

# Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu

Yrd. Doç. Dr. Mehmet Özcan\*

“... ve savaşlar artık fare (mouse) tarafından yönetilecek”.<sup>1</sup>

İnsanoğlu yeryüzünde varolduğu günden bu yana sürekli olarak bir arayış içindedir. Avcılıktan tarıma geçilmesi ile yerleşik toplumların ilk örnekleri görülmeye başlanmıştır. Toplum yaşamını belirli ölçüde etkileyen bu gelişmeler yüzyıllar boyunca devam etmiş, Batı'daki sanayi veya teknoloji devrimi sayesinde ortaya çıkan makineleşme, toplum yaşamını derinden etkilemiştir. Günlük yaşamın her alanını etkileyen ve kolaylaştıran sanayi devrimi ile yaşamın rengi daha önceleri görülmemiş bir şekilde farklılık göstermeye başlamıştır. Endüstri devrimi de denilen bu gelişmeler, özellikle 20. yüzyılın ikinci yarısından itibaren konu ile yakından ilgilenen kişilerin bile takip etmede zorluk çektiği bir hıza ulaşmıştır.

Bu gelişmelerin tam aksine insanlığın ilk günü ile birlikte ortaya çıkan “iyi” kötü” kavramları hiç değişmeden günümüze kadar gelmiştir. Sanayi devrimi ile ortaya çıkan teknolojik gelişmeler özellikle savaş sanayiindeki buluşlar, “iyilere” olduğu kadar “kötülere” de olanaklar sunmuş, insanlığın mahvına neden olabilecek yeni silahlar ortaya çıkmıştır.<sup>2</sup>

Dünya 1970'li yıllarda yeni bir teknoloji devrimi ile karşı karşıya gelmiştir. Bu yeni devrimin adı “Bilişim devrimi”dir. Özellikle 1990 sonrası gelişen ağı sayesinde tüm dünyayı saran internet, devletlerin ulusal güvenliklerini her yönü ile tehdit etmeye başlamıştır. Uluslararası alışveriş şirketleri yüzünden gümrük sistemleri, “Hacker” ler yüzünden en gizli devlet sırları, hergün mantar gibi artan korsan siteler yüzünden gerçek hayatın sanal aleme de taşınması gereken hukuk sistemleri uygulanamamasından dolayı tehdit altındadır. Özellikle büyük kentlerin altyapı ve iletişim alanları büyük bir tehdit altındadır.

Bilgisayarın uzay çağını geride bırakarak, bilgi toplumunu oluşturmadaki önemi yadsınamayacak kadar büyüktür. Bugün hayatımızın her alanına girmiş olan bilgisayarlar, bankalardan marketlere, evlerden karakollara, polisten suç örgütlerine kadar, yaşamımızın her alanına girmiş ve artık yaşamımızın ayrılmaz bir parçası haline gelmiştir.

İnternetin dünya çapında yaygınlık kazanması ile mekan kavramı bir anlamda ortadan kalkmış, kıtalararası iletişim ve bilgi aktarımı bir tuşa basmaktan ibaret hale gelmiştir. Teknolojideki bu gelişmelerden toplumlar pozitif anlamda yararlandıkları gibi, organize suç örgütleri ve terör örgütleri de, gelişen bu teknolojiyi yakından takip ederek, hem kazançlarını katlamakta, hem de geleneksel suç türlerinin dışında yeni suç türleri geliştirmektedirler.

Devletlerin iç güvenliğini tehdit eden ve hedefine ulaşmada hiçbir sınır tanımayan suç örgütleri, bilgisayar teknolojisi yardımıyla tahminlerin ötesinde bir mobilite kazanarak uluslararası suç trafiğine yeni bir boyut kazandırmıştır. Globalleşmenin karanlık yüzü olarak adlandırabileceğimiz bu gelişme toplumsal huzur ve barışı ve ulusal güvenliğimizi ciddi şekilde tehdit etmektedir.

\* Polis Akademisi Öğretim Üyesi  
TADOC Bilişim Suçları Araştırma Merkezi Başkanı.

<sup>1</sup> Shekhar Gupta, *Indian Express*, November, 18, 1998.

<sup>2</sup> Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy” [www.nautilus.org/info-policy/workshop/papers/denning.htm](http://www.nautilus.org/info-policy/workshop/papers/denning.htm)

Devletin en önemli kurumlarının internet sitelerinin "hacker" lar tarafından çöktürülmesi 21. yüzyılda bilişim suçlarının, ulusal güvenliği tehdit eden en önemli suç türleri arasında yerini alacağına önemli bir kanıt olmuştur.

### ***Suçlar fırsatları takip eder***

50 yıl öncesinin meşhur Amerikan banka soyguncusu Willie Sutton'a sormuşlar; Niçin banka soymakta bu kadar ısrar ediyorsun?. "Çünkü orası paranın bulunduğu yer" diye yanıtlamış Sutton. Kriminolojideki suçların fırsatları takip ettiği ilkesini veciz bir şekilde açıklayan bu yanıtta yola çıkarak suçları önlemenin en etkin yolunun bireyleri suç işlemeye götüren fırsatların ortadan kaldırılması gerektiği ön plana çıkmaktadır.

Ancak suç işlemek için sadece fırsatların varlığı yetmez. Suç işleme iradesine veya motivasyonuna sahip failer olmalıdır. Ayrıca yeterli koruma veya gözetimin olmaması da gerekmektedir. Hiçbir hırsız balkon kapısı açık bir daire varken balkon kapısının demir parmaklıklarla korunmuş ve kilitlemiş bir daireyi soymaya teşebbüs etmez.

Kriminolojinin bu temel ilkesi bir banka soygunu veya araba hırsızlığında geçerli olduğu kadar bilişim suçları alanında da geçerlidir. Fırsatların ortaya çıkmasında, diğer bir deyişle bilişim suçunun işlenmesinin önlenmesinde herşeyi devletten, polisten beklemek bizi istediğimiz sonuçlara götürmeyecektir. Bireyler ve kurumlar evlerini ve işyerlerini korudukları gibi bilgisayarlarını da yapılacak olası saldırılara karşı korumak zorundadır.

### **Bilişim Suçlarını suç işlemeye iten nedenler nedir?**

Bilişim suçlarını suç işlemeye iten nedenler arasında geleneksel olarak bireyleri suç işlemeye götüren nedenlerden farklı, yeni bir neden görmek neredeyse olası değildir. İntikam alma duygusu, güce sahip olma, açgözlülük, şehvet, macera veya "yasak meyveyi tatma" arzusu gibi geleneksel olarak bireyleri suç işlemeye götüren nedenler bilişim suçları anlamında da bireyleri suç işlemeye götüren nedenler olmaktadır.

Büyük bir bilgisayar sistemi üzerinde izinsiz olarak etkin olabilmek, belki de bir güç gösterisi olarak o bireyi fazlasıyla mutlu etmektedir. Çalıştığı şirkette haksız şekilde işinden atılan bir bilgisayar mühendisinin eski şirketinin bilgisayar sistemine verdiği zarar veya ideolojik olarak mücadele içinde olduğu bir devlete karşı o devlet kurumlarının bilgisayar sistemlerine zarar vermek intikam duygusu ile işlenen suçlardır. Bu kişilerin şirketin merkezine geleneksel bir suç türü olan bomba koyması veya devlet güvenliğini temsil eden güvenlik kuvvetlerine karşı silahlı saldırıda bulunması da intikam duygusu ile işlenmiş suçlardır. Bilişim suçlarının bir çoğu macera arayan kişiler tarafından bilinmeyi keşfetme güdüsüyle işlenir. Bilişim alanında suç işleyebilmek için gerekli teknolojik bilgi düzeyinin yüksekliği göz önüne alınırsa, kompleks yapıdaki bilgisayar güvenlik sistemlerine zarar verme yoluyla, suç faillerinin kendilerini ispatlama güdüsü veya bir meydan okuma güdüsü ile hareket ettikleri de unutulmaması gereken bir motivasyondur.<sup>3</sup>

Dikkat edilirse yukarıda saymış olduğumuz ve bireyleri suça iten nedenlerin neredeyse hiç biri yeni değildir. Yenilik belki de sadece teknolojinin bu güdüler ile hareket etmeyi kolaylaştırması konusunda tahmin edilemeyen kapasitesidir.

<sup>3</sup> Peter Grabowsky, "The Mushrooming of Cybercrime" Prepared for Presentation at the Symposium on the The Rule of Law in the Global Village, Palermo, 14 December 2000. s.3. [www.odccp.org/palermo/grabowsky.doc](http://www.odccp.org/palermo/grabowsky.doc).

## İnternetin hayatımızdaki yeri

Uluslararası Taylor Nelson Sofres şirketinin Türkiye iştiraki TNS Siar, Türk İnternetçilerinin nüfusunu belirlemek için bir anket düzenledi. Araştırma kent nüfusu üzerinde gerçekleştirildi. Yani 31 Milyon kişiyi 'örnekleyecek' bu anket, 12 yaş üstü, kent nüfusunu temsil eden 1200 kişilik örnekleme kullanılarak yapıldı. Sonuçta, bu nüfusun yüzde 18'inin son 1 ayda herhangi bir yerden internet kullandığı ortaya çıktı. Yani 5.6 Milyon kişi. Bu 5.6 Milyon kişinin, 1.8 Milyonu İnternete hergün giren kişiler...<sup>4</sup>

Yeni bir araştırma, dünya genelinde 474 milyon kişinin evinden internete bağlandığını ortaya koydu. Nielsen NetRatings şirketinin yaptığı araştırmaya göre, 2001 yılının son çeyreğinde 15 milyon kişi daha evinden internete bağlanmaya başladı.

Dünyanın en çok evden internet bağlantısı olan ülkesi ABD. ABD, 186 milyon kişiyle, bütün web nüfusunun yüzde 39'una sahip. Avrupa, Ortadoğu ve Afrika'da 128 milyon, Asya Pasifik ülkelerinde ise 104 milyon internet kullanıcısı bulunuyor. Şirketin analistlerinden Richard Goosey'a göre, araştırma, söz konusu bölgelerde internetin günlük yaşamın bir parçası haline geldiğini gösteriyor.

Goosey, Latin Amerika gibi diğer bölgelerde de hızlı bir büyüme yaşandığı ve önümüzdeki bir yıl içinde internet bağlantısı sayısında hızlı bir yükselme beklendiğini söyledi. Bütün bu bilgiler, Haziran ve Eylül ayları arasında dünya çapında yapılan 40 bin araştırmanın sonuçlarından derlenmiştir.<sup>5</sup>

## Bilişim suçu türleri

Genel olarak üç ana başlık altında toplanabilecek olan bu suç türleri gelişen teknolojiye paralel olarak sürekli artmaktadır. Bilişim sektöründe teknolojik gelişme akıl almaz hızda seyretmektedir. Microsoft firmasının sahibi Bill Gates bir konuşmasında bilgisayar sektöründeki bu gelişmenin hızını anlatmak için şöyle bir benzetme yapmış:

"Eğer Volkswagen firması son 25 yıl içinde bilgisayar sektörü kadar hızlı gelişmiş olsaydı bugün 500 dolara alacağımız arabalara 25 dolarlık benzin koyup dünya turu atmamız mümkün olacaktı" demiştir.

Aşağıda bir kısmı sıralanan bilişim suçları sadece bu sayılanlar ile sınırlı değildir. Biz bu çalışmada örnekleme olması için birkaç suç türünü sıralayacak ve ulusal güvenliğe tehdit boyutu açısından siber terör üzerinde durmaya çalışacağız.

Öncelikle bilgisayar bir saldırının hedefi olabilir. Bu durumda bilgisayarın gizliliği, bütünlüğü ve sunmakta olduğu hizmetler tehdit altındadır. Bu yolla ya bilgisayarın içindeki bilgiler veya sağladığı hizmetler izinsiz olarak kullanılır ve hedef alınan bilgisayar maddi zarar görür. Şubat 2000 de ortaya çıkan ve birçok internet sitesinin ciddi anlamda zarar gördüğü, "I Love You" virüsü bu saldırılardandır.

Ünlü anti-virüs firması MessageLabs'ın verilerine göre şirket bu yıl her 18 saniyede bir virüs yakaladı. Kurdukları tarayıcı sistemlerle virüs avlayan MessageLabs, 2001 yılı içinde 1.6 milyon virüsü durdurmayı başardı. Geçen yıl sadece 184 bin virüs yakalayan şirket yetkilileri bu yılın virüsler açısından hayli yoğun geçtiğini belirtmektedirler.

Şirket yetkilileri bu yıl her 370 e-mail'den birinin virüslü olduğunu, bu rakamın 2000 yılında her 700 mesajda, 1999'da ise her 1400 mesajda bir olduğunu belirtiyor. Rakamlar her yıl virüs sayısının katlanarak arttığını gösteriyor.<sup>6</sup>

<sup>4</sup> <http://www.Haberyolu.com>. Erişim tarihi: 11. 12. 2001.

<sup>5</sup> <http://www.hurriyetim.com.tr>. Erişim tarihi: 11.12. 2001.

<sup>6</sup> <http://www.imedya.com/> erişim.19.12.2001

Bilişim suçları bazen şirketleri ekonomik anlamda gerçekten çok zor durumlarda bırakmaktadır. Örneğin 1999 yılında Amerikan eBay şirketine yapılan saldırılar sonucu bu şirketin 5 gün içinde pazar değerinin %26'ını kaybettiği belirtilmektedir.<sup>7</sup>

İkinci olarak bilgisayar suç işlemek için bir araç olarak kullanılabilir. Bu grupta yer alan suç türleri kolluk güçlerinin aslında gerçek hayatta hergün karşılaştığı klasik suç türlerinden farklı değildir. Geleneksel suç türleri örneğin tehdit, şantaj, dolandırıcılık gibi suçlar internet ortamında bilgisayar ve bilgisayar sistemleri aracılığıyla, gittikçe artan bir şekilde icra edilmektedir.

Üçüncü olarak bilgisayarlar, belleğinde yasadışı bilgi, resim ve belgelerin depolanması yoluyla suça karışmakta ve kolluk güçlerinin ilgi alanına girmektedir.<sup>8</sup> Birçok terör örgütü internet üzerinden propaganda başta olmak üzere, patlayıcı madde yapımı, örgüt elemanlarının eğitilmesi gibi birçok illegal faaliyet icra edilmektedir. Nitekim Emniyet Teşkilatı'nın Hizbullah terör örgütü ile mücadelesindeki başarısının temelinde bu örgütün bilgisayarlarında yapılan araştırmalar sonucu elde edilen veriler bulunmaktadır. Benzer şekilde uyuşturucu ticareti yapan ve bilgi teknolojilerini kullanan bir şebekenin iletişim ağı bir bilgisayarın içindeki bilgiler sayesinde ortaya çıkarılabilir.

### **Üç ana başlık altında ele alınan bu suç türlerinin bir kısmı şunlardır;**

#### **a. Telekomünikasyon hizmetleri hırsızlığı:**

Günlük yaşamda onlarca örneği ile karşılaşılabilecek olan bu suç türünün mali boyutların nereye kadar gidebileceği konusunda verilecek şu örnek sanırım yeterli olacaktır: ABD'de bir hacker yetkisiz olarak Scotland Yard'ın telefon ağına girip bu ağ üzerinden 620.000 sterlin değerinde (1 trilyon TL'yi aşan bir değer) uluslararası telefon görüşmesi yapmıştır veya yaptırmıştır<sup>9</sup>. Saldırıların ülkelerin ekonomik bütünlüğüne olan zararları gerçekten hayal sınırlarını zorlamaktadır.

#### **b. Bilgisayar sistemlerinin başka suç işlemek için kullanılması**

Özel ve kamu sektöründeki tüm yasal örgütlerin ve kurumların iletişim sistemlerini kullandıkları kayıtlarını bilgisayar ortamında tuttukları gibi suç örgütleri de çalışmalarını bilgisayar teknolojisi ile güçlendirmiş ve çeşitlendirmiştir.

Telekomünikasyon sistemleri uyuşturucu ticareti, kumar, fuhuş, kara para aklama, çocuk pornografisi ve yasadışı silah ticareti alanlarında organize suç örgütleri tarafından etkin bir şekilde kullanılmaktadır. Şifre sistemlerini çok iyi şekilde kullanabilen bu örgütler yasa uygulayıcıların takibinden bu şifreleme sayesinde kurtulabilmektedir.

#### **c. Bilgi Korsanlığı, Sahtecilik ve Kalpazanlık**

Özellikle telif hakları sahipleri için büyük mali kayıplara neden olan yeni teknolojik gelişmeler sayesinde, telif hakkının konusu olan her türlü materyel izinsiz olarak çoğaltılabilmekte ve bu çoğaltılan kopyaları piyasada orijinalinden ayırmak gerçekten zor olmaktadır. Bu şekilde her yıl telif hakkı ihlal edilen eserlerin sahiplerin 15 milyar ile 17 milyar dolar arasında mali kayıpları olduğu tahmin edilmektedir.

Amerikan endüstrisine yabancı korsanlar tarafından verilen zarar 1998 yılı itibariyle, 10 milyar dolar, film endüstrisinde 1.8 milyar dolar, müzik endüstrisinde, 1.2 milyar dolar

<sup>7</sup> <http://www.telegraph.co.uk/> Erişim tarihi: 03/10/2001.

<sup>8</sup> James K. Robinson, "Internet as the Scene of Crime" International Computer Crime Conference, Norway, May29-31, 2000. <http://www.cybercrime.gov/roboslo.html>.

<sup>9</sup> Tendler S, & Nuthall, N, (1996) "Hackers Leave Red-Faced Yard with \$1.29m Bill" *The Australian*, 6 August, 37.

yazılım alanında 3.8 milyar dolar, basılı kitap sektöründe ise 670 milyon dolar olmak üzere yaklaşık olarak toplam 17.4 milyar dolar olarak tahmin edilmiştir. Hatta James Bond'un "*The World is Not Enough*" adlı filme resmi olarak piyasaya arz edilmeden internette bedava olarak ulaşmak mümkün olmuştur.

Digital teknoloji ayrıca kalpazanlık ve sahtecilik konularında organize suç örgütlerine sahte para, kimlik, pasaport vb. belge düzenleme olanağı vermiştir. Gelişen teknolojiyi yakından takip eden bu örgütlerin yaptığı sahte belge ve kalp paraların kalitesi gittikçe artmaktadır. Kolluk kuvvetlerin bu sahte belge ve paralarla yapmış olduğu mücadele daha da zorlaşmaktadır.

#### **d. Kötü, Çirkin görüntü ve kayıtların yayılması**

İçeriğinde ırkçı propagandadan bomba yapımına, pornografik görüntüden on-line kumar sitelerinin adreslerine kadar farklı bilgi ve görüntü bulunan birçok bilginin internet yoluyla yayılmasıdır.

#### **e. Tehdit ve Gasp**

Bilgisayar teknolojisini çok iyi kullanan bir kısım suçlular internet üzerinden bazı firmaları bilgisayar sistemlerini çökertmekle tehdit ederek haraç toplama yoluna gitmektedirler. Bilgisayar sistemi tehdit edilen firmalar maruz kaldıkları tehdidin büyüklüğü nedeniyle bazen haraç ödeme yoluna gitmektedirler. Örneğin 1993-1995 yılları arasından İngiltere ve ABD'de bu gruplara haraç olarak 42.5 milyon sterlin ödendiği belirtilmektedir.<sup>10</sup>

Maxus takma adını kullanan 18 yaşındaki bir hacker geçen yıl Amerikan on-line müzik şirketi olan *cdUniverse*'in sitesinden 300.000 kredi kartının numaralarına ulaşmış ve bu şirketten numaraları açıklamama karşılığında 100.000 Amerikan doları haraç talep etmiştir. Şirket bu bedeli ödemeye yanaşmayınca Maxus kurduğu bir sitede bu numaraları yayınlamıştır. Numaraların sahipleri haberdar olmuşsa kredi kartlarını iptal etmişler veya *cdUniverse*'den yaptıkları alış-verişlere ait hesap ekstrelerini kontrol etmişlerdir. Ancak bazı bu kredi kartları ile internet üzerinden başka alış-verişler yapıldığı açıklanmıştır.<sup>11</sup>

#### **f. Siber Terör**

21. yüzyılın en önemli güç kaynağı hiç şüphesiz 'bilgi'dir. Bilgiyi elinde tutan gücü de elinde tutmuş olmaktadır. Bilginin gücüyle teknolojik alandaki gelişmeler tüm yaşamımızı olumlu yönde etkiliyor. İnternet, bilgisayar, uydular, cep telefonları... Bunlar sadece günlük yaşamımıza giren teknolojinin ürünlerinden bazıları. Yine bilginin gücünü kullanarak aynı araçlar birer silaha dönüşebilmekte ve karşımıza siber savaş ve siber terör kavramları çıkmaktadır.<sup>12</sup>

Siber terör, yeni yüzyılda terörizmin yeni yüzü olarak yansıyacaktır ki teröristlerin elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin

<sup>10</sup> Peter Grabowsky, a.g.e. s. 7.

<sup>11</sup> <http://www.telegraph.co.uk/12/01/2000>, Erişim tarihi: 03/10/2001.

<sup>12</sup> Faruk Örgün, *Küresel Terör*, Okumuş Adam Yay. İstanbul 2001.

çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir.<sup>13</sup>

## Tanım

Terör kavramına ilişkin olarak unsurları yaklaşık olarak birbirlerine çok yakın olmakla birlikte farklı tanımlara yer verilmektedir. Genel kabul görmüş ortak bir tanımlanmadığından<sup>14</sup> farklı terör tanımları ile karşılaşmak mümkündür. Bal, politik terörü, *politik talep ve dürtülerle örülen şiddet veya şiddet tehdidi içeren siyasal hareketler olarak tanımlamaktadır*. Terörün amacı hedef olarak seçtiği kişileri veya eşyalara verdiği zararın çok daha ötesinde, topluma ve devlete yönelik mesajlar içermektedir. Terörizm propaganda olmadan yaşayamaz. Politik terörün amacı tek başına şiddet değil, bu şiddet yolu ile kamuoyunda oluşturmak istediği baskı ortamı ve bu ortamın sağladığı korku ve yılgınlık ile kendisine taraftar bulmaktır. Şiddet ve baskının temel hedefi, güvenlik güçleri ve devleti temsil eden kişiler olmakla birlikte PKK örneğinde de görüldüğü gibi sivil, çocuk, kadın, yaşlı ayırımı yapmadan her canlı hatta hayvanlar ve tarladaki ürünler bile bu şiddetin mağduru olabilmektedir.<sup>15</sup>

Terörizm ise, şiddetin veya tehdidin sistematik olarak, belirli bir amaç için kullanılmasında denilebilir. Terörizm bir grup veya ferdin diğer bir grup veya ferdi baskı altında tutması için kullandığı bir araç haline gelebilir.<sup>16</sup>

Terörizmin bir başka tanımı ise; belirli bir siyasal hedefe ulaşmak veya siyasal bir davayı yüceltmek amacıyla ve genelde kurulu düzeni değiştirmeye veya sözkonusu siyasal davaya boyun eğmeye mecbur etmek için başvuru zorlayıcı ve şiddet içeren davranışlardır.<sup>17</sup>

*Siber terörizm ise belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır.*<sup>18</sup>

*Siber terörizmi klasik anlamda terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak icra edilmesi olarak tanımlamak da mümkündür.*

İngiltere, Terörizm Yasası 2000'de siber terörizmi "hükümeti etkilemek ya da toplumu korkutmak amacıyla elektronik sistemlerin içine izinsiz girmek veya bu sistemleri bozmak" olarak tanımlamaktadır. Bu yeni yasaya göre bir grup internet eylemcisi Başbakan'a e-mail protestosu gerçekleştirir ve bu e-mail sisteminde bir çöküntüye neden olursa buna terörizm adı verilebilecektir.<sup>19</sup>

Siber terörizmi tanımlarken temelde terörizm olgusunun nitelikleri değil ancak terör olgusunun nasıl yaşama geçirildiği önem arz etmektedir. Temel amacı bir kısım siyasal

<sup>13</sup> Sertoğlu S., *Sabah Gazetesi*, 06.12.1999.

<sup>14</sup> Devlete karşı terör (aşağıdan terör) ve devlet terörü (yukarıdan terör) kavramları için bkz; Mustafa Gündüz, "Türkiye'de Terör: Nedenleri ve Çözüm Önerileri" içinde; Ceza Adalet Sistemi ve Polis Sempozyumu, Ankara, 1998. s.304.

<sup>15</sup> İhsan Bal, *Prevention of Terrorism in Liberal Democracies - A Case of Turkey*, Basılmamış Doktora Tezi, Leicester University, 1999, s.54.

<sup>16</sup> Karamatullah P. Gori, "Terörizm ve İnsan Hakları-Nerede Çizgi Çekelim" " içinde; *I. Milletlerarası Doğu ve Güneydoğu Anadolu'da Güvenlik ve Huzur Sempozyumu*, 27-27-28 Mart 2000, s. 194.

<sup>17</sup> Hamit Ersoy; "Ulusal çıkar Aracı Olarak Uluslararası Politikada Terörizm", içinde; *I. Milletlerarası Doğu ve Güneydoğu Anadolu'da Güvenlik ve Huzur Sempozyumu*, 27-27-28 Mart 2000, s. 997. Başka yüzlerce tanımlamayı, buraya taşımış olsaydık göreceğimiz ortak özellik terör eylemlerinin şiddet unsurundan bağımsız olamayacağı gerçeğidir. Terör örgütleri bu şiddet eylemleri ile politik isteklerine ulaşmak için çaba harcarken hem eylemlerini gerçekleştirdiği ülkenin içinden hem de dış ülkelerden destekler almaktadırlar. Globalleşen dünyada herhangi bir terör örgütünün dış destek almadan eylemlerini uzunca bir zamana yayması olası değildir. Terörizm, bir laboratuvarın "surrealist izolasyon" ortamında ortaya çıkan bir olgu değildir. Terörizm, sömürgeci düzenin (*şeklen*) ortadan kalktığı, sona erdiği kaos ortamında boy atıp gelişmiş bir oluşumdur. Bkz. Karamatullah P. Gori, a.g.m. s. 193.

<sup>18</sup> "Cybercrimes: Infrastructure Threats from Cyberterrorist," *Cyberspace Lawyer*, 4 No 2. Cyberspae Law 23.

<sup>19</sup> [http://www.programcilik.com/haber/hl\\_26-04-02-3-2001.html](http://www.programcilik.com/haber/hl_26-04-02-3-2001.html)

sonuçlara ulaşmak olan insanların, ellerine geçirdikleri yeni teknolojik donanımlar ile terör eylemini gerçekleştirmek için yola koyulmuş olmalarıdır. Dolayısıyla terörizmde felsefi olarak köklü bir değişimden bahsetmek güçtür ancak yöntemler ve araçlarda önemli değişimler olmuştur denebilir. **Bu bağlamda Siber terörizm araçları bakımından ileri teknoloji ve bilgiyi kullanarak klasik terörizm tanımlamasının yeni şekliyle devamıdır denebilir.**

Ancak klasik anlamda terör ile siber terör arasında bazı farklılıklar vardır, bunlar;

- Öncelikle terör örgütleri klasik anlamda eylem yaparken bir ölçüde hayatlarını da gerektiğinde ortaya koymak zorundadırlar. Eline silah veya bomba alan bir terörist muhtemeldir ki bir polis veya asker tarafından tesirsiz hale getirilsin. Ancak dünyanın herhangi bir yerinde internete bağlanan bir terörist (siber terörist) çayını ve sigarasını içerken istediği ülkenin toplumsal yaşamına ciddi zararlar verecek eylemlerini kendi yaşamını hiç tehlikeye atmadan gerçekleştirebilir. Ayrıca siber terörizm kamu binaları veya havaalanları gibi terörist saldırıların hedefi olan bina ve yerlerin fiziki güvenliklerinin artırılmalarına paralel olarak daha cazibeli hale gelmektedir. Çünkü, terörist kendine çok daha güvenli bir ortamda saldırısını hazırlayabilmektedir.

- İkinci olarak terörün asıl amacından yola çıkarak ulaşılan farklılıktır. Terörün asıl amacı yapmış olduğu eylemler ile hedef aldığı siyasal rejim ve topluma bir mesaj vermektir. Terörde şiddet ve zarar verme araçtır. Hatta IRA'nın birçok kez yaptığı gibi insanların zarar görmesini minimuma indirebilmek için yapacağı eylemi, eylemden kısa bir süre önce haber verir. Ancak siber terörde sanal şiddet bir araç olmaktan çıkıp bir amaç haline gelebilmektedir.

Bilgisayar teknolojileri sayesinde bir terörist büyük bankaların, finans kurumlarının ve borsaların bilgilerini ve iletişimini alt üst edebilir. Bu durumda o ülkenin ekonomik yaşamının ne olacağını düşünmek bile gerçekten akıllara durgunluk verecek niteliktedir. Veya büyük bir ilaç firmasının bilgisayarlarına giren teröristler çok kullanılan birkaç ilacın içeriğini küçük değişiklikler yaparak insan yaşamına son verecek veya ciddi rahatsız edecek şekilde değiştirebilirler. Veya doğalgaz istasyonlarının bilgisayarlarında basınç göstergeleri üzerinde yapacakları değişiklikler ile doğalgaz hatlarını evlerinden patlatmayı başarabilirler.

- Üçüncü olarak geleneksel terör eylemi yoluyla yapılmak istenen propaganda geniş kitlelere ulaşabilse de, eylemin bizzat kendisi lokaldir. Bir devlet kurumunun binası hedef alınmışsa, o bina çökebilir ve içindeki şahıslar yaşamlarını yitirebilir. Ancak, siber terörde eylemin direk fiziki etki alanı, bilgisayarı yönlendiren fare'nin bir hareketiyle inanılmaz şekilde genişletilebilir. Bir tıklama ile devlete ait binlerce internet sitesi aynı anda çökertilebilir. Hatta bir anda birçok ülkede bulunan siteler aynı anda çökertilebilir. Yani bir tıklama ile birden çok eylem birden çok yerde gerçekleştirilebilir. Siber terör eylemi yoluyla yapılan eylemler, gündelik yaşamda bireyleri çok daha fazla etkileyebilme yeteneğine sahip olacaktır. Örneğin büyük kentlerde bilgisayarlar aracılığıyla yönetilen su ve elektrik dağıtım şebekelerinin merkezlerine yapılacak olan saldırılar o şehirde yaşayan tüm bireyleri doğrudan etkileyecektir. Veya Türk Telekom'un sitesine saldıran bir hacker belirli bir aya ait tüm telefon faturaları üzerinde değişiklik yapabilir. Tüm abonelerin telefon ücretlerini onar milyon azaltabileceği gibi yüzer milyon artırabilir veya ödenmemiş borçları ödendi şeklinde gösterebilir. Bu tür bir saldırıya hedef olan bir devlet kurumunun içine düşeceği

karmaşanın yarattığı toplumsal huzursuzluk bir devlet kurumuna ait binanın bombalanmasında daha fazla olacaktır.

- Dördüncü olarak Siber terörizmin psikolojik etkisi, bilgisayar ve bilgi teknolojisine uzananlarla sınırlı kalacağından veya hedefler bizatihi sembolik değil ve fakat gerçek olduğundan, klasik ve modern çağ terörizmi kadar yaygın bir dalga içermeyebilecektir. Ayrıca siber terörde insanların ölmesi ya da yaralanması (şimdilik) söz konusu olmadığından kamuoyundan duygusal bir tepki doğması daha az olacaktır.
- Beşinci olarak terör örgütlerini fiziki güç kullanımı söz konusu olduğundan elemanlarını en azından belirli bir yaşın üzerindeki kişilerden seçer. Ancak siber terör de çocuk denecek yaştaki insanlar siber terörün aracı haline gelebilirler. Macera arayan ortaokul ve lise gençliği özellikle ABD’de Pentagon’un veya diğer devlet birimlerinin web sitelerine saldırmaktadırlar.
- Son olarak siber teröristler klasik teröristler gibi eylemlerini gerçekleştirmek için bomba veya silahlara değil sadece bir bilgisayar ve modeme gereksinim duyarlar.

### **Terörizmin Propaganda Aracı Olarak İnternet**

Terörizm ve internet iki şekilde birbirleri ile ilintilidir: Birincisi, internet terör örgütleri mensuplarının birbirbirleri ile iletişim kurmada, şiddet ve nefret içerikli mesajlarını kitlelere, sempatanlarına ulaştırmada bir forum haline gelmiştir. İkincisi, terör örgütü elemanları bireysel olarak veya grup halinde bilgisayar ağlarına saldırabilir ve siber terör ve siber savaş olarak nitelediğimiz eylemleri gerçekleştirebilirler.

Türkiye’de de görüldüğü gibi terör örgütleri interneti daha çok propaganda aracı ve iletişim aracı olarak kullanmaktadır. Bazen elemanları arasında şifreli e-mailler aracılığıyla iletişim kurarak terör eylemlerini planlayan terör örgütlerinin, interneti daha çok politik ve ideolojik anlamda bir propaganda aracı olarak kullandığı görülmektedir. Örneğin 1996 yılında Peru’nun Lima şehrinde Japon Büyükelçiliğine saldırarak diplomatik, askeri ve siyasi personeli rehin alan *Tubac Amaru* adlı terör örgütünün ABD’de ve Canada da bulunan sempatanları örgütün faaliyetini destekleyen birçok site kurmuşlardır. Bu sitelerde, propaganda ve eyleme destek ile birlikte örgütün Japon Büyükelçilik binasına saldırı planlarını da yayınlamışlardır. Meksika’da faaliyet gösteren Zapatista’lar (Zapatista National Liberation Army) 1994 ayaklanmasından bu yana internet üzerinden yoğun bir propaganda faaliyeti içine girmiştir. Kolombiya’da faaliyet gösteren The Revolutionary Armed Forces of Colombia örgütü, Peru’daki Shining Path örgütü interneti propaganda aracı olarak etkin şekilde kullanan terör örgütleridir. Genel olarak Latin Amerika menşeli terör örgütleri net ortamını etkin olarak kullanan terör örgütleridir. Bu örgütler ve diğerleri web sayfalarında linkler vererek terör eğitimi konusunda sempatanlarını eğitmektedir. Bu sitelerde Teröristin El Kitabı, Teröristin Yemek Kitabı (Terrorist’s Handbook, Terrorist’s Cookbook) gibi eserlerde bomba yapımı en ince detayları ile anlatılmakta ve bir teröristin bilmesi gereken bir çok konuda ayrıntılı bilgiler yer almaktadır.<sup>20</sup>

Hamas ve Hizb-ut-Tahrir gibi radikal örgütler de interneti propaganda aracı olarak kullanmaktadırlar. Lübnan da bulunan İran yanlısı Hizbullah örgütü, internet üzerinden kitap ve diğer yayınlarını satarak örgüte mali destek sağlamaktadır. Hamas ve İslami Cihad örgütlerinin, teröristlere internet üzerinden haritalar, fotoğraflar ve bomba yapımında kullanılan teknik bilgileri ayrıntılı bir şekilde ulaştırdıkları bilinmektedir.

<sup>20</sup> <http://www.adl.org/terror/focus>

Hindistan'da faaliyet gösteren Harkat-ül-Ansar adlı terör örgütünün bir militanı olan Halid İbrahim, Amerikan Savunma Bakanlığı'nın sitesinin kırılması ile elde edilen askeri yazılımları Chamelon adlı 18 yaşındaki bir hacker'den 1000 ABD Doları karşılığında satın almaya çalışmış ancak alışveriş gerçekleşmemiştir.<sup>21</sup>

İnternet propaganda aracı olarak sadece terör örgütleri tarafından kullanılmamaktadır. NATO'nun Sırp saldırılarından sonra müdahale ettiği Kosova' da ve Yugoslavya'nın diğer bölgelerinde ABD ve NATO uçakları, Miloseviç rejiminin tüm iletişim araçlarını bombalayarak devre dışı bıraktıkları halde İSS' lara ve Yugoslavya'ya internet bağlantısını sağlayan uydu linklerine zarar vermemek için özel çaba harcamışlardır. James P. Rubin bu politikayı şu sözlerle açıklamıştır:

"İnternete tam ve kesintisiz ulaşım Sırp halkının Miloseviç rejiminin Kosova'da icra ettiği soykırım ve cinayetleri insanlığa karşı işlenen suçları öğrenmesine yardımcı olacaktır."

Çünkü internette Kosova konusunda yoğun tartışmalar yapılmakta ve hergün yeni bilgi ve haberler tüm dünyaya farklı siteler tarafından yayılmakta idi.<sup>22</sup>

### **E-Mail Bombardmanı**

Günümüzde bir çok kişi haberleşmesini artık elektronik posta dediğimiz e-mail adresleri aracılığıyla yapmaktadır. Özellikle uzak şehir dışı ve yurtdışında bir kişi ile iletişim kurulacak ise akla ilk gelen e-mail adresine bir mektup göndermektir. Hergün işyerimize gittiğimizde ilk yaptığımız e-maillerimi okumak olmaktadır. Ancak e-mail adresimize yüzlerce binlerce mektup gelirse iletişim kurabilmemiz olanaksız hale gelecektir. E-mail adresimiz tıkanacak ve almayı beklediğimiz postaları alamaz duruma geleceğiz. Terör örgütleri bu şekilde protesto amaçlı olarak devlete ait siteleri e-mail bombardımanına tutmaktadırlar. Bilinen ilk e-mail bombardımanı ayrılıkçı Tamil Gerillaları tarafından gerçekleştirilmiştir. Tamil Gerillaları Sri Lanka'nın yurtdışı temsilciliklerine binlerce e-mail göndermişlerdir. Mail de şu ifade yer almaktadır:

**"We are the Internet Black Tigers, and we are doing this to disrupt your communication"**

Tamil gerillalarının saldırıları günlük ortalama 800 mail olmak üzere yaklaşık 2 hafta sürmüştür. Savaş Altyapı Sistemleri Çalışmaları Merkezi'nin başkanı olan William Church, Tamil gerillalarının o dönemlerde gerçekleştirmiş olduğu kanlı saldırılardan sonra kamuoyunda ciddi anlamda destek yitirdiğini ve bu eylem ile yeniden destek kazandığını belirtmiştir. Saldırının Sri Lanka'nın dış temsilciliklerinde istenilen korkuyu ve endişeyi (ki bunlar terör eyleminin asıl amacıdır) oluşturduğu kabul edilmiştir.

E-mail bombardımanı Kosova savaşı sırasında da her iki taraf tarafından karşılıklı olarak kullanılmıştır. San Francisco'da bulunan bir İSS (IGC) ise İspanya'nın Bask bölgesinin bağımsızlığını savunan Euskal Herria Journal'e servis sağladığı için e-mail bombardımanına maruz kalmıştır. Ancak bu sefer protestonun amacı sansür talebi olmuştur. Gelen yoğun saldırılar nedeniyle IGC istemeyerek de olsa Journal'e servis sağlamayı sona erdirmek zorunda kalmıştır. Journal'e daha sonra İngiltere'de İnternet Freedom Campaign sitesi servis sağlamaya başlamıştır. Ancak bir ay içinde Scotland Yards Anti-Terör birimi İnternet Freedom Campaign sitesini Journal'e servis sağladığı için kapatmıştır.<sup>23</sup>

<sup>21</sup> Detroit News, 9 Kasım 1998.

<sup>22</sup> D.E. Denning, a.g.m. s.1.

<sup>23</sup> D.E. Denning, a.g.m. s.16.

Euskal Herria Journal olayı internet üzerinden yapılan terör propagandalarına cevap vermek üzere kullanılabilecek çok güzel bir örnektir. Terörle mücadelede halkın desteği alınarak bu tür internet üzerinden yapılan saldırılara misilleme yapılabilir. E.H.Journal olayı Hacktivism olarak adlandırılan bu karşı saldırıların etkilerinin ne kadar güçlü olabileceğini göstermesi açısından önemli bir örnektir. Türkiye’de sivil toplum örgütleri, bölücü terör örgütlerine servis sağlayan kuruluşların web sitelerine bu tür protesto eylemleri gerçekleştirebilir. Ancak bu tür eylemlerin protestoyu aşmaması (sanal savaşa dönüşmemesi) ve tamamen sivil girişimciler tarafından gerçekleştirilmesi gerekmektedir.

11 Eylül saldırılarından sonra ihkak-ı hak müessesesinin farklı bir versiyonu sanal alemde eşi görülmemiş bir “siber savaş” başlamıştır. Hem Amerikan yanlıları hem de karşıtları yoğun bir saldırının içine girmişlerdir. Taliban.com veya Talibanonline.com gibi adreslerin yanında Filistin, Pakistan ve Afganistan kaynaklı web siteleri de bu yoğun saldırıların hedefi haline gelmiştir. Genelde e-mail bombardımanı şeklinde geçen bu savaş sitelerin tamamen çökertilmesi şeklinde de gerçekleştirilmiştir. Alman hacker Kim Schmitz tarafından kurulan Youth Intelligent Hackers Against Terror (YIHAT) net ortamında terör örgütleri hakkında bilgi toplayıp bu bilgileri Amerikan yetkililerine vermektedir. Bu örgüt Al-Kaide ve Usame bin Laden’e ait hesapların bulunduğu bir Sudan bankasına saldırı düzenledikleri belirtmişlerdir.<sup>24</sup>

FBI bu sanal savaş üzerine yaptığı açıklamada: “Bu ülkeye hizmet ettiğini sananlar (yurtseverler) aslında ülkeye zarar vermektedir, bu yapılanlar 5 yıl hapis cezası gerektiren suçtur” açıklamasında bulunmuştur.<sup>25</sup>

FBI sanırım iki konuyu göz önünde tutarak bu açıklamayı yapmıştır. Birincisi hiçbir meşru gerekçe yasalar ile belirlenmiş görevliler dışındaki insanların intikam duygularıyla bu tür saldırısına izin veremez. İkincisi ise yapılan bu saldırıların bir tür savaş başlatacağı ve bu savaşta karşı tarafın da teknolojik olarak donanımlı olduğunu bilmesidir. Hem ABD içindeki hem ABD dışındaki anti-Amerikan gruplar Amerikan devlet sitelerine saldırmakta ve gerçekten büyük zararlar vermektedirler. FBI bu tür saldırılara çanak tutma şeklinde algılanılabilecek olan Amerikan yanlısı saldırıların bu nedenler ile sona erdirilmesini talep ediyor olabilir.

Siber terörizm 21. yüzyılda ulusal güvenliği tehdit eden en önemli terör olayı haline geleceğini daha 20. yüzyılın sonlarında belli etmiştir. Özellikle gelişmiş olan ülkelerde ulusal bilgi sistemleri, kamu kurumları, bankalar, büyük şirketler hacker’ların ve siber teröristlerin saldırılarına hedef olmuştur. Bilgisayarların ve sistemlerin çökertilmesi, bilgilerin silinmesi, vergilerin silinmesi, yatırım hesaplarında veya alışverişlerde yapılan sahtecilik ve tehdit gibi yollarla yapılan saldırılar milyarlarca dolar maddi kayba neden olmaktadır.

İngiltere’de siber terörizm konusunda dünyada ilk defa yapılan bir araştırma 2 Nisan 2001 de kamuoyuna açıklanmıştır. Siber terör ile mücadelede etkin bir konuma sahip olan Communications Manegament Association (Haberleşme Yönetim Kurumu) tarafından yapılan bu araştırma, arasında ülkenin en büyük şirketleri ve kamu kurumları bulunan 172 kurumda yapılmıştır.

Araştırma sonuçlarına göre katılan kurumların neredeyse yarısı, internet casusluğu<sup>26</sup> olarak da anılan güvenlik ihlallerini kurumlarının yaşamlarına karşı büyük bir tehdit olarak algılamaktadırlar. Aynı zamanda bu tehlikelere karşı kurumlarının hazır olmadıklarını belirtmişlerdir. Araştırma yapılan kurumların % 48’i geleceklerinin siber terör tehdidi

<sup>24</sup> Cyber Protests Related to the War on Terrorism: The Current Crises, <http://www.nipc.gov/>

<sup>25</sup> Robert Lemos, “Hackers Divided Over Response to Terrorism” <http://www.cnet.com/news/>

<sup>26</sup> Netspionage kavramının karşılığı olarak kullanılmıştır.

dolayısıyla risk içinde olduğunu kabul etmiştir. % 60'ı siber terörizmin kurumsal yaşamlarını "önemli" veya "çok önemli" şekilde tehdit ettiğini kabul etmişlerdir.<sup>27</sup>

### **Türkiye'de Siber Terör :**

Türkiye'de sanal ortama ve terör örgütlerinin kullanımına bakıldığında, bilgisayar teknolojisi internet ve diğer teknolojik gelişmelerin yakından takip edildiği ve amaçlar doğrultusunda etkin olarak kullanıldığı görülmektedir. Hatta bu amaçla teknik konularda ihtiyacı giderecek örgüt elemanları yetiştirilmektedir. İnternet üzerinden haberleşme, propaganda yapma, eğitim amaçlı CD'ler ve bildiriler hazırlama şeklinde faaliyetleri içinde oldukları bilinmektedir.

Yukarıda dünyadan örnekler verdiğimizde de görüldüğü gibi Türkiye'de de terör örgütleri internet ortamını öncelikle propaganda ve eğitim amaçlı olarak kullandıkları görülmektedir. Bölücü örgütler özellikle PKK, sıcak terör eylemlerini yapamaz hale geldikten sonra "siyasallaşma" sürecine girmiş ve konuda yoğun bir çaba göstermektedir. Bu alanda kullandıkları en önemli araç internet ortamıdır. Yüzlerce web sitesinden yoğun bir propaganda faaliyeti yürütmektedirler.

Terör örgütlerinin gelişen teknolojiyi kullanarak eğitim ve propaganda faaliyetlerinin yanısıra bilişim teknolojisinden yararlanarak devletin kullandığı link hatlarına, bilgi işlem ve veri merkezlerine, bakanlıklara, PTT-Telekom, EGM ve TSK gibi önem arz eden birimlerin sistemlerine sanal saldırılarda bulunabilecekleri veya tahrip edici virüsler aracılığıyla bu sistemleri çökertmek için uğraş verdikleri konusunda istihbari bilgiler mevcuttur.<sup>28</sup>

Terör örgütlerinin bu eylemlerine örnek vermek gerekirse aşağıdaki iki örnek bu örgütlerin terörün yeni yüzü ile tanışmada gecikmiş olmadığını kanıtlamaktadır.

#### **Örnek Olay 1:**

İstanbul Emniyeti tarafından 1999 yılında İBDA-C terör örgütüne yönelik olarak düzenlenen operasyonda 33 örgüt mensubu, hedef şahıslara ait fotoğraflar ile birlikte yakalanarak gözaltına alınmıştır. Şahısların sorgulamalarında web sitesinde "İBDA-C Hedef Listesi" başlığı altında ele geçen fotoğrafları yayınladıkları tespit edilmiştir. Konuya ilişkin olarak yapılan araştırmada yasa dışı örgütün, web sitesinde oluşturduğu hedef listesinden başka "bomba yapımı ve bombalama, silah atış bilgisi, polis takibi ve tarassut, polis sorgusu, kırsalda yön tayini ve ilkyardım" konularında örgüt mensuplarını bilgilendirdiği ortaya çıkarılmıştır.

#### **Örnek Olay 2:**

1998 yılında Denizli'de DHKP/C terör örgütüne yönelik olarak yapılan operasyonlarda yakalanan teröristlerin ifadelerinde; komşu bir ülkede bulunan örgüt evinde eğitildikleri, kapta askeri ve siyasi eğitimin yanında, uydu telefonu internet üzerinden haberleşme ve şifreli görüşmeler konusunda eğitildikleri, örgütün üst düzey yöneticileri ile uydu telefonlarıyla haberleştikleri mesaj alışverişlerini internet aracılığıyla yaptıkları, cihazların şarj işlemlerini güneş ışığından enerji üreten solar sistemi ile sağladıkları anlaşılmıştır.<sup>29</sup>

<sup>27</sup> Nick Hopkins, "Cyber Terror Threatens UK's Biggest Companies" <http://www.guardian/Archive.co.uk>, Erişim tarihi: 19.12.2001.

<sup>28</sup> Fatih Yamaç, "Siber Terörizm" Emniyet Genel Müdürlüğü TEMÜH Daire Başkanlığı Psikolojik Kursu Notları

<sup>29</sup> Fatih Yamaç, "Siber Terörizm" Emniyet Genel Müdürlüğü TEMÜH Daire Başkanlığı Psikolojik Kursu Notları.

Emniyet kaynaklarına göre Őu an Őlkenin bŐtŐnlŐđŐ aleyhine faaliyet gŐsteren zararlı internet sitesi sayısı yaklaşık 7000 civarındadır. Bu sitelerden 150 tanesi aktif olarak hergŐn ortalama 500-1000 kiŐinin ziyaret ettiđi ve ođunluđu yurtdiŐından yŐnetilen sitelerdir. Genelde com, org.net uzantılı olan bu siteler Amerika, Almanya, Hollanda ve diđer Batı Avrupa Őlkeleri Őzerinden yayın yapmaktadır.

Bu sitelere karŐı gŐvenlik gŐçlerinin yapabileceđi etkin mŐcadelenin uluslararası iŐbirliđi olmadan yŐrŐtŐlmesi olası deđildir. Ancak uluslararası iŐbirliđi abalarına olumlu yanıt almak hi te kolay deđildir. Almanya, Belika ve Hollanda devletlerine DiŐiŐleri Bakanlıđı aracılıđıyla yapılan ve Őlkelerinde TŐrkiye aleyhine faaliyet gŐsteren zararlı sitelerin kapatılmasını talep eden yazıların hibirine olumlu yanıt alınamamıŐtır. Fehriye Erdal olayında bile iadeye yanaŐmayan ve iŐbirliđi konusunda ayak direten bu Őlkelerden ŐzgŐrlŐđŐn simgesi sayılabilecek sanal ortamda iŐbirliđi beklemek belki de aŐırı iyimserlik olacaktır.

O zaman akla Őu soru gelmektedir: Peki internette ŐzgŐrlŐklerin bir sınırı olmayacak mıdır? Belki de yanıtı bulunması gereken soru da budur. Gerek alemdeki terŐrist ile sanal alemdeki terŐristler arasında ne gibi fark var ki sanal alemde terŐristin yapmıŐ olduđu eylemler dokunulmaz olarak kabul edilmektedir.

Sorun yine terŐr olgusu ve terŐrist kavramı Őzerinde batı ile ortak bir anlayıŐın sađlanamamasında dŐđŐmlenmektedir. DŐŐŐnceyi aıklama suu - terŐrizm arasındaki izgide batı ile aramızda mevcut bulunan yaklaŐım farklılıđı siber terŐr - dŐŐŐnceyi aıklama suu bađlamında ok daha belirgin olarak ortaya ıkacaktır. Sanal ŐzgŐrlŐđŐn sınırını izmeden uluslararası alanda yapılacak iŐbirliđi abaları da Őlkemiz aısında istenilen sonuları dođurmayacaktır.

Siber terŐr, teknolojik olarak geliŐmiŐ Batı toplumları iin Őncelikli tehlike olsa da bu geliŐmekte olan Őlkeler iin tehlike arz etmez anlamına gelmemektedir. Batının bu terŐr olgusu ile karŐılaŐmasından sonra vereceđi tepkilerin ne olacađı ABD'ye yapılan saldırının ardından ortaya ıkmaya baŐlamıŐtır. 11 EylŐl saldırılarını bir siber terŐr olayı olarak kabul edilmesi belki zorlama bir yorum olacaktır ama, Pentagon'un kırılmaz denilen gŐvenlik Őifrelerinin kırılması, hava radar sistemlerinin devre dıŐı bırakılması, dŐŐen uakların pilotlarından kaırılma sinyalleri alınmaması gibi unsurlar ŐstŐste gelince bu saldırıların en azından teknoloji yođun bir saldırı olduđu konusunda ortak bir gŐrŐŐ oluŐmuŐtur. Siber terŐr belki bu saldırılardan ok daha ađır sonular dođuracak niteliklere sahiptir.

Ancak 11 EylŐl saldırısından sonra batı kamouyunun iinde bulunduđu psikolojik ortamdan en iyi Őekilde yararlanarak yaklaŐım farklılıklarını asgariye indirmenin yolları aranabilir. Őzellikle ABD'de siber terŐr korkusu nedeniyle aŐađıda Őrnekleri verildiđi gibi son gŐnlerde sanal ŐzgŐrlŐkler konusunda farklı yaklaŐımlar sergilendiđi gŐzlemlenmektedir.

11 EylŐl saldırılarının ardından gŐvenlik tedbirlerini arttıran ABD yŐnetimi bilindiđi gibi interneti de yakından takip etmektedir. FBI en son New York'ta kurulan ve IRA'yı destekleyen bir web sitesini dolaylı olarak kapattı. IRA, ABD'nin terŐrist gruplar listesinde yer alıyor.

Kapatılan "www.iraradio.com"un yetkilisi ise IRA (İrlanda Cumhuriyetci Ordusu) ile bir ilgilerinin olmadıđını, adreslerindeki IRA kısaltmasının "İrlanda Cumhuriyet Eylemcileri"ni temsil ettiđini iddia ediyor. Sitenin sahibi Travis Towle'a gŐre FBI, servis sađlayıcı Őirketten siteyi kapatmasını istemiŐ, aksi halde terŐre destek vermek sulamasıyla karŐı karŐıya kalacađını belirtmiŐ. Őirketin yŐnetim kurulu da kapatılma durumunda tŐm mal varlıđına el konulacađından korktuđu iin siteyi kendileri kapatmıŐ. Kapatılan "www.iraradio.com"un ana sayfasında son alınan karar ve gerekesine iliŐkin bilgiler yer alırken, Őirketin terŐrŐ

desteklemediğinin altı çiziliyor. Sayfanın en başında da FBI, CIA, MI6 gibi istihbarat birimlerine sitenin bir haber sitesi olduğu hatırlatılıyor. IRA, geçtiğimiz haftalarda yeniden açıklanan ABD'nin terör listesinde yer alan gruplardan biri ve gruba para yardımında bulunanlar hapis cezasıyla karşı karşıya kalabiliyor.<sup>30</sup>

ABD'de ortaya çıkan bu gelişmelere paralel olarak Batı Avrupa ülkelerinde de bir takım gelişmeler beklenmelidir. Çünkü 11 Eylül saldırılarının devamı olacağı yönündeki beklentiler tüm batı kamuoyunu derinden etkilemiştir. Nitekim İngiltere'de benzer uygulamalar başlamıştır. Londra merkezli *Sakina Security* (Güvenlik) adli web sitesi, patlayıcı hazırlama konusunda bilgiler içerdiği ve terör örgütlerine destek sağladığı gerekçesiyle kapatıldı.<sup>31</sup> Terörizm ile mücadele konusunda dünyada hiçbir zaman bu denli konsensus sağlanamamıştı. Belki bu psikolojik ortamda Türkiye'nin terör ve terörizmin her türlüünü lanetleyen yaklaşımı Batı tarafından paylaşılabilir.

### Farklı Bir Açıdan Ulusal Güvenlik

Hayati önem taşıyan tüm bilgiler, askeri stratejiler, güvenlik bilgileri, hastane kayıtları, iş planları ya da suç dosyaları bilgisayar ortamında saklanıyor. Biz onlara çok güveniyoruz ama onlar bizim güvendiğimiz kadar güvenilir değil. Bilgisayarlar üzerinde teknolojinin tüm imkanlarını kullanarak oluşturduğumuz güvenlik kuşakları bilgisayarı yöneten farenin birkaç hareketi ile devre dışı kalabilecek durumda. Yirminci yüzyılın sonlarının en büyük iki korkusu tek bir kelimedede birleşti ve "**siber terör**" doğdu.<sup>32</sup>

Başta ABD olmak üzere birçok devlet gizli devlet sırlarının terör örgütlerinin veya diğer devletlerin ellerine geçmesinden derin kaygılar duymaktadır. Nitekim son saldırılardan sonra ABD hükümeti kendine ait özel bir internet sitesi kurma planları üzerinde çalışmaktadır. Fiziki olarak internetten ayrı olarak kurulacak olan yeni network veya intranet devlete ait bilgileri hacker ve virüslerin tehditinden uzak tutmayı hedefliyor. Yetkililerin bilgisayar sektöründeki uzmanlara "GOVNET" projesinin ne kadar mal olacağı konusunda araştırma yaptırdığı belirtilmektedir. Bir Beyaz Saray sözcüsü, "Siber-uzayımızı hacker'lar, terörist gruplar ve siber silahlarını bize karşı kullanmak isteyen yabancı devletlerden korumak zorundayız" diyerek yönetimin internet güvenliği konusundaki endişelerini dile getirmektedir.<sup>33</sup>

Siber istihbarat, siber savaş ve siber terör kavramlarını daha iyi değerlendirebilmek için teknolojinin nasıl kullanıldığı ve teknolojinin verdiği açıklarla ilgili bazı örnekler sıralamak yararlı olacaktır. Teknolojinin en önemli ürünlerinden bilgisayar ve internet için duyulan güven kaygısı aslında pek de yersiz değil ve sadece ABD ile de sınırlı değildir. "Siber İstihbarat" kitabında bilgisayar ve yazılım dünyasının duayeni 'Microsoft' hakkında yazılanlar korkuları haklı çikartmaktadır.<sup>34</sup>

"Fransız İstihbarat Servisi ve Savunma Bakanlığı'nın hazırladığı 100 sayfalık "Bilgi Sistemleri Güvenliği: Bağımlılık ve Maruz Kalma" başlıklı rapor Microsoft hakkında farklı bir bakış açısı getirmektedir. Bu rapor, Fransa'nın Microsoft hakkındaki şüphe ve korkularını ifade etmektedir. Rapordaki ifadeler aynen şöyle; 'Bu durum ABD istihbarat servisleriyle çatışma riski yaratmaktadır...' Fransızlar tüm dünyada ve kendi ülkelerinde kullanılan bu sisteme güvenmiyorlar. Nedeni sistemin içinde bir casusluk programının varlığına ilişkin şüpheleridir. Sistemin şeffaf olmadığını söylemelerinin altında yatan gerçek de budur.

<sup>30</sup> [www.hurriyet.com.tr](http://www.hurriyet.com.tr). Erişim tarihi: 12 Ekim 2001.

<sup>31</sup> [www.hurriyet.com.tr](http://www.hurriyet.com.tr). Erişim tarihi: 05 Ekim 2001

<sup>32</sup> Faruk Örgün, a.g.e.

<sup>33</sup> [www.hurriyet.com.tr](http://www.hurriyet.com.tr). Erişim tarihi: 05 Ekim 2001

<sup>34</sup> Nedret Ersanel, Siber İstihbarat, Ankara 2001, s.24.

Microsoft'ta bir takım 'arka kapılar' olduğuna dair yaygın söylentileri duymuşlardır ve bağlantılı olarak içini bir türlü tam olarak göremedikleri bu arka kapılar yoluyla gizli bilgilerin Amerikan istihbarat servislerine aktığına inanmaktadırlar."

Fransa'nın endişelerini Rusya'da da görmek olasıdır. Rusya lideri Putin'in orduda ve savunma sanayiinde Microsoft işletim sistemlerinin ve yazılımlarının kullanılmasını bilgi güvenliği açısından yasakladığı belirtilmektedir. Lenta Rus Ajansı'nın haberine göre Putin, 27 Mart'ta yapılan başkanlık seçimlerinin sonuçlarının açıklanmasından bir gün sonra aldığı yasaklama kararını Savunma Bakanlığı eliyle bütün ilgili kurumlara bildirmiş. Yine aynı habere göre, Rusya Savunma Bakanlığı'nın tavsiye ettiği programlar arasında DOS benzeri ya da RED-HUT Linux gibi işletim sistemleri bulunuyormuş. Bunun nedeni olarak ise Microsoft Windows'un bütün sürümlerinde gizli kodlar ve anahtarlar yerleştirilmesi endişesi olarak belirtilmektedir.<sup>35</sup>

### **ECHELON: Dünyanın Gözleri ve Kulakları**

Elektronik istihbarat dünyasının en gizli ve en çok konuşulan sistemi ECHELON. Bu sistem, genel kaniya göre Amerika, İngiltere, Kanada, Avustralya ve Yeni Zelanda arasında kurulmuş bir sistemdir. Sistem, dünya çevresinde beş ana stratejik uydu kullanıyor. Bu uyduların her birinin yeryüzü üzerinde bir ana üssü yani istasyonu bulunuyor. Ayrıca sistem 100'ün üzerinde irili ufaklı uyduyu da kullanıyor ve yönlendiriyor. Bu uydular eliyle sistemin dinlemediği, görmediği, izlemediği pek bir şey bulunmuyor. İletişim imkanlarının hemen hemen neredeyse tamamını tarayabiliyor ve kontrol altında tutabiliyor. Telefon, cep telefonu, e-mailler, faks, tele-faks, bilgisayar ve hatta okyanusun altından geçen iletişim hatlarının tamamı izlenebiliyor. Konuya daha da açıklık kazandırılması için sadece telefon izleme ve dinleme rakamlarını aktaralım. Echelon dakikada 2 milyon, günde ise tam 3 milyar telefon görüşmesini izliyor ve dinliyor. Üstelik bu rakamlar yalnız 1998 yılını içermektedir... Sistem bu işlemi yaparken sadece kayıt etmekle kalmıyor. Bir yandan da konuşmanın yapıldığı çıkış noktasını tespit etmeye çalışıyor. Dünya üzerindeki net koordinatlarını ele geçirinceye değin. Böylece evinizin posta adresi şekilleniyor.<sup>36</sup>

İçinde Türkiye'nin de bulunduğu birçok ülkede yerleştirilen radyo antenleri sayesinde uydudan yapılan iletişimi takip eden sistem birçok yöntemle bilgileri toplamaktadır. Bunların başında anahtar sözcükler gelmektedir. Bu anahtar sözcükler sayesinde iletişim kaydedilmekte ve bilgiyi isteyen ülkeye verilmektedir. Anahtar sözcük yerine şahıs ve yer isimleri de kullanılmaktadır.<sup>37</sup>

Bu sistem sayesinde birçok ülkenin en hassas gizli bilgilerinin diğer ülkelerin özellikle ABD'nin eline geçmesi büyük olasılıktır. Bilgi savaşlarının başladığı<sup>38</sup> değişen dünya şartlarında gizli bilgilerin dost bile olsa başka ülkelerin eline geçmesinin riski, bugün Afganistan'da Taliban'ın ABD uçaklarına yine ABD füzeleriyle (dost olduğu dönemde verdiği) karşılık vermesi ile çok iyi anlaşılmaktadır.

Eğer bu sistem söylendiği gibi askeri değil de sadece özel iletişimi takip ediyorsa bu durumda da özel yaşamın dokunulmazlığı veya şirketlerin telefonlarının dinlenmesi ile teknoloji casusluğuna kadar gidebilecek amaçlar ile kullanılmış olabilir. Nitekim İngiliz

<sup>35</sup> Nedret Ersanel, Siber İstihbarat, Ankara 2001, s.27.

<sup>36</sup> Nedret Ersanel, Siber İstihbarat, Ankara 2001, s24-25, aktaran; Faruk Örgün, a.g.e.

<sup>37</sup> [www.aclu.org/echelonwatch/faq.html](http://www.aclu.org/echelonwatch/faq.html). "Answer to Frequently Asked Questions About Echelon" Erişim tarihi: 08/09/2001.

<sup>38</sup> Bkz. Adrew Rathmell, Cyber-terrorism: The Shape of Future Conflict, [www.kcl.ac.uk/orgs/isca/Old/rusi.html](http://www.kcl.ac.uk/orgs/isca/Old/rusi.html) Erişim tarihi: 03/10/2001. ve, Lawrence T.Greenberg, & Seymour E. Goodman, & Kevin J. Soo Hoo, *Information Warfare and International Law*, <http://www.dodccrp.org/iwilindex.htm>, Erişim tarihi: 01.05.2001.

İstihbarat Örgütü MI5, İngiliz şirketlerinin uluslararası yatırımları için bilgi toplayabileceği ve bu şirketlerin ortakları ve muhtemel ortakları hakkında bilgi verebileceğini toplantıya çağırıldığı 64 büyük İngiliz şirketinin yöneticilerine belirtmiştir.<sup>39</sup>

### **Siber terör ile Mücadelede Karşılaşılan Zorluklar**

İnternetin sınır tanımayan özelliğinin de büyük katkısı ile bilgi küreselleşmektedir. Küreselleşen bu bilgiden suç örgütleri de önemli oranlarda yararlanmakta ve internet üzerinden bomba yapım tekniklerini anlatma gibi fantazilere sahip olabilmektedir. Organize suç gruplarının ve terör örgütlerinin ellerinde bulundurdukları karapara ile teknik altyapılarını hızla geliştirmesi, oyunu güvenlik güçlerinin aksine bir kurala bağlı olmaksızın oynaması ve gerektiğinde bu alana çok büyük mali kaynaklar aktarması, devletlerin bilişim suçları ile mücadelede ciddi zorluklar ile karşılaşmasına neden olmaktadır.

Bunun yanında bilişim teknolojilerinde meydana gelen başdöndürücü gelişmeler, yasaların bu gelişmeler karşısında yetersiz kalmasına neden olmaktadır. 50 yıl öncesinin meşhur Amerikan banka soyguncusu Willie Sutton'a sormuşlar; Niçin banka soymakta bu kadar ısrar ediyorsun?. "Çünkü orası paranın bulunduğu yer" diye yanıtlamış Sutton. Kriminolojideki suçların fırsatları takip ettiği ilkesini veciz bir şekilde açıklayan bu yanıtta yola çıkarak bilgisayar teknolojileri alanında meydana gelen gelişmelerin sanal alemin teröristlerine çok büyük fırsatlar doğurduğunu belirtmek gerekmektedir.

Bu gelişmeler ne yazık ki yasa uygulayıcılarının önüne gerçekten yeni ve önemli sorunlar getirmektedir. Devletlerin bilişim suçları ve siber terör ile mücadelede karşılaştıkları bu sorunları genel olarak üç ana gruba ayırmak mümkündür;

#### **• Teknik zorluklar**

Teknik zorluklar deyince aklımıza kolluk güçlerinin bilişim suçları ve siber terör ile mücadele ederken, suçluları yakalama ve araştırma konusunda karşılaştıkları zorluklar gelmektedir.

Bu zorlukların başında da suçun işlendiği yerin tespiti gelmektedir. Örneğin Yeşilköy havalimanının hava trafik kontrol mekanizmalarını değiştirmeye çalışan bir siber terörist (hacker) veya çocuk pornografisi içerikli dosyaları internet üzerinden yayan bir sapık veya elektronik ticaret yoluyla alışveriş yapan bir şirketin bilgisayarlarına girerek kredi kartı numaralarını izinsiz ele geçiren bir hacker'ın nerede olduğunun tespiti veya bu işlemleri nereden gerçekleştirdiği suçun takibi için hayati önem arz eder. İnternet üzerinden yapılan tüm işlemler iletişimdir. Tüm bu iletişimin tespit edilmesi gerekir. Sanal suçluyu tespit etmek için kolluk güçleri, yapılan bir saldırıdan, gönderilen bir e-mail ya da elektronik tehditten kimin sorumlu olduğuna karar vermek zorundadır. Dolayısıyla kolluk her olayda, mağdurun bilgisayarından başlayarak geriye doğru failin bilgisayarına kadar iz sürmek zorundadır.<sup>40</sup> Kolluk güçlerinin bu konudaki teknik ve personel donanımının yetersizliği göz önüne alınırsa bu işin ülkemizin asayiş ve güvenliğine ne kadar büyük bir tehdit oluşturduğu ortaya çıkacaktır. Belki daha da kötüsü yukarıda örnekleri verilen ve elektronik ortamda işlenen bu suçların takibi için uluslararası işbirliğinin mutlaka yapılmasını gerekli kılan durumların ortaya çıkmasıdır. Suçun işlendiği ülkede, icra edilen eylemin suç kapsamına girmediği veya siber

<sup>39</sup> www.milliyet.com.tr./2001/09/09.

<sup>40</sup> Ken Hewe, "Prosecuting Foreign-Based Computer Crime – Where International Law and Technology Collide" [www.odccp.org/palermo/convmain.html](http://www.odccp.org/palermo/convmain.html).

teröristin (hackerin) kimliğini etkin şekilde gizlediği durumlarda elektronik takibin sonuçsuz kalması büyük olasılıktır.<sup>41</sup>

25 yıl önce asayiş polisleri belki hiç denecek kadar az şekilde uluslararası işbirliğine gereksinim duymakta idiler. Ancak bilgi çağı ile birlikte, bir çok ülkede durum değişti. Herkes bilmektedir ki artık suçlular sadece ulusal sınırlar dahilinde faaliyet göstermemektedirler. İletişim ağlarının artmasına paralel olarak artış gösteren elektronik ticaret, iş yaşamını ve ticareti, suçlular karşısında daha edilgen bir duruma getirmiştir. İnternetin küresel niteliği suçluların da küreselleşmesini ve kimliklerini çok rahat şekilde saklamasını sonucunu doğurmuştur. Terörizmden uyuşturucu kaçakçılığına, çocuk pornografisinden fikri hakların ihlal edildiği tüm suçlarda veya elektronik ticaret şirketlerine yönelik saldırılarda, suç örgütleri elemanları dünyanın birbirine çok uzak ve farklı ülkelerinde oturarak ortak eylem gerçekleştirebilmektedirler.

Suçluların bu kadar etkin bir şekilde uluslararası işbirliği yaptığı bilgi çağında, toplumu ve yasaları korumakla yükümlü görevliler ne yazık ki bu işbirliği ve dayanışmayı gösterememektedir. Suçlular birçok farklı ülkedeki İnternet Servis Sağlayıcılarını (İSS) kullanarak internetteki izlerinin takibini zorlaştırmaktadırlar. Hatta bazı olaylarda failin ve mağdurun, yani suçun işlendiği bilgisayar ile mağdur bilgisayar aynı ülke sınırları içinde olduğu halde, suçluya ulaşabilmek için uluslararası işbirliği gerekebilir. Örneğin Ankara Kızılay'daki bürosunda oturan bir Siber terörist (hacker) hemen ötesinde Bakanlıklar da bulunan Başbakanlık'ın bilgisayar sistemini çökertmek veya zarar vermek için hazırladığı iletiyi Paris, Londra ve New York'taki İSS üzerinden bu bilgisayara ulaştırabilir. Bakanlıklar ve Kızılay bölgesinin bağlı bulunduğu Çankaya İlçe Emniyet Amirliği bu olayı aydınlatabilmek için Paris, Londra ve New York polis teşkilatları ile ortak çalışmak zorundadır.

Tüm bu çalışmaları yapan ve sonuçta saldırının yapıldığı bilgisayara ulaşan polis bu bilgisayarın bir internet kafe'de olduğunu tespit etmesi durumunda ne olacağını hep beraber düşünmemiz gerekecek. Kim sorumlu? İnternet kafe sahibi mi yoksa kim olduğu bilinmeyen meçhul kullanıcı mı? Veya failin bilgisayarına şehiriçi telefon kulubesinden bağlandığını ve saldırıları buradan gerçekleştirdiğini düşünelim. Bu durumlarda güvenlik güçlerinin faili tespit etmesi mümkün olmayacaktır.

Görüldüğü gibi siber terör eylemlerini ve bilişim suçlarını birkaç ülke üzerinden gerçekleştiren bu tür failer mücadeleyi gerçekten zorlaştırmaktadırlar. Söz konusu, sadece mağdur ile failin bulunduğu iki ülke olsa belki karşılıklı yasal işbirliği ile olayı kısa sürede aydınlatmak mümkün olacaktır. Ancak üçüncü, dördüncü ve hatta beşinci ülkeler devreye girince gerekli yazışmalar ve diğer usule ilişkin işlemler nedeniyle kolluk güçleri suç teşkil eden verilere ulaşmadan bu veriler ortadan kaldırılabilir veya artık bunlara ulaşmak olanaksız hale gelebilir. Dolayısıyla teknik olarak işbirliği neredeyse imkansız hale gelmektedir.

Yukarıda Kızılay'dan yapıldığı varsayılan saldırının Paris'ten yapıldığını varsayalım. Paris'ten Londra'ya oradan ABD'ye oradan da Bakanlıklar'daki Başbakanlık'ın internet sitesine yapılan saldırının kaynağını bulabilmek için Türk yetkilileri istisnalar hariç, mağdurun bilgisayarından yola çıkarak sadece ileti zincirinin bir önceki halkası olan ABD'deki İSS'ya ulaşabilir. Çünkü mağdurun bilgisayarı, genelde zincirin bir önceki halkasını gösterir. Daha önceki halkayı gösterse bile bu halkada yer alan adres sahte veya geçici olarak kapatılmış olabilir. Normal olarak internetin yapısı gereği ileti zincirinin ilk halkasını (Paris) göstermesi de mümkün değildir. Bu durumda Türk yetkilileri ABD'den sonra Londra ile oradan da Paris ile kontak kurmak zorundadır. Bu işlemlerin kısa sürede bitirilmesi gerektiği düşünülürse (Çünkü

---

<sup>41</sup> James K. Robinson, a.g.e. s.3.

bir nevi olay yeri incelemesi yapma gibi bir durum söz konusu) elektronik takip konusunda ulusların karşı karşıya kaldığı tehdit çok iyi anlaşılacaktır. Ayrıca zincire dahil olan ülkeler arasındaki saat farkları yüzünden bir ülke kolluk güçlerinin acil ihtiyacı olan bir durumda coğrafi olarak çok uzak olan bir ülke polislerinin ilgili bürosunda sadece bir tek gece nöbetçisi (büyük olasılıkla teknik ayrıntıları bilmeyen) bulunabilir. Sonuç olarak suçlar cezalandırılmadığı gibi yeniden saldırı yapma şansına sahip olabilirler.

Bu tür suçlarla mücadelede ulusların coğrafi sınırların varlığı ve bir ülke kolluğunun bir başka ülke sınırları içinde operasyon yapması mümkün olmadığı için bu suçlarla mücadelede geleneksel olarak devletler arasında mevcut bulunan yargısal işbirliğine yeni bir anlayış getirmek zorunluluğu vardır. Çünkü internet sınır tanımadığı gibi siber suçlar da sınır tanımamaktadır. Güvenlik güçleri bu suçlar ile mücadelede daha önce hiç olmadığı kadar işbirliğine muhtaç ve karşılıklı bağımlıdır.

Siber suçlar ile mücadelede devletlerin yapacağı yargısal işbirliği yaşamsal öneme sahip olsa da bu, suçların takip ve tarassutunda yeterli değildir. Bu suçlar ile mücadelede kolluk kuvvetlerinin karşılıklı yardımlaşması yanında bilişim sektörü de uluslararası işbirliğinde kolluk güçlerine yardımda bulunmalıdır. Özellikle log dosyaları, e-mailler ve elektronik delil niteliğine sahip diğer dosyalar sektör tarafından iyi korunmalı ve gerektiğinde hızlı bir şekilde bu delilleri isteyen ülkeye teslim edilmelidir. Gecikme durumunda bu bilgilerin değiştirilmesi veya silinmesi olasıdır.

Bir diğer sorun ise siber suçların suçlarını işlemek için kaleşnikoflara veya diğer ateşli silahlara gereksiniminin ortadan kalkmasıdır. Bu suçluları mağdurlarına ulaştıracak tek ihtiyacı sadece bir bilgisayar ve modemdır. Tüm dünyayı etkileyen virüs saldırıları buna en güzel örnektir. Örneğin Arjantinli Kalamar adlı bir bilgisayar korsanı "Here you are" "Here you have", "Hi, check this" gibi başlıklara sahip ve ekinde ünlü Rus tenisçi Anna Kournikova'nın seksi pozlarını içeren bir virüsü mail aracılığıyla tüm dünyaya yaymıştır. Kournikova'nın resminin üzerine tıklama yapılan her bilgisayar kaçınılmaz olarak çökmüştür.<sup>42</sup> İngiltere Dışişleri Bakanı Robin Cook, bu virüs saldırısından sonra bir saat içinde ulusal alarm verildiğini açıklamıştır.<sup>43</sup>

Bu tür saldırılarda saldırıya cevap verme süresi modern dünyada devletlerin kaosa sürüklenmesine veya istikrarı korumasında temel belirleyici faktör olacaktır. Ne kadar kısa sürede önlem alınabilirse zarar o oranda az olacaktır. Saldırlara karşı önlem alma süresi uzadıkça ülkenin kaosa sürüklenmesi de o denli kaçınılmaz olacaktır.

Cook, siber teröristlerin ülkeye vereceği zararların askeri saldırılardan daha tehlikeli olabileceğini belirtmektedir. Zira bilgisayarlar ülkenin içme suyu şebekesi, enerji ve ulaşım şebekelerini kontrol etmektedir.

Her gün gelen e-maillerimize baktığımızda hotmail sitesinde şöyle bir ifade ile karşılaşırız;

"Her 5 bilgisayardan 1 tanesinin virüs saldırılarından zarar gördüğünü biliyor musunuz?"

Yüzde yirmilik bu oran gerçekten toplum hayatında suç oranının ne kadar büyük olduğunu göstermektedir.

Elektronik takip konusunda karşılaşılan teknik zorluklar bu sayılanlardan ibaret değildir. Hacker'lerin bir kısmı elektronik "parmak izi" bıraksa da bir çok profesyonel hacker

<sup>42</sup> Radikal Gazetesi 14 Şubat 2001.

<sup>43</sup> Richard Norton Taylor, "Hackers Could Halt UK, Says Cook" <http://www.guardian/Archive.co.uk>, Erişim tarihi: 19.12.2001.

siber alanda izlerini nasıl saklayacaklarını çok iyi bilmektedir. Teknolojinin gelişmesine paralel olarak bu suçlular ve teröristler tahmin edilemeyecek yollarla tüm devletleri ve insanlığı hedef almaktadırlar. Eşzamanlı olarak kablosuz ve şifreli olarak yapılan iletişimi güvenlik güçleri nasıl tespit edebilecektir.? Bir ülkeye yerleşen suçlular eğer sadece diğer ülkelerde yerleştirilen çıkış kapılarını kullanan uydu ve kablosuz iletişim olanaklarını kullanıyorsa bu suçlular nasıl takip edilecek?<sup>44</sup> Bu sorunların üstesinden gelmek belki de mümkün olmayacaktır. Cinayet nasıl insanoğlu ile beraber varılmaya devam ediyorsa siber suçlarda aynı şekilde varlığını sürdürecektir. Ancak siber suçların potansiyel tehdit olarak ürkütücülüğü bu suçlar ile mücadeleye özel bir önem verilmesini gerektirmektedir.

- **Yasal zorluklar**

Hızla gelişen teknoloji karşısında hukukun geride kaldığı bu teknolojik ve beraberinde getirdiği sosyal değişime ayak uyduramadığı genel kabul görmüş bir gerçekliktir. Belki bu eleştiri özellikle Türkiye gibi içtihat hukukunun çok gelişmediği hukuk sistemleri için daha doğru bir yargı olacaktır. Yasaların çıkarılma süreçlerinde meydana gelen tıkanmalar veya yetersizlikler siber suçlar alanında da kendini göstermekte ve sektörün ihtiyaçlarına cevap verecek nitelikte yasalar çıkarılmamaktadır.

Bilişim suçlarını bu suçları işlemekten vazgeçirmenin en önemli yollarının başında etkin bir şekilde takip ve cezalandırma olanağı veren yasalara sahip olunması gelmektedir. Genel olarak bu yasaların çıkarılması konusunda ülkeler hızlı hareket edememektedirler. Bunların yanında bazı ülkelerin bu suç türlerini suç kapsamına alan düzenlemeleri henüz yapmamış olmaları kara para aklama da olduğu gibi "yeni suç cennetleri"nin doğmasına neden olacaktır. Bu nedenle siber suçların tehdit boyutu tüm ülkeler tarafından yeterince anlaşılmalı ve yapılacak olan yasal düzenlemeler tüm ülkeleri kapsamalıdır. Virüs yazımı ve dağıtılması veya bir sitenin çökertilmesi bazıları tarafından basit bir suç olarak algılanabilir ancak bu suçların sonuçları çok ağır olabilmektedir. J. Chirac'ın G8 Zirvesinde belirttiği gibi internet nasıl uluslararası niteliğe sahip ise bu suçlar ile mücadelede kullanılacak hukuk kuralları da evrensel olmalı ve uluslararası yasal bir sistem oluşturulmalıdır.<sup>45</sup> Yani internetin ulaştığı yere mutlaka hukuk kuralları da etkin olarak ulaşmalıdır. Suçun işlendiği ülkede siber suçlar cezalandırılmıyorsa yapılacak işbirliğinin hiçbir anlamı olmayacaktır.

30 yıl Newsweek dergisinin dış haberler muhabirliği yapan ve halen Washington'daki Stratejik ve Uluslararası Araştırmalar Merkezi Başkanlığını yürüten Arnaud de Borchgrave, siber terörizmin veya diğer siber suçların bir çoğunun uluslararası polis işbirliği zorunlu kıldığını belirtmekte ve terör örgütlerinin ulusal egemenlik sınırları denilen duvarın arkasından bizlere güldüğünü düşünmektedir. Borchgrave'e göre ulusal egemenlik kavramının geleneksel imtiyazları sadece iletişim devrimi ile değil, terör örgütleri ve hatta bireylerce kullanılan virüsler, solucanlar, truva atları ve zaman-mantık bombaları gibi yeni silah türleri tarafından ortadan kalkmaya başlamıştır. Kabul etsek de etmesek de şu an içinde bulunduğumuz şartlar kötüler için çalışmaktadır.<sup>46</sup>

Siber terörizm ile mücadele kaçınılmaz olarak sınır ötesi operasyon ve işbirliği gerektirmektedir. Bunu sağlamanın iki yolu vardır: Ya uluslararası işbirliği ya da bir ülke kendisine yapılan bir saldırıda bir diğer ülkenin sınırları içinde izin alarak veya almadan operasyon gerçekleştirecektir. Bu ise uluslararası hukuka uygun bir işlem olmayacaktır.

---

<sup>44</sup> James K. Robinson, a.g.e. s. 5.

<sup>45</sup> James K. Robinson, a.g.e. s. 5.

<sup>46</sup> ----- "Cyber Terrorism" *American Banker* 08.09.1997, <http://www.infowar.com/> Erişim tarihi: 14.12.2001.

Siber suçları cezalandıran ülkelerde ise yapılması gereken şey teknolojinin gelişmesine paralel olarak hukuk sistemlerinin de güncel ihtiyaçlara göre yenilenmesidir. Özellikle Usul hukukundaki ciddi anlamda revizyon gereken durumlar söz konusu olabilecektir. Örneğin bazı ülkelerin ilgili mevzuatında İSS'nin düzenli aralıklar ile sahip oldukları verileri silmelerini emretmektedir. Ancak bu yapılırsa kolluk güçlerinin silinen bu veriler arasında bulunan ve muhtemel olarak bir olayın aydınlatılmasını sağlayacak olan bir delilin yok edilme olasılığı göz ardı edilmektedir. Bu ülkeler elektronik takip konusunda ciddi sıkıntılara neden olan bu uygulamalarının güvenli bir internet düşüncesiyle ne kadar bağdaştığını açıklamak durumundadırlar.<sup>47</sup>

Uluslararası alanda soruna çözüm bulmak için bazı çalışmalar da yapılmaktadır. Bunların en önemlisi olan Avrupa Konseyi'nin önderliğinde hazırlanan Siber Suçlar Konvansiyon'undan söz etmek gerekir.

Avrupa Konseyi (AK) bünyesinde yer alan European Committee on Crime Problems (Avrupa Suç Problemleri Komitesi) Kasım 1996'da siber alanda<sup>48</sup> işlenen suçlar üzerinde çalışmak üzere bir uzmanlar komitesi oluşturdu. Komite'nin bu kararından sonra Bakanlar Komitesi, 4 Şubat 1997'de yaptıkları toplantıda "The Committee of Experts on Crime in Cyber-space" adı altında yeni bir komite oluşturulmasına karar verdi. Bu komite çalışmalarına Nisan 1997 de başladı. Uzun süren çalışmalar ve tartışmalardan sonra komite Siber Suçlar Konvansiyonu'nun tasarısını ve açıklayıcı raporu Avrupa Suç Problemleri Komitesi'ne Haziran 2001'de sundu.

Konvansiyon 8 Kasım 2001'de Avrupa Konseyi Bakanlar Komitesinde kabul edilerek 23 Kasım 2001'de Budepeşte'de düzenlenen Siber Suçlar Uluslararası Konferansı'da imzaya açıldı.

43 Avrupa konseyi ülkesinin yanısıra ABD, Canada, Japonya ve Güney Afrika'nın katkılarıyla hazırlanan Konvansiyona, Budapeşte'de 26 AK ülkesi ile ABD, Kanada, Japonya ve Güney Afrika imza koymuşlardır. Konvansiyon üçü AK ülkesi olmak kaydıyla beş ülke tarafından onaylandıktan sonra yürürlüğe girecektir.

Konvansiyon sivil toplum kuruluşları ve internet servis sağlayıcıları tarafından şiddetle eleştirilmektedir. Bu grupların öncelikli itirazları Konvansiyon'un muğlak ifadelerle sahip olduğu, servis sağlayıcılara ağır yükler getirdiği, gizlice hazırlandığı dolayısıyla hazırlanışı sırasında çıkar gruplarının görüşlerinin yeterince dikkate alınmadığı gibi konularda yoğunlaşmaktadır.

4 bölüm ve 48 maddeden oluşan Konvansiyon, 1. bölümde siber alanda işlenen 9 ayrı suçu 4 farklı kategoride tanımlama yoluna gitmiştir. 2. bölümde ulusal düzeyde bu suçlara karşı (ceza ve ceza usule ilişkin) alınması gereken önlemler, 3. bölümde uluslararası işbirliği ve 4. bölümde son hükümlere yer vermiştir.<sup>49</sup>

İnternette faaliyet gösteren nefret ve şiddet içerikli ırkçı sitelere karşı Konvansiyon'a bir protokol eklenmesi konusunda çalışmalar yapılmaktadır. Net ortamında 2500'ü ABD'de olmak üzere toplam 4000 civarında ırkçı site olduğu bilinmektedir.<sup>50</sup>

- **Operasyonel zorluklar**

---

<sup>47</sup> James K. Robinson, a.g.e. s. 6.

<sup>48</sup> Siber alan, iletişim ve bilgi sistemlerinin birbirleri ile bağlanarak oluşturduğu alana verilen isimdir.

<sup>49</sup> Convention on Cybercrime and its Explanatory Report; <http://www.legal.coe.int/> Erişim tarihi. 15.11. 2001.

<sup>50</sup> Wendy McAuliffe, "Europe Hopes To Outlaw hate Speech Online" <http://news.cnet.com/news> Erişim tarihi. 22.12. 2001.

Teknik ve yasal zorlukların yanında bu suçlar ile mücadele eden kolluğun önündeki diğer en büyük sorun operasyonel zorluklardır. Dünyanın neresinde olursa olsun her ülke, iletişim cihazları marifetiyle işlenen kompleks teknik ve yasal özellikler gösteren bu suçlarla mücadelede, yüksek teknolojiyi iyi takip eden, kendisini bilgisayar ve telekomikasyon konusuna adanmış uzman görevlilere gereksinim duymaktadır.<sup>51</sup>

Ayrıca bu suçlar ile mücadele edecek kolluk güçleri çalışma saatleri konusunda çoğu zaman özveri göstermek durumundadır. Üzerinde yoğunlaşılacak bir olayın ne zaman biteceği çoğu zaman belli olmayacaktır. Çalışan personel mesai bitiminde işini bırakıp ayrılma olanağına çoğu zaman sahip olamayacaktır. Bu birimlerde kolluk güçlerinden personel olduğu kadar bilgisayar ve elektronik mühendisleri de olmalıdır. Ancak özel sektör ile ücret konusunda genelde yarışamayan kamu sektörü çoğu zaman elindeki nitelikli elemanları özel sektöre kaptırmaktadır. Mevcut haliyle çok az bir personel ile hizmet veren bu üniteler personel açısından ciddi anlamda takviye edilmelidir.

Bir diğer sorun ise nitelik olarak yetkin personelin malzeme olarak da en yeni teknoloji ile takviye edilmesi sorunudur. 20 yıl önce göreve başlayan bir polisin en önemli ihtiyacı bir silah ve cop idi. Ancak şu an bilgi işlem bürosunda çalışacak veya terör şubesinde yasadışı internet adreslerini takip edecek olan bir memurun çok yeni teknoloji ile donatılmış en son yazılımlara sahip bir bilgisayara ihtiyacı vardır. Ancak bu bilgisayarı sık aralıklarla yenilemez veya geliştirmeyen iseniz polisin suç örgütleri karşısında yetersiz kalması kaçınılmaz olacaktır. Gün gelecek otomatik lazerli silahla saldırı yapan teröristlere karşı tabanca ile karşılık vermek gibi kolluk kendi sitelerini bile korumadan aciz kalacaktır.

Ayrıca bu personel aynı zamanda siber suçlar ile ilgili düzenli hizmet-içi eğitimden geçirilmeli bu konuda eksiklikleri giderilmelidir.

#### • **Mağdur davranışlarından kaynaklanan zorluklar**

Siber alanda ortaya çıkan suçlar ile mücadelede mevcut polise tedbirler ile veya bu alanda düzenleme yapan birimlerin yapacağı çalışmalar ile başarılı olmak mümkün değildir. Siber alanda güvenliğin sağlanması birçok kuruluşun çabası yanında potansiyel mağdurların davranışlarına da bağlıdır. Bu konuda ele alınması gereken iki husus vardır. Birincisi, bilgisayar kullanıcılarının yeterli güvenliği sağlama konusunda takındıkları tavrıdır. Saldırıya açık bir şekilde bekleyen bilgisayarlar en büyük tehdit altında olanlardır. Genel olarak belirtildiği gibi hiç kimse sokak ortasında bırakmayacağı bir malını veya bilgisini bilgisayarda da bırakmamalıdır. En azından dosyalara kolay tahmin edilemeyecek şifreler konulmalıdır.

İkincisi ise özellikle ticari hayatta, bu tür saldırılarda ticari itibar kaybı veya başka nedenlerden dolayı yapılan saldırıların kolluk güçlerine bildirilmemesidir. Büyük firmalar özellikle bankalar ticari itibarları zedelenir korkusuyla polis ile işbirliğinden kaçınmakta olayı örtmeye çalışmaktadırlar. Örneğin bir büyük bankanın bilgisayar sistemine giren kişiler gelen yurtdışı havaleler hakkında tüm detayları öğrenerek alıcıya ait bilgileri de öğrenip sahte kimlik hazırlamışlardır. 7-8 farklı ilde bu bankanın şubelerinden sahte kimlikler ile gelen havaleleri çekmişlerdir. Bu olayın başka bilgisayar sistemine girilerek bilgilerin alınması dışında bu bilgileri elde etme olanağının olmamasına rağmen banka yetkilileri olayı kabul edip bilgisayar güvenlik sistemlerini güçlendirme yerine sistemlerinin kırılmasının mümkün olmadığını düşünmekte ve olayı kabul etmemektedirler. Çünkü bu olayın duyulması durumunda ticari yaşamda bir takım zorluklar ile karşılaşacaklardır. Öte yandan hackerler bir sonraki

<sup>51</sup> James K. Robinson, a.g.e. s. 6.

saldırısında belki de daha büyük zarar verebilir. Eğer olayın üstündeki sis perdesinin kaldırılmasında mağdur taraf yardımcı olmaz ise bu tür saldırılara yasal bir çözüm bulmak o denli zor olacaktır. Bu anlamda genel olarak asayişe intikal eden bilişim suçlarının sayısı da gelişmiş batılı devletlere oranla çok azdır. Sayının az olmasının nedenlerinin biri de mağdurların olayı yetkili makamlara bildirmemesi veya ihbar etmemesidir.

### **Siber teröre karşı korunma yolları:**

Bilindiği gibi hassas bilgilere sahip bir çok kamu kurum ve kuruluşu tüm dünya ile bağlantılı olan "internet" yerine sadece kapalı sınırlar içinde hareket eden "intranet" kullanmaktadır. Bu şekilde dışarıya bağlantısı olmayan kapalı bir istem ile dış dünyadan gelecek saldırılardan belirli yöntemler ile kendilerini korumaktadır.

Ancak "intranet" ler de sanıldığı kadar güvenli değildir. Özellikle kullanıcı sayısı arttıkça, kurum büyüdükçe ve personel sayısında artış oldukça güvenlik azalmaktadır. Kendini dışarıya karşı güvende hisseden sistem içten gelecek saldırılara karşı korumasızdır. Veya içeriden dışarıya destek verilmesi durumunda (bu kasıtlı veya yeni işe başlamış bir personel olabilir) saldırı çok daha kolaylaşır.<sup>52</sup> Bu nedenle "intranet" sisteminin güvenliği konusunu da şüphe ile yaklaşmak zorunluluğu vardır. Teknik ayrıntıları değinmeden sadece bu konuda şu çözüm önerilebilir: İtranet sistemini çok büyük kurumlarda bölümlere ayırmak ve küçük parçacıklar halinde tutmak gerekir. Yapılan bir saldırıda zararı en aza indirmenin tek yolu hedefi küçültmektir. Büyük sistemlerin siber terör konusunda daima birinci hedef haline gelecekleri ve teröristlerin öncelikler arasında yer alacağında şüphe duyulmamalıdır. Zira fizik alemde olduğu gibi sanal alemde de terörist yaptığı saldırı ile gündemin birinci sırasına oturmayı hedefleyecektir. Bunun içinde yaptığı eylemin ses getirici bir eylem olması için çaba harcayacaktır.

Terörist siber terör eylemini gerçekleştirirken "ben siber bir eylem gerçekleştiriyorum o halde bu alanın dışına çıkmamam gerekir" diye bir düşünce içinde hareket etmez. Dolayısıyla fizik alemdeki saldırılarını siber ortam ile desteklediği gibi siber ortamda yapacağı saldırıları fizik alemdeki eylemleri ile de destekleyebilir. Kanımca 11 Eylül saldırıları bu tür bir saldırı idi. Teröristler, saldırılarına önceden pilotluk eğitimi almak, uçuş rotalarını belirlemek, güvenlik önlemlerini geçerek pilot kabinine girmek gibi fizibilite çalışmaları yaparak hazırlanmışlardır. Ancak bunların yanında pilotun yere sinyal göndermesini engelleyici veya kulenin denetimini engelleyici veya kırılmaz denilen Pentagon'un güvenlik sistemlerini kırmak gibi bir takım teknoloji-yoğun fizibilite çalışması içine de girmiştir ki, bu da saldırıların siber terör boyutu olarak değerlendirilebilir. Siber saldırı, fiziki saldırıyı kolaylaştırmak ve şiddetini maksimum hale getirebilmek için kullanılan önemli bir araç olmuştur.

ABD Kongre Komisyonu, terör örgütleri tarafından büyük yıkımlara neden olan saldırı çeşitleri arasında siber saldırıları da saymaktadır.<sup>53</sup> Bir terör saldırısında terör örgütü tarafından iletişimin engellenmesi fiziki saldırının şiddetini artırmada önemli bir etkiye sahiptir. Bunu bilen terör örgütleri eylemlerini daima siber alanda destekleyeceklerdir.

Tarihin Sonu kitabının yazarı Francis Fukuyama, Soğuk savaşın sona ermesinden sonra Sovyetler Birliği'nde sayıları büyük rakamlara ulaşan, normal şartlarda yasal olarak özel veya kamu kesiminde önemli işler yapabilecek olan çok yetenekli bir insan kaynağını başı bozuk ve dağınık bir halde dışarıda bırakıldığını belirtmektedir. Bu kişilerin siber terörizm özellikle siber mafya olarak adlandırılan organize suç faaliyetleri gibi birçok illegal aktivitenin

<sup>52</sup> Lebin Cheng, "Virtual Private Corporation: Information Security Infrastructure Restructuring Strategy for Countering for Cyber-Terrorism", <http://www.isi.edu/gost/cctws/lebinc.html>

<sup>53</sup> Patrick Thibodeau, War Against Terrorism Raises IT Security Stakes", <http://www.computerworld.com>, 24.Sep,2001. erişim tarihi: 14.12.2001.

içinde yer alması kaçınılmazdır.<sup>54</sup> Özellikle SSCB'den geriye kalan birçok mafya ve organize suç örgütlerinin bu alanda faaliyet göstermesi büyük olasılıktır.

### **Sonuç:**

Bilişim suçlarının önlenmesi kanun koyucuları ve uygulayıcıları için hiç te kolay olmayacaktır. Çünkü bilgisayar teknolojisi ve internet bu alanda çalışan kişilerde belirli düzeyde teknolojik bilgi gerektirmektedir. Bu bilgiyi eğitim dönemlerinde almamış olma hem polisler ve hem de yargı mensuplarının bu alanda suçlular karşısında genel olarak etkin olamamama ihtimali büyüktür.<sup>55</sup>

Bilişim alanında ortaya çıkan suçlar ile mücadelede mevcut polisiye tedbirler ile veya bu alanda düzenleme yapan birimlerin yapacağı çalışmalar ile başarılı olmak mümkün değildir. Siber alanda güvenliğin sağlanması birçok kuruluşun çabası yanında potansiyel mağdurların davranışlarına da bağlıdır. Saldırıya açık bir şekilde bekleyen bilgisayarlar en büyük tehdit altında olanlardır. Genel olarak belirtildiği gibi hiç kimse sokak ortasında bırakmayacağı bir malını veya bilgisini bilgisayarda da bırakmamalıdır. En azından dosyalara kolay tahmin edilemeyecek şifreler konulmalıdır.

Sınır tanımayan özelliğe sahip olan bilişim suçları ile mücadelede başarılı olabilmek için;

- a. yasal,
- b. teknolojik
- c. bilişim sektörü bazında çözümler bulmak zorunludur.

Devletlerin sınırlı kapasiteleri nedeniyle yasaların etkin bir şekilde korunması neredeyse mümkün olmamaktadır. Çok fazla yasal düzenleme yapma veya kısıtlayıcı yasalar çıkarmak da hem teknolojik gelişmeleri hem de ticari hayatı etkileyebilir. Bazı alanlarda kuralların devlet yerine serbest rekabet ortamında belirlenmesi bilişim suçları ile mücadelede daha etkin olabilmektedir.

Bu bağlamda özel sektörün bu alanda yapacağı katkıların önemi çok büyüktür. Tüm ülkeler ortak çalışsa bile bilişim suçlarının tehdidi karşısında başarılı olmaları mümkün değildir. Mutlaka özel sektör çözüm bulmada ortak olmalıdır. Olaya ülkemiz açısından bakacak olursak Türkiye'nin en iyi üniversitelerinin bilgisayar ve elektronik mühendisliği bölümlerinden kaç mezunun kamuda işe başladığını sorgulamak gerekir. Yok denecek kadar azdır. Yetenekli gençler daha eğitim dönemlerinde ulusal ve uluslararası firmalar tarafından kapışılmaktadır. Teknik bilgi, kaynak ve nitelikli personel açısından özel sektör kamuya göre daha avantajlıdır. Bu nedenle sektör internet ortamının güvenliği (özel bilgisayar ağlarının) konusunda etkin çalışmalar yapmalıdır. Gerekliğinde kolluk güçlerine maddi delil ve özellikle eğitim konusunda yardımlarda bulunmalıdır. Kolluk güçlerinin yurtdışı eğitimi konusunda ayıracakları fonlar sayesinde kendi geleceklerini garanti altına almış olacaklardır.

Bilgisayar sistemlerinin tüketicileri olarak da kabul edilebilecek olan bireyler, sorumlu davranışları ile bu suçlar ile mücadelede yardımcı olacaktır. Herkes evini hırsızların giremeyeceği şekilde güvenlik önlemini alsa, nasıl hırsızlık olaylarında önemli düşüş olacağı bir gerçek ise, bilişim alanında da tüketiciler, kurallara uygun olarak gerekli güvenlik önlemlerine uymuş olsa bilişim alanında görülen suçlarda bir azalma olacaktır. Bankaların tüm güvenlik önlemlerine karşın hala banka soyulduğu gibi, tüketiciler ve kolluk gerekli koruyucu önlemleri almış olsa bile bilişim suçları bitmeyecektir. Ama ulusal güvenliği tehdit eder şekilde

<sup>54</sup> ----- "Cyber Terrorism" *American Banker* 08.09.1997, <http://www.infowar.com/> Erişim tarihi: 14.12.2001.

<sup>55</sup> Peter Grabowsky, a.g.e. s. 2.

veya elektronik ticaret yapan firmaların uykularını kaçırarak kadar büyük oranlarda gerçekleşmeyecektir.

Yukarıda geniş şekilde açıklandığı gibi bu suçlar ile mücadelede uluslararası işbirliği olmadan başarılı olmak mümkün değildir. Ancak bu işbirliği nasıl sağlanacak. Uluslararası işbirliği konusunda İnterpol bünyesinde özel bir birim oluşturularak ortak ve hızlı elektronik takip yapma olanağı sağlanabilir<sup>56</sup>. Bunun için belki işbirliği alanları öncelikle belirlenecek suç türleri arasında bir pilot uygulama yapılabilir. Türkiye bu durumda son dönem terör olayları nedeniyle ortaya çıkan şartlarda kendisinin öncelik verdiği suç türleri arasında terör suçlarını dahil edebilir. Ancak devlet güvenliği aleyhine sadece propaganda ile sınırlı kalan zararlı siteler konusunda beklediğini bulması mümkün değildir.

Tüm bu önlemlerin yanında uzun soluklu bir çözüm yolu ise, siber etik dediğimiz sanal alemde davranış kuralları konusunda özellikle genç kuşağın eğitilmesi gerekmektedir. Günlük yaşamında hırsızlık yapmayı ahlaki değerleriyle veya toplumsal statüsü ile bağdaştıramayan bir genç net ortamında çok rahat hırsızlık yapabilmekte veya başkalarına zarar vermektedir. İnternet çağının gençlerinin içine düştüğü sanal alem- gerçek alem çatışmasının eğitimle ortadan kaldırmak gereklidir. Gençler ilköğretimden başlayarak siber etik konusunda eğitilmelidir. Bu çalışma, ABD'de olduğu gibi özel sektör ile işbirliği çerçevesinde yürütülebilir. Türkiye gibi sanal aleme sonradan dahil olan ülkeler gelişmiş batı ülkelerine göre bu konuda daha şanslıdır. Sanal aleme kullanan gençliği hala eğitme olanağımız vardır.

11 Şubat ta ABD'de Dünya Ticaret Merkezine yapılan saldırıların hemen ardından ABD ve dünyanın diğer bölgelerinde felaketten rant sağlamak için yapılan çabalara ait aşağıda vereceğimiz örnek, bilişim etiği ile ilgili olarak çok çaba harcanmasını gerektirdiğini net olarak ortaya koymaktadır. Haberi aynen buraya almak istiyorum:

*"Sabah saatlerinde ardarda gelen saldırılarla sarsılan ABD'de insanlar televizyonlara kilitlenmiş dehşet görüntülerini izlerken bazı internet kullanıcılarının ilk tepkisi felaketi tanımlayan domain adreslerini üzerlerine kaydettirmek oldu.*

*İlk uçağın çarptığını duyar duymaz isim kaydeden siteye girdiğini ancak "Worldtradecentercrash.com" adresinin birkaç saniye önce başka birisinin adına kaydedildiğini öğrenen Amerikalı Jim Burke, "wtccrash.com" adresini alabilmiş. Bu iki adresin daha ikinci uçak güney kuleye çarpmadan alınması, kullanıcıların ne kadar hızlı hareket ettiğinin bir kanıtı.*

*Olay günü gelişmeler sürerken yüzlerce kişi Dünya Ticaret Merkezi'ne yapılan saldırıları ifade eden "wtccras.net", "wtccrash.org", wtccplanecrash.com", "tradecentercrash.com" gibi adresleri kaydettirdi. İkinci uçağın çarpmasından sonra da çoğul ifade taşıyan "worldtradecentercrashes.com" ve "wtccrashes.com" adresleri İsviçreli bir internet kullanıcısı tarafından alındı.*

### **FELAKETİN ADRESLERİ KAPIŞ KAPIŞ !**

*New York'taki saldırıları saat 09:43'de Pentagon'a yapılan saldırılar izleyince bu kez "pentagonattack.com", "pentagondisaster.com" ve "pentagoncrash.com" adresleri dakikalar içinde kaydedildi.*

*Bir Kanadalı, kulelerin yıkılışını ifade eden "wtctowercollapse.com" adresini ilk kulenin yıkılışından hemen sonra almayı "başardı". İki kule de yıkıldıktan sonra "tradetowerscollapse.com", "twintowercollapde.com", "wtccollapse.com", "wtccollapse.net"*

<sup>56</sup> İnterpol bilgi teknolojileri konusunda bir çalışma grubu oluşturmuştur. Bkz. Hans Corell, Inroductory Remarks and Concluding Remarks, of Panel on "The Challenge of Borderless Cyber-Crime" Symposium on the The Rule of Law in the Global Village, Palermo, 14 December 2000.

*(bir Koreli aldı) gibi o korkunç günü anlatan adresler dünyanın dört bir yanındaki kullanıcılar tarafından kaydedildi.*<sup>57</sup>

Yine son günlerde ABD’de ortaya çıkan şarbon hastalığına konusunda da benzer bir olay yaşanmıştır. Şarbona karşı etkili olan “ciprofloxacın” adlı antibiyotiği pazarlayan onlarca web sitesi ortaya çıktı. Bu sitelerin bir kısmı online eczanelere ait olmasına rağmen çoğunluğun hayali şirketler olması da gerçekten düşündürücüdür.<sup>58</sup>

Hani derler ya “koyun can derdinde kasap mal derdinde” aynen böyle bir durum. Bu iki örnek, batı toplumunun bilişim etiği konusunda içinde bulunduğu acınılası durumu çok bariz olarak ortaya koymaktadır. Ülkemizde toplumsal değerlerini henüz tam olarak yitirmediği düşüncesiyle sanal etik veya bilişim etiği konusunda bir an önce eğitsel faaliyetlerin başlamasının çok yararlı olacağını düşünmekteyiz.

---

<sup>57</sup> [www.hurriyet.com.tr/](http://www.hurriyet.com.tr/) Erişim tarihi; 01.10.2001.

<sup>58</sup> [www.hurriyet.com.tr/](http://www.hurriyet.com.tr/) Erişim tarihi; 15.10.2001.