir ilaç şirketine ait X ilacının kanser riskini arttırdığını, oysa kendi Y ilacının astıma iyi geldiğini ve hiçbir yan etkisi olmadığını bir internet kampanyasıyla hiç kendi adı geçmeden yayabilir. Böyle bir kampanya hemen hemen bedavaya mal olurken, karşı tarafa trilyonlar kaybettirebilir. Buna benzer örnekler de çoğaltılabilir. Böylesi bir saldırı, bir ülkenin kaderini etkileyebilir, bir şirketin iflasına yol açabilir ya da bir politikacının tamamen önünü kapatabilir...

Global Bilgi Savaşı

Bu grupta yer alan saldırı türleri, endüstri, global ekonomi güçlerini, tüm ülke ve devletleri hedef almaktadır. Sadece araştırma verileri üzerine değil, devletler arası sırların çalınmasına kadar uzanan bir çizgide gelişmektedir. Dünya için en tehlikeli olabilecek tür bilgi savaşı da bu gruptur. Artık konu para kaybı ya da kişisel bilgi kaybından öte tüm dünyayı etkileyecek zararları içermektedir. Bilgi savaşı her geçen gün, teröristlere ve birbirine düşman devletlere yeni ufuklar açmakta, yeni yok etme olanakları sunmaktadır. Örneğin, gerekli donanıma sahip bir diktatör Amerika'nın banka sistemini göçertip, Wall Street'i yok edebilir... [5]

VAROLAN ve OLASI BİLGİ SAVAŞI SİLAHLARI

Bilgisayar Virüsleri

"Virüs, kendisini daha geniş programların içine kopya edebilen ve bu programı değiştirilebilen parçalı bir koddur. Virüs ancak içinde bulunduğu program çalışınca, aktif hale geçer. Program çalışınca, virüs kendisini tekrar etmeye başlar ve başka programlara da yayılarak, onları da etkiler." Virüsler, bütün bilgisayar ortamlarında bilinirler. Bilgi Savaşlarında, sıklıkla kullanılan bir savaş aleti olmaları da bu anlamda şaşırtıcı değildir. İstihbarat teşkilatlarının ya da orduların, düşmanlarının telefon sistemlerine virüs yaymaları normal bile karşılanabilir. Günümüz telefon sistemleri, bilgisayarlarla kontrol edildiğine göre, ana vericiye virüs yollamak herhangi bir bilgisayara virüs yollamak kadar kolaydır.

Kurtlar(Worms)

"Kurt (worm) bağımsız bir programdır. Kendi kendine çoğalarak, bir bilgisayardan ötekine kopyalanır, genellikle de bir

network sistemine yayılır. Virüslerden farklı olarak, diğer programlara sıçramaz." Kutlar, veri yok etmemekle birlikte, network içinde dolaşarak, iletişimi yok edebilir. Ancak, bir kurt veri yok edicisine de dönüştürülebilir. Örneğin, bir bankanın network sistemine yerleşen bir kurt, o bankanın şubeleriyle olan tüm iletişimini kesebilir.

Truva Atları (Trojan horses)

"Truva Atı, bir program içinde gizlenen ve gizli bir işlev yapan parçalı bir koddur. Virüsleri ya da kurtları saklamak için sıklıkla kullanılan bir mekanizmadır." Çoğunlukla e-maillerin içine yerleştirilerek yollanan Truva Atları, bir programın içine yerleşir ve o program çalıştırılana kadar, aktif hale geçmez. Truva Atı aktif hale geçince, bir sistemdeki korunmasız host ve serverler hakkındaki bilgileri ele geçirir ve karşı tarafa bulduğu bilgileri yollar. Böylece eğer bilgisayarınıza bir Truva Atı gönderilirse, bilgisayarınız tamamıyla başka birisinin kontrolü altına geçer. Truva atını yollayan kişi, e-maillerinizi okuyabilir, CD-ROM'unuzu açıp kapatabilir, her türlü belgenize ulaşabilir, parolalı bilgilerinizi dahi kolaylıkla okuyabilir. Zekice yazılmış bir Truva Atı, kendisini asla belli etmeyeceği ve hiçbir iz bırakmayacağı için, onun nerede olduğunu bulmak neredeyse imkansızdır.

Mantık Bombası (Logic Bombs)

"Bomba, virüs, kurt ya da başka bir sistemi yaymak için kullanılan bir truva atı türüdür. Bağımsız bir program ya da bir sistem programcısı tarafından yazılmış, bir kod olabilir." Dışarıdan çalıştırılması mümkün olan mantık bombası, bir bilgisayarın harddisk ya da posta dokümanlarının formatını etkileyebilir. Günümüzde büyük yoğunlukla Amerikan yazılımları kullanılmaktadır. Microsoft ya da UNIX sistemleri dünya bilgisayar sistemlerinin neredeyse tamamını ellerinde tut-

maktalar. Bu durumda, Amerikan Devletinin, başka ülkelere ihraç edilen programların hepsine truva atı yüklenmesini istediğini düşünün. Böylece, örneğin CIA, dünyanın her yerinden bilgisayar sistemlerine bağlanarak, istediği her bilgiyi alabilecektir. Ømbalarında olduğu gibi, tüm sistem üreticilerinin böyle bir mekanizmayı başka ülkelere ihraç ettikleri yazılımların içine yerleştirdiklerini düşünün. Böylece tüm bilgi savaşı ajanları, istedikleri her bilgiye elleriyle koymuş gibi ulaşabileceklerdir. Bu belki de, stratejik planlar ve uygulamalar için en kullanışlı yol olacaktır. En canlı istihbaratlar bu şekilde yapılacaktır.

Tuzak Kapıları (Trap doors)

"Tuzak kapısı ya da arka kapı, bir sistemin içine yaratıcısı tarafından yerleştirilen bir mekanizmadır. Tuzak kapısının *fonksiyonu, yaratıcısının sistemin içine, normal sistem koruyucularını* aşarak, sızmasını sağlamaktır." Mantık Bombalarında olduğu gibi, tüm sistem üreticilerinin böyle bir mekanizmayı başka ülkelere ihraç ettikleri yazılımların içine yerleştirdiklerini düşünün. Böylece tüm bilgi savaşı ajanları, istedikleri her bilgiye elleriyle koymuş gibi ulaşabileceklerdir. Bu belki de, stratejik planlar ve uygulamalar için en kullanışlı yol olacaktır. En canlı istihbaratlar bu şekilde yapılacaktır.

Mikroçipler (Chipping)

Yazılımın yanı sıra donanımın içine de bilinmeyen işlevler yerleştirmek mümkündür.Günümüz mikroçipleri, üreticisi tarafından biçimlendirilebilen ve bilinmeyen işlevler yapabilecek olan, milyonlarca entegre devre içermektedir. Bu devreler, bir süre sonra tükenmek üzere yapılabilir, belli bir frekanstan sinyal aldıktan sonra silinebilir ya da radyo sinyalleri yollayarak bulundukları yeri belli edebilirler. Bu ve benzeri senaryolar çoğaltılabilir. Mikroçiplerle ilgili başlıca problem,

çipin, bilgi savaşçısı için kullanışlı ve doğru bir yere yerleştirilip yerleştirememiş olmasıdır. Bu problem de, Bilgi Savaşları ile ilgilenen ülkenin üretilen çiplerin içine ek özellikler yerleştirmesiyle çözümlenmektedir.

Nano Makineleri

Nano makineleri ve mikroplar bir sisteme çok ciddi zararlar verebilir. Virüslerden farklı olarak bu tür savaş araçları, hem yazılıma hem de donanıma saldırıda bulunabilir. Nano makineleri, karıncadan bile daha küçük boyutta robotlardır. Düşmanın bilgi merkezine yayılarak kullanılırlar. Nanolar, bir ofisin içindeki her türlü boşluktan süzülerek, bir bilgisayar buluncaya kadar ilerlerler. Boyutları çok küçük olduğu için, bilgisayarın içindeki en küçük deliklerden bile geçebilirler. Elektronik devreleri kullanılmaz hale getirirler. Donanımı yok etmenin başka bir yolu da özel üretilmiş mikroplardır. Bu mikroplar bildiğimiz kadarıyla yağ yemektedirler. Ya silisyum yiyenleri geliştirilirse? Bir bilgisayar laboratuarındaki tüm entegre devreleri, bir siteyi, bir binayı hatta bir şehri yiyip yok edebilirler

Elektronik Sıkışıklık

Eskiden (bazen günümüzde de), elektronik sıkıştırma metodu, düşmanın iletişim kanallarını bloke ederek, onun bilgi almasını engellemek için kullanılırdı. Bu metodun ikinci aşaması, iletişim trafiğini bloke etmek yerine, düşmanı yanlış bilgilendirmektir. Yanlış bilgilendirme metodu, "Hafif Savaş" başlığı altına da alınabilir.

HERF Silahları ve EMP Bombaları

HERF (High Energy Radio Frequency) Yüksek Enerji Radyo Frekansının kısaltmasıdır. HERF silahları, elektronik bir hedefi, yüksek radyo frekansıyla vurarak, onu saf dışı bı-

rakır. Zarar hafif (ör: sistem kapanır ancak yeniden çalıştırılabilir) ya da çok sert olabilir (ör: sistem donanımı fiziksel zarar görebilir). Elektronik devreler, pek çok kişinin zannettiğinden daha hassastır. Fazla yüklemeyi kaldıramazlar.

HERF silahları aslında, radyo ileticisinden başka bir şey değildir. Hedefe konsantre radyo sinyali gönderirler. Hedef bir binanın tüm network sistemi ya da günümüzün elektronik donanımlı, uçakları, arabaları olabilir. İçindeki insanlar için ölümcül sonuçlar doğuracak, hareket halindeki bir araç da olabilir. EMP (Electromagnetic Pulse) Elektromanyetik Atış anlamına gelmektedir. Kaynak nükleer ya da nükleer olmayan patlamalar olabilir. Oldukça geniş bir alandaki tüm bilgisayar ve iletişim sistemlerini yok etmek üzere, özel kuvvet ekipleri tarafından kullanılır. EMP bombası, HERF'ten daha küçük ebattadır ancak aynı zararı verebilir. EMP tek bir hedefi değil, bombanın etrafındaki tüm donatımı yok eder.[6]

BÖLÜM 3

ABD'NİN SİBER RÜYASI

Siber saldırı beklentisi

1994 yılının Ekim ayında Pentagon'a bağlı olarak çalışan Savunma Bilimi Kurulu raporu, ABD'nin stratejik amaçlı ve sanki birbiriyle bağlantısız "hacker" saldırıları görüntüsü altında ifşa edilen bilinçli bir dış siber saldırıya maruz kalabileceği ve bu saldırıdan ABD'nin haberi bile olmayabileceği konusunda uyarmıştı. Bilgi Savaşı kavramı üzerine çalışmalarını resmi olarak ilk kez 1992 Aralık ayında başlatan ABD Genelkurmayı 1996 yılında Bilgi Savaşlarını ilk kez su şekilde resmi tanıma döktü: Ulusal Askeri Stratejiler doğrultusunda; kendi bilgi ve bilgi sistemlerimizi koruyup,etkin bir şekilde kullanırken, diğer bilgi ve bilgi sistemlerini etkilemek.Bilgi savaşları konusunda ABD savunma çevreleri içinde başı çeken Hava Kuvvetleri'nin Bilgi Savaşları tanımı ise şöyleydi:

"Dost Kuvvetleri benzer eylemlere karşı korurken, düşmanın bilgi ve bilgi sistemlerini iptal etmeye, kullanmaya, çarpıtmaya veya yok etmeye yönelik bilgi ortamında uygulanan her türlü eylem...." Aynı Hava Kuvvetleri bir bilgi saldırısını ise resmi olarak şöyle tanımlamakta: "Düşmanın bilgilerini, bilginin içinde bulunduğu fiziksel ortamı görünürde değiştirmeden, doğrudan bozmak veya; Bilginin içinde bulunduğu fiziksel ortamı görünürde değiştirmeden, düşmanın bilgisini manipule etme veya yok etme yolunda yapılan eylemler."

1996'yılının sonlarına doğru konu ile ilgili raporunu hazırlayan ABD Savunma Bilim Kurulu Bilgi Savaşları ile ilgili yönetime aşağıdaki önerileri getirdi:

*Bilgi Savaşları ile ilgili merkezi bir sorumlu nokta belirleyin. C3I'den sorumlu Savunma Bakan Yardımcısı bu kişi olabilir.

*Bilgi Savaşlarında savunmaya yönelik bir yapı oluşturun.Bir siber saldırı ile ilgili stratejik işaretleri ve uyarıları sağlayabilecek, istihbarat ve tehdit değerlendirmeleri yapabilecek bir merkez kurun.

*Konu ile ilgili bilinci arttırın. Üst düzey hükümet ve endüstri liderlerinin tehditler konusunda bilinçli olmasını sağlayın.

*Kamu altyapılarının bağımlılık ve zaaflarının haritasını çıkarın.

*Tehdit durumlarını ve bu tehditlere verilecek tepkileri belirleyin

*Bilgi Savaşına hazırlık durumunu değerlendirin

*Küçük ve maliyetsiz tedbirlerle, siber alandaki savunma çok büyük oranda geliştirilebilir. Bu tedbirleri uygulayarak, bilgi altyapılarının güvenliğini arttırın

*En kötü senaryoyu göz önünde tutarak, minimum gerekli bilgi altyapısını belirleyin ve kurun

*Bilgi ağlarının güvenliği konusunda ticari ürünler bulunsa da,askeri standartta teknolojiler geliştirmek Ar-Ge çalışmalarına ağırlık verin

*Başarı için kalifiye eleman çalıştırın

*Konu ile ilgili yasal altyapıyı oluşturup,sorunları çözün

*Kritik altyapıların savunulmasında tam rol alın

*Gerekli kaynakları ayırın

1995 yılının Aralık ayında ABD Genelkurmayı Savunma Bakanlığı'na yolladığı ortak planlama dokümanında, gelecek için gerekli olan savaş kabiliyetlerini ise şöyle sıralamıştı:

*Savaş alanı konusunda hakim bilgi,

*Nokta atış kabiliyetleri,

*Düşman ve dostun tanımlanabilmesi,

*Elektronik savaş,

*Bilgi Savaşları,

*Eşzamanlı lojistik.Kuvvetler arasında eşzamanlı olarak bilgi aktarımı.

1990'ların başından itibaren Bilgi Savaşları konusunu her alanda tartışmaya başlayan ABD bu konuda ilk kapsamlı adımlarını yeni atmaya başladı. ABD eski Başkanı Clinton, 22 Ocak 1998 tarihinde Ulusal Bilimler Akademisi'nde yaptığı konuşmada, kimyasal silahlardan siber teröristlere kadar bir çok yönden ülke güvenliğini tehdit altına alabilecek gelişmelere karşı savunmak için 10 milyar dolarlık bir planı açıkladı ve bu 10 milyar doların 1.46 milyarının hükümetin bilgisayar güvenliğinin arttırılması yolunda kullanılacağını söyledi.. ABD Başkanı Kongre'ye sunduğu 2000 yılı bütçe tasarısında ise, kimyasal savaşlardan,siber saldırılara kadar "egzotik terörizm" olarak adlandırdığı tehditlere karşı savunmanın ulusal savunma stratejisinin ağırlık noktasını oluşturacağını belirterek, Kongre'den bu yönde 2.8 milyar dolar vermesini istedi. Clinton, bu miktarın, elektronik terörist saldırılara karşı hızla tepki verebilecek bilgisayar uzmanlarının istihdam masraflarını da içereceğini vurguladı.

22 Mayıs 1998'de Başkan Clinton tarafından yayınlanan 63 numaralı Başkanlık Karar Direktifi(Presidential Decision

Directive) ise yönetimin Kritik Altyapılar ile ilgili politikasının temel belgesi olarak tarihe geçti. Bu direktif kritik altyapıyı, "ekonominin ve hükümetin minimum operasyonu için gerekli olan fiziki ve siber sistemler" olarak tanımlıyordu. Bilgi Savaşı kavramını, bilgi ağlarının da ötesine taşıyan bu rapor ABD'nin konu ile ilgili ulusal politikasını ise şöyle belirliyordu:

"ABD ulusal kritik altyapılarını koruma yeteneğine ve bu yeteneği sürdürebilecek kapasiteye Başkan'ın bu direktifi imzaladığı tarihten en geç 5 sene sonra; bu konu ile ilgili asgari operasyonel yeteneklere ise en geç 2000 yılı içinde ulaşmak zorundadır. Bu noktada kritik fonksiyonların kesilmesine veya manüplasyonuna ancak kısa,sık olmayan,kontrol edilebilir,coğrafi olarak izole ve en az zarar verecek şekilde izin verilebilir."

Direktifte yer alan diğer ana unsurlar söyle sıralanabilir:

*Kritik Altyapıların savunması ile ilgili Federal hükümetin belirleyeceği öncü kurumun belirleyeceği kişiler, kritik sektörlerle işbirliği içinde her bir sektör için, o sektörün konu ile ilgili açıklarını belirleyen,bu açıkları gidermeye yönelik bir plan içeren, sektörün altyapısına yönelebilecek saldırıları teşhis edebilecek ve karşılıklı verebilecek bir sistem öneren bir Ulusal Altyapı Güvence Planı oluşturacaklar.

*Federal Hükümet dört unsur çerçevesinde konu ile ilgili örgütlenecek.

*Her bir altyapı hedefi için, ABD hükümeti içinden bir kurum, ilgili sektörler bağlantı kurmakla görevlendirilecek ve o sektörün bütün içindeki koordinasyonundan sorumlu olacak

*Kritik altyapıların korunmasına yönelik her bir fonksiyonla ilgili olarak, devlet içinde öncü kurumlar belirlenecek ve bu kurumlar fonksiyonel koordinatörler olarak ABD'nin konu ile ilgili faaliyetlerinin koordinasyonunu sağlayacak

*Sektörlerden sorumlu kurum temsilcileri,fonksiyonel koordinatörler,ilgili departman ve kurumlardan temsilciler ki buna Ulusal Ekonomik Konsey de dahil, Kritik Altyapı Koordinasyon Grubu (KAKG) adı altında ve Güvenlik,Altyapı Savunması ve Terörizmden sorumlu Ulusal Koordinatör başkanlığında toplanarak, bu direktifin gereklerinin koordinasyonu ve uygulanmasından sorumlu olacak. Ulusal Koordinatör Başkan tarafından atanacak ve Başkan'ın Ulusal Güvenlik Konularındaki danışmanı aracılığı ile rapor verecek

*Öncü kurumların, Ulusal Ekonomik Konseyin ve Ulusal Koordinatörün tavsiyeleri doğrultusunda, Başkan, altyapı sektörünün önde gelen temsilcileri, eyalet ve yerel yöneticilerden oluşan bir grubu Ulusal Altyapı Güvence Konseyi olarak atayacak.Konsey Başkanı, Başkan tarafından atanacak.

*Her kurum ve departman, özellikle siber ortamdaki sistemlerinin korunmasından kendi sorumlu olacak.Baş Bilgi Yetkilisi kurumun bilgi güvenliğinden sorumlu olacak ve departmanın diğer kritik altyapılarının güvenliğinden sorumlu olmak üzere Baş Kritik Altyapı Güvenliği Sorumlusu atanacak.

*Bu direktifin yayınlanmasından 180 gün sonra her departman ve kurum kendi altyapısının savunmasına yönelik bir plan geliştirecek. Kurumlar arası bağımlılıklarının koordinasyonu Ulusal Koordinatör tarafından üstlenilecek ve KAKG, bu planlarının denetimini gerçekleştirecek. Bu direktifin yayınlanmasından en geç 2 sene sonra bu planlar uygulamaya sokulmuş olmak zorunda. Bu planlar her iki senede bir gözden geçirilecek.

*FBI, mevcut yapılanmasını genişleterek, Ulusal Altyapıyı Koruma Merkezi (National Infrastructure Protection Center - NIPC) kuracak ve bu merkez kritik altyapılara yönelik tehdit-

lerin değerlendirilmesi,uyarı, yasal araştırma ve gerekli tepkiyi gösterme merkezi olarak işlev görecek. Ayrıca Ulusal Koordinatör ve Sektörel Koordinasyon sorumluları, fonksiyonel koordinatörler, Ulusal Ekonomik Konsey temsilcileri ile birlikte kritik altyapıları işleten özel sektör temsilcilerini, konu ile ilgili özel sektör bilgi paylaşma ve analiz merkezi kurması yolunda teşvik edecekler.

ABD Savunma Sektörünün Bilgi Savaşları ile İlgili Kurumsal Altyapısı

1990'larda ABD'de Bilgi Savaşı kavramı doğrultusunda gelişen tartışmalar, bilgi teknolojilerinin hızla toplumun can damarını teşkil eden kritik altyapılar ile ayrılmaz bir şekilde entegre olması nedeniyle Altyapı Savaşları kavramı doğrultusunda sürmektedir. Bu tartışmaları ortak tanımlar ve ortak kurumlar çerçevesinde odaklama çabaları sürse de, ABD'nin savunma kurumları bünyesinde bilgi savaşları ile ilgili yaşanan dağınık yapılanma, yeni çağın gereklerini eski çağın yapıları üzerine monte etmeye çalışan anlayışın güzel bir örneğini teşkil etmektedir. 1994 yılında Savunma Bilim Kurulu'nun raporu sonrasında şekillenmeye başlayan bu dağınık yapılanmanın ana maddeleri ise şöyle sıralanabilir:

*1995 yılı Mayıs ayında Savunma Bakanı Yardımcısı'nın başkanlığında toplanan ve Genelkurmay Başkan Yardımcısını da içeren Bilgi Savaşı Yönetim Kurulu oluşturuldu. Bu kurulu desteklemek üzere, C3I'dan sorumlu Savunma Bakanı Yardımcısı'nın başkanlığını yaptığı bir Bilgi Savaşı Konseyi devreye sokuldu ve C3I'dan sorumlu Savunma Bakan Yardımcısı konu ile ilgili sekreterya işlerini yürütmek üzere 10 kişilik bir Bilgi Savaşları Direktörlüğü oluşturdu.

*1994 Ekiminde servisler arasında imzalanan anlayış notu çerçevesinde, Genelkurmay Başkanlığı bünyesinde Bilgi

Savaşlarının sorumluluğu Operasyonlardan sorumlu Direktörlük, J3, C4I Direktörlüğü arasında paylaşıldı. Bu paylaşım ile ilgili ana sorun hiç kimsenin sorumlu konumda olmaması ve söz konusu bölümlerin iş temposu içinde bilgi savaşları konusuna yeteri kadar zaman ayrılamamasından kaynaklanmaktadır. Saldırı amaçlı Bilgi Savaşı konusunda ise Genelkurmay bünyesinde sorumluluğu Bilgi Savaşları Özel Teknik Operasyonlar Bölümü üstlenmiştir.Bu bölüm, çok gizli teknik operasyonları yürütmektedir.Bu bölüm aynı zamanda Genelkurmay bünyesinde Komuta Kontrol Savaşının bütün unsurlarının koordinasyonundan da sorumludur.

*San Antonio,Texas'da Ekim 1994'te kurulan Birleşik Komuta Kontrol Savaş Merkezi(Joint Command and Control Warfare Center - JC2WC) , operasyonlar sırasında bilgi teknolojilerinin kullanımı ile ilgili doğabilecek sorunlar ve yaklaşımlardan sorumludur. Özellikle ABD'nin yurtdışındaki operasyonları sırasında bu merkez yoğun bir işyükü ile karşı karşıya kalmakta ve bizzat operasyon bölgesine giderek birliklere destek vermektedir.

*Joint Comsec Monitoring Activity (JCMA) yine ABD Genelkurmayı bünyesinde faaliyet gösteren ve 1993 yılında Genelkurmay ve Ulusal Güvenlik Ajansı (NSA) arasında gerçekleştirilen protokol ile kurulmuş olan bir birimdir. Bu kurum savunma bakanlığı bünyesindeki telekomünikasyon ve otomatik bilgi sistemlerinin denetiminden sorumludur.Savunma Bakanlığı'nın telefonlarının dinlenmesinden bu kurum sorumlu değildir. Bilgi sistemlerinin güvenliğini test etmeye yönelik deneyimine JC2WC'dan çok JCMA sahiptir.

* Daha önce Elektromagnetik Uyumluluk Merkezi olarak adlandırılan merkez, 1994 Eylül ayında Genelkurmay J6'sının direktifi ile Joint Spectrum Center (JSC) ismini aldı ve bu

merkez iletişim spectrumlarının denetimi, bu spectrumların yönetimi ve bu spectrumlara sızılmasını veya bloke edilmesini engelleme görevlerini üstlendi. JSC, JCMA ve JC2WC arasında resmi olmayan bir koordinasyon geleneği bulunsa da, operasyonlara da komutanların konu ile ilgili ihtiyaçlarına bu kurumlar ayrı ayrı cevap vermektedir.

*Genelkurmay dışında komutanlıklar bünyesinde ise bilgi savaşları ile ilgili olarak ayrı ayrı merkezler kurulmuştur. Bu konuda öncülük Hava Kuvvetlerinin elindedir. 1995 Eylülünde Hava Kuvvetleri Komutanlığı tarafından yayınlanan ve Hava Kuvvetleri Doktrini'nin Bilgi Savaşlarını da kapsayacak şekilde nasıl yenilenmesi gerektiğini belirleyen raporu öncesinde, 1993 yılı Ekim ayında San Antonio,Texas' da Hava Kuvvetleri Bilgi Savaşları Merkezi kurulmuştu (AFIWC). Bu merkez Hava Kuvvetleri İstihbarat Ajansı'na bağlı olarak oluşturuldu. JC2WC ile yakın çalışan bu merkezin kurulmasının ardından, Hava Kuvvetleri ilk Bilgi Savaşları Birliği'nin 1 Ekim 1995 yılında Güney Carolina'daki Shaw Hava Üssü'nde oluşturdu. Bu birliğin görevi Hava Kuvvetleri Komutanlığı bilgisayarlarını korumak ve düşman bilgisayarlara sızmak olarak tanımlandı.

*Donanma Bilgi Savaşları Faaliyet Birimi (NIWA) 1994 Ağustosunda faaliyete geçirdi. Donanma Güvenlik Grubu'nun altında çalışan bu birim Ford Meade, Maryland'de konuşlanmış durumda ve Ulusal Güvenlik Ajansı ile doğrudan bağlantılı olarak çalışır. Donanma aynı zamanda Filo Bilgi Savaşları Merkezini (FIWC) Little Creek,Virginia'da oluşturdu ve bu grup NIWA ile Atlantik ve Pasifik Donanmaları arasındaki bağı teşkil ediyor. FWIC kısa vadeli operasyonel gerekler üzerinde yoğunlaşırken, NIWA daha uzun vadeli stratejik yaklaşımlarla ilgili bir kurumdur.

*Deniz piyadeleri kendi merkezlerini kurmak yerine, ilgili bilgi savaşı merkezlerine temsilci subayları atadılar ve bu yolla koordinasyonu sağladılar.1995 Şubat ayında onaylanan bir planla donanma ve deniz piyadelerinin Bilgi Savaşları ve Komuta Kontrol konusunda tam bir entegrasyon sağlanması kararlaştırıldı.

*Kara Kuvvetleri Bilgi Savaşı Merkezleri konusundan en son davranan komutanlık oldu. Kara Bilgi Savaşları Merkezi, Ordu İstihbarat ve Güvenlik Komuta Merkezi'ne(INSCOM) bağlı olarak 1995 Mayısında kuruldu. Bu kurum, Hava ve Donanmanın aksine, önceki yapıların yeni donatılarla ve görevlerle bezenmesinden farklı olarak , tamamen sıfırdan oluşturuldu. Bilgi Savaşı Merkezleri arasından personel olarak en düşük sayıya da burası sahip.

*İstihbarat kurumları , yani Savunma İstihbarat Ajansı, Merkezi Haberalma Ajansı ve Ulusal Güvenlik Ajansı, bilgi savaşı ile ilgili faaliyetlerini koordine etmek için kendi aralarında bir ofis kurdular. Aynı zamanda Ulusal Güvenlik Ajansı, 1989 yılında, 1987 yılında yasalaşan Ulusal Bilgisayar Güvenliği Yasası'nın uygulanması için, Ulusal Standartlar ve Teknoloji Enstitüsü(NIST) ile bir anlaşma imzaladı. Bu anlaşma ile NSA, ulusal bilgi güvenliği politikaları konusundan en güçlü kurum haline geldi.

*1963 yılında kurulmuş olan National Communication System'in (NCS) görevi ulusal güvenlik ve acil durum iletişimlerinin koordinasyonunu sağlamaktadır. NCS direktiflerini doğrudan Milli Güvenlik Kurulu'ndan alır fakat Savunma Bakanlığı tarafından yönetilir. Bu kurum hem askeri , hem sivil acil durumlarında faaliyete geçmekle yükümlüdür.

*Reagan döneminde kurulan Ulusal Güvenlik Telekomunikasyon Danışman Konseyi (National Security Telecommunications Advisory Council - NSTAC) Başkana ulusal güven-

lik ve acil durumlara hazır olma konusunda danışmanlık yapmakla görevlidir. Bu yapı, büyük telekomuniskasyon ve savunma bilgi sistemlerini üreten firmaların başkanlarından oluşur.

*Federal İletişim Komisyonu (Federal Communications Commission - FCC) kamu telefon ağının güvenilirliği ve mahremiyet konularında söz sahibidir. 1991 yılında telefon sistemindeki kapsamlı arızalar üzerine FCC, 1992 yılında Ağ Güvenilirlilik Konseyi adı altında yeni bir komisyon oluşturdu ve bu komisyon "Ağ Güvenilirliği" isimli 1000 sayfalık bir doküman hazırladı.FCC 1994 Haziranında bu komisyonun yetkilerini ve görev tanımını değiştirerek, görevini sürdürmesini sağladı. Bugün bu komisyon bünyesinde telefon şirketleri, ekipman üreticileri, eyalet ve federal hükümet temsilcileri, kurumsal ve bireysel tüketici temsilcileri bulunmaktadır.

Görüldüğü üzere, ABD'nin Bilgi Savaşları konusunda kafası hayli karışmış durumdadır. Bu yönde her kurumun kendi bünyesinde konu ile ilgili bir birim açmasının getirdiği zorluklar sadece koordinasyon zorluğu ile sınırlı kalmayıp, aynı zamanda olaya kapsamlı bir yaklaşımı da engellemektedir. Yukarıda bahsettiğimiz ve 22 Mayıs 1998'de ABD Başkanı Clinton tarafından yayınlanan direktif, bu dağınıklığı toparlama yolunda önemli bir adım teşkil etse de, raporun özü yine de varolan kurumların koordinasyonu yönünde adımlar içermektedir. ABD'deki mevcut durumun belli başlı zaafları ise şöyle sıralanabilir:

*Bilgi Savaşları konusunda askeri kesimin üzerinde anlaştığı doktrinel bir tanım bulunsa da, özel sektörü de kapsayan bir uzlaşma sağlanamamıştır. Bilgi çağında güvenlik sorununun artık sadece askeri kesimi ilgilendirmediği göz önüne alındığında, ortak kavramlar üzerinde sivil-asker uzlaşmasının sağlanması büyük önem taşımaktadır.

*Bilgi Savaşları ile ilgili tartışmalar şekillenirken, Toffler, gibi savunma çevrelerinde büyük prim yapan fakat bazı akademisyenlerce "azgelişmiş mtv mantığı" taşımakla suçlanan kişilerin yeni çağın savunma doktrinlerinin şekillendirilmesinde büyük ağırlık taşıdığı gözlemlenmektedir. Yeni savunma doktrinlerinin şekillenmesine, medyatik figürlerin kulağa hoş gelen genellemelerinden çok, akademisyenlerin bilimsel tartışmaları önayak olmalıdır.

*Kurumlar bünyesinde bilgi savaşları ayrı bir operasyonel alan olarak algılandığı için, her kurum kendi bünyesinde konu ile ilgili yeni yatay ve dikey hiyerarşiler yaratmakta ve bu hem kurum içi hem kurumlar arası yeni koordinasyon sorunları ortaya çıkmaktadır.

*Bilgi Savaşları'nın savunma ve saldırıdan oluşan iki yüzü bulunduğu gözönüne alınırsa, ABD'nin savunma yönüne ağırlık verirken, saldırı yönündeki stratejisini yeteri kadar geliştiremediği gözlemlenmektedir. Bu eksiğin arkasında, dünyanın en gelişmiş bilgi ağlarına sahip olan ülke olmaları nedeniyle, olası bir siber saldırıya en açık ülke olmaları gerçeği ve bu zaaftan dolayı herhangi bir saldırgan tavrın rakiplerin çok daha acımasız bir saldırısını kışkırtabileceği endişesi yatmaktadır.

*Kendi devlet yapısı içinde gerekli mekanizmaları ve yapıları oluşturmaya çalışan ABD, özel sektör ile uyumu temsilciler ve koordinatörler ile sağlamaya çalışmaktadır ki, bu sivil ile asker çizgisinin iyice kaybolacağı gelecekte, gerekli verimi sağlamayacaktır. Devlet , özel sektör ve vatandaş önceden üzerinde tartışılan ve uzlaşılan bir ortak mutabakat çerçevesinde yeni çağın savunma yapılarını birlikte oluşturmak zorundadır.

*ABD'nin sivil kesimle dayanışmasının firmalarla sınırlı olduğu görülmektedir. Halbuki sivil kesim sadece firmalardan

ibaret olmayıp, kritik altyapılar konusunda devlete önemli destek sağlayabilecek sivil toplum kuruluşları ve bilgisayar güvenliği çerçevesinde hayli yetkin bireyleri de içermektedir. Devlet, bir protokol çerçevesinde bu kurumlara "milli servet" gözü ile bakmalı ve tehdit durumlarında bu güçlerden gerektiği şekilde yararlanmalıdır. Bu açıdan "hacker"larını yakalayıp hapse atan ABD ile, bu yetenekleri sisteme kazandırıp, devlet adına çalıştıran İsrail iki ayrı yaklaşımı temsil etmektedir.

Ağustos (2001) başında Çin Ordusu'nun yayın organı olan "The Liberation Army Daily" gazetesinde, siber savaş yeteneklerine sahip sivillerden ve askeri personelden oluşan yeni bir birim oluşturulması gerektiği yolunda bir haber yeraldı. Bu haber, ABD'nin Çin'in Belgrad'daki büyükelçiliğini "yanlışlıkla" bombalamasının ardından, ABD'deki bir çok bilgisayar sisteminin Çin kaynaklı siber saldırılara maruz kalmasının ertesinde yayınlandı. Son günlerde bilgi coğrafyasında sıkça duyulmaya başlanan bu tür haberler, 1980'lerden bu yana küresel anlamda varolmaya başlayan ve siber korsanların dilediklerince cirit attıkları bu coğrafyada artık devletlerin de ciddi anlamda bayrak göstermeye başladığının işaretidir. Bu coğrafyada oluşan yeni dengeler çerçevesinde, devletler sadece siber korsanlara karşı değil, diğer devletlere karşı da aktif güvenlik politikaları uygulamak zorunda kalacaklardır. Bilgi coğrafyasında yaşanan çatışmaların sessiz ve kansız olma özelliği, bu coğrafyada devletlerin ve devlet dışı unsurların karşı tarafa saldırma ve zarar verme eğilimini artıran bir özellik olmasından dolayı, diğer coğrafyaların aksine bilgi coğrafyası fütursuz davranışları primlendiren yapısı ile, dünyanın en "kanlı" ve "gürültülü" coğrafyası olma özelliğini kazanacak; devletler ve devlet dışı unsurlar birbirleri ile sürekli çatışma ve aktif savunma halinde olacaklardır.Türkiye

bu coğrafyanın bilincinde olarak, aktif bir savunma ve saldırı doktrini geliştirmeli ve bilgi çağının bu yeni güvenlik anlayışını mevcut yapılara eklemlemek yerine, toplumsal yapılanmasını bu yeni güvenlik doktrini çerçevesinde oluşturmalıdır.Burada önerilecek olan bilgi çağı güvenlik şablonu aşağıdaki temel direklere dayanmaktadır:

a) Savunma ve Saldırı Politikası

b) Yasal Çerçeve ve Toplumsal Mutabakat

c) Kritik Altyapılar

d) Sivil ve Askeri Siber Güçler

e) Stratejik Sektör ve Ürünler

Kritik Altyapılar

ABD'de Başkan'ın talimatı ile sektör ve devlet temsilcilerinden oluşan bir ekip, ülkenin en kötü şartlar altında ayakta kalabilmesi için gerekli olan en elzem altyapıları tespit etmek için toplanmıştır. Söz konusu direktif altyapıyı, "ekonominin ve hükümetin minimum operasyonu için gerekli olan fiziki ve siber sistemler" olarak tanımlarken, Başkan tarafından oluşturulan ve ilgili her devlet birimi ile sektörden temsilcilerin oluşturduğu bu komite, ulaştırmadan, su sistemlerine, uydu iletişim sistemlerinden dağıtım sistemlerine kadar çok geniş bir yelpazede ABD'nin kritik altyapısını tespit etmiştir. Bu yapıların tespitinden sonra, söz konusu yapıların güvenlik açısından birbiri ile koordinesi, saldırılara karşı korunması, v.s. gibi konularda yürütme ve denetlemeyi üstlenecek idari, teknik ve yasal alt ve üst yapılar oluşturulmuştur. ABD'deki çıkar mekanizmaları doğrultusunda bu oluşumlar genellikle devlet yetkilileri ile özel sektör temsilcilerinden oluşan karma yapılar sergilemektedir. [7]

BÖLÜM 4

ENFORMASYON SAVAŞININ AŞAMALARI

ABD Hava Kuvvetleri Akademisi bünyesindeki Ulusal Stratejik Araştırmalar Enstitüsü (Institute for National Strategic Studies), enformasyon savaşını şu aşamalarda ele alıyordu:

1. Komuta-kontrol savaşı,
2. İstihbarat odaklı savaş,
3. Elektronik savaş,
4. Psikolojik savaş,
5. Hacker ve siber savaş,
6. Ekonomik enformasyon savaşı.

ABD Başkanı George W. Bush, (2001) temmuz ayında Brüksel'de gerçekleştirilen NATO Zirvesi'nde, ABD'yi hedef alan siber saldırıların kitle imha silahları kullanılarak yapılan saldırılarla aynı anlamı taşıdığını söylemişti.

Sanal saldırıya gerçek mermi

Şubat 2002'de ABD Senatosu'nda bir alt komitede konuşan Bush'un en üst düzey sanal güvenlik danışmanı Richard Clarke ise, birçok kişinin kanını donduran şu sözleri dile getirdi: "Şer ekseninde yer alan Iran, Irak ve Kuzey Kore'nin yanı sıra Çin ve Rusya da ABD'ye karşı siber askerler yetiştirmektedir. Altyapımızı hedef alabilecek bu saldırılara bundan sonra aralarında askeri operasyonların da bulunduğu tüm

olanaklarla karşılık vereceğimizi duyururuz." Bush'un ve güvenlik danışmanının sözleri, İmparatorluğun enformasyon savaşını ne kadar önemsediklerini ortaya koyuyor. Bütçede "sanal güvenlik" harcamalarına ayrılan kaynak da bunu doğruluyor. ABD hükümeti, 2002 yılı içinde 2,7 milyar dolar , 2003'de ise 4,2 milyar dolar harcayacağını açıkladı.

Peki ama bu devasa bütçe gerçekten de "güvenlik"e mi harcanacak? O konudaki kuşkuların tamamen hakli olduğunu ABD'nin bizzat kendisi haklı çıkarıiyor: Genel Denetim Kurumu'nun (U.S. General Accounting Office) 2000 Eylül'ünde yayınladığı bir rapora göre 24 kamu kuruluşundan16'si denetim sonucunda "F" puanını, yani "çok zayıf" aldı. Bunun anlamı, ABD'nin "sanal güvenlik" adı altında ayırdığı milyarlarca doların gerçekten de sanal kamu güvenliğine ayrılmadığı. Peki paralar nereye gidiyor? Saldırı ve taarruz amaçlı projelere!..[6]

Burada ortaya çıkan bir başka soru ise 1945 yılından bu yana dünyanın süper gücü ABD gerçekten bir sanal tehlike ile karşı karşıya mı ? Yoksa ABD, dünyayı kontrol etme, izleme ve dinleme adına bazı ülkeleri sözde potansiyel tehdit gösterip, kendi projelerine geçerlilik kazandırmak mı istiyor ? Kuşku dolu bu çalışmalara milyarlarca dolar ayıran ve bir Pearl Haurbor'a göz yummuş olan ABD'nin dünyada söz sahibi olma adına neler yapabileceğini kestirmek gerçekten güç değil....

Sanal dünyayla bütünleşen saldırganlık

Merkezi Berlin'de bulunan Enformasyon Toplumu ve Güvenlik Politikaları Araştırma Grubu'nun (Fog:IS) verileri somut olarak ortaya koyuyor ki: ABD, 1990'lu yıllardan itibaren yoğunlaşarak enformasyon savaşı alanında saldırı ve taarruz amaçlı faaliyet göstermek üzere, düzinelerce askeri birim

ve eğitim kuruluşunu hayata geçirdi.Bu birimlerin listesi, ABD'nin saldırgan tavrının, sanal ortamla bütünleşerek daha da geliştirileceğinin somut bir kanıtı.Geçtiğimiz ayın sonunda ABD Hükümeti'nin terörle mücadele amacıyla bir dezenformasyon bürosu kurduğunu ve ardından, gelen tepkiler üzerine bu büroyu dağıttığını duyurması dahi bir bakıma bu enformasyon savaşı mekanizmasının bir hamlesiydi.

Müttefiklerin de canı yanacak

ABD, "şer ekseni" ve terörü gerekçe göstererek enformasyon savaşı alanında "ağır silahlanma" hareketi içindedir. ABD'nin söz konusu stratejik yönelimi, yalnızca "düşmanları"nin değil, zaten ECHELON'dan canı yanan "müttefiklerinin" de benzer faaliyetler yürütmesini kaçınılmaz kılacak. Fog:IS'in verilerine göre, ABD ordusuna bağlı ve enformasyon savaşı alanında taarruz ve saldırı amaçlı olarak faaliyet gösteren kuruluşlar şöyle sıralanıyor:

I. MERKEZİ KURULUŞLAR

1-Savunma Bakanlığı-Department of Defense (DoD) Merkezi Washington D.C., Pentagon'da. Bakanlığa bağlı enformasyon savaşı birimleri:

* **Office of the Assistant Secretary of Defense (C3I)**-Komuta-kontrol, iletişim ve istihbarat sistemleri (command, control, communications and intelligence) alanında görev yapan müsteşar. Savunma Bakanı'nın enformasyon savaşı konularında danışmanı, ayrıca politik-stratejik planlama ve örgütlenmeden sorumlu. Pentagon'un Enformasyon Savaşı yöneticisi.

* **Directorate for Information Warfare** - C3I'den sorumlu müsteşarı enformasyon savaşı planlama ve icrası sırasında destekler.

* **Information Warfare Executive Board (IWEB):** Savunma Bakan yardımcısı tarafından yönetilir. Planlama ile enformasyon savaşının siyasi gelişmelere yansıması ve hukuksal açıdan değerlendirilmesinden sorumludur.

* **Information Warfare Council (IWC)**- IWEB'e düzenlediği seminerler ve sanayi ile doğrudan kurduğu bağlantılarla destek verir.

* **Deputy Assistant Secretary of Defense (Security & Information Operations):** ABD'nin enformasyon sistemlerinin korunmasına yönelik birimdir.

2. Genelkurmay Başkanlığı-Joint Staff Merkezi Washington D.C. :Pentagon'da. Enformasyon savaşı alanında kuvvet komutanlıkları kendi bünyelerinde "silahlandıklarından", genelkurmay başkanlığının pek etkin olmadığını söylemek mümkün. Yine de ABD Genelkurmay Baskanlığı'na bağlı iki birim bulunuyor:

* **J-33-Special Technical Operations Division**-Operasyonlardan sorumlu J-3 Karargahının bir parçası. Genelkurmay'a destek vermekle yükümlü, ancak Ulusal Güvenlik Kurulu, CIA ve NSA'ya da enformasyon operasyonlarının icrası sırasında yardımcı oluyor. Bu tür harekatlarla ilgilenen en üst askeri birim. Pentagon'un "çok gizli" departmanlarından Özel Teknik Operasyonlar Merkezi'ni (Special Technical Operations Center) yürütür, yine aralarında hacker savaş yönetimi, enerji silahları ve stratejik savaş yönlendirmesinin de bulunduğu pek çok görevi icra eder.

* **J6K-Information Warfare Division**-Enformasyon sistemlerinden sorumlu ("Information Systems CHECK") J-6 Karargahının bir parçası. Savunma amaçlı siber savaş yönetiminde genelkurmaya destek verir. Gerekli güvenlik önlemlerinin geliştirilmesi ve icrasından sorumludur.

3. Savaş Analiz Genel Karargahı- Joint Warfare Analysis Center (JWAC):Merkezi Virgina, Dahlgren'de yer alır. Altyapı ağlarına saldırı için hedef ve silah seçimi konusunda teknik analizler hazırlar, daha sonra bu analizlerin değerlendirilmesinde de görev alır. Dünyanın birçok ülkesinin altyapıları hakkında verinin toplandığı bu birimde JWAC, genelkurmaya olasi hedeflerin belirlenmesi için çalışır.

4. Hava Komuta Karargahı-US Space Command : Merkezi Colorado, Peterson hava üssündedir. Ekim 99'dan itibaren ABD silahlı kuvvetleri bilgisayar sistemlerinin güvenliğinden, ekim 2000'den sonra da bilgisayar saldirilarindan sorumlu oldu. Bünyesindeki birim:

***Bağımsız Stratejik Öneri Grubu-** (Independent Strategic Advisory Group-Computer Network Defense/ Computer Network Attack): Başkanlığını Hava Kuvvetleri Akademisinde siyaset bilimleri profesörlüğü yapan General James P. McCarthy'nin yaptığı, savunma ve saldırı amaçlı bilgisayar saldırıları alanında danışmanlık yapan bir kurul.

5. Joint Task Force-Computer Network Operations (JTF-CNO)- Merkezi Virginia, Arlington'dadır. US Space Command'in bir parçası. Savunma ve saldırı amaçlı gerçekleştirilen askeri bilgisayar ağı operasyonlarının koordinasyonundan sorumlu. ABD silahli kuvvetlerine bilgisayar hizmetleri sunan Defence Information Systems Agency (DISA) bünyesinde yer almaktadır.

6. Joint Information Operations Center (JIOC)- Merkezi Texas'daki Kelly Hava Üssünde yer almaktadır. Bu birimde kuvvet komutanlıklarından yaklaşık 150 kişinin yani sıra üç müttefik ülkenin (bu ülkelerin Kanada, İngiltere ve Avustralya'nın olduğu tahmin edilmektedir) askeri temsilcileri yer almaktadır. Ekim 1998'de kuruluşu gerçekleşti. Tüm kuvvet komutanlıklarının merkezi destek ve araştırma birimi. NSA ve

Hava Kuvvetleri İstihbarat Ajansı ile çok yakın çalışmaktadır. Bilgisayar savaşlarının icrasının yanı sıra psikolojik savaş, kesif, elektronik savaş ve benzeri operasyonların icra edilmesi de görev alanlarına girer. JIOC, askeri operasyonların gerçekleştirildiği bölgelere 10'ar kişilik timler gönderir.

NSA:300 bini aşkın personel!

7. Ulusal Güvenlik Ajansı/Merkezi Güvenlik Hizmetleri- National Security Agency (NSA)/Central Security Service (CSS): Merkezi Maryland, Fort Meade'dedir. ABD silahlı kuvvetlerinin istihbarat ve karşı istihbarat örgütüdür. Yeryüzünün hemen her yerine dağılmış üsleri bulunur. Matematikçiler için dünyadaki en büyük işveren olarak kabil ediliyor ve ayni zamanda bilgisayar teknolojileri alanındaki özel gelişmelerin kaynağı... Örgüt hakkında tam bir gizlilik söz konusudur; personel sayısının 300 bini aştığı tahmin edilmekte, bütçesi ise kamuoyuna yansıtılmamaktadır. NSA bünyesinde yer alan enformasyon savaşı birimleri:

* **P42 Enformasyon Savaşı Destek Birimi** -(Information Warfare Support Cell): NSA'nın gizli programlarında "Özel Teknik Ofisi" olarak da hizmet veren birim bünyesinde siber saldırı amaçlı hedef tesbiti ve keşif uzmanları yer almaktadır.

* **National Security Incident Response Center (NSIRC)**- Bilgisayar güvenlik sorunları hakkında bir merkezi veritabanını yürütmektedir. Hacker teknikleri hakkında ayrıntılı bilgiyi derleyerek sunmakla görevlidir.

8. Teknik Enformasyon Operasyonları Merkezi-Information Operations Technical Center (IOTC): Merkezi Maryland, Fort Meade'dedir. NSA, CIA ve ABD Genelkurmay'ının ilgili birimlerinin işbirliğiyle 1997 yılında kuruldu. NSA ile yakın şekilde çalışarak enformasyon savaşında kullanılmak üzere özel teknolojiler geliştiriyor.

9. Enformasyon Sistemleri Savunma Ajansı-Defense Information Systems Agency (DISA): Merkezi Virgina, Arlington'dadır. Pentagon'un altyapısını yürütür. Muhtelif enformasyon sistemlerini planlar, geliştirir, diğer sistemlere entegre eder ve birçoğunun da isletilmesini sağlar. ABD silahlı kuvvetleri savunma amaçlı enformasyon savaş etkinliklerinin teknik koordinasyon merkezidir. [8]

II. KUVVET KOMUTANLIKLARINA BAĞLI KURULUŞLAR

1. Hava Kuvvetleri Komutanlığı-Department of the Airforce. Merkezi Washington D.C., Pentagon'da. ABD silahlı kuvvetleri bünyesinde enformasyon savaşını teknik ve operasyonel kullanmaya dönük en hızlı ilerleme kaydeden hava kuvvetleri komutanlığıdır. Bünyesinde konuyla ilgili oluşturduğu birimler:

***Enformasyon Savaşı Bölümü**-Information Warfare Divison (XOFE): Operasyon ve strateji planlamasından sorumlu.

***Özel Programlar Bölümü**-Special Programs Division (INXI): "Düşmanlar ve olası düşmanların" sistemleri ve teknikleri hakkında keşif icra eder.

***Hava Kuvvetleri Özel Soruşturmalar Bürosu**-Air Force Office of Special Investigations : ABD hava kuvvetlerindeki bilgisayar ağı sızma ve kırma olaylarını araştırır. Bu amaçla kullanmak üzere Bolling hava üssünde bir laboratuar da kurdu.

***Enformasyon Koruma Bölümü**-Information Protection Division : Bilgi teknolojileri güvenliğinden sorumlu.

***Elektronik Sistemler Merkezi**-Electronic Systems Center : Elektronik programlar yürüten bu birim, kendi bünyesinde bir enformasyon savaşı bölümü de kurmuş durumda.

***Rome Laboratuvarı**: ABD Hava Kuvvetlerinin araştırma laboratuarı, kendi organizasyonu kapsamında çalışan ve enformasyon savaş teknolojileri üzerinde faaliyet gösteren bir birime sahip.

* IWTPIPT : Görev alanı, enformasyon savaşı teknolojilerinin ABD hava kuvvetlerinde uygulanmasıdır.

2. Hava İstihbarat Ajansı-Air Intelligence Agency (AIA)Merkezi Texas'daki Kelly Hava Üssü'ndedir. 1993 Ekim ayında kuruldu. Şubat 2001'den beri Hava Harp Karargahı'nın (Air Combat Command) bir parçası. Operasyonel enformasyon savaşı konusunda en büyük organizasyon. Bilgisayar saldırılarının yanı sıra elektronik savaş uygulamaları, kitle iletişim araçları, keşif ve diğer operasyonlardan sorumlu. AIA'nin yaklaşık 16 bin personeli var. NSA ve DIA ile yakın işbirliği içinde çalışıyor. 1,1 milyar doları bulan yıllık bütçesi hava kuvvetleri, NSA ve DIA tarafından ortaklaşa paylaşılıyor.

3. Hava Kuvvetleri Enformasyon Savaşı Merkezi-Air Force Information Warfare Center (AFIWC) Merkezi Texas'daki Kelly hava üssündedir. Hava Kuvvetleri enformasyon savaşı etkinliklerinin ana birimi. 1993 Eylül ayında kuruldu. Taktik operasyonlar, simülasyon, eğitim-geliştirme, araştırma ve destek, görev alanlarından. İstek durumunda, komuta düzeyine destek vermek üzere askeri operasyonların gerçekleştirildiği yerlere 25'er kişilik "enformasyon savaşı ekipleri" gönderiyor. AFIWC'ye bağlı birlikler, ABD dışında Güney Kore'deki Osan hava üssü, Almanya'nın Ramstein kentinde bulunan ABD hava kuvvetleri ana karargahı ve 2000 yılından beri de Hawaii'deki ABD hava kuvvetleri karargahında yer almaktalar.

4. Hava Kuvvetleri Araştırma Laboratuvarı-Air Force Research Laboratory (AFRL) Merkezi New York, Rome'da-

dır. Enformasyon savaşı teknolojileri alanında çalışan bir birime sahiptir.

5. Deniz Kuvvetleri Komutanlığı-Department of the Navy Merkezi Washington D.C., Pentagon'da. Konuyla ilgili oluşturduğu iki birim var:

***Enformasyon Savaşı/Savaş Komuta Kontrol Bölümü**-Information Warfare/Command and Control Warfare Division (N64): ABD Deniz Kuvvetleri Komutanlığı karargahının bir parçası. Deniz kuvvetlerine bağlı birliklerin enformasyon savaşı etkinliklerinin planlaması ve uygulamasından sorumlu.

***Enformasyon Savaşı ve Enformasyon Yönetimi Bürosu-** Information Superiority & Sensor Security (N812D) bölümünün bir parçası. Tedarik ve enformasyon savaşı alanında *"silahlanmadan" sorumlu.*

6. Hava ve Deniz Savaş Sistemleri Karargahı-Space and Naval Warfare Systems Command.Merkezi California, San Dieogo'da. Bünyesindeki PD-16 birimi, deniz kuvvetlerine enformasyon savaşı sistemleri geliştirmekte ve destek sunmaktadır. ABD Deniz Kuvvetleri tedarik faaliyetlerinin merkezi koordinasyon kuruluşu ve NSA ile iletişim noktası olarak görev yapmaktadır.

7. Deniz Enformasyon Savasi Harekati-Naval Information Warfare Activity (NIWA) Merkezi Maryland, Fort Meade'dedir. 1994 Ağustos'unda kurulmuştur. NSA bünyesindedir ve ABD Deniz Kuvvetleri enformasyon savaşı faaliyetlerinin teknik koordinasyon merkezidir. Enformasyon savaşında kullanılacak teknolojiler için Ar-ge faaliyetleri yürütmekte, ayrıca teknoloji de tedarik etmektedir. NIWA'ya "enformasyon savaşı için silahlanma" projelerini geliştirme ve tedarik etme konusunda özel yetki verilmiştir.

8. Filo Enformasyon Savaşı Merkezi-Fleet Information Warfare Center (FIWC) Merkezi Virginia, Little Creek Amphibious üssünde yer almaktadır. 1995 Ekim ayında kurulmuştur. NIWA ile ABD Atlantik ve Pasifik donanmaları arasında bağlantı işlevi görmektedir. ABD Deniz Kuvvetleri'ne bağlı tüm uçak gemilerinde personeli bulunmaktadır. NIWA uzun vadeli çalışmalar yürütürken FIWC, enformasyon savaşında somut ve operasyonel uygulamalara imza atar.

9. Kara Kuvvetleri Komutanlığı-Department of the Army Merkezi Washington D.C., Pentagon'da. Konuyla ilgili birimleri:

***Enformasyon Operasyonları Bölümü**

***IW General Officer Steering Group**-ABD Kara Kuvvetleri'nde enformasyon savaşı yöntemlerinin icrasından sorumlu birçok çalışma grubundan biri. Bu birim planlama ve operasyon yönetimini koordine etmenin yanı sıra Enformasyon Operasyonları bölümüne de danışmanlık hizmeti vermektedir.

10. Kara Enformasyon Savaşı Harekatı-Land Information Warfare Activity (LIWA) Merkezi Virgina, Fort Belvoir'dadır. 1995 Mart'ında kurulan birim, İstihbarat ve Güvenlik Karargahı'nın (U.S. Army Intelligence and Security Command) bir parçasını oluşturmaktadır. Operasyon halindeki komutanlara destek sağlamaktadır. Bu destek kapsamında çatışma bölgelerine ekipler de yollar. Kuvvet komutanlığının "zayıf ve saldırılabilir noktalar"ı ortaya çıkarma analizi çalışmalarında, kendisine bağlı "Kızıl Ekipler" (Red Team) ve Bilgi İşlem Acil Karşılık Ekipleri (Computer Emergency Response Teams) ile yer alır.

11. İstihbarat ve Enformasyon Savaşı Karargahı- Intelligence and Information Warfare Directorate Merkezi New

Jersey, Fort Monmouth'dadır. Bu bölüm kapsamında enformasyon savaşı için iki birim kurulmuştur:

*__Ar-ge ve Mühendislik Merkezi__-Research Development and Engineering Center : Elektronik savaş uygulamaları, dinleme, bilgisayar operasyonları vb alanlarda Ar-ge çalışmaları yürütmektedir.

*__Yazılım Mühendisliği Merkezi__-Software Engineering Center : Enformasyon savaşı uygulamaları için yazılımlar geliştirmektedir.

12. Marine Corps (MC) Merkezi-Virginia, Quantico'da yer alan Marine Corps Karargahı'ndadır. Aslında pek enformasyon savaşı uygulamalarıyla içli dışlı olduğu söylenemez. Gerekli durumlarda diğer kuvvet komutanlıklarının olanaklarından yararlanır. Bu, söz konusu birimlerde bulunan irtibat subayları aracılığıyla gerçekleşir. Yine de MC bünyesinde konuyla ilgili iki birim bulunmaktadır:

*__Enformasyon Savaşı Çalışma Grubu__-Information Warfare Working Group :Enformasyon savaşı uygulamalarının eşgüdümünden sorumludur.

*__Assistan Chief of Staff for C4I/Director of Intelligence__- Savunmaya dönük enformasyon savaşı uygulamaları icra eder.[9]

III. EĞİTİM VE GELİŞTİRME AMAÇLI KURULUŞLAR

1-__Enformasyon Savaşı ve Strateji Okulu__-School of Information Warfare and Strategy Merkezi Washington D.C., Fort McNair'dedir. 1994 yılında, Ulusal Savunma Üniversitesi (National Defence University) bünyesinde kurulmuştur. Askeri strateji ve operasyonlar alanında ar-ge etkinlikleri icra eder, enformasyon savaşı alanında subayları eğitir.

2. Müşterek Komuta, Kontrol ve Enformasyon Savaşı Okulu-Joint Command, Control & Information Warfare School (JCIWS) Merkezi Virginia, Norfolk'dadır. Enformasyon savaşı operasyonları için eğitim verir.

3. Hava Kuvvetleri Akademisi-Air Force Academy Merkezi Colorado, Colorado Springs'dedir.

***Ulusal Güvenlik Araştırmaları Enstitüsü**-Institute for National Security Studies: Çok uzun süredir enformasyon savaşı uygulamalarını stratejik, tarihi ve hukuki yönden işleyen bir araştırma programı.

4. Hava Öğretileri Araştırma ve Eğitim Yüksek Okulu-College of Aerospace Doctrine Research, and Education (CADRE) Merkezi Alabama, Maxwell hava üssünde yer almaktadır. Operasyonlar alanında eğitim ve geliştirme hizmeti vermektedir. CADRE bünyesinde bir Enformasyon Savaşı bölümü yer almaktadır.

5. Deniz Lisansüstü Okulu-Naval Postgraduate School Merkezi California, Monterey'dedir. Okul bünyesinde bulunan Enformasyon Savaşı Akademi Grubu, enformasyon savaşı uygulamalarında ar-ge çalışmaları gerçekleştirmektedir. Oldukça etkin bir isim olan, Pentagon danışmanı John Arquilla tarafından yönetilir. Arquilla, "enformasyon savaşı" kavramını ilk ortaya atan kişi olarak bilinmektedir.

6. Deniz Savaş Yüksek Okulu-Naval War College Merkezi Massachusetts, Newport'da bulunmaktadır. Okulun komutanlığı 1998 temmuz ayından beri Amiral Arthur K.Cebrowski tarafından yürütülmektedir. Cebrowski, daha önce ABD Deniz Kuvvetleri Komutanlığı bünyesindeki enformasyon savaşı uygulamaları da görev alanına giren N6 departmanının sorumluluğunu üstlenmiş, ayrıca komutanlık bünyesinde "2000 yılı krizi"ni yönetmişti.

7. Kara Kuvvetleri Savaş Yüksek Okulu-Army War College Merkezi Pennsylvania, Carlisle'dedir. Okul bünyesinde yer alan Stratejik Arastırmalar Enstitüsü, enformasyon savaşı ve ilgili alanlarda da stratejik-askeri araştırmalar gerçekleştirmektedir.

8. Dış Askeri Araştırmalar Ofisi-Foreign Military Studies Office Merkezi Kansas, Fort Leavenworth'dadır. ABD dışındaki ülkelerin askeri yapılanmaları, teknik donanımları ve stratejik yansımaları hakkında araştırmalar icra eder. Uzun süredir enformasyon savaşı alanında çalışan bir isim olarak bilinen Timothy L. Thomas da bu birimde görev yapmaktadır.[10]

ELEKTRONİK HARP VE SENARYOLAR

Günümüzde askeri birimlerin küçülmesi, hareket kabiliyetlerinin artması ve modernleşmesi, haberleşme ihtiyacının çeşitlenmesine ve daha fazla önem karasına neden olmuştur. Haberleşmenin kesiksiz ve güvenilir olması amacıyla, teknolojinin imkanları ile birlikte çeşitli Elektronik Korunma Tedbiri (EKOT) teknikleri geliştirilmiştir. Bu gelişmeler Elektronik Karşı Tedbir cihazlarının da yeniden gözden geçirilmesine ve bazı konseptlerin değişmesine sebep olmaktadır. Bu yazıda Haberleşme Elektronik Harp (EH) cihazlarının sistem özelliklerinin belirlenmesindeki yaklaşım açıklanmaktadır.

HF' den çok kanallı telsizlere kadar uzanan haberleşme frekans bantları, , hem çok geniş hem de bu bantlardaki telsiz faaliyetleri çok yoğundur. Bu frekans bandını kapsayabilecek ve onlarca çevrime karşı etkili olabilecek bir Elektronik Harp (EH) sistemi geliştirilmesi çok güç hatta imkan sızdır. Bu nedenle, geliştirilecek EKT sisteminin özelliklerini doğru olarak saptamak gerekmektedir.

Haberleşme Elektronik Karşı Tedbir cihazlarının sistem gereklerinin belirlenmesi için gerçek ortama yakın senaryoların hazırlanması gerekmektedir. Barış zamanı, bu senaryolara cevap verebilecek EH sistemlerinin. geliştirilmesi, kriz döneminde sürprizlerle karşılaşılması ihtimalini en aza indirir. Düşman haberleşme ağının zafiyete uğratılması ancak ortamdaki hangi telsizlerin öncelikle karıştırılması gerektiğinin bilinmesi ile mümkündür. Düşman için en kritik haberleşme birimlerinin belirlenmesi ise ilgili hedeflerin teknik ve taktik özelliklerinin çok iyi analiz edilmesi ile mümkün olabilir. Bu da senaryo ve değerlendirme çalışmaları yapılması ile gerçekleştirilir. Bu çalışmalar üç başlık altında toplanabilir:

* Senaryolar,

* Senaryoların değerlendirilmesi,

* Veri Tabanı.

Senaryolar değişik yoğunluktaki ortamlar için hazırlanmalı ve sayısal değerlerle ifade edilebilmelidir. Yüksek yoğunluklu tel siz haberleşmesi gerektiren ve kolordu (Corps) seviyesinde kuvvetlerin dağıldığı bir ortam için hazırlanacak senaryo, gerçek kriz dönemi için iyi bir örnektir. Ancak düşük yoğunluklu telsiz haberleşmesinin olduğu ve düşmanın düzenli kuvvetlerinin yanı sıra, gerilla, terörist, kaçakçı gibi küçük ve düzensiz grupların da bulunduğu senaryolar dikkate alınmalıdır. Bu tip ortamlara cevap verebilecek EH sistemlerinin teknik ve taktik özelliklerinin belirlenmesinde, senaryoların değerlendirilmesi ikinci adımdır. Senaryoların değerlendirilmesi çalışmalarında;

* Hedefin önemi,

* Hedefin karıştırılabilirliği,

* Hedefin önceliği gibi parametreler değerlendirilir.

Hedefin öneminin belirlenmesi; Hedefin fonksiyonu (komuta kontrol, hava savunma, atış kontrol, lojistik vb.), hedefin haberleşme süresi (saniye, saat, gün vb.), hedef kontrol seviyesi (tümen, tugay, takım vb.), hedefe bağlı alt birlik sayısı, hedefin etkinliği gibi parametrelerin değerlendirilmesi ile gerçekleştirilir. Hedefin karıştırılabilirliğinin belirlenmesi; mesaj uzunlukları (bits, Kbits vb.), mesaj süreleri (msan, san, saat vb.), haberleşme mesafesi (Km), asıl muharebe hattından (FEBA) uzaklığı, tespit etme olasılığı, anten kazancı gibi parametrelerin değerlendirilmesi ile gerçekleştirilir.

Hedefin önemi, hedefin karıştırılabilirliği ve hedefin yedek haberleşme imkanının değerlendirilmesiyle hedefin önceliği belirlenir. Böylece frekans bantlarına göre öncelikleri belirlenmiş hedeflere karşı geliştirilecek EH sistemin en önemli sistem gereklerinden olan;

* Platform (kara konuşlu, UAVUnmanned Air Vehicle, helikopter, UEJ-Unattended Expendable Jammer, vb.),

* EDT- Elektronik Destek Tedbir alt yapısı (arama almaç hızı, DF-Direction Finding gereksimi, vb.),

* Hedef sayısı,

* EKT modları gibi özellikler belirlenir.

Yukarıda açıklanan hedefin önemi ve karıştırılabilirliği gibi parametrelerin belirlenmesi için sayısal bilgilere ihtiyaç vardır. Bu bilgiler ise teknik ve taktik veri tabanı hazırlanması ile mümkün olabilir. Teknik veri tabanı firma broşürleri, çeşitli yayınlar ve diğer istihbarat bilgilerinin derlenmesi ile oluşturulan standart bir yapıdadır.Taktik veri tabanı ise teknik veri tabanına göre çok daha değişik yapıda ve senaryoların değerlen dirilmesinde en önemli araçlardandır. Bu veri tabanının hazırlanmasında senaryolardan faydalanılır. Bu nedenle

taktik veri tabanı standart bir yapıda değildir. Coğrafi sınırların ve öncelikli hedeflerin değişikliği doğal olarak senaryoların farklı olmasını getirmektedir. Veri tabanındaki çeşitli alanların maksimum, minimum, toplam ve ortalama değerlerinin hesaplanması ile ilgili senaryodaki çevrim sayısı, gönderme süreleri ve aktiviteleri gibi taktik değerler hesaplanır. Taktik veri tabanında bulunması gereken bazı parametreler şunlardır;

* Çevrimlerin muharebe hattından olan uzaklıkları,
* Çevrimlerin birbirine olan uzaklıkları,
* Çevrim sayısı,
* Çevrimdeki alt istasyon sayısı,
* Aktivite süreleri,
* Frekans kullanım yüzdeleri,
* Frekans bandı,
* Komuta seviyesi.

Bu parametrelerden de görülebileceği ilgili alanların hesaplanması ile EKT cihazlarının en önemli sistem gereklerinden olan ve yukarıda verilen özellikleri belirlenmiş olur. Özet olarak, EKT sisteminin teknik ve taktik parametrelerinin belirlenmesinde, öncelikle senaryo belirleme ve değerlendirme çalışmalarının yapılması gerektiği açıktır. EKT sisteminden, bu frekans bandındaki tüm haberleşme yayınlarına karşı etkinlik beklenmesi mümkün değildir. Ancak hedeflerin çok iyi analizi ile, öncelikli hedefler belirlenmeli ve bunlara karşı geliştirilecek bir sistemden daha yüksek olasılıkla karıştırma etkinliği sağlanmalıdır. Bazı hedeflere karşı yüksek etkinlik, tüm hedeflere karşı kısmi etkinliğe tercih edilmelidir. [11]

BÖLÜM 5

ULUSAL BİLGİ GÜVENLİĞİ

TEKNOLOJİK GELİŞMELER

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler yeni bir çağ yaratmıştır. Bilgi çağı olarak adlandırılan bu çağda ekonomide ve sosyal yaşamda klasik paradigmalar yetersiz kalmakta; teknolojik gelişmeler yeni yapılar, yaklaşımlar yaratmaktadır.Bu nedenle, bilgi güvenliğine ilişkin ulusal bir politika oluşturmanın temel koşullarından birisi, bilgi ve iletişim teknolojilerinde gözlenen gelişmelerin bilinmesidir. Bu noktada, söz konusu teknolojik gelişmelerin ne olduğunu ve ne yönde olacağını doğru anlamak ve içeriğini doğru belirlemek son derece önemlidir:

Kriptoloji, Internet'in yaygınlaşması ve bir ticaret medyası halini almaya başlamasıyla, bilgi güvenliğinin sivil uygulamalarına tanık olmaya başlamıştır. Bu uygulamalar kısaca "açık anahtarlı altyapılar (Public Key Infrastructure-PKI)" olarak isimlendirilebilir. Açık anahtarlı altyapılar, bir gizli ve açık anahtar çifti ve bu çiftle sağlanan "elektronik kimlik, sayısal imzalama ve şifreleme" işlevleriyle, gerekli kurumsal ve yasal yapılanma üzerine kurulmuştur. Burada şu noktalar önemlidir:

(a) Kripto işlemleri donanım üzerinden yazılıma kaymıştır. Örneğin kripto teçhizatı, saklanması, imhası ve benzeri unsurlar bu altyapıda karşılaşılan ve kullanılan terimler değildirler.

(b)Söz konusu yazılımlarda kullanılan algoritmalar tümüyle kamuya açıktır. Bunun anlamı, bu algoritmaların çok sayıda taraf tarafından testinin yapılabilir olması ve bu yolla güvenilirliğinin artmasıdır.

(c)Anahtarların üretilmesi, saklanması ve tüm işlevlerin yürütülmesi için uluslararası açık standartlar belirlenmektedir (X.509 elektronik kimlik belgesi standardı, PKCS açık anahtarlı altyapılar standartları gibi). Bu standartların dışına çıkmak pratik değildir.

(d)Açık anahtarlı altyapıların gerektireceği yasal düzenlemeler de, (onay kurumlarının yapılandırılması, sayısal imzanın kabulü, vb.) uluslararası uyumun gereği olarak yerine getirilecektir.

Konu ile ilgili ilk yasa ABD'de Utah eyaletinde kabul edilmiştir (1995). Bunu Almanya (1997) ve Singapur (1998) sayısal imza yasaları izlemiştir. Halen Avrupa Topluluğu üye ülkelerinde böyle bir yasa için çalışmalar sürmektedir. Genel eğilimlerin dışında geliştirilmeye çalışılacak uygulamalar sosyal ve ekonomik açıdan zararlı olabilecek, uluslararası standartlara uymayan yapılanmalar ülkeleri yalnızlığa itecektir.

Internet yalnızca bir iletişim altyapısı değildir. Kimi yorumlara göre bilginin yaratılması ve paylaşılması için bir "özgürlük ortamı" anlamına da gelmektedir. Gerçekten de Internet sınırsız bilginin yayılmasının medyası olmuştur. Bu bağlamda, kriptografik ürünler hızla ve kolaylıkla yayılabilmektedir. Bu durum, ABD'deki aksi yönde gayretlere karşın değişmemiş aksine gelişmiştir. Örneğin, ABD tarafından sınırlandırılmış pek çok ürünü, ABD üzerinden ya da dünyanın başka bir köşesinden Internet aracılığıyla edinmek "teknik olarak" son derece kolaydır. "Teknik yöntemlerle" bunun önüne geçilme-

si olanaksızdır. Dolayısıyla, "Internet'teki bu durumun denetlenmesi" amacıyla yapılacak girişimler "teknik açıdan geçersizdir". Bunun yanında şu noktalar da dikkat çekicidir:

*Internet protokolü IP'nin gelecekti versiyonu IP v6, IP düzeyinde "şifreleme" sağlayacaktır. Bu durumda anahtarların saklanması da olanaksızlaşacaktır.

*Bilgi ve iletişim teknolojilerinde, ulusal devlet politikaları "teknolojik yansızlık" ilkesini benimsemişlerdir. Bunun anlamı kamunun, gelişme aşamasında bir teknolojiyi diğerlerine üstün saymaması ya da tercih etmemesidir. Diğer bir deyişle, teknolojilerin açık rekabet ortamında birbirlerine üstünlüklerinin sağlanmasıdır.

Bütün bu teknolojik gelişmeler göz önüne alındığında oluşturulacak politika ilkelerinin ve kurumsal yapılanma önerilerinin, ileride sorunlar yaratabilecek uygulamalardan kaçınılması gerektiğini göstermektedir. Yukarıda sözü edilen teknolojik tarafsızlık ilkesi, teknolojik açık rekabet ortamının sağlanması gibi konular göz önüne alındığında oluşturulacak politikaların bunlarla çatışmaması gerekmektedir. IP v6 ve sonrası gelişmelerin ışığında, teknik açıdan gerçekleştirilemeyecek görevler, kurumsal önerilerde yer almamalıdır. Bu nedenle, gelişmiş ülkeler bu yeni gelişmelere karşı tedbirler almak almak konusunda çok temkinli davranmaktadırlar. Mevcut yasalarla sahip oldukları yetkileri de, kulanım alanlarına açıklık getirerek sınırlamaktadırlar.

Diğer Ülkelerdeki Durum

Birkaç yüzyıllık geçmişi olan demokrasinin, çağımızda ortaya çıkan çok yoğun bilgi transferi ihtiyacına ayak uydurmasını sağlayacak arayışlar sürmektedir. Demokratik ülkeler, kriptografik yazılım ve donanım kullanımı sözkonusu olduğunda kişisel/ticari özgürlüklerle ve devlet/kamu güvenliği

arasında bir denge bulmaya çalışmaktadırlar. Bilgi güvenliği, uzun yıllar boyunca ve özellikle soğuk savaş döneminde, askeri ve diplomatik haberleşmenin önemli bir parçası olarak ele alınmıştır. Bu açıdan bakıldığında kavram, bilginin güvenli iletimi kadar, "hasım ulusların" elektronik istihbarat yöntemleriyle dinlenmesi olarak anlaşılmıştır. Özellikle gelişmiş uluslar, bu amaçlarla soğuk savaş döneminin hemen başlarında çeşitli kurumlar ihdas etmişlerdir.

ABD

Kişisel özgürlüklerin zedelenmemesi prensibinin neredeyse anane haline geldiği bu ülkede, devlet, vatandaşlarının haberleşmenin mahremiyeti konusunda hakları ile terörizm, kaçakçılık ve devlete karşı işlenen diğer suçların önlenmesi konusunda dengeleri de kurmuş bulunmaktadır. ABD'de 1952 yılında kurulan "Ulusal Güvenlik Teşkilatı (National Security Agency)" bu dengenin içinde kendine özgü bir yere sahiptir. NSA, ABD çıkarları doğrultusunda bir yanda uluslararası elektronik istihbarat yapmak ve öte yanda Amerikan devletinin bilgi güvenliğini sağlamaktan sorumludur. NSA, uzman teknik fonksiyonları sağlamaktan sorumlu kılınan Savunma Bakanı'nın yetki, kontrol ve yönlendirmesinde ve Savunma Bakanlığı bünyesinde bağımsız bir teşkilat olarak kurulmuştur.

NSA'nın günümüzde aldığı biçim hakkında şu noktalar önemlidir:

·NSA, tam olarak bir "elektonik istihbarat" örgütüdür. Hatta bu öyledir ki; NSA "ABD İsthibarat Topluluğu (US Intelligence Community)" içinde, CIA, FBI, "Ordu İsthabarat (Army Intelligence)" ve Savunma Bakanlığı gibi toplam 13 federal kurumdan birisidir ve bu kuruluşundan beri değişmemiştir. Ayrıca, 1972 yılında kurulan "Merkezi Güvenlik Birimiyle

(Central Security Service)" NSA ve ordu istihbarat birimleri arasında tam bir işbirliği sağlanarak Savunma Bakanlığının kriptografik çalışmaları tek bir bünyede verilmeye başlanmıştır.

·NSA "diğer uluslar ve onların tarafları için istihbarat ve karşı istihbarat" in istihbarat etkinlikleriyle sınırlıdır. Amerika'da oturma izni olan yabancılar, Amerikan vatandaşları ve Amerikan özel sektör kurumlarının gizlilik haklarına aykırı yasadışı istihbarat yürütmesi anayasa ve NSA'in kuruluş yasasıyla kesinlikle yasaklanmıştır. Bunun ötesinde, gizlilik ve haberleşme özgürlüğü yasalarıyla kişiler kendileri hakkında NSA gizlilik yasasında tanımlana "kimlik bilgilerine" erişme hakkına sahiptirler. Haberleşme özgürlüğü kapsamına giren "hükümet kayıtlarının" NSA tarafından tutulması yasayla engellenmiştir.

*NSA "ithalat ve ihracat politikalarının" belirlenmesinde görevli değildir ve kendi dışında oluşan politikalara tabiidir. ABD'de bu politikalar "Başkanlık" düzeyinde saptanır.

*·NSA'in ABD'deki "kriptografi üretimini" kontrol altında tutmak, söz konusu ürünleri sertifikalandırmak türünden hiç bir işlevi ve görevi yoktur. Hatta, özel üreticiler kamuya ürünlerini satarlarken dahi, NSA'in onayını almak zorunda değildirler. Tam aksine, NSA, gelişmiş yeteneklerinden ABD özel sektörünün de yararlanmasını sağlamak amacıyla, özel sektörün isteğine bağlı olarak danışmanlık vermektedir.(Bkz. The National Security Agency http://www.nsa.gov/about_nsa/faqs_internet.html)

*Kamuda bilgi güvenliği standartlarının belirlenmesi ve uygulanması da NSA'in görevleri arasında değildir. ABD'de bu işlevi, Amerika Standartlar Enstitüsü (National Institute of Standarts and Technology) "Federal Bilgi İşleme Standartla-

rı (Federal Information Processing Standarts)" yayınlarıyla yerine getirmektedir. Bu bağlamda Madde 8'in çeşitli bendlerinde ve farklı biçimlerde tekrar edilen "usuller ve yöntemler belirlemek, altypıları korumak" fiileriyle ifade edilen ve temelde kamuda bilgi güvenliği standartlarının altyapılar, ürünler ve uygulamalar açısından saptanmasına dönük olduğu anlaşılan işlevler bu kapsama girmektedir.

*1993 yılı Nisan ayında Clinton yönetimi NSA tarafından hazırlanan/önerilen yeni bir kriptoloji politikasını ortaya koymuştur. Başkan Bush zamanından başlayarak yürütülen bu çalışmaların odak noktası hükümet tarafından geliştirilen Clipper adlı bir kripto çipidir. Özel sektör tarafından üretilen her türlü güvenli iletişim ürünlerine yerleştirilmesi önerilen bu çipe karşı çok büyük bir tepki oluşmuştur. Bu tepkilerin kaynağında, her çip için özel olarak üretilen anahtarların bir kopyasının hükümet tarafından tutulması ve tamamen yasal olmayan hiçbir nedene dayanarak bu çipler üzerinden geçen trafiğin dinlenmeyeceğinin hükümet tarafından garanti edilmesine rağmen, yeterli güvenin oluşturulamaması bulunmaktadır. Ayrıca, hükümet tarafından geliştirilen anahtar algoritmasının açıklanmaması sonucunda algortimanın denenmesinin ve güvenilirliğinin kanıtlanamayacak olması, bunun sonucunda tüketicilerin bu ürünlere rağbet etmeyeceğinin ortaya çıkması, gittikçe önem kazanan kriptoloji sanayiinde dünya pazarlarında rekabet şansının kapalı bir algoritma kullanılarak üretilen ürünlere dayanarak korunamayacağı gibi endişeler ortaya çıkmış ve bu çip istenen kullanım yaygınlığına ulaşamamıştır.

Öte yandan "yaşamsal altyapıların korunması" (critical infrastructure protection) yeni bir kavram olarak dünya ülkelerinin gündemine girmiştir. Yaşamsal altyapıların korunması kavramı, ekonominin ve devletin minimum düzeyde işleyişi

için gerekli fiziksel ve ağsal sistemleri kapsamaktadır. Amaç, ülkenin düşmanlarının, bunlar ister başka ülkeler, ister ülke içindeki gruplar ve bireysel olsun, "geleneksel olmayan" yöntemlerle yapacakları saldırıların engellenmesidir. Açıktır ki, bu tehditler, devletin elektronikleşmesi ve açık ağları kullanmasının yaygınlığıyla doğru orantılıdır. Yaşamsal altyapıların korunması için ABD 42. Başkanı Bill Clinton, 1998 yılında bir Beyaz Belge direktifleri yayınlamıştır. Bu belgede dikkat çeken unsurlar şunlardır:

·Devlet içinde öncü kurumlar tespit edilmiştir. Her öncü kurum çeşitli sektörleri paylaşmışlardır. Örneğin, Ticaret Bakanlığı iletişim ve enformasyon sektörüne; Hazine Bakanlığı bankacılık ve finans sektörüne, FBI polis, acil durum ve adalet konularına; CIA dış istihbarata; Dışişleri Bakanlığı dışişleri sektörüne; Savunma Bakanlığı savunma sektörüne liderlik edecek kurumlar olarak belirlenmişlerdir. Ayrıca, Bilim ve Teknoloji Politika Genel Müdürlüğü, Ulusal Bilim ve Teknoloji Konseyi'nin programları aracılığıyla araştırma ve geliştirme çalışmalarını eşgüdümlemekle görevlendirilmiştir. Öncü kurumların seçilmesinin nedeni, bu konuda, özel sektör/kamu sektörü işbirliğini gerektirmesi ve gereksiz hükümet düzenlemeleri yaratmaktan kaçınılmasıdır.

***Ulusal Eşgüdümcü-** Güvenlik, Altyapı Koruma ve Karşiterörizm Ulusal Koordinatörü bu direktifin eşgüdümünden sorumludur.

***Uyarma ve Bilgi Merkezleri-** Başkan, bu görevle FBI'yi sorumlu kilmiştir.

***National Infrastructure Protection Center (NIIPC)-** Bu heyeti, FBI, bilgisayar suç uzmanları, Savunma Bakanlığı, İstihbarat topluluğu ve önder kurumların temsilcilerinden oluşur.

İngiltere ve Almanya

NSA dışında gelişmiş ülkelerden anılan iki diğer örnek kurum İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters) ve Almanya'daki Enformasyon Teknolojileri Güvenlik Kurumudur (Bundesamt für Sicherheit in der Informationstechnik). İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters), NSA'ya çok yakın işlevler yürütmektedir. GCHQ'nun da oluşumu soğuk savaş dönemine dayandırılmaktadır.

Enformasyon Teknolojileri Güvenlik Kurumu (BSI) ise NSA ve GCHQ örneklerinden farklı olarak, istihbarat işlevi olmayan bir kurumdur. BSI bir Alman kamu kurumu olarak, bilgi ve bilgisayar sistemleri güvenliği konularında araştırma yürüten bir kurumdur. Araştırma sonuçları, kamuda söz konusu güvenlik uygulamalarının yapılmasına yarar sağlamaya çalışmaktadır. Kurum adli olaylarda da emniyete talep olduğu takdirde danışmanlık hizmeti verebilmektedir.

Alman Hükümeti de söz konusu teknolojiyi yasaklamak üzere girişimlerde bulunmaya başlamıştır. 4 Mayıs 1995 tarihinde Alman Parlamentosu "Telekomünikasyon İzleme Kanunu" adı altında ülkede tasarlanan ve kullanılan telefon, GSM, ISDN ve bilgisayar şebekesi tarayıcılarının, devlet birimleri tarafından gerektiğinde dinlenmesini sağlamak için standart bir ara bağlantı sağlamaları konusunda bir kanun teklifini onaylamıştır. Kanunun özünü, güçlü delillere dayanarak bağımsız bir yargıç kararı olmadan özel haberleşmenin dinlenememesi oluşturmaktadır. Yargıcın gerekli gördüğü durumlarda, bu kanuna göre çağrı oluşturma bilgilerine ve GSM kullanıcılarının hücreler arasında izlenmesini sağlayacak bilgilere erişilmesi mümkün hale gelmektedir. Almanya, bu dü-

zenlemesiyle, Avrupa ülkeleri arasında bireyi devlete karşı üst düzeyde güvenceye alan bir ülkelerin öncülüğünü yapmaktadır.

Norveç

Norveç'te kriptografik ürünlerin yurt içerisinde kullanımında herhangi bir yasaklama yoktur ve ithalatında da kontrol bulunmamaktadır.Norveç Wassenaar Anlaşması'nın bir üyesidir ve bu bağlamda kriptografik ürünlerin ihracatını 1987 tarihli bir yasayla kontrol etmektedir. İhracat kontrolü Dışişleri Bakanlığı'nın sorumluluğundadır. Norveç yasaları Wassenaar Antlaşması'nda yer alan genel yazılım istisnaisini gözetmektedir. Ayrıca, İnternet'in genel yazılım notunun uygulanması ve kriptografik ürünlerin iletilmesi için yeterli bir temeli teşkil ettiği benimsenmektedir.Norveç'te yürütülmekte olan Kamu Sektörü Ağ Projesinde, sayısal imza sayısal kimlik belgesi ürünlerinin oluşturulması hedeflenmektedir. Bu projenin "açık anahtarlı altyapılar" (PKI) için yasal, teknik ve organizasyonel düzenlemeler için deneme olduğu ve temel teşkil edeceği planlanmaktadır.

ABD'de kriptografik teçhizat Wassenauer ilkeleri gereğinde "mühimmat" gibi görmektedir. "Mühimmat kavramı" askeri bir terim olarak, kriptografik ürünlerin, 1998 Wassenaar düzenlemesinde, "askeri ve ticari olmak üzere çift kullanımlı" teknolojilerden sayılmaya başlanmasıyla ilgilidir. Bunun anlamı, bu düzenlemeye imza koyan ülkelerin, kriptografi ürünlerinin ithalat ve ihracında "uyumlu" politikalar izleme niyetinde olduklarıdır. Ancak Wassenaar bir anlaşma değildir ve yaptırımı yoktur. Nitekim, İsviçre hükümeti 1998 düzenlemesinin "liberal politikalarında" bir değişikliğe neden olmayacağını ve İsviçre firmalarının dünya pazarından en yüksek payı almaları konusundaki desteğinin devam edeceğini açıklamıştır

(Bkz. Crytography and Liberty 1999, EPIC). Wassenaar üyesi İrlanda ise, en başından beri ABD ve İngiltere'nin aksi yönünde politikalar izlemiştir. İrlanda'nın bir firması olan "Baltimore Inc." bugün dünyanın en önde gelen bilgi güvenliği firmalarından birisidir.

ABD, 1998 Wassenaar düzenlemesinin aksi yönünde, ihraç politikalarını 2000 yılıyla beraber değiştirmiştir. Wassenaar 1998 açık bir biçimde Internet tarayıcılarında 56 bit anahtar uzunluğunda kriptoya izin verirken, ABD bu yılın başından itibaren 128 bit anahtar uzunluğunu ihraç etmeye başlamıştır. ABD kökenli web sunucuları da paralel bir biçimde 128 bit SSL destekler bir biçimde ihraç edilmeye başlanmıştır. Ülkemizde bazı bankaların internet sayfalarında bu konunun uygulaması görülmektedir.Bu değişimde, "ticari çıkarların" ağır bastığı vurgulanmaktadır. Değişiklik, tümüyle liberal bir politika değilse de, geçmiş uygulamalara göre liberalleşme anlamına gelmektedir.

Fransa

Fransa'da da kriptografik yazılım ve donanım "mühimmat" olarak tanımlamakta ve işlem görmektedir. Yasa ile kriptografik teçhizatın ihracatı ve kullanımı devlet denetimine tabi kılınmıştı. Bir süre, Fransa'da faaliyet gösteren yabancı şirketler "ulusal güvenlik" nedeni ile kullandıkları anahtarları Fransız hükümetine bildirmek zorunda kaldılar. Ancak daha sonra bu politikalardan vazgeçilmiştir. Almanya, Finlandiya ve İtalya en başından beri liberal politikalar, izlerken, Fransa 1999 yılında gösterdiği değişimle ilginç bir uyum örneği sergileşmiştir. Fransa'da da artık sadece "beyan" yöntemi uygulanmaktadır. Gerçekten de Fransa yakın zamana kadar, "sertifikalandırma" yöntemiyle ihracat ve ithalatı kontrol altında tutmaya çalışırken, 1999 yılı başında Başbakan'ın birinci ağızdan açıklamalarıyla sadece ticari politikalarında değil an-

cak tüm ulusal politikalarında önemli değişikliklere gittiğini duyurmuştur. Avrupa Birliği, diğer ulusal politika konularında olduğu gibi, ihracat ve ithalat izinlerinde de ABD'ye oranla çok daha liberal politikalar izlemektedir. Son olarak, 22 Mayıs 2000 tarihinde Lizbon'daki Dışişleri Bakanları toplantısında onaylanan bir düzenlemeyle, kriptolojik ürünlerin ihracatına getirilen sınırlamalar büyük ölçüde kaldırıldı. Bu düzenlemeyle, ihracat yapacak firmaların, ürünün son kullanıcısının Avrupa Birliği ülkelerinde veya aralarında Kanada, Japonya, ABD, Avustralya ve Yeni Zelanda'nın da bulunduğu 10 ülkeden birinde olduğunu beyan etmeleri yeterli olacaktır. Avrupa Birliği ve adı geçen diğer ülkeler bu alanda dünya pazarının %80'ini oluşturmaktadırlar. Bu hamleyle, AB ülkeleri firmaları bu pazarda özellikle ABD'li firmalara karşı büyük avantaj sağlamış olacaktır. Bu nedenle, çok yakında ABD'li firmaların hükümete baskı yaparak kendi ülkelerinde de benzer bir düzenlemenin yapılmasını istemeleri beklenmektedir. OECD'nin 1998 yılında gerçekleştirdiği "Kriptografi Teknolojilerindeki Kontroller" başlıklı envanter çalışmasının raporu 1999 yılında yayınlanmıştır. Bu envantere göre kriptografik ürünlerin ihracat ve ithalatından sorumlu kurumlar büyük çoğunlukla ekonomiden ya da sanayi ve ticaretten sorumlu bakanlıklardır. Envantere göre yalnızca Avustralya ve Türkiye'de sorumlu bakanlıklar olarak Savunma Bakanlıkları belirtilmiştir. Türkiye'de ayrıca Dış Ticaret Müsteşarlığı da sorumlu kurum olarak belirtilmektedir.

Türkiye'de Durum

Ulusal Güvenliği ilgilendiren bilginin örgütlenmesi açısından "gizlilik dereceli" bilginin ne olduğunu nasıl üretileceği, korunacağı, nakledileceği, kullanılacağı ve imha edileceği konusunda devletin yasal hazırlığı ve düzenlemesi tam bulunmamaktadır. Bu yasal düzenlemeler ise geçici olarak kurulup sonra dağıtılan birtakım platformların üstesinden gele-

bileceği gibi basit bir yasa ya da mevzuat değil çok karmaşık bir yasalar zinciridir ve gelişen teknoloji nedeni ile sürekli güncellenmek ve teknolojiye uygun hale getirilmek zorundadır. [12]

BÖLÜM 6

ECHELON

Echelon 11 Eylül'ün şifresini çözemedi

11 Eylül'deki saldırı sonrasında Echelon gibi yüksek teknolojiye sahip bir sistemin kurucusu olan ABD'nin, bu saldırıları neden önceden haber alamadığı tartışıldı. 11 Eylül saldırılarının, ABD'nin dünyadaki hakimiyetini pekiştirme operasyonunun bir parçası olduğu şeklindeki komplo teorilerilerini şimdilik bir yana bırakırsak, NSA'nın 11 Eylül saldırılarını haber alamamasında en önemli neden olarak kriptoloji gösteriliyor. Bu görüşe göre, bazı ülkeler gizlice haberleşmelerini dinleyen büyük "kulaklar"dan, bazı firmalar da bilgisayar korsanlarından korktukları için, şifreleme sistemleri büyük önem kazandı. Bu şifreleme sistemleri doğal olarak, teröristler tarafından da yaygın bir şekilde kullanılıyor. Soğuk Savaş bitene kadar modern elektronik şifreler yalnız belli çevrelerce kullanılabildi. Bunlar askeri personel, casuslar ve diplomatlardı. Bu çevreler dışında şifre kullanılabilmesi için, kullanılan şifrelerin gizli servislerce çözülebilecek cinsten olması gerekliydi.

Echelon'un çözemediği şifre

1991'de birden herşey değişti; genç bir Amerikalı bilgisayarcı Phil Zimmerman, kendi bulduğu, çözümü son derece zor, çok basit bir şifre programını ücretsiz olarak internet aracılığıyla bütün dünyaya yaydı. Bu şifre PGP (Pretty Good Privacy) olarak biliniyor (anlamı: Mükemmel Sır Saklama). NSA'yı ve dünyanın bütün gizli servislerini bir korkudur aldı; onlar ki yıllardır güvenli bir iletişim için en iyi şifreyi arayıp du-

ruyorlardı. PGP'den sonra ona benzer daha mükemmel şifreler bulundu. NSA bilgisayarları bunların hiçbirini, ya da hemen hemen hiçbirini, çözemiyor. Bunun için 250 haneli sayılarla oluşturulan ve çözümü süper bilgisayarların bin yıllarını alabilecek bu şifrelerin çözümü için NSA, kuramsal olarak bunları birkaç saniye içinde çözebilecek kuantum bilgisayarların gelişmesini sabırsızlıkla bekliyor ve bu araştırmaları cömertçe destekliyor. Şifreleme teknolojilerinin önümüzdeki yıllarda uzun süre tartışılacak bir konu olduğu belirtiliyor. Burada devletler, giderek karmaşıklaşan yapıları nedeniyle şifreleri çözmekte zorlandıklarından yeni alternatifler arıyor. Üstelik bu giderek zorlaşan şifreleme sistemlerinin internet üzerinden ücretsiz indirilebiliyor olması, herkesin mesajlarını şifreli olarak göndermesine olanak sağlıyor. Bu durum, ağlar üzerindeki dolaşan bilgileri alıkoyma yeteneği azalan Echelon gibi sistemlerin sahiplerini tedirgin ediyor. Tahminlere göre, 11 Eylül'ü Echelon sistemi, saldırıyı düzenleyenlerin yüksek güvenlikli şifreleme sistemleri kullanarak haberleşmesi nedeniyle haber alamadı.

"Arka kapı" tehlikesi

Siber uzayda dolaşan bilgileri okuma yeteneğini kaybettiği zaman, değerli bir silahını kaybetmiş olacak olan devletler, yazılımların sadece kendileri tarafından açılabilecek "arka kapı"lar bırakılarak hazırlanmasında ısrarlı. Buna "anahtar rehim" veya "anahtar geri alma sistemi" deniliyor. Amerikan popüler söyleminde bu durum "Chipper Chip" olarak bilinir. İddialara göre, Microsoft, ABD çıkarları ve bazı ticari sırları elde etmek için, ürettiği yazılımlarda bir açık kapı bırakıyor ve bu açık kapı sayesinde, ABD askeri ve istihbarat birimleri, üzerinde Microsoft yazılımı bulunan bilgisayarlardan kullanıcı farkına bile varmadan bilgi alabiliyorlar. Bilindiği gibi, başını Rusya, Çin ve Fransa'nın çektiği bazı devletler, bu tehlike-

ye karşı ülke sırları ve askeri güvenliği sağlamak için, Linux tabanlı "Milli İşletim Sistemi" üretme yoluna gidiyorlar.

Echelon'u örseleme günü: Jam Echelon Day!

Echelon'un varlığının öğrenilmesinden sonra, Echelon karşıtı sivil gruplar oluşmaya başladı. Echelon karşıtlarının açtığı ve http://uid0.sk/echelon/mail_en.php adresinden ulaşılabilen bir siteden, sistemi kilitlemek için, mesaj göndermek mümkün olabiliyor. Echelon'un tehlikeli olarak tanımlamış olabileceği kelimeler, gönderilecek mesaja yazılıyor ve bu mesaj Echelon'un kurulduğu gün olan 21 Ekim günü postalanmak üzere saklanabiliyor veya hemen gönderilebiliyor. Bu yöntemin Echelon'a karşı etkili olup olmadığı bilinmiyor. Sistemin büyüklüğü ele alındığında, "Echelon Day" kapsamında gönderilen mesajların, sembolik kalacağı varsayılabilir. Bu eylemin amacı olsa olsa, insanları Echelon hakkında bilgilendirmek ve Echelon'a karşı tepkisiz kalınmayacağını, projenin sahiplerine göstermektir.

50 yıldır dinliyorlar

1960'da Rusya'ya iltica eden iki NSA görevlisi ABD'nin 40 ülkenin haberleşmesini dinlediğini açıkladı. AB bu olayı sürekli inkar etti. Dünyadaki bütün telefon, faks, telsiz, SMS ve elektronik posta iletişimini dinleyen dev bir kulak: Echelon. Amerika Birleşik Devletleri'nin sürekli inkar ettiği Echelon'un varlığı resmi olarak ilk kez, 23 Mayıs 1999'da Avustralya, Canberra'daki Savunma Sinyalleri Müdürlüğü (DSD) Başkanı Martin Brady'nin yaptığı açıklamayla kabul edildi. Brady, ülkesinin 50 yıldır varolan ve gizlenen küresel bir elektronik izleme sisteminin parçası olduğunu kabul eden ilk kişi oldu. Bu gelişme, üye ülkeleri en çok da ABD ve İngiltere'yi rahatsız etti. Sisteme 5 ülke üye idi ve diğer üyeler, Yeni Zelanda ve Kanada idi. Ayrıca, çeşitli müttefik ülkelerde de Echelon'un üsleri bulunuyordu.

Dünyanın gizli bir kulak tarafından dinlendiği aslında 1960 yılında ortaya çıkmıştı. Rusya'ya iltica eden iki NSA görevlisi, Bernon Mitchell ve William Martin, 6 Eylül 1960'da Moskova'da bir basın toplantısında NSA'nın 2000 dinleme istasyonuyla, bunların kurulu oldukları ülkeler de dahil olmak üzere en az 40 ülkenin gizli haberleşmesini dinlediğini açıkladılar. Dünyanın her yanına dağılmış olan istasyonlardaki binlerce analistin mesajlarını izlediği "mimli" kişiler arasında, Afrikalı gerilla liderlerinin yanısıra, Vietnam Savaşı'na karşı çıkan aktris Jane Fonda ile bebek bakımı uzmanı Dr. Benjamin Spock da bulunuyordu.

Avrupa'nın yüzde 90'ını dinliyor

Sistemin varlığının ilk kez Echelon'a üye ülkelerden biri olan Avustralya tarafından kabul edilmesinden sonra Avrupa Birliği harekete geçti. ABD'den istihbari olarak geri kalmamak için, hemen bir rapor hazırlattı. Echelon hakkında Avrupa Parlementosu'ndaki ilk rapor 1988'de yayınlandı. AB raporuna göre ABD, Avrupa'daki telefon, faks ve e-posta haberleşmelerinin yüzde 90'ını Echelon sistemiyle denetliyordu. Raporun açıklanmasının ardından İtalya, Echelon'un bilgi toplama yöntemlerinin İtalyan kanunlarına aykırılığının incelenmesi için bir komisyon kurdu. Danimarka Parlamentosu da benzer bir araştırma başlattı. Ve 1999'da, ABD'deki elektronik mahremiyet örgütü EPIC, Echelon'la ilgili olarak ABD hükümetini mahkemeye verdi.

AB'nin 'Echelon'u Enfopol

AB raporunun hazırlanmasının amacı, ABD'nin dünyayı dinleme faaliyetlerinin bir benzerinin Avrupa Birliği tarafından gerçekleştirilmesiydi. AB'ye üye ülkeler, ABD'nin internet de dahil olmak üzere dünya iletişimini gizli bir biçimde takip etmekte kullandığı Echelon adlı sistemine bir "rakip" çıkarma

hazırlığı yapıyor. AB'nin dinleme sistemine Enfopol adlı veriliyor. Öte yandan ABD ve Echelon üyeleri olan, İngiltere, Yeni Zelanda, Kanada, Avustralya'nın yanısıra, Rusya, Çin, Danimarka, Hollanda, İsviçre, Fransa ve İsrail gibi devletlerin de benzer sistemler kullandığı biliniyor.

Ticarî sırları da çalıyorlar

Echelon'un ortaya çıkışıyla birlikte, ABD'nin uluslararası ihalelere girecek Amerikan şirketleri için rakiplerin sırlarını çalmak için de sistemi kullandığı öne sürüldü. İddiaya göre, ABD firmalarının katılacağı ihalelerde rakip şirketlerin iletişimi dinlenerek milyarlarca dolarlık kazanç sağlandı. Avrupa Birliği, İngiltere dışında bu ağa karşı engelleme çalışmalarını yoğun şekilde sürdürüyor.

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 haberleşmeyi 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 zaptediyor ya da özel uydularla haberleşme sinyallerini topluyor.

Kökleri Enigma'ya kadar uzanıyor

Echelon'un kökleri İkinci Dünya Savaşı yıllarına kadar uzanıyor. Nazi 'Almanya'sına karşı savaşta ittifak yapan İngiltere ve ABD, doğal olarak istihbarat alanında da yakın bir işbirliği yaptılar. Alman şifre makinesi Enigma'nın şifresini çözmekle görevlendirilen matematikçi ve bilgisayar teknolojisinin önderi Alan Turing ve ekibi, şifreyi başarıyla çözdü ve anahtarını Amerikalılar'a da verdi. Amerikalılar da Japon-

lar'ın askeri şifrelerini çözerek İngilizler'e verdi. İki ülke bu yolla düşmanlarının radyo haberleşmelerini dinlediler ve yüzbinlerce gizli mesajı çözdüler. Savaşın sona ermesinin ardından NSA ve İngiliz Devlet İletişim Karargahı GCQH 1947 yılında UKUSA (İngiltere-ABD) anlaşmasını imzaladılar. Daha sonra İngiliz Uluslar Topluluğu üyesi Kanada, Avustralya ve Yeni Zelanda'nın elektronik istihbarat birimleri de anlaşmaya katıldı. Nihayet Batı Almanya, Danimarka, Norveç ve Türkiye de UKUSA kapsamına "üçüncü ülkeler" olarak eklendiler. İngilizce konuşan beş ülke dünyanın çeşitli bölümlerindeki haberleşmeyi izlemek üzere işbirliği yaptılar. İngiltere'nin payına Afrika ile Urallar'a kadar Avrupa düştü. Kanada, kuzey enlemleri ve Kuzey Kutbu'ndaki, Avustralya da Okyanusya'daki iletişimi izleme sorumluluğunu üstlendiler. Echelon sisteminde üye ülkeler adına Amerikan Ulusal Güvenlik Ajansı (NSA), Kanadalı (CSE), İngiliz (GCHQ), Yeni Zelandalı (GCSB) ve Avustralya'daki DSD (Savunma Sinyalleri Müdürlüğü) görev yapıyor.

Dünyanın En büyük Kulağı : NSA

Amerika'da dinleme faaliyetlerini yürüten üç ayrı kuruluş bulunuyor; NSA (Ulusal Güvenlik Ajansı), FBI (Federal Araştırma Bürosu) ve CIA. ABD'nin 'en büyük kulağı' olan NSA, Başkan Harry S. Truman'ın 24 Ekim 1952'de imzaladığı 'çok gizli' genelgeyle kuruldu. Truman bu yeni kuruluşa, dünya çapında iletişim istihbaratı görevi verdi. Önceleri diplomatların ve askerlerin şifreli telsiz görüşmelerini dinleyen NSA, daha sonraları uluslararası sivil telefon görüşmelerini de hedefleri arasına aldı. 1960'lı ve 70'li yıllarda ortaya çıkan yönlü telsiz haberleşme ve uydu teknolojisi NSA'nın işini daha da kolaylaştırdı. Artık havaya çıkan hiçbir radyo sinyali, hiçbir telefon görüşmesi NSA'nın dünya yüzeyine dağılmış binlerce uzmanının eline düşmekten kurtulamıyordu. NSA, kurulduktan hemen sonra, gizli bir iç yönetmelik çıkararak CIA ile işbölümü

yaptı. CIA de bir yıl sonra, kendi sınırlarının belirlemek amacıyla FBI ile pazarlığa oturdu. CIA'nin ülke içindeki faaliyet alanı çizildi. NSA'da halen 21 bin personel görev yapıyor. Bu rakam bazı iddialara göre 50 bin civarında. ABD, elektronik istihbarat için yılda 20 milyar dolar harcıyor. NSA'nın yıllık bütçesi ise 3,6 milyar dolar. NSA'nın Boeing 707 uçak gövdeleri üzerinde geliştirilen RG-135 tipi uçakları ABD hava kuvvetleri içinde bağımsız olarak görev yapıyor. ABD donanma gemileri görünümündeki gemileri okyanus ve denizleri denetliyor. NSA'nın yer istasyonlarının ABD büyükelçiliklerinde ya da ABD'ye dost ülkelerin topraklarında, evsahibi ülkelerin denetimine tâbi olmaksızın faaliyette bulunduğu sanılıyor. Sistemin parçaları, internet, yeraltı ve denizaltı haberleşme kabloları, telsiz haberleşmesi ya da büyükelçiliklere yerleştirilen gizli aygıtlar aracılığıyla yapılan her türlü iletişimi ele geçiriyor ve uydular vasıtasıyla NSA merkezine iletiliyor.

Echelon'un uydu haberleşmelerini dinleyen gelişmiş anten sistemleri, ABD, İtalya, İngiltere, Türkiye, Yeni Zellanda, Kanada, Avustralya, Pakistan, Kenya topraklarında ve muhtemelen diğer bazı ülkelerde de faaliyette. Echelon'un üye ülkelerin yanısıra açıklanmayan müttefik ülkelerde de dinleme sistemleri var. Bunlardan biri Kıbrıs Rum Kesimi'nde. Rumlar tarafından yakın geçmişte bu üs aleyhinde gösteriler düzenlenmişti. İddialara göre, Echelon sistemine ait Türkiye'de de üsler bulunuyor. Bu üssün Karamürsel'de olduğu iddia ediliyor. Öte yandan Echelon'un miadını doldurduğu düşünülen cihazları çoğu zaman bulundukları ülkenin istihbarat servislerine veriliyor. Bu iddiaya göre de, MİT'in elinde de Echelon'un eski cihazları bulunuyor.

'Umbra Gamma' gizlilik!

UKUSA sistemi çerçevesindeki haberalma çalışmalarında, öteki örgütlere kıyasla çok daha sıkı gizlilik kuralları uy-

gulanıyor. Sistemdeki izleme istasyonlarında görev alan her kişi, bildiklerini "ömrü boyunca" saklı tutmayı taahhüt ediyor, göreve başladığında bir "endoktrinasyon" sürecine tabi tutuluyor, her somut proje için bu endoktrinasyon tekrarlanıyor. Echelon ve kardeşlerindeki en düşük gizlilik derecesi, öteki haberalma örgütlerinin "çok gizli" (top secret) kategorisinin de üzerinde "top secret umbra" damgası taşıyor. Gizlilik derecesi daha yüksek dökümanlaraysa "Umbra Gamma" damgası vuruluyor.

Gelişmiş bilgisayarlar kullanılıyor

UKUSA ittifakının çerçevesine giren tüm haberalma ağı, bir tür İnternet gibi çalışıyor. Tüm istasyonlar, bir servis sağlayıcı gibi çalışan NSA'nın "Platform" adlı merkezi bilgisayar sistemiyle irtibatlı. Sistemde ayrıca Embroidery (Nakış) Tideway (Med kanalı) Oceanfront (Okyanus kıyısı) gibi alt bilgisayar sistemleri bulunuyor. Ayrıca çaşitli birimlerin telekonferans yoluyla haberleşmesini sağlayan Gigster adlı, şifreli bir kanal da var. ABD ve İngiliz askeri haberleşme uyduları Milstar ve Skynet'in yanısıra, okyanus diplerindeki iletişim kabloları da çeşitli birimler arasında irtibat sağlıyor. Sistem, topladığı istihbarat bilgilerini de 1996 yılında NSA'nın Fort Meade'deki merkezinde kurulan ve internet esaslarına göre çalışan "Intelink" adlı bir bilişim ağıyla paylaşıyor. Intelink, ABD'nin 13 ayrı istihbarat örgütüyle bazı dost istihbarat örgütlerini birbirine bağlıyor. Yetkili kullanıcılar bir "ana sayfa" üzerindeki haritanın çeşitli yerlerine tıklayarak istedikleri ülke hakkındaki istihbarat bilgilerine ulaşabiliyorlar. 1982 yılında eski NSA direktörü William Studeman'ın verdiği bilgiye göre tek bir istihbarat toplama sistemi, yarım saat içinde 1 milyondan fazla girdi sağlayabiliyor. Filtreler, bunların 6500'ü dışındakileri atıyor. Bunlardan 1000 kadarı, bir sonraki kademeye iletilmeye değer bulunuyor. Analistler bunların içinden normal

olarak 10 tanesini seçiyor ve bunlardan yalnızca bir tanesi sonunda bir rapor haline geliyor. Haritalarda tüm dünyayı ince bir ağ gibi ören bu dev elektronik istihbarat ağı içinde Echelon'un 1970'li yıllarda ortaya çıktığı ve iletişimin büyük ölçüde haberleşme uyduları aracılığıyla yapılmaya başlamasıyla birlikte öneminin giderek arttığı sanılıyor.

Echelon sisteminin verimliliği için internetin yaygınlaşması büyük kolaylık sağladı. Uluslararası internet ağlarının kilit noktalarına (Router) veri iletişimini filtreden geçiren adlı "Sniffer" sistemler kullanılıyor. Öte yandan, kıtalararası iletişim hatlarını dinlemek (ABD'nin okyanus tabanındaki telefon hatlarını kontrol altında tutabilmek için bu kablolara dinleme cihazları yerleştirdiği bilinmektedir; bu cihazlardan biri 1982'de kabloların bakımını yapan bir Fransız sualtı ekibi tarafından bulunmuştur) gibi çeşitli yöntemlerle, dünya üzerindeki iletişim sistemlerinden geçen veri paketleri Echelon tarafından toplan-maktadır. Echelon tarafından toplanan bütün bilgiler, otomatik olarak Echelon ağına bağlı "filtre" bilgisayarların içinden geçiriliyor. Her an, yüzbinlerce görüşme Echelon'a yakalanıyor. Telefon görüşmelerinin ses kayıtları, hassas "ses tanıma" yazılımları ile taranıp otomatikman metne dönüştürülüyor. Bu metinlerde, önceden tespit edilen "tehlikeli" "anahtar sözcük" olup olmadığı sınanıyor. Eğer böyle bir kelime saptanırsa, bilgisayarlar otomatik olarak o görüşmeyi hem ses hem de metin biçiminde dosyalıyor. Ardından, görüşmeyi kimin yaptığı tespit ediliyor ve görüşmeyi yapan kişi izlenmeye alınıyor.

Elektronik sinyal istihbaratı

Elektronik dinleme operasyonuna sinyal ihtihbaratı (Signal Intelligence) ya da kısaca (Sigint) deniliyor. ABD, birkaç müttefikiyle birlikte yürüttüğü "Sigint" sistemiyle her gün dün-

yanın her tarafından milyonlarca mesajı yasal olmayan yollarla zaptedip inceliyor. Bu sinyal istihbaratının yanısıra, genel elektronik istihbarat sisteminin bir parçası olarak IMINT (görüntü istihbaratı) devrede. IMINT, fotoğraf uydularıyla resim çekerek ve radar uydularıyla karaları ve denizleri tarayarak gerçekleştirilen bir casusluk sistemi. Bu görevi yürüten Ulusal İstihbarat Ofisi (NRO), Amerikan gizli servisleri arasında en küçüğü. 2000 kadar görevli, uyduları yörüngesinde tutmak ve yönlendirmekten sorumlu. Bu görevliler uydularla elde edilen gizli bilgileri ABD Merkezî Haberalma Örgütüne (CIA) ve Amerikan ordusuna dağıtıyor. Sinyal istihbaratı yalnızca ABD'nin tekelinde değil. Bu alanda en büyük istihbarat faaliyeti NSA tarafından yürütülmekteyse de, başta Rusya, Çin, Fransa olmak üzere başka bazı ülkeler de kendi sinyal istihbarat ağlarını geliştirmeye çalışıyorlar. Hatta, Danimarka, Hollanda ve İsviçre gibi ülkelerin de görece küçük Echelon türü dinleme istasyonları geliştirdikleri bildiriliyor.

Havada, Karada ve Denizde ECHELON

Uydular ;Dünya yörüngesindeki NSA'ya ait uydular, Echelon projesi için, ses, görüntü ve internet trafiğini gaspedip NSA'ya gönderiyor.

Denizaltılar;ABD nükleer denizaltıları, kıtalar arasında haberleşmeyi sağlayan okyanus diplerindeki kablolara gizlice alıcılar yerleştiriyor.

Gemiler ;Echelon sistemi için çalışan gemiler okyanuslarda sürekli seyir halindeler. Bu gemiler topladıkları bilgileri NSA merkezine iletiyor.

Uçaklar ;Boeing 707 gövdeleri üzerinde geliştirilen RG-135 tipi uçaklar, taşıdıkları süper bilgisayarlarla Echelon için çalışıyorlar.

Yer istasyonları ;Yer istasyonları genelde ABD'nin büyükelçiliklerinde kurulu ve evsahibi ülkelerin denetimi olmaksızın görev yapıyor.

İnternetin Yaygınlaşması Bu Planın Bir Parçası mı ?

Küresel bir bilgi ağı olan internetin yaygınlaşması ve e-devlet projelerinin geliştirilmesinin en önemli amaçlarından biri, kitlelerin daha iyi izlenmesidir. İnternet ne kadar çok yaygınlaşırsa, Echelon gibi kulaklara sahip ülkeler, ağ üzerinde dolaşmakta olan daha fazla bilgiyi alıkoyacaklardır. İnterneti kullanan, onun e-posta, haber grupları, web sayfaları, sohbet odaları gibi hizmetlerini kullanan herkes arkasında iz bırakmaktadır. Örneğin, ücretsiz e-posta adresi veren bir şirkete veya bir siteye kayıt olurken verdiğimiz bilgiler sadece o hizmeti aldığımız şirketin eline geçmez. Şirketler ticari olarak bunu başka firmalara satabileceği gibi, siber ağlar üzerinde dolaşan bu bilgiler Echelon ve benzeri sistemler tarafından yakalanır. Benzer şekilde, e-devlet projesi de hükümetlerin vatandaşlarını fişlemek ve davranışlarını izlemesinden başka bir şey değildir. E-devlet projesi, devletle olan ilişkilerimizde, bürokrasiyi azaltarak büyük yararlar sağlarsa da, bireyler için yarardan çok zarar getirebilir.

Echelon üsleri kapatılacak

NSA ve Amerikan ordusu, gelecekte uzaydan casusluk sistemlerini havada onlarca saat kalabilen pilotsuz uçaklarla tamamlamayı düşünüyor. Gelecek yıllarda casus uydular ve pilotsuz uçaklar, çok yükseklerden dünyayı dinleyen "büyük kulaklar" olacaklar ve IOSA (Integrated Overhead Sigint Architecture) mimarisi altında birleştirilecekler; bunlar sayesinde NSA'nın bir düşü gerçekleşecek: yabancı ülkelerdeki NSA istasyonlarını kapatmak. NSA, savaş karşıtlarının gösterilerine, parlamento araştırmalarına -en son Avrupa Parlamento-

su örneği- ve yerel görevlilerin kaçmasına neden oldukları için çok göze batan bu istasyonları kapatmayı planlıyor. Geleceğin IOSA projesiyse uyduların başka uydularca dinlenmesine ve pilotsuz uçaklarla istihbarata yönelik. Toplanan bilgiler derhal röle (aracı) uydularla ABD'ye iletilerek işlenecek. (13)

EKLER

AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ*

Avrupa Konseyi Siber Suç Sözleşmesi, 23 Kasım 2001 tarihinde Budapeşte'de, 26'sı üye Avrupa Ülkesi ile ABD, Japonya, Kanada ve Güney Afrika dahil, 30 ülke tarafından imzalandı. Otuz ülkenin şimdi sözleşmeyi, 30 Haziran 2003 tarihine kadar, kendi iç hukuklarına göre uyarlamaları gerekiyor. Sözleşme, Siber Suçlar hakkındaki ilk uluslararası belge olarak kabul ediliyor.

Sözleşmede Tanımlanan Suçlar:

_ Bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar (virus dağıtılması, şirketlerin gizli bilgilerine ulaşılması gibi).

_ Bilgisayarlarla ilişkili suçlar (sanal sahtecilik ve sahtekarlık suçları).

_ İçerikle ilişkili suçlar (çocuk pornografisine sahip olmak ve uluslar arası düzeyde dağıtımını yapmak gibi).

_ Fikri mülkiyet haklarının ihlali ile ilgili suçlar.

AVRUPA SUÇ SORUNLARI KOMİTESİ (CDPC)

SİBER SUÇLAR SÖZLEŞMESİ

8 Kasım 2001'de Avrupa Konseyi Bakanlar Komitesi'nce onaylandı ve ve 23 Kasım 2001'de, Budapeşte'de Uluslararası Siber Suç Konferansı'nda imzaya açılarak kabul edildi.

* Bu sözleşme metni Türkçe'de ilk kez yay>nlanmaktad>r.

Giriş

Avrupa Konseyine üye Ülkeler ve bu belgeyi imza eden diğer Ülkeler;

Avrupa Konseyinin amacının üyeler arasında daha geniş bir birlik sağlamak olduğu düşüncesinden hareketle;

Bu Konvansiyona taraf olan diğer Ülkelerle işbirliğinin geliştirilmesi amacıyla;

Toplumun siber suçlara karşı korunması için atılacak diğer adımlarla birlikte gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi yollarıyla ortak bir cezaî politikanın öncelikli olarak kabul edilmesi gereğiyle;

Bilgisayar ağlarının sayısal hale gelmesinin, tek bir noktaya yönelmesinin ve sürekli küreselleşmesinin beraberinde getirdiği önemli değişikliklerin bilincinde olarak;

Bilgisayar ağlarının ve elektronik bilgilerin cezaî suçların işlenmesi amacıyla kullanılabileceği ve bu tür suçlara ilişkin delillerin bu ağlarda saklanabileceği ve bu ağlar aracılığıyla aktarılabileceği riskini göz önünde bulundurarak;

Siber suçlara karşı mücadelede Ülkelerle özel sektör arasında işbirliğinin gerekliliği ve bilgi teknolojilerinin kullanımı ve geliştirilmesine ilişkin meşru hakların korunması ihtiyacının bilincinde olarak;

Siber suçlara karşı etkili mücadelenin cezaî hususlar konusunda artan, hızlı ve verimli bir uluslararası işbirliğiyle gerçekleşeceğine inanarak;

Bu Konvansiyonun, bilgisayar sistemlerinin, ağlarının ve bilgisayar verilerinin gizliliğine, doğruluğuna ve ulaşılabilirliğine zarar verici faaliyetlerin, ayrıca bu sistemlerin, ağların ve verilerin kötü amaçlı kullanımının engellenmesi, ayrıca bu tür

faaliyetlerin cezaî niteliklerini belirlemek ve söz konusu cezaî suçlarla etkili biçimde mücadele edilmesi için gerekli yetkilerin temin edilmesini sağlamak, ayrıca, bu tür cezaî suçların hem ulusal hem de uluslararası düzeyde belirlenmesi, soruşturulması ve yargıya götürülmesini kolaylaştırmak ve hızlı ve güvenilir bir uluslararası işbirliğinin sağlanması için gerekli düzenlemelerin yapılmasını temin etmek için gerekli olduğu inancıyla;

Her bir bireyin herhangi bir müdahale olmaksızın düşünme, düşündüklerini ifade etme, her türlü bilgiyi ve düşünceyi sınırsız şekilde aramak, almak ve iletme hakkını ve özel hayata saygıya ilişkin hakları teyit eden 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Konvansiyonu, 1966 Birleşmiş Milletler Uluslararası Sivil ve Siyasi Haklar Sözleşmesi ve diğer insan hakları anlaşmalarının gereken şekilde belirttiği üzere, yasaların yürürlüğe sokulması hususu ile temel insan haklarına saygı konusunda sağlıklı bir denge belirlenmesine ihtiyaç duyulduğunu bilerek;

1981 Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Konusunda Avrupa Konvansiyonu tarafından da belirtilen kişisel bilgilerin korunmasına hususuna da gerekli önemi vererek;

1989 Birleşmiş Milletler Çocuk Hakları Konvansiyonu ve 1999 Uluslararası Çalışma Örgütü Çocuk İşçilerin Kötü Durumları Konvansiyonunu göz önünde bulundurarak;

Cezaî hususlarda işbirliğine ilişkin mevcut Avrupa Konseyi konvansiyonlarını ve Avrupa Konseyine üye Ülkeler ve diğer Ülkeler arasındaki benzer nitelikli anlaşmaları dikkate almak, ayrıca, işbu Konvansiyonun bilgisayar sistemlerine ve verileriyle ilgili cezaî suçlara ilişkin soruşturmaları ve yasal işlemleri daha etkin kılmak amacıyla başka konvansiyonları

desteklemek ve cezaî suçlara ilişkin olarak elektronik ortamda delil toplanabilmesini sağlamak amacına yönelik olduğu hususunun üzerinde durmak suretiyle;

Siber suçlara karşı mücadelede uluslararası anlayış ve işbirliğini geliştirici nitelikteki gelişmelere ve Birleşmiş Milletlerin, OECD'nin, Avrupa Birliğinin ve G8 ülkelerinin bu çerçevedeki çalışmalarına gereken önemi vererek;

İletişime müdahale edilmesi konulu istinabe müzekkerelerine ilişkin olarak, Cezaî Meselelerde Yardımlaşma Hakkında Avrupa Konvansiyonunun uygulanması hakkındaki R (85) sayılı Tavsiye Kararını, telif ve benzeri haklar alanında korsanlık hakkındaki R (88) 2 sayılı Tavsiye Kararını, emniyet birimlerinin kişisel bilgileri kullanımını düzenleyen R (87) 15 sayılı Tavsiye Kararını, telekomünikasyon hizmetleri ve bu çerçevede özellikle telefon hizmetleri alanında kişisel verilerin korunması hakkındaki R (95) sayılı Tavsiye Kararını, bilgisayar suçlarının tanımlanmasına ilişkin olarak ulusal yasama mercilerine kılavuzluk eden ve bilgisayarla ilgili suçlar hakkındaki R (89) 9 sayılı Tavsiye Kararını, ayrıca, Bilgi Teknolojisi konusundaki cezaî usuller hukukunun sorunları hakkındaki R (95) 13 sayılı Tavsiye Kararını dikkate alarak;

Ulusal ceza hukuku hükümlerini birbirine benzer kılmak ve siber suçlara ilişkin olarak daha etkin sorgulama yapılmasını sağlamak amacına yönelik olan ve Bakanlar Komisyonunun, Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu tarafından siber suçlara yönelik olarak yaptığı çalışmaları desteklemesini tavsiye edici nitelikteki 21. Avrupa Adalet Bakanları Toplantısı (Haziran 1997, Prag) 1 sayılı Kararını, ayrıca, 23. Avrupa Adalet Bakanları Toplantısında (Haziran 2000, Prag) alınan ve toplantıya katılan tarafları, uygun çözümler bulmak suretiyle mümkün olan en fazla sayıda Ülkenin işbu Konvansiyona taraf olmasını temin etmek üzere ça-

lışmalarına devam etmek yönünde teşvik edici nitelikte olan ve, hızlı ve verimli işleyen uluslararası ölçekte ve siber suçlara karşı mücadelenin özel şartlarını göz önünde bulundura-cak bir işbirliğine olan ihtiyacı belirten 3 sayılı Kararı dikkate almak suretiyle;

Avrupa Konseyi Devlet ve Hükümet Başkanları tarafından 10-11 Ekim 1997 tarihinde Strazburg'da yapılan İkinci Zirve'de kabul edilen ve yeni bilgi teknolojilerinin gelişimi konusunda Avrupa Konseyinin standartları ve değerlerine dayanan ortak tepkiler verme amacına yönelik dayalı Eylem Planını göz önünde bulundurarak;

Aşağıda belirtilen hususlarda mutabık kalmışlardır:

Kısım I - Terimler

Madde 1 - Tanımlar

İşbu Konvansiyonda kullanılan aşağıdaki terimler aşağıdaki anlamları ifade edecektir:

a. "bilgisayar sistemi" terimi, bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı ifade edecektir;

b. "bilgisayar verisi" terimi, bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsepti ifade edecektir;

c. "hizmet sağlayıcı" terimi aşağıdaki anlamları ifade edecektir:

1. hizmetlerinden faydalanan kullanıcılara bir bilgisayar aracılığıyla iletişim kurma imkânı sağlayan her türlü kamu ve özel sektör tüzel kişisi, ve

2. söz konusu iletişim hizmeti veya bu hizmetin kullanıcıları adına bilgisayar verilerini işleyen veya saklayan diğer her türlü kişi ve kuruluş.

d. "trafik bilgileri" terimi, bir bilgisayar sistemi kullanılarak yapılan bir iletişime ilişkin olarak, söz konusu iletişim zincirinin bir halkası konumunda bulunan bir bilgisayar sistemi tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, saatini, tarihini, boyutlarını, süresini veya bu iletişimde kullanılan hizmetin tipini gösteren herhangi bir bilgisayar verisini ifade edecektir.

Bölüm II - Ulusal Düzeyde Alınacak Önlemler

Kısım 1 - Maddî Ceza Hukuku

Başlık 1 - Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar

Madde 2 - Yasadışı Erişim

Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar söz konusu *suçu, bilgisayar verilerinin* elde edilmesi amacıyla veya sahtekârlığa yönelik başka bir amaçla güvenlik sisteminin ihlal edilmesi şeklinde, veya, başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilirler.

Madde 3 - Yasadışı Müdahale

Taraflardan her biri, aşağıda sözü edilen bilgisayar verilerinin üzerinde bulunduğu bir bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verile-

rin bulunduğu bilgisayar sistemi üzerinden veri iletimine haksız surette dahil olma fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar söz konusu suçu, sahtekârlık amacını güden bir fiil şeklinde, veya, başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilirler.

Madde 4 - Verilere Müdahale

1. Taraflardan her biri, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiillerinin, kasıtlı olarak yapıldıklarında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

2. Taraflar, yukarıda Paragraf 1'de tanımlanan fiili, söz konusu fiilin ciddi zararla sonuçlanması şartına bağlama haklarını saklı tutabilirler.

Madde 5 - Sistemlere Müdahale

Taraflardan her biri, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

Madde 6 - Cihazların Kötüye Kullanımı

1. Taraflardan her biri, aşağıdaki fiillerin, kasıtlı ve haksız olarak yapıldıklarında kendi ulusal mevzuatı kapsamında ce-

zaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. Aşağıda sıralanan unsurların, Madde 2 ila 5'te tanımlanan fiillere yönelik olarak kullanılmak amacıyla üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı veya başka surette elde edilmesi:

1. Bilgisayar yazılımları da dahil olmak üzere, esas itibarıyla Madde 2 ila 5'te tanımlanan fiillerden herhangi birinin yapılması amacıyla tasarımlanmış veya bu amaca uygun hale getirilmiş cihazlar;

2. bir bilgisayar sisteminin tamamına veya bir kısmına erişim sağlayan bilgisayar şifreleri, erişim kodları veya benzeri veriler;

b. yukarıda (a)(1) ve (2) numaralı paragraflarda sözü edilen unsurların, Madde 2 ila 5'te tanımlanan fiillere yönelik olarak kullanılmak amacıyla elde bulundurulması. Taraflar, alacakları önlemlerde, cezaî sorumluluk doğması için söz konusu unsurlardan belli bir sayıda elde bulundurulması şartı getirebilirler.

2. Yukarıda Paragraf 1'de tanımlanan üretim, satış, kullanım amacıyla tedarik, ithal, dağıtım, başka surette elde etme veya elde bulundurma fiillerinin, işbu Konvansiyonun 2 ila 5 numaralı maddelerinde tanımlanan fiillere yönelik olarak kullanılmak amacıyla değil de, örneğin, bir bilgisayar sisteminin yetkili kişilerce test edilmesi veya korunması amacıyla yapıldığı durumlarda, işbu madde hükümleri cezaî yükümlülük doğurur şekilde yorumlanmayacaktır.

3. Taraflardan her biri, söz konusu hakkın 1(a) ve 2 numaralı paragraflarda belirtilen unsurların satışına, dağıtımına ve başka suretle kullanıma sunulmasına ilişkin durumlarda kul-

lanılmaması şartıyla, işbu maddenin 1 numaralı paragrafını uygulamama haklarını saklı tutmaktadır.

Başlık 2 - Bilgisayarlarla İlişkili Suçlar

Madde 7 - Bilgisayarlarla İlişkili Sahtecilik Fiilleri

Taraflardan her biri, söz konusu verilerin doğrudan doğruya okunabilir ve anlaşılabilir nitelikte olup olmadığına bakılmaksızın, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme fiilinin, söz konusu farklı verilerin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi amacıyla, kasıtlı olarak ve haksız şekilde yapıldığında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar, bu gibi durumlarda cezaî sorumluluğun ortaya çıkmasını, hile veya benzeri bir sahtekârlık niyetinin mevcut olması şartına bağlayabilirler.

Madde 8 - Bilgisayarlarla İlişkili Sahtekârlık Fiilleri

Taraflardan her biri, aşağıdaki faaliyetlerde bulunmak suretiyle bir başkasının mülkiyetinin ziyaına sebep olma fiilinin, kasıtlı ve haksız olarak yapıldığında, kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. Sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilemez kılma;

b. Sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme.

Başlık 3 - İçerikle İlişkili Suçlar

Madde 9 - Çocuk Pornografisiyle İlişkili Suçlar

1. Taraflardan her biri, aşağıdaki fiillerin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. bir bilgisayar sistemi üzerinden dağıtmak amacıyla çocuk pornografisi üretmek;

b. bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak ya da çocuk pornografisine erişim sağlamak;

c. bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ya da yaymak;

d. kişinin, bir bilgisayar sistemi üzerinden kendisi ya da başkası için çocuk pornografisi temin etmesi;

e. bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda çocuk pornografisi bulundurmak

2. Yukarıdaki paragraf 1'de geçen "çocuk pornografisi" terimi aşağıdakileri görsel anlamda teşhir eden pornografik malzemeler anlamına gelmektedir:

a. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı;

b. Cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı;

c. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren görüntüler;

3. Yukarıdaki paragraf 1'de geçen "reşit olmayan kişi" terimi, 18 yaşından küçük kişiler anlamına gelmektedir. Ancak, Taraflardan herhangi biri, daha düşük bir yaş sınırı belirleyebilir. Söz konusu yaş sınırı 16'dan az olmayacaktır.

4. Taraflardan her biri, paragraf 1(d) ve 1(e), ayrıca 2(b) ve 2(c)'yi kısmen uygulama ya da hiç uygulamama haklarını saklı tutar.

Başlık 4 - Telif Haklarının Ve Benzer Hakların İhlaline İlişkin Suçlar

Madde 10 - Telif haklarının ve benzer hakların ihlaline ilişkin suçlar

1. Taraflardan her biri, kendi yasalarında tanımlandığı şekliyle telif haklarının ihlali fiilinin, Edebi ve Sanatsal Eserlerin Korunmasına Yönelik Bern Konvansiyonu çerçevesindeki 24 Temmuz 1971 tarihli Paris Yasası, Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Telif Hakları Anlaşması uyarınca, kasıtlı olarak, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla yapıldığında, kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Sözü geçen Konvansiyonlar çerçevesinde verilen ahlakî haklar bu hükme tabi değildir.

2. Taraflardan her biri, kendi yasalarında tanımlandığı şekliyle telif haklarına benzer hakların ihlali fiilinin, Roma'da imza edilen Oyuncuların, Fonogram Yapımcılarının ve Yayım Kuruluşlarının Korunması Hakkında Konvansiyon (Roma Konvansiyonu), Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Oyunculuk ve Fonogramlar Anlaşması uyarınca, kasıtlı olarak, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla yapıldığında, kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Sözü geçen Konvansiyonlar çerçevesinde verilen ahlakî haklar bu hükme tabi değildir.

3. Taraflardan herhangi biri, belirli durumlarda işbu maddedeki paragraf 1 ve 2 çerçevesinde cezaî yükümlülük ihdas

etmeme hakkını, bu konuda başka yasal yolların bulunması ve bu hakkın saklı tutulmasının söz konusu Tarafın işbu maddedeki paragraf 1 ve 2'de belirtilen uluslararası belgelerdeki uluslararası yükümlülüklerin dışına çıkmasına sebep olmaması şartıyla, saklı tutar.

Başlık 5 - İlave Yükümlülük ve Yaptırımlar

Madde 11 - Teşebbüste bulunmak ve yardım ya da yataklık etmek

1. Taraflardan her biri, işbu Konvansiyonun 2 ila 10. Maddelerinde tanımlanan suçların işlenmesine, söz konusu suçların işlenmesi maksadıyla yardım veya yataklık edilmesi fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

2. Taraflardan her biri, işbu Konvansiyonun 3 ila 5, 7, 8, 9 (1) a ve 9 (1) c Maddelerinde tanımlanan suçları işlemeye teşebbüs edilmesi fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

3. Her bir Ülke, işbu Maddedeki paragraf 2'yi kısmen uygulama ya da hiç uygulamama hakkını saklı tutar.

Madde 12 - Kurumsal Yükümlülük

1. Taraflardan her biri, müstakilen ya da bir tüzel kişilik birimi adına hareket eden ve tüzel kişilik nezdinde aşağıda belirtilen bakımlardan önde gelen bir konumu haiz olan herhangi bir kişi tarafından tüzel kişilik menfaatine işlenen ve işbu Konvansiyonda tanımlanan bir cezaî suça ilişkin olarak tüzel kişiliklerin yükümlü tutulabilmesini temin etmek için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. tüzel kişiliği temsil etme yetkisi bakımından;

b. tüzel kişilik adına karar alma yetkisi bakımından;

c. tüzel kişilik dahilinde kontrolde elinde tutma bakımından.

2. Paragraf 1'de belirtilenlere ek olarak, paragraf 1'de belirtilen bir kişi tarafından gözetim ya da denetim yapılmamasının işbu Sözleşmede tanımlanan bir cezaî suçun tüzel kişilik yetkilerine tabi herhangi bir kişi tarafından tüzel kişilik menfaatine işlenmesine sebep olması halinde tüzel kişiliğin yükümlü tutulabilmesini temin etmek üzere gerekli işlemleri yapacaktır.

3. İlgili Tarafın yasal düzenlemelerine tabi olmak kaydıyla, bir tüzel kişiliğin yükümlülüğü cezaî, adlî ya da idarî nitelikli olabilir.

4. Söz konusu yükümlülük, ilgili suçu işleyen kişinin cezaî yükümlülüğünün hilafına olmayacaktır.

Madde 13 - Yaptırımlar ve Önlemler

1. Taraflardan her biri, Madde 2 ila 11'de tanımlanan cezaî suçların, özgürlüklerin kısıtlanmasını da içeren etkin, adil ve caydırıcı yaptırımlarla cezalandırılabilmesini temin etmek amacıyla gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

2. Taraflardan her biri, Madde 12 uyarınca yükümlü tutulan tüzel kişiliklerin, parasal cezalarını da içeren cezaî nitelikli olan ya da olmayan etkin, adil ve caydırıcı yaptırımlara tabi olmalarını temin edeceklerdir.

Kısım 2 - Usul hukuku

Başlık 1 - Genel Hükümler

Madde 14 - Usul hükümlerinin kapsamı

1. Taraflardan her biri, işbu Kısımda belirtilen yetki ve usullerin esas alınması suretiyle bazı cezaî soruşturma ve işlemlerin yapılabilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

2. Madde 21'de aksi özellikle belirtilen durumlar hariç olmak üzere, Taraflardan her biri, paragraf 1'de değinilen yetki ve usulleri aşağıdakilere ilişkin olarak uygulamaya koyacaktır:

a. İşbu Konvansiyonda Madde 2 ila 11'de tanımlanan cezaî suçlar;

b. Bir bilgisayar sistemi aracılığıyla işlenen diğer cezaî suçlar;

c. Cezaî bir suça ilişkin olarak elektronik ortamda delil toplanması.

a. Taraflardan her biri Madde 20'de belirtilen önlemleri, kendisi tarafından belirlenecek suçlara ya da suç kategorilerine ilişkin olarak uygulama hakkını saklı tutar. Ancak, ilgili Tarafça söz konusu önlemlerin uygulandığı suçlar ya da suç kategorileri, yine ilgili Tarafın Madde 21'de belirtilen önlemleri uyguladığı suçlardan daha sınırlı bir çerçevede olmayacaktır. Taraflardan her biri, suç ya da suç kategorilerinin, Madde 20'de belirtilen önlemin en geniş şekilde uygulanabilecek olmasını sağlamak üzere en geniş şekilde belirlenmesi gerektiğini göz önünde bulunduracaktır.

b. İşbu Konvansiyonun kabul edildiği dönemde yürürlükte bulunan ulusal mevzuatındaki sınırlamalar dolayısıyla işbu Madde 20 ve 21'de belirtilen önlemleri herhangi bir hizmet sağlayıcının bilgisayar sistemi üzerinden iletişime ilişkin olarak uygulayamayan herhangi bir Taraf,

i. söz konusu sistemin belirli bir kullanıcı grubunun menfaatine işletiliyor olması,

ii. söz konusu sistemin halka açık iletişim şebekelerini kullanmıyor olması ve halka açık ya da özel nitelikli başka bir bilgisayar sistemine bağlı olmaması,

halinde, söz konusu aktarıma ilişkin olarak bu önlemleri uygulamama hakkını saklı tutar.

Taraflardan her biri, Madde 20 ve 21'de belirtilen önlemlerin en geniş şekilde uygulanabilecek olmasını sağlayacak şekilde görüş bildirilmesi gerektiğini göz önünde bulunduracaktır.

Madde 15 - Şartlar ve Önlemler

3. Taraflardan her biri, işbu Kısım çerçevesindeki yetki ve usullerin belirlenmesi, uygulanması ve geçerli kılınması hususlarının, ilgili Tarafın ulusal yasalarındaki şartlara ve önlemlere tabi olmasını temin edecektir. Söz konusu hususlar, insan hakları ve özgürlüklerinin, ve bu çerçevede İnsan Haklarının ve Temel Özgürlüklerin Korunması Hakkında 1950 tarihli Avrupa Konseyi Konvansiyonu çerçevesinde, 1966 tarihli Sivil ve Siyasi Haklar Hakkında Uluslararası Birleşmiş Milletler Anlaşması çerçevesinde, ayrıca yürürlükte bulunan diğer uluslararası insan hakları belgeleri çerçevesinde üstlenilen yükümlülüklerden doğan hakların gerekli ölçüde korunmasını temin edecek ve hakkaniyet ilkesinin tesis edilmesini sağlayacaktır.

4. Yukarıda belirtilen şartlar ve önlemler, ilgili yetki ya da usulün niteliği göz önüne alındığında uygun olduğu ölçüde, söz konusu yetki ya da usulün kapsamı ve süresine ilişkin adli ya da başka nitelikli bağımsız gözetim, gerekçelerin haklılığına ilişkin başvuru işlemi, ya da sınırlama yapılmasını da, diğer hususlarla birlikte, içerecektir.

5. Kamu yararının, özellikle de adaletin sağlıklı şekilde yürütülmesinin söz konusu olduğu durumlarda, Taraflar, işbu

Kısımda belirtilen yetki ve usullerin, üçüncü şahısların yetki, sorumluluk, ve meşru menfaatleri üzerindeki etkisini göz önünde bulunduracaktır.

Başlık 2 - Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması

Madde 16 - Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması

1. Taraflardan her biri, yetkili mercilerinin bir bilgisayar sistemi aracılığıyla saklanan bazı bilgisayar verilerinin, bu çerçevede trafik bilgilerinin, korunmasının kolaylaştırılması yönünde talimat vermeleri ya da söz konusu hususu benzer şekilde temin etmelerini sağlamak amacıyla, özellikle bilgisayar verilerinin kaybedilmesinin ya da değiştirilmesinin söz konusu olabileceğine dair gerekçelerin mevcut bulunduğu durumlarda, gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

2. Herhangi bir Tarafın, bir kişinin mülkiyetinde ya da kontrolünde bulunan saklı bazı bilgisayar verilerinin korunması amacıyla ilgili kişiye talimat vermek suretiyle yukarıdaki paragraf 1 hükmünü yürürlüğe sokması halinde, söz konusu Taraf, ilgili kişinin bu bilgisayar verilerinin doğruluğunu azami 90 gün olmak üzere gereken süre boyunca korumasını temin etmek ve bu suretle yetkili mercilerin bu bilgilerin açıklanmasını isteyebilmelerini sağlamak üzere gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

3. Taraflardan her biri, bilgisayar verilerini koruması gereken görevlinin ya da başka bir kişinin bu hususa ilişkin usulleri ilgili Tarafın ulusal mevzuatında belirtilen süre boyunca gizli tutması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

4. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Madde 17 - Trafik Bilgilerinin Korunmasının Kolaylaştırılması ve Kısmen Açıklanması

1. Taraflardan her biri Madde 16 uyarınca korunması gereken trafik bilgilerine ilişkin olarak aşağıdaki hususlara ilişkin olarak gerekli olabilecek yasama işlemlerini ve diğer işlemlerini yapacaktır:

a. trafik bilgilerinin korunması işleminin kolaylaştırılması hususunun, söz konusu bilgilerin bir ya da birden daha fazla hizmet sağlayıcı tarafından iletilmiş olmasına bakılmaksızın sağlanması;

b. ilgili Tarafın yetkili merciine veya bu merciin belirlediği bir kişiye, ilgili Tarafın söz konusu hizmet sağlayıcıları ve bilgilerin iletildiği yolu belirleyebilmesini sağlayacak ölçüde açıklama yapılması işleminin kolaylaştırılması.

2. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Başlık 3 - Üretim Talimatı

Madde 18 - Üretim Talimatı

1. Taraflardan her biri, yetkili mercilerinin aşağıdaki hususlarda talimat verme konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. Söz konusu Tarafın ulusal sınırlar içinde bulunan bir kişinin, söz konusu kişinin mülkiyetinde ya da kontrolünde bulunan ve bir bilgisayar sisteminde veya bilgisayar verilerini saklamak için kullanılan başka bir cihazda saklanan bazı bilgisayar verilerini vermesi yönünde;

b. Söz konusu Tarafın ulusal sınırları içinde hizmet veren bir hizmet sağlayıcının, mülkiyetinde ya da kontrolünde bulunan ve sözü geçen hizmete ilişkin olan abone bilgilerini vermesi yönünde;

2. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

3. İşbu maddede kullanılan "abone bilgileri" terimi, bilgisayar verisi şeklinde ya da başka şekillerde saklanan, ve hizmet sağlayıcının elinde bulunan ve verilen hizmetlere ilişkin olan trafik ya da içerikle ilgili bilgilerinin haricindeki bilgiler anlamına gelmektedir. Bu bilgiler kullanılarak;

a. kullanılan iletişim hizmetinin türü, teknik imkanlar ve hizmet süresi;

b. abonenin kimliği, posta ya da bulunduğu yerin adresi, telefon numarası ve aboneye ulaşılabilecek diğer numaralar, hizmet sözleşmesi veya düzenlemesi esas alınarak verilen fatura ve ödeme bilgileri;

c. hizmet sözleşmesi veya düzenlemesi esas alınarak verilen ve iletişim ekipmanının kurulduğu bölgeye ilişkin olan diğer bilgiler belirlenebilmektedir.

Başlık 4 - Saklanan bilgisayar verilerinin aranması ve bunlara el koyulması

Madde 19 - Saklanan bilgisayar verilerinin aranması ve bunlara el konulması

1. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde aşağıdakileri arama ya da bunlara benzer şekilde erişim sağlama konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. bir bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan bilgisayar verileri; ve

b. bilgisayar verilerinin saklandığı cihazlar.

2. Tarafların her biri, yetkili mercilerinin paragraf 1 (a) uyarınca belirli bir bilgisayar sisteminde ya da bu sistemin bir parçasında arama yapması ya da bunlara erişim sağlaması söz konusu olduğunda, ayrıca, aranan verilerin kendi ulusal sınırları içindeki başka bir bilgisayar sisteminde ya da bu sistemin bir parçasında saklandığına dair gerekçeleri bulunduğunda, söz konusu mercilerin arama ya da erişim işlemlerini bu sistemi kapsayacak şekilde genişletebilmelerini sağlamak üzere gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

3. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine el koyma ya da bunları başka şekillerde koruma altına alınması konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Bu işlemler arasında, aşağıdakilerin yapılabilmesine yönelik yetkilerin sağlanması bulunacaktır:

a. herhangi bir bilgisayar sistemine ya da bu sistemin bir parçasına veya bilgisayar verilerinin saklandığı cihazlara el konulması ya da bunların benzer şekilde koruma altına alınması;

b. bu bilgisayar verilerinin kopyalanıp alıkonulması;

c. söz konusu saklı bilgisayar verilerinin doğruluğunun muhafaza edilmesi; ve

d. erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez kullanılamaz hale getirilmesi ya da silinmesi.

4. Taraflardan her biri, yetkili mercilerinin ilgili bilgisayar sisteminin işleyişi hakkında ya da bu sistem içindeki bilgisayar verilerinin korunması için kullanılan önlemler hakkında

bilgi sahibi olan herhangi bir kişiye, paragraf 1 ve 2'de belirtilen işlemlerin yapılabilmesi için gerekli bilgileri makul şekilde vermesi yönünde talimat vermesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

5. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Başlık 5 - Bilgisayar verilerini gerçek zamanlı olarak toplanması

Madde 20 - Trafik bilgilerinin gerçek zamanlı olarak toplanması

1. Taraflardan her biri, yetkili mercilerinin aşağıdaki hususlarda yetkili olması için gerekli olabilecek yasal işlemleri ve diğer işlemleri yapacaktır:

a. trafik bilgilerinin gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplanması ya da kaydedilmesi, ve

b. herhangi bir hizmet sağlayıcının, mevcut teknik imkanlar çerçevesinde

i. trafik bilgilerini gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplamasının ya da kaydetmesinin, ve

ii. trafik bilgilerinin gerçekli zamanlı olarak toplanması ya da kaydedilmesi konusunda yetkili mercilerle işbirliği yapmasının ve onlara bu hususta yardımcı olmasının temin edilmesi

Söz konusu trafik bilgileri, bir bilgisayar sistemi üzerinden aktarılan ve ilgili Tarafın ulusal sınırları içinde özel iletişim sayılan bilgilerdir.

2. Yerleşik ulusal hukuki düzenlemeler dolayısıyla paragraf 1 (a)'da belirtilen işlemleri yapamayan herhangi bir Taraf, bunların yerine, kendi ulusal sınırları içinde özel iletişim sayılan trafik bilgilerinin gerçek zamanlı olarak söz konusu sınırlar dahilindeki teknik imkanlar kullanılmak suretiyle toplanması ya da kaydedilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapabilir.

3. Taraflardan her biri, bir hizmet sağlayıcıyı işbu Maddede verilen herhangi bir yetki hakkındaki esasları ve bilgileri gizli tutmakla yükümlü kılmak için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

4. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Madde 21 - İçerikle ilgili bilgilere müdahale edilmesi

1. Taraflardan her biri, yetkili mercilerinin, ulusal yasalarca belirlenecek ciddi nitelikli suçlara ilişkin olarak aşağıdakilerin yapılması hususunda yetkili kılınması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. İçerikle ilgili bilgilerin gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplanması ya da kaydedilmesi, ve

b. herhangi bir hizmet sağlayıcının, mevcut teknik imkanlar çerçevesinde

i. içerikle ilgili bilgileri gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplamasının ya da kaydetmesinin, ve

ii. içerikli ilgili bilgilerin gerçekli zamanlı olarak toplanması ya da kaydedilmesi konusunda yetkili mercilerle işbirliği yapmasının ve onlara bu hususta yardımcı olmasının temin edilmesi

İçerikle ilgili söz konusu bilgiler, bir bilgisayar sistemi üzerinden aktarılan ve ilgili Tarafın ulusal sınırları içinde özel iletişim sayılan bilgilerdir.

2. Yerleşik ulusal hukuki düzenlemeler dolayısıyla paragraf 1 (a)'da belirtilen işlemleri yapamayan herhangi bir Taraf, bunların yerine, kendi ulusal sınırları içinde özel iletişim sayılan içerikli ilgili bilgilerin gerçek zamanlı olarak söz konusu sınırlar dahilindeki teknik imkanlar kullanılmak suretiyle toplanması ya da kaydedilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapabilir.

3. Taraflardan her biri, bir hizmet sağlayıcıyı işbu Maddede verilen herhangi bir yetki hakkındaki esasları ve bilgileri gizli tutmakla yükümlü kılmak için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

4. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Kısım 3 - Yargı Yetkisi

Madde 22 - Yargı Yetkisi

1. Taraflardan her biri, işbu Konvansiyonda Madde 2 ila 11 arasında tanımlanan suçlara ilişkin olarak yargı yetkisi tesis etmek için gerekli olabilecek yasama işlemlerini ve diğer işlemleri, söz konusu suçların

a. İlgili Tarafın ulusal sınırları içinde; ya da

b. İlgili Taraf bandırası taşıyan seyir halindeki bir gemide; ya da

c. İlgili Tarafın yasaları çerçevesinde kayıtlı bulunan bir uçakta; ya da

d. d. İlgili Tarafın vatandaşlarından biri tarafından işlenmesi, ve söz konusu suçların işlendikleri yerde ceza hukuku-

na tabi bulunması ya da herhangi bir Ülkenin yargı yetkisine sahip olduğu sınırlar dışında işlenmesi hallerinde yapacaktır.

2. Taraflardan her biri, işbu maddede ya da herhangi bir bölümünde paragraf (1) b ila (1) d çerçevesinde belirtilen yargı yetkilerini yalnızca belirli durum ve şartlarda uygulama ya da uygulamama hakkını saklı tutar.

3. Taraflardan her biri, ulusal sınırları dahilinde bulunan bir zanlının yalnızca tabiyeti esas alınarak bir iade talebini müteakiben başka bir Tarafa iade edilmemesi durumunda, işbu Konvansiyonda Madde 24 paragraf 1'de belirtilen suçlara ilişkin olarak yargı yetkisi tesis etmek için gerekli olabilecek işlemleri yapacaktır.

4. İşbu Konvansiyon herhangi bir ulusal hukuk çerçevesinde uygulanan cezaî yargı yetkisini kapsam dışı bırakmamaktadır.

5. Herhangi bir suç zannına ilişkin olarak birden fazla Tarafın işbu Konvansiyona göre yargı yetkisine sahip bulunduğunu iddia etmesi halinde, söz konusu Taraflar dava için en uygun yargı merciinin belirlenmesi amacıyla görüş alışverişinde

Bölüm III - Uluslararası işbirliği

Kısım I - Genel ilkeler

Başlık 1 - Uluslararası işbirliğine ilişkin genel ilkeler

Madde 23 - Uluslararası işbirliğine ilişkin genel ilkeler

Taraflar, işbu bölüm hükümleri çerçevesinde ve, cezaî meselelerde uluslararası işbirliğine ilişkin uluslararası belgelerin, tek taraflı ya da karşılıklı mevzuata dayalı sözleşmelerin, ve ulusal yasaların bilgisayar sistemlerine ve verilerine ilişkin soruşturma ve davalarda, ya da cezaî suçlara ilişkin

olarak elektronik ortamda delil toplanması amacıyla mümkün olan en geniş biçimde kullanılabilecek şekilde uygulanması vasıtasıyla işbirliğine gideceklerdir.

Başlık 2 - İadeye İlişkin İlkeler

Madde 24 - İade

a. İşbu madde, Taraflar arasında işbu Konvansiyonda Madde 2 ila 11 çerçevesinde tanımlanan cezaî suçlara ilişkin olan iade işlemleri konusunda, söz konusu suçların, ilgili Tarafların yasaları çerçevesinde en az bir yıl özgürlükten mahrum bırakılması şeklinde ya da daha ağır nitelikli bir ceza ile cezalandırılabilir olması şartıyla, geçerli olacaktır.

b. Tek taraflı ya da karşılıklı mevzuat ya da iade anlaşması, bu çerçevede Avrupa İade Sözleşmesi (ETS No.24) esas alınmak suretiyle varılan ve iki ya da daha fazla taraf arasında yürürlükte bulunan anlaşmalar çerçevesinde asgari bir cezanın uygulanmasının söz konusu olduğu durumlarda, söz konusu anlaşma ya da sözleşme çerçevesindeki asgari ceza geçerli olacaktır.

1. İşbu Maddede paragraf 1 çerçevesinde tanımlanan cezaî suçlar, iki ya da daha fazla Taraf arasındaki iade anlaşmaları çerçevesinde iadeye konu olabilen suçlar olarak addedilecektir. Taraflar, bu suçları söz konusu iade anlaşmaları çerçevesinde iadeye konu suçlar olarak addedecekleri yönünde taahhütte bulunmaktadırlar.

2. İade işlemini bu konuda bir anlaşma olması şartına bağlayan herhangi bir Tarafın, kendisi ile iade anlaşması bulunmayan bir Taraftan iade talebi alması halinde, talebi alan Taraf, işbu Konvansiyonu, işbu maddede paragraf 1 çerçevesinde tanımlanan herhangi bir cezaî suça ilişkin olarak gerekli hukuki zemin sayabilir.

3. İade işlemini bu konuda bir anlaşma olması şartına bağlamayan Taraflar, işbu maddede paragraf 1'de tanımlanan cezaî suçları, birbirleri arasında iade işlemi yapılmasına konu olan suçlar olarak tanıyacaklardır.

4. İade işlemi, bu işlemi gerçekleştirmesi talep edilen Tarafın yasalarındaki şartlara ya da yürürlükte bulunan iade anlaşmalarına, ayrıca iade işlemi gerçekleştirmesi talep edilen Tarafın bu işlemi gerçekleştirmeyi reddetmesine zemin teşkil eden gerekçelere tabi olacaktır.

5. İşbu maddede paragraf 1 çerçevesinde belirtilen bir cezaî suça ilişkin olarak iade işlemi gerçekleştirilmesi yönünde bir talebin, yalnızca iadesi istenen kişinin tabiyeti dolayısıyla veya iade işlemi gerçekleştirmesi talep edilen Tarafın söz konusu suça ilişkin olarak yargı yetkisini haiz olduğunu düşünmesi sebebiyle reddedilmesi halinde, iade işlemi gerçekleştirmesi talep edilen Taraf, kendisinden bu işlemi talep eden Tarafın isteği üzerine, meseleyi dava edilmesi amacıyla yetkili mercilerine iletecek ve nihai sonucu iade talebinde bulunan Tarafa gereken şekilde bildirecektir. Bu merciler, kararlarını verirken ve soruşturmalarını sürdürürken, benzer nitelikte bir suçun kendi yasaları çerçevesinde söz konusu olmuş olması durumunda hareket edecekleri şekilde çalışacaklardır.

a. Taraflardan her biri, herhangi bir anlaşmanın olmadığı durumlarda iade ya da geçici tutuklama talebini iletecek ya da bu yönde bir talebi alacak yetkili mercilerden her birinin adını ve adresini Avrupa Konseyi Genel Sekreterine, onay, kabul, tasdik ya da giriş belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde, bildirecektir.

b. Avrupa Konseyi Genel Sekreteri, Tarafların yukarda belirtilen şekilde tespit ettikleri yetkililerin kaydını tutacak ve bu

kaydı sürekli güncelleyecektir. Taraflar, bu kayıtta yer alan bilgilerin her zaman doğru olmasını temin edeceklerdir.

Başlık 3 - Yardımlaşmaya ilişkin genel ilkeler

Madde 25 - Yardımlaşmaya ilişkin genel ilkeler

1. Taraflar, bilgisayar sistemleri ve verileriyle ilgili cezaî suçlara ilişkin soruşturma ve davaların yürütülmesi ya da cezaî bir suça ilişkin olarak elektronik ortamda delil toplanması konusunda birbirlerine mümkün olan en geniş ölçüde yardımcı olacaklardır.

2. Taraflardan her biri, Madde 27 ila 35 çerçevesindeki yükümlülüklerin yerine getirilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaklardır.

3. Taraflardan her biri, acil durumlar söz konusu olduğunda faks ve elektronik posta gibi hızlı iletişim araçlarıyla yardım verilmesi ya da irtibat kurulması talebinde bulunabilir. Ancak, söz konusu araçların güvenlik ve doğruluk açısından gerekli ölçülerde olması (gerektiği takdirde şifreleme kullanarak) ve kendisinden talepte bulunulan Tarafın isteği üzerine resmi teyit mesajı gönderilmesi gerekecektir. Kendisinden talepte bulunulan Taraf, ilgili hızlı iletişim araçları vasıtasıyla iletilen talebi kabul edecek ve bu talebe gerekli cevabı verecektir.

4. İşbu Bölümdeki Maddelerde açıkça belirtilen durumlar hariç olmak üzere, karşılıklı olarak yardım verilmesi hususu, kendisinden talepte bulunulan Tarafın yasalarındaki şartlara veya karşılıklı olarak yardım verilmesine ilişkin anlaşmaların şartlarına, ayrıca kendisinden yardım talep edilen Tarafın bu talebi reddetmesine gerekçe olabilecek şartlara tabi olacaktır. Kendisinden talepte bulunulan Taraf, Madde 2 ila 11 çerçevesinde belirtilen suçlara ilişkin olarak yardım vermeyi, yal-

nızca söz konusu suçları mali nitelikli olarak değerlendirdiği gerekçesine dayanarak, reddetme hakkını kullanmayacaktır.

5. Kendisinden talepte bulunulan Tarafın, işbu bölüm hükümlerine uygun olarak, yardım verme hususunu, ilgili suçun işlendiği her iki yerde de cezaî nitelik taşıması şartına bağlayabildiği durumlarda, talep edilen yardıma konu olan söz konusu suça zemin teşkil eden fiilin yardım talep eden Tarafın yasaları çerçevesinde cezaî nitelik taşıması halinde bu şart, kendisinden yardım talep edilen Tarafın bu suçu yardım talep eden Tarafla aynı kategoriye koymasına ya da aynı terimlerle tespit etmesine bakılmaksızın, yerine getirilmiş sayılacaktır.

Madde 26 - Anında İletilen Bilgiler

1. Herhangi bir Taraf, ulusal yasalarının sınırları çerçevesinde, kendi yürüttüğü soruşturmalar çerçevesinde edindiği bilgileri, bunların açıklanmasının söz konusu bilgileri alan Tarafa işbu Konvansiyonda tanımlanan cezaî suçlara ilişkin soruşturma ve davaların başlatılması konusunda yardımcı olacağını ya da ilgili Tarafın işbirliği talebinde bulunmasını temin edeceğini düşündüğü takdirde, başka bir Tarafa önceden izin almaksızın iletebilir.

2. Söz konusu bilgiler verilmeden önce, bu bilgileri veren Taraf bilgilerin gizli tutulmasını ya da belirli şartlarda kullanılmasını talep edebilir. Bilgileri alan Taraf, bu talebin gereğini yerine getiremeyecek olması halinde bilgileri veren Tarafa bildirimde bulunacak, bilgileri veren Taraf da bilgilerin yine de verilip verilemeyeceğini tespit edecektir. Bilgileri alan Tarafın belirli şartlar çerçevesinde kabul ettiği bilgiler, söz konusu Taraf açısından bağlayıcı olacaktır.

Başlık 4 - Uluslararası anlaşmaların yürürlükte bulunmadığı durumlarda gelen yardım taleplerine ilişkin usuller

Madde 27 - Uluslararası anlaşmaların yürürlükte bulunmadığı durumlarda gelen yardım taleplerine ilişkin usuller

1. Tek taraflı ya da karşılıklı mevzuata dayalı herhangi bir yardım anlaşması ya da düzenlemesinin söz konusu olmadığı durumlarda işbu maddede paragraf 2 ila 10 çerçevesinde geçen hükümler geçerli olacaktır. Bu tür bir anlaşma ya da düzenlemenin söz konusu olduğu durumlarda, ilgili Taraflar bu anlaşmaların yerine bu madde hükümlerinin bir kısmını ya da tamamını geçerli saymayı kabul etmedikleri takdirde, işbu madde hükümleri geçerli olmayacaktır.

a. Taraflardan her biri yardım taleplerinde bulunmak, bu taleplere cevap vermek, bu taleplerin gereğini yerine getirmek, ya da bunların gereğini yerine getirecek mercilere bu talepleri iletmekle görevli bir merci ya da merciler belirleyecek.

b. Söz konusu merciler birbirleriyle doğrudan haberleşeceklerdir

c. Taraflardan her biri, herhangi bir anlaşmanın olmadığı durumlarda işbu paragraf gereğini yapacak yetkili mercilerden her birinin adını ve adresini Avrupa Konseyi Genel Sekreterine, onay, kabul, tasdik ya da giriş belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde, bildirecektir.

d. Avrupa Konseyi Genel Sekreteri, Tarafların yukarda belirtilen şekilde tespit ettikleri yetkililerin kaydını tutacak ve bu kaydı sürekli güncelleyecektir. Taraflar, bu kayıtta yer alan bilgilerin her zaman doğru olmasını temin edeceklerdir.

2. İşbu Madde çerçevesindeki karşılıklı yardım talepleri, talepte bulunan Tarafça tespit edilecek usullere göre işleme konacaktır. Kendisinden talepte bulunulan Tarafın yasalarında bu hususa aykırı bir durum varsa bu hüküm geçerli olmayacaktır.

3. Kendisinden talepte bulunulan Taraf, Madde 25 Paragraf (4) çerçevesindeki red gerekçelerine ek olarak, aşağıdaki hususlar söz konusu olduğunda yardım vermeyi kabul etmeyebilir:

a. yardım talebine konu olan suçun kendisinden yardım talep edilen Tarafça siyasi suç ya da siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; ya da

b. söz konusu talebin gereğinin yerine getirilmesinin kendisinden yardım talep edilen Tarafın egemenliğine, emniyetine, kamu düzenine ya da diğer önemli menfaatlerine zarar verici olarak değerlendirilmesi

4. Kendisinden talepte bulunulan Taraf, herhangi bir talebe ilişkin olarak işlem yapmasının yetkili mercilerince sürdürülmekte olan cezaî soruşturma ya da işlemlere zarar vermesinin söz konusu olabileceği durumlarda, bu talebe ilişkin işlemleri tehir edebilir.

5. Kendisinden talepte bulunulan Taraf, yardım vermeyi red ya da tehir etmeden önce, ve gerekli durumlarda yardım talep eden Tarafla görüş alışverişinde bulunarak, yardımın kısmen verilip verilemeyeceği ya da bazı şartlara tabi olarak verilebileceği hususunu karara bağlar.

6. Kendisinden talepte bulunulan Taraf, yardım talebinin işleme konmasından hasıl olan neticeyi talepte bulunan Tarafa bildirecektir. Talebin reddi ya da tehiri halinde bunlara ilişkin gerekçeler bildirilecektir. Talebin yerine getirilmesini imkansız kılan ya da önemli ölçüde geciktirecek olan gerekçeler de bildirilecektir.

7. Talepte bulunan taraf, kendisinde talepte bulunulan Tarafın, işbu Bölüm çerçevesinde iletilen taleplerin esasına ve içeriğine ilişkin bilgileri, söz konusu talebin karşılanması için

bilgilerin gizli tutulmamasının gerekli olduğu durumlar hariç olmak üzere, gizli tutmasını isteyebilir. Kendisinden talepte bulunulan Taraf, bilgilerin gizli tutulmasına ilişkin talebi gerçekleştiremeyecek olması halinde, bu durumu talepte bulunan Tarafa derhal bildirecek, ve talepte bulunan Taraf talebin yine de gerçekleştirilip gerçekleştirilmeyeceği yönünde karar verecektir.

a. Acil durumlarda, yardım talepleri ya da bu taleplere ilişkin yazışmalar, doğrudan talep eden Tarafın adli mercileri aracılığıyla kendisinden yardım talep edilen Tarafın adli mercilerine iletilebilir. Bu tür durumlarda, yardım talep eden Taraf, yapılan yazışmaların bir nüshasını yetkili mercii aracılığıyla kendisinden yardım edilen Tarafın yetkili merciine gönderecektir.

b. İşbu paragraf çerçevesinde iletilecek talepler ve sair yazışmalar Interpol aracılığıyla gönderilebilir.

c. İşbu maddenin (a) paragrafına uygun olarak talepte bulunulması ve ilgili merciin bu talebe ilişkin olarak işlem yapamıyor olması halinde, söz konusu merci, talebi ulusal düzeyde yetkili olan mercie iletecek ve bu durumu yardım talep eden Tarafa bildirecektir.

d. İşbu paragraf çerçevesinde iletilen ve zorlayıcı unsurlar içermeyen talepler ya da yazışmalar, talepte bulunan Tarafın yetkili mercilerince kendisinden talepte bulunulan Tarafın yetkili mercilerine doğrudan iletilebilir.

e. Taraflardan her biri, işbu paragraf çerçevesinde iletilen taleplerin daha etkin şekilde ele alınabilmesi için yetkili mercie iletilmesi gerektiğini Avrupa Konseyi Genel Sekreterine, onay, kabul, tasdik ya da giriş belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde, bildirecektir.

Madde 28 - Kullanımda gizlilik ve sınırlama

1. Tek taraflı ya da karşılıklı mevzuata dayalı herhangi bir yardım anlaşması ya da düzenlemesinin söz konusu olmadığı durumlarda işbu madde hükümleri geçerli olacaktır. Bu tür bir anlaşma ya da düzenlemenin söz konusu olduğu durumlarda, ilgili Taraflar bu anlaşmaların yerine bu madde hükümlerinin bir kısmını ya da tamamını geçerli saymayı kabul etmedikleri takdirde, işbu madde hükümleri geçerli olmayacaktır.

2. Kendisinden talepte bulunulan Taraf, aşağıdaki şartlara bağlı olarak herhangi bir talep karşılığında bilgi ya da malzeme verebilir:

a. Hukuki yardım talebinin bu şartın yerine getirilmemesi halinde karşılanamadığı durumlarda söz konusu bilgi ya da malzemelerin gizli tutulması, ya da

b. Söz konusu bilgi ya da malzemelerin talepte belirtilenler dışında başka bir soruşturma ya da yasal işlem için kullanılmaması

3. Talepte bulunan Taraf, paragraf 2'de belirtilen şartları yerine getiremeyecek olması halinde, diğer Tarafı bu konuda bilgilendirecek, diğer Taraf da bilgilerin her halükarda verilmesini isteyip istemediği konusunda karar verecektir. Şartın kabul edilmesi talepte bulunan Taraf açısından bağlayıcı olacaktır.

4. Paragraf 2'de belirtilen şartların yerine getirilmesi kaydıyla bilgi ya da malzeme veren herhangi bir Taraf, diğer Tarafın söz konusu şarta ilişkin olarak bilgilerin ve malzemelerin nasıl kullanıldığı konusunda açıklama yapmasını isteyebilir.

Kısım 2 - Özel Hükümler

Başlık 1 - Geçici önlemlerin alınması konusunda yardımlaşma

Madde 29 - Saklanan bilgisayar verilerinin korunmasının kolaylaştırılması

1. Taraflardan herhangi biri, başka bir Tarafın ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla saklanan ve talepte bulunan Tarafın araştırma, erişim, el koyma ya da benzer şekilde elde tutma amacıyla yardım talebine konu etmeyi düşündüğü ya da açıklanmasını talep edeceği verilerin korunması işleminin kolaylaştırılmasını söz konusu Taraftan talep edebilir.

2. Paragraf 1 çerçevesinde bilgilerin korunması amacıyla yapılan talepler:

a. Verilerin korunmasını isteyen mercii

b. cezaî soruşturmaya ya da işleme konu olan suç ve ilgili esasların özetini

c. saklanan bilgisayar verilerini elinde bulunduran kişiyi ya da bilgisayar sisteminin yerini belirleyebilmek için elde bulunan bilgileri

d. verilerin korunmasının gerekliliğini; ve

e. ilgili Tarafın saklanan bilgisayar verilerine ilişkin olarak araştırma, erişim, el koyma ya da benzer şekilde elde tutma işlemi ve açıklama yapılması amacıyla yardım talebinde bulunmayı düşünüyor olduğunu belirtici nitelikte olacaktır.

3. Kendisinden talepte bulunulan Taraf, ilgili talebi aldıktan sonra ilgili verileri ulusal yasalarına uygun olarak korunması işleminin kolaylaştırılması için gerekli önlemleri alacaktır. Herhangi bir talebe cevap verilmesinin söz konusu oldu-

ğu durumlarda, verilerin korunmasının, ilgili suçun her iki Tarafın sınırları dahilinde de cezaî niteliğinin bulunması şartı aranmayacaktır.

4. İşbu Konvansiyonda Madde 2 ila 11 çerçevesinde tanımlananlar dışındaki suçlara ilişkin olarak verilerin araştırılması, verilere erişim sağlanması, el konulması ya da verilerin benzer şekilde elde tutulması veya açıklanması amacıyla yardım sağlanması amacına yönelik bir talebe cevap vermek için ilgili suçun her iki Tarafın sınırları dahilinde de cezaî niteliğinin bulunması şartını arayan bir Taraf, söz konusu şartın verilerin açıklandığı tarihte yerine getirilemiyor olduğunu gösteren gerekçeler bulunması halinde, işbu madde çerçevesinde verilerin korunması amacıyla iletilen talepleri reddetme hakkını saklı tutar.

5. Yukarıdakilere ek olarak, verilerin korunması amaçlı bir talep ancak aşağıdaki durumlarda reddedilebilir:

a. yardım talebine konu olan suçun kendisinden yardım talep edilen Tarafça siyasi suç ya da siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; ya da

b. söz konusu talebin gereğinin yerine getirilmesinin kendisinden yardım talep edilen Tarafın egemenliğine, emniyetine, kamu düzenine ya da diğer önemli menfaatlerine zarar verici olarak değerlendirilmesi.

6. Kendisinden yardım talep edilen Taraf, verilerin korunması işleminin verilere gelecekte ulaşılamamasına sebep olacağını ya da yardım talep eden Tarafın yürüttüğü soruşturmanın gizliliğini zedeleyeceğini ya da buna başka şekillerde zarar vereceğini düşünmesi halinde, bu düşüncesini yardım talep eden Tarafa en kısa sürede bildirecek, talepte bulunan Taraf da yardım talebinin gereğinin her halükarda yapılmasını isteyip istemediği yönünde karar verecektir.

7. Paragraf 1'de belirtilen talebe cevaben yerine getirilen koruma işlemi en az 60 gün sürecek, bu suretle talepte bulunan Tarafın verilerin araştırılması, verilere erişim sağlanması, el konulması ya da verilerin benzer şekilde elde tutulması veya açıklanması amacıyla talepte bulunabilmesi sağlanacaktır. Bu yönde bir talebin alınmasının ardından, veriler söz konusu talep konusunda bir karar verilene dek korunacaktır.

Madde 30 - Korunan trafik verilerinin açıklanması işleminin kolaylaştırılması

1. Özel iletişim sayılan trafik verilerinin korunmasına ilişkin olarak Madde 29 çerçevesinde iletilen talebin yerine getirilmesi sırasında, kendisinden yardım talep edilen Tarafın başka bir Ülkedeki bir hizmet sağlayıcının söz konusu iletişimin sağlanmasında dahli bulunduğunu keşfetmesi halinde, söz konusu Taraf, talepte bulunan Tarafa, ilgili hizmet sağlayıcının ve verilerin aktarıldığı yolun belirlenmesi için gerekli olacak ölçüde trafik verisini en kısa sürede açıklayacaktır.

2. Paragraf 1 çerçevesinde trafik verilerinin açıklanması işlemi ancak aşağıdaki durumlarda gerçekleşmeyebilir:

a. yardım talebine konu olan suçun kendisinden yardım talep edilen Tarafça siyasi suç ya da siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; ya da

b. söz konusu talebin gereğinin yerine getirilmesinin kendisinden yardım talep edilen Tarafın egemenliğine, emniyetine, kamu düzenine ya da diğer önemli menfaatlerine zarar verici olarak değerlendirilmesi.

Başlık 31 - Soruşturma yetkileri konusunda yardımlaşma

Madde 31 - Saklanan bilgisayar verilerine erişilmesine ilişkin yardımlaşma

1. Taraflardan herhangi biri, kendisinde talepte bulunulan Tarafın ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla saklanan verilerin, bu çerçevede Madde 29 uyarınca korunan verilerin, söz konusu Tarafça araştırılması, bunlara erişilmesi, el konulması ya da bunların benzer şekilde elde tutulması ya da açıklanması amacıyla söz konusu Taraftan talepte bulunabilir.

2. Kendisinden yardım talep edilen Taraf, bu talebe, Madde 23'te belirtilen uluslararası belgelerin, düzenlemelerin ve yasaların, ayrıca işbu Bölümün ilgili hükümlerinin uygulamaya konması suretiyle cevap verecektir.

3. Söz konusu talebe cevap verilmesi işlemi aşağıdakiler söz konusu olduğunda daha hızlı gerçekleştirilecektir:

a. ilgili verilerin kaybolmasının ya da değiştirilmesinin söz konusu olabileceğine dair gerekçeler bulunması; ya da

b. paragraf 2'de belirtilen belge, düzenleme ve yasaların başka şekillerde hızlı bir işbirliği sağlıyor olması

Madde 32 - Saklanan bilgisayar verilerine izinli şekilde ya da bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlamak

Herhangi bir Taraf, diğer Tarafın iznini almaksızın:

a. kullanıma açık (herkesin ulaşabileceği bir kaynaktan gelen) saklı bilgisayar verilerine, bu verilerin coğrafi konumuna bakılmaksızın erişebilir; ya da

b. ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla, başka bir Taraf dahilinde bulunan saklı bilgisayar verilerine, bu verileri söz konusu bilgisayar sistemi üzerinden açıklama yetkisini haiz olan kişinin iznini yasal olarak aldıktan sonra erişebilir ya da bunları alabilir.

Madde 33 - Trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma

1. Taraflar, kendi ulusal sınırları içinde özel iletişim olarak görülen ve bir bilgisayar sistemi üzerinden aktarılan trafik verilerinin gerçek zamanlı olarak toplanması için birbirlerine yardımcı olacaklardır. Paragraf 2'ye tabi olmak kaydıyla, bu yardım ulusal yasalarda belirtilen şartlara ve usuller çerçevesinde gerçekleşecektir.

2. Taraflardan her biri, en azından, ulusal sınırlar içinde trafik verilerinin gerçek zamanlı olarak toplanabilmesini mümkün kılanlara benzer nitelikteki cezaî suçlar konusunda yardım sağlayacaktır.

Madde 34 - İçerikle ilgili verilere müdahale edilmesi konusunda yardımlaşma

Taraflar, bir bilgisayar sistemi aracılığıyla aktarılan özel iletişimlere ilişkin içerik bilgilerinin gerçek zamanlı olarak toplanması veya kaydedilmesine ilişkin olarak, ulusal yasalarının izin verdiği ölçüde birbirlerine yardımcı olacaklardır.

Başlık 3 - 24 saat 7 gün boyunca elverişli ağ

Madde 35 - 24/7 Ağı

1. Taraflardan her biri, bilgisayar sistemleri ve verileriyle ilgili cezaî suçlar konusundaki soruşturma ve davaların yürütülmesi ya da cezaî bir suça ilişkin olarak elektronik ortamda delil toplanabilmesi işlemlerine ilişkin olarak en kısa sürede yardım temin edilmesini sağlamak üzere haftanın 7 günü 24 saat boyunca elverişli olan bir irtibat noktası belirleyecektir. Söz konusu yardım, aşağıdakilerin kolaylaştırılması ya da ulusal yasa ve uygulamaların uygun görmesi halinde doğrudan yapılması ile olacaktır:

a. teknik görüş verilmesi;

b. Madde 29 ve 30 uyarınca verilerin korunması; ve

c. Delil toplanması, yasal bilgilerin verilmesi, şüphelilerin yerlerinin bulunması.

a. Tarafların irtibat noktaları hızlı iletişim sağlanmasına elverişli nitelikte olacaktır.

b. Herhangi bir Tarafın belirlediği irtibat noktasının, ilgili Tarafın uluslararası yardımlardan ya da iadeden sorumlu merciinin ya da mercilerinin bir parçası olmaması durumunda, söz konusu irtibat noktasının ilgili merci ya da mercilerle hızlı bir şekilde koordinasyon sağlayabilecek nitelikte olması gerekmektedir.

2. Taraflardan her biri, ağın rahat biçimde işletilmesini sağlayacak eğitimi ve teçhizatı haiz personel bulunmasını temin edecektir.

Bölüm IV - Diğer Hükümler

Madde 36 - İmza ve yürürlük

1. İşbu Konvansiyon, Avrupa Konseyine üye Ülkelerin ve bu belgenin hazırlanmasında payı bulunan üye olmayan Ülkelerin imzasına açık olacaktır.

2. İşbu Konvansiyon, tasdik edildikten, kabul edildikten ve onaylandıktan sonra yürürlüğe girecektir. Tasdik, kabul ve onay evrakı Avrupa Konseyi Genel Sekreterine teslim edilecektir.

3. İşbu Konvansiyon, en az üçü Avrupa Konseyi üyesi olan beş Ülkenin, işbu Konvansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettikleri tarihten sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır.

4. İşbu Konvansiyon, Konvansiyonun bağlayıcılığını kabul eden Ülkelere ilişkin olarak, söz konusu Ülkelerin işbu Kon-

vansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettikleri tarihten sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır.

Madde 37 - Konvansiyona Katılım

1. İşbu Konvansiyonun yürürlüğe girmesinin ardından Avrupa Konseyi Bakanlar Kurulu, Konvansiyonu İmza Eden Ülkelerle görüş alışverişinde bulunup onların oybirliğiyle ilgili karara varmalarının ardından, Konsey üyesi olmayan ve işbu Konvansiyonun hazırlanmasında payı bulunmayan herhangi bir Ülkeyi Konvansiyona katılmaya davet edebilir. Bu konudaki karar, Avrupa Konseyi Yasası Madde 20 (d)'de belirtilen çoğunluk tarafından ve Bakanlar Kurulunda bulunmaya yetkili İmza Eden Ülkelerin yetkili temsilcilerinin oybirliğiyle alınacaktır.

2. İşbu Konvansiyon, paragraf 1 çerçevesinde Konvansiyona katılan herhangi bir Ülkeye ilişkin olarak, söz konusu Ülkenin işbu Konvansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettiği tarihten sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır.

Madde 38 - Belirli Bölgelerde Yürürlük

1. Ülkelerden herhangi biri, tasdik, kabul, onay ya da katılım belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde işbu Konvansiyonun hangi bölge ya da bölgelerde yürürlükte bulunacağını belirleyebilir.

2. Taraflardan herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben yazılı beyanda bulunmak suretiyle, işbu Konvansiyonun söz konusu beyanda belirtilen bölgelerde de yürürlüğe girmesini temin edebilir. İşbu Konvansiyon, söz konu-

su bölgelerde, Genel Sekreterin belirtilen beyanı teslim aldığı tarihten sonraki üç ayın ardından gelen ayın ilk gününde yürürlüğe girecektir.

3. Yukarıdaki iki paragraf çerçevesinde iletilen herhangi bir yazılı beyan, bu beyanda belirtilen bölgelere ilişkin olarak, Avrupa Konseyi Genel Sekreterine hitaben gönderilecek bir bildirimle geri çekilebilir. Söz konusu beyanın geri çekilmesi işlemi, bu bildirimin Genel Sekreter tarafından teslim alındığı tarihten sonraki üç ayın ardından gelen ayın ilk gününde yürürlük kazanacaktır.

Madde 39 - Konvansiyonun Sonuçları

1. İşbu Konvansiyon, Taraflar arasında yürürlükte bulunan çok taraflı ya da ikili anlaşmaları ya da düzenlemeleri, ve bu çerçevede aşağıdakilerin hükümlerini, desteklemek amacına yöneliktir:

n 13 Aralık 1957 tarihinde Paris'te imzaya açılan Avrupa İade Konvansiyonu (ETS No. 24)

n 20 Nisan 1959 tarihinde Strazburg'ta imzaya açılan Cezaî Meselelerde Yardımlaşma Hakkında Avrupa Konvansiyonu (ETS No. 30)

n 17 Mart 1987 tarihinde imzaya açılan Cezaî Meselelerde Yardımlaşma Hakkında Avrupa Konvansiyonuna İlişkin Ek Protokol (ETS No. 99)

2. İki ya da daha fazla sayıda Tarafın işbu Konvansiyonda ele alınan konulara ilişkin olarak daha önceden yapmış bulundukları bir anlaşma olduğu veya bu konuları başka şekillerde karara bağlamış oldukları takdirde, veya bunların gelecekte söz konusu olmaları halinde, ilgili Taraflar bu sözleşme ya da anlaşmaları da uygulama veya ilişkilerini bunlara uygun olarak düzenleme hakkını haiz olacaklardır. Ancak,

Tarafların işbu Konvansiyonda ele alınan hususlara ilişkin meseleleri işbu Konvansiyonda belirtilen şekilde karara bağlamamış olmaları halinde, bu Tarafların hususa ilişkin olarak alacakları kararlar işbu Konvansiyonun amaç ve ilkeleriyle tutarsız olmayacaktır.

3. İşbu Konvansiyon içeriği, Taraflardan herhangi birine ilişkin diğer haklar, sınırlamalar, yükümlülükler ve sorumlulukları etkilemeyecektir.

Madde 40 - Yazılı Beyanlar

Ülkelerden herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben yazılan bir bildirim vasıtasıyla, tasdik, kabul, onay ve katılım belgesini imzaladığında ya da teslim ettiğinde, Madde 2, Madde 3, Madde 6, paragraf 1 (b), Madde 7, Madde 9, paragraf 3 ve Madde 27, paragraf 9 (e) çerçevesinde belirtilen şekilde ek unsurlar talep edebileceğini beyan edebilir.

Madde 41 - Federal Ülkelere ilişkin Hüküm

1. Federal bir Ülke, işbu Konvansiyonda Bölüm II çerçevesinde belirtilen yükümlülükleri, merkezi hükümeti ile federal Ülkeyi oluşturan Eyaletler ve benzer nitelikteki idari bölgeler arasındaki ilişkilerin dayandığı esaslarla tutarlı şekilde kabul etme hakkını, Bölüm III çerçevesinde işbirliğine gidebilecek olmak şartıyla, saklı tutar.

2. Söz konusu hakkı Paragraf 1'de belirtilen şekilde saklı tutan bir federal Ülke, bu hakkın saklı tutulmasına ilişkin şartları, Bölüm II'de belirtilen işlemlerin yapılmasına ilişkin yükümlülüklerden hariç tutulacak ya da bu yükümlülükleri önemli ölçüde azaltacak şekilde uygulayamaz.

3. Federal hükümet, işbu Konvansiyonun, federal Ülkeyi oluşturan ve federasyonun anayasal sistemi gereği yasama

işlemleri yapması gerekmeyen Eyaletlerin ya da diğer idari birimlerin yargı yetkisine tabi bulunarak uygulanan hükümlerine ilişkin olarak, söz konusu Eyaletlerin yetkili mercilerini federal hükümetin tercih ettiği görüşü de ileterek bilgilendirecek ve bu mercileri söz konusu hükümlerin gereğini yapmaları hususunda teşvike çalışacaktır.

Madde 42 - Hakların Saklı Tutulması

Ülkelerden herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben yazılan bir bildirim vasıtasıyla, tasdik, kabul, onay ve katılım belgesini imzaladığında ya da teslim ettiğinde, Madde 4, paragraf 2, Madde 6, paragraf 3, Madde 9, paragraf 4 ve Madde 10, paragraf 3, Madde 11, paragraf 3, Madde 14 paragraf 3, Madde 22, paragraf 2, Madde 29, paragraf 4, ve Madde 41, paragraf 1 çerçevesinde belirtilen hakları saklı tutabileceğini beyan edebilir. Bunların dışında saklı tutulabilecek başka bir hak bulunmamaktadır.

Madde 43 - Saklı tutulan hakların durumu ve hakların saklı tutulması işleminden vazgeçilmesi

1. Madde 42 çerçevesinde herhangi bir hakkı saklı tutan bir Taraf, söz konusu hakkı saklı tutma fiilinden, Genel Sekretere hitaben yazılı bildirimde bulunmak suretiyle kısmen ya da tamamen vazgeçebilir. Vazgeçme işlemi, ilgili bildirimin Genel Sekreter tarafından alındığı tarihte yürürlük kazanacaktır. Söz konusu bildirimde, vazgeçme işleminin bildirim dahilinde belirtilen tarihte yürürlük kazanacağının belirtilmesi ve bu tarihin bildirimin Genel Sekreter tarafından alındığı tarihten sonrasına denk düşmesi halinde, vazgeçme işlemi daha sonraki tarihte yürürlük kazanacaktır.

2. Herhangi bir hakkı Madde 42'de belirtilen şekilde saklı tutan herhangi bir Taraf, söz konusu saklı tutma fiilinden şartlar elverdiğinde vazgeçecektir.

3. Avrupa Konseyi Genel Sekreteri, Madde 42'de belirtilen şekilde bir ya da birkaç hakkı saklı tutan Taraflarla, söz konusu saklı tutma fiilinden vazgeçmelerinin temini amacıyla belirli aralıklarla gerekli görüşmelerde bulunabilir.

Madde 44 - Değişiklikler

1. Herhangi bir Taraf işbu Konvansiyonda değişiklik yapılması amacıyla teklifte bulunabilir. Söz konusu değişiklikler Avrupa Konseyi Genel Sekreteri tarafından Avrupa Konseyine üye Ülkelere, işbu Konvansiyonun hazırlanmasında payı bulunan üye olmayan Ülkelere, ayrıca, Madde 37'ye uygun olarak işbu Konvansiyona katılan ya da katılmaya davet edilen herhangi bir Ülkeye bildirilecektir.

2. Herhangi bir tarafın yapılmasını teklif ettiği değişiklikler, Suçlarla İlgili Problemler Hakkında Avrupa Komisyonuna bildirilecek, bu Komisyon da teklif edilen değişikliğe ilişkin görüşünü Bakanlar Kuruluna sunacaktır.

3. Bakanlar Kurulu, yapılması teklif edilen değişikliği ve Suçlarla İlgili Problemler Hakkında Avrupa Komisyonunun bu konudaki görüşünü değerlendirdikten ve üye ülke olmayan Taraflarla görüş alışverişinde bulunduktan sonra değişikliği kabul edebilir.

4. Bakanlar Kurulunun işbu maddedeki paragraf 3 çerçevesinde kabul ettiği değişikliğe ilişkin metin, kabul edilmesi amacıyla Taraflara gönderilecektir.

5. İşbu Maddedeki Paragraf 3 çerçevesinde yapılması kabul edilen herhangi bir değişiklik, Tarafların tamamının söz konusu değişikliği kabul ettiklerini Genel Sekretere bildirdikleri tarihten sonraki otuzuncu günde yürürlüğe girecektir.

Madde 45 - Anlaşmazlıkların Çözümü

1. Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, İşbu Konvansiyonun yorumlanması ve uygulanmasına ilişkin olarak sürekli şekilde bilgilendirilecektir.

2. Taraflar arasında işbu Konvansiyonun yorumlanması ya da uygulanmasına ilişkin olarak herhangi bir anlaşmazlık doğması halinde, Taraflar bu anlaşmazlığı görüşme yoluyla ya da kendilerinin tercih edeceği başka bir barışçıl yolla gidermeye çalışacaklardır. Bu çerçevede söz konusu anlaşmazlığın, ilgili Tarafların üzerinde anlaşacağı şekilde, Suçlarla İlgili Problemler Hakkında Avrupa Komisyonuna, kararları Tarafları bağlayıcı bir tahkim heyetine, ya da Uluslararası Adalet Divanına iletilmesi söz konusu olabilecektir.

Madde 46 - Tarafların Görüş Alışverişinde Bulunmaları

1. Taraflar, gerekli durumlarda, aşağıdaki hususların kolaylaştırılması amacıyla görüş alışverişinde bulunacaklardır:

a. işbu Konvansiyondan verimli bir şekilde kullanıma konması ve uygulanması, bu çerçevede bu hususlara ilişkin problemlerin ve işbu Konvansiyon çerçevesinde iletilen beyanlara ya da saklı tutulan haklara ilişkin neticelerin belirlenmesi;

b. siber suçlara ilişkin olan önemli hukuki, siyasi ya da teknolojik gelişmeler ve elektronik ortamda bilgi toplanması konularında bilgi alışverişinde bulunulması;

c. Konvansiyonun başka belgelerle desteklenmesi ya da Konvansiyonda değişiklik yapılması.

2. Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, paragraf 1'de belirtilen görüş alışverişlerinden hasıl olan neticeler konusunda belirli aralıklarla sürekli bilgilendirilecektir.

3. Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, gerekli durumlarda, paragraf 1'de belirtilen şekilde görüş alışverişinde bulunulmasını kolaylaştıracak ve Taraflara, işbu Konvansiyonun başka belgelerle desteklenmesi ya da Konvansiyonda değişiklik yapılması konusunda yardım etmek

üzere gerekli işlemleri yapacaktır. İşbu Konvansiyon yürürlüğe girdikten sonra en geç üç yıl içinde Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, Taraflarla işbirliğine giderek Konvansiyon hükümlerinin gözden geçirecek ve gerekli değişikliklere ilişkin teklifte bulunacaktır.

4. Masrafların Avrupa Konseyince üstlenildiği durumlar hariç olmak üzere, paragraf 1 hükümlerinin yerine getirilmesi için yapılan harcamalar Taraflarca kendilerinin belirleyeceği şekilde karşılanacaktır.

5. Avrupa Konseyi Sekreterliği, Taraflara, işbu Madde çerçevesindeki işlemlerin yapılması konusunda yardımcı olacaktır.

Madde 47 - Konvansiyondan Ayrılma

1. Taraflardan herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben bildirimde bulunmak suretiyle işbu Konvansiyondan dilediği zaman ayrılabilir.

2. Konvansiyondan ayrılma işlemi, ilgili bildirimin Genel Sekreter tarafından alınmasından sonraki üç ayın bitiminden sonraki ayın ilk gününde yürürlük kazanacaktır.

Madde 48 - Bildirimler

Avrupa Konseyi Genel Sekreteri, Avrupa Konseyine üye Ülkelere, işbu Konvansiyonun hazırlanmasında payı bulunan üye olmayan Ülkelere, ayrıca, işbu Konvansiyona katılan ya da katılmaya davet edilen Ülkelere aşağıdaki hususlarda bildirimde bulunacaktır:

a. Herhangi bir belgenin imza edilmesi;

b. Herhangi bir tasdik, kabul, onay ya da katılım belgesinin teslim edilmesi;

c. İşbu Konvansiyonun Madde 36 ve 37 uyarınca yürürlüğe girdiği herhangi bir tarih;

d. Madde 40 ve 41 çerçevesinde iletilen herhangi bir beyan ya da Madde 42 çerçevesinde herhangi bir hakkı saklı tutma fiili;

e. İşbu Konvansiyona ilişkin başka işlemler, bildirimler ve sair muhaberat.

NOTLAR

1- Erdal Kaplanseren NTV-MSNBC 13 Eylül 2001

2- http://www.bianet.org/diger/makale8063.htm

3-http://www.program.arsivi.com/haber/haber.asp?id=445

4- Time Dergisi 21 Ağustos 1995

5- http://www.sanalteror.gen.tr/bilgi/nedir.html

6- http://www.sanalteror.gen.tr/bilgi/varolan.html

7- ttp://sunsite.bilkent.edu.tr/Bilisim/bilgikuvvetleri-c.txt

8- http://www.ainfos.ca/tr/ainfos00485.html

9- http://www.ainfos.ca/tr/ainfos00485.html

10- http://www.ainfos.ca/tr/ainfos00485.html

11- http://www.ainfos.ca/tr/ainfos00485.html

12-http://www.bilten.metu.edu.tr/publications/ubg.html

13- Teröristleri Duyamayan Dev Kulak: Echelon, Raşit Gültekin, TÜBİTAK Bilim- Teknik Dergisi, Ekim 2001.

14- Echelon Sistemi, İlkin Mekhrabov, ODTÜ Biltek dergisi, Ocak 2000.

15- İnternet Suçları ve Mahremiyet, M. Niyazi Tanılır, Liberte Yay. 2002.

16- http://www.c4group.net/ivhp/sibersucsozlesmesi.php

Siber Savaş

'Kıyametin İlk Halkası

"Şubat 2002'de ABD Senatosu'nda bir alt komitede konuşan Başkan George W.Bush'un en üst düzey sanal güvenlik danışmanı Richard Clarke, birçok kişinin kanını donduran şu sözleri dile getirdi: "Şer ekseninde yer alan İran, Irak ve Kuzey Kore'nin yanı sıra Çin ve Rusya da ABD'ye karşı siber askerler yetiştirmektedir. Altyapımızı hedef alabilecek bu saldırılara bundan sonra aralarında askeri operasyonların da bulunduğu tüm olanaklarla karşılık vereceğimizi duyururuz." Bush'un ve güvenlik danışmanının sözleri, imparatorluğun enformasyon savaşını ne kadar önemsediklerini ortaya koyuyor. Bütçede "sanal güvenlik" harcamalarına ayrılan kaynak da bunu doğruluyor. ABD hükümeti, sanal güvenlik için 2002 yılı içinde 2,7 milyar dolar, 2003'de ise 4,2 milyar dolar harcayacağını açıkladı.

Peki ama bu devasa bütçe gerçekten de "güvenlik"için mi harcanacak? O konudaki kuşkuların tamamen haklı olduğunu ABD'nin bizzat kendisi ortaya çıkarıyor: Genel Denetim Kurumu'nun (U.S. General Accounting Office) 2000 Eylül'ünde yayınladığı bir rapora göre 24 kamu kuruluşundan 16'sı denetim sonucunda "F" puanını, yani "çok zayıf" aldı. Bunun anlamı, ABD'nin "sanal güvenlik" adı altında ayırdığı milyarlarca doların gerçekten de sanal kamu güvenliğine ayrılmadığı. Peki paralar nereye gidiyor? Saldırı ve taarruz amaçlı projelere!..

Burada ortaya çıkan bir başka soru ise şu: 1945 yılından bu yana dünyanın süper gücü ABD gerçekten bir sanal tehlike ile karşı karşıya mı? Yoksa ABD, dünyayı kontrol etme, izleme ve dinleme adına bazı ülkeleri sözde potansiyel tehdit gösterip, kendi projelerine geçerlilik mi kazandırmak istiyor? Kuşku dolu bu çalışmalara milyarlarca dolar ayıran ve bir Pearl Haurbor'a göz yuman ABD'nin dünyada söz sahibi olma adına neler yapabileceğini kestirmek gerçekt

5500000

arşiv KİTAPLARI

ISBN 975-97955-0-7