T.C
İstanbul Üniversitesi
Sosyal Bilimler Enstitüsü
Kamu Hukuku Ana Bilim Dalı

Yüksek Lisans Tezi

SİBER TERÖR

Hikmet Topal

2501010229

Tez Danışmanı : Prof.Dr. Kayıhan İçel

İstanbul 2004

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

TEZ ONAYI

KAMU HUKUKU Anabilim Dalında **2501010229** numaralı **HİKMET TOPAL'IN** hazırladığı "**SİBER TERÖR**" konulu **YÜKSEK LİSANS / ~~DOKTORA~~ TEZİ** ile ilgili **TEZ SAVUNMA SINAVI,** Lisansüstü Öğretim Yönetmeliği'nin 10.Maddesi uyarınca **08.11.2004 PAZARTESİ** günü saat **15.00'de** yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin ~~.....kabulüne.....~~'ne* **OYBİRLİĞİ /OYÇO~~KLUĞUYLA~~** karar verilmiştir.

JÜRİ ÜYESİ	KANAATİ (2)	İMZA
PROF.DR. KAYIHAN İÇEL	Kabul	
PROF.DR. FÜSUN SOKULLU AKINCI	Kabul	
DOÇ.DR. YENER ÜNVER	Kabul	
DOÇ.DR. AYŞE NUHOĞLU	Kabul	
YRD.DOÇ.DR. ALİ KEMAL YILDIZ	Kabul	

Besim Ömer Paşa Caddesi Beyazıt-34452-İstanbul
Tel:0212 440 00 00Fax: 0212 520 85 04

ABSTRACT

İnformation Revolution which starts with human beings steps on the moon ends by finding internet, abolishing all borders of world in the twentie century.

World becomes global by abolishing all borders on the earth. İn the global world someone claims history comes to an end. However thinking that history end by one country's final victory, is a big mistake, because global world brings new dangers and contradictions; and history is still being written by blood, gun powder and tears. One of the new dangers for a humanity is Cyber Terror.

Cyber terror comes from an untouchable, invisible imaginary universe and unfortunately cyber terror is the most dangerous threat which can eradicate all humanity on the world. Because, world is not turning on its axis, it starts to turn on the computer keys. Furthermore cyber terror is product of the İnformation Warfare which appears as a dark side of information revolution.

As result of these reasons, cyber terror is selected as the subject of this thesis.

ÖZ

Yirminci yüzyılda, insanoğlunun Ay'daki adımlarıyla başlayan ve İnternetin keşfedilmesiyle tamamlanan Bilgi Devrimi dünyadaki tüm sınırları ortadan kaldırdı. Sınırların kalkmasıyla küreselleşen dünyayla beraber tarihin de sonuna gelindiği iddia edildi. Ancak tarihin bir devletin nihai zaferiyle sona erdiğini düşünenler yanıldı.

Çünkü küreselleşen dünya yeni çelişkileri ve tehlikeleri beraberinde getirdi. Ve tarih hala kan, gözyaşı ve barutla yazılmaya devam etti. İşte bu yeni tehlikelerden bir tanesi de Siber Terör dür.

Siber terör, görülmeyen, dokunulamayan sanal evrenden gelen ve de ne yazık ki insanlığı yok edebilecek en büyük tehdittir. Çünkü dünya kendi ekseninin üzerinde değil bilgisayar tuşlarının üstünde dönmeye başlamıştır. Ayrıca siber terör de bilgi devriminin, karanlık yüzü olan bilgi savaşlarının bir ürünüdür.

Bu nedenlerdir ki bu tezin konusu olarak Siber Terör seçilmiştir.

Önsöz

Tarihin ilk sayfalarından itibaren farklı politik görüşleri savunanların, bu politik görüşlerini şiddet yoluyla toplumlara empoze etmeye çalışmasının sonucunda terör kavramı ortaya çıkmıştır.

Terör kavramının tarihsel süreçte geçirdiği en büyük evrimi, bilgi devriminin Siber Terörü yaratmasıdır.

Bu çalışmada, yirmi birinci yüzyılda İnternet sayesinde evlerimizin içine kadar girebilen, evrensel barış için en ciddi tehditlerden biri olan siber teröre ışık tutmaya, bu yakın tehlike hakkında alınması gereken tedbirler ortaya konmaya çalışılmıştır.

Bu tezde bir an olsun bile benden esirgemediği eşsiz desteği ve katkıları için hocam Sayın Prof. Dr. Kayıhan İçel'e minnet duygularımı sunarım.

Ayrıca bu çalışmada beni sabırla destekleyen başta üstadım Av. Mehmet Fatih Kayagil'e olmak üzere Aileme, Ceza Hukuku ve Kriminoloji Ana Bilim Dalındaki değerli hocalarıma ve akademisyen arkadaşlarıma teşekkür ederim.

TABLOLAR **Sayfa**

KISALTMALAR

CSİS	Centerfor Strategic and İnternational Studies
DoD	Deparment of Defence
Dos	Denial of Service
DDos	Distributed Denial Of Service
EMP	Electromagnetic Pulse
FBI	Federal Burerau of İnvestigation
HERF	High Energy Radio Frequency
İSS	İnternet Servis Sağlayıcıları
NİPC	Natıonal İnfrastructure Protection Center
TDK	Türk Dil Kurumu

İÇİNDEKİLER

GİRİŞ

Aydınlanma Devrimiyle beraber Ortaçağın karanlığından çıkan insanlık bilginin aydınlık yüzüyle geleceğine ışık tutmaya başladı.

Bilgi meşalesi, bir taraftan parlak ateşiyle insanlığın önündeki engelleri aşmasını sağlarken diğer taraftan bilgiye sahip olan insanların bu meşaleyi iktidar arzusuyla tutuşturması sonucunda Ay'ın karanlık yüzü barut, kan ve göz yaşları olarak ortaya çıktı.

Coğrafi Keşifler sonucunda beyaz insanın yeni kıtaya adım atmasıyla beraber kesilen Latin Amerikanın damarlarından hala tüm şiddetiyle kanların akmaya devam etmesi ve Atom Devriminin, Hiroşima da milyonlarca insanın ölümüyle ilan edilmesi gibi.

Fakat On dokuzuncu yüzyılın ilk yarısında telgrafın, ikinci yarısında telefonun, yirminci yüzyılın başında bilgisayarın ve ikinci yarısında İnternetin keşfedilmesiyle yapılan Bilgi Devrimi, sonunda tüm sınırları kaldırarak dünyayı küreselleştirmiştir. Böylece kimilerine göre Tarihin sonuna gelinmişti.

Ancak ne yazık ki 11 Eylül' de New York'ta daha sonra Irak'ta , İstanbul'da ve Madrid'de akan kanlar tarihin hala barut ve göz yaşlarıyla yazılmaya devam ettiğini göstermektedir.

İşte bu noktada Bilgi Devrimi ve Küreselleşmenin çelişkilerinden yeni bir kavram olan Siber Terör çıkmıştır.

Ayrıca siber terör, sanal dünyanın gerçek dünyayı yönetmeye başlamasının da bir sonucudur. Artık dünya kendi ekseninin üzerinde değil bilgisayar tuşlarının üstünde dönmektedir.

Eskiden ateşli silahların gücüne sahip olanlar iktidar olurken; yakında bilgisayarlar teknolojisinin gücünü elinde tutanlar, bizi yönetmeye başlayacaklar.

Bunun ilk adımlarından biride siber terördür. Bu nedenle de bu tezin konusu olarak Siber Terör seçilmiştir.

Bu tezde siber terör ve onun eylemlerinin genel özellikleri açıklanmaya çalışılacaktır.

Siber terör, bir bilgi savaşı yöntemi olduğundan ilk önce Bilgi Savaşları kavramını irdeledikten sonra siber terör kavramının temel karakteri ortaya konulacak ve sonuçta da siber terör eylemlerinin hukuksal boyutu tartışılacaktır.

Ancak bu çalışma siber terör olgusuna bir giriş niteliği taşımaktadır. Bunun nedeni öncelikle bu kavramın dünyada çok yeni bir kavram olması ve de gerçek anlamda bir siber terör eyleminin henüz gerçekleşmemiş olmasıdır.

Bu durum, siber terörü varsayımsal olarak incelemek zorunda bırakmaktadır.

Ayrıca siber terörle ilgili tüm literatürün yabancı dillerde olması bu çalışmayı daha da zorlaştırmıştır. Bunun yanı sıra siber terörün bilgi devrimin tüm öğeleriyle yakın ilgisinin olması çalışma alanını çok genişletmektedir. Özellikle bilgisayar teknolojisiyle olan ilişkisi en az bilgisayar mühendisi kadar bu teknoloji konusunda bilgi sahibi olmayı gerektirmektedir.

Ne yazık ki Hukuk Fakültesi mezunu olan bir insanın bu teknolojiye yeterli derece vakıf olması çok zordur.

Kaldı ki bu tezin bilimsel ve akademik anlamda ilk çalışma olmasının getirdiği acemilikler de eklenince bu kadar kapsamlı bir konuya sadece bir giriş yapabileceğini söylemek gerçekçi olacaktır.

Bu gerçek de bizleri Bilgi Savaşlarının tam ortasına düşürmektedir.

I.BİLGİ ŞAVAŞLARI

A)Bilgi Savaşı Nedir

Günümüzde sıklıkla kullanılan "Bilgi Savaşı" deyimi çoğunlukla yanlış anlaşılmakta ve daha çok üstün teknoloji silahları ile yapılan savaşları çağrıştırmaktadır.

Bunun nedeni bilgi savaşı kavramının savaş meydanlarında, taktiksel ve stratejik yanıltma, savaş propagandası, kumanda ve kontrol sistemlerinin bozulması gibi yöntemlerin kullanılması olarak kavranılmasıydı.

Ancak bugün teknolojinin gelişmesiyle beraber; artık bilgi savaşı terimi geleneksel savaş meydanının arkasında, askeri bağlantıları olmayan yer ve kişileri kapsamaktadır.[1]

Kısaca, bilgi savaşı deyimi, askeri bir boyutunun olmasıyla beraber daha çok bilgi sistemlerini çökertmeye yönelik İnternet savaşlarını tanımlayan bir deyimdir.

Bu nedenle doktrinde bilgi savaşları ifadesinin yanı sıra siber veya net savaşları deyimleri de kullanılmaktadır.[2]

Bilgi savaşını şu şekilde tarif edebiliriz:

"Bilgi savaşı, rakip bilgi sistemlerini istismar etmek, bozmak veya imha etmek için, diğer bilgi sistemlerinin, savunma veya saldırı amaçlı kullanılmasıdır."[3]

---

[1] Wınn Schwartau, **"An İntroduction To İnformation Warfare"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s29

[2] **Matthew J. Littleton, İnformatıon Age Teroroism, (Çevrimiçi)** http://www.fas.org/irp/threat/cyber/docs/npgs/app_a.htm#frmconve **04 Nisan 2004**

[3] Michele Zanini,SeanJ.A. Edwards, **"Networking of Teror İn The İnformation Age",** Networks And Netwars, ed: John Arquilla, David Ronfeldt,Santa Monica,,Rand,2001

Bu nokta da karşımıza şu soru gelmektedir:

Bilgi sistemleri nedir? Bilgi sistemleri, bilgiyi yaymak, göstermek, iletmek, yedeklemek için gerekli makine, personel ve ekipmanı kullanarak oluşturulmuş altyapılar, organizasyonlar ve işlemcilerdir.[4]

Özetle, bilgi savaşı; karşı tarafa ait, bilgi tabanlı işlemcileri, bilgi sistemlerini, bilgisayar tabanlı network sistemlerini etkileyecek bir hareket gerçekleştirmek ve kendi sistemlerini korumak anlamına gelmektedir.Ancak, bilgi sistemlerine yönelik hangi eylemlerin bilgi savaşı içerisinde değerlendirileceği başka bir sorundur.

Bunun için CSİS, çok kapsamlı bir çalışmayla, ne tür eylemlerin bilgi savaşı yöntemi olarak adlandırılması gerektiğini araştırmış ve bu çalışma, bilgi savaşı eylemlerini, kaynaklarına, biçimlerine, taktiksel amaçlarına göre sınıflandırmıştır. Böylece bilgi savaşı eyleminin üç boyutu ortaya çıkmıştır.[5] Bunlar :

1) Bir bilgi sistemine içerden veya dışardan bir saldırının yapılması

2) Saldırının taktiksel amaç ve hedeflerine göre bilgi sistemlerinin istismar veya imha edilmesi ve bozulması.[6]

3) Dört çeşit saldırının yapılabilecek olması

a) Data Saldırıları : Sistemin içine datalar sokarak, sistemin bozulması,

b) Software Saldıraları : Sisteme girerek, programların çökertilmesi

c) Hacking ve Cracking Saldırları: Bilgi sistemlerine girerek, onlara zarar vermek,

d)Fiziksel Saldırılar: Bunlar, bombalama, imha etme gibi klasik saldırı eylemlerinin bilgi sistemlerine karşı yapılmasıdır.

---

[4] Wınn Schwartau, s.36
[5] Anthony H. Cordesman, Justin G. Cordesman, **Cyber Threat,İnformation Warfare and Criticial İnfrastructure Protection**,Londan,Praeger,s.55
[6] İbid., s.56

Bu açıklamalardan sonra bilgi savaşı şu şekilde tanımlanabilir.

Bilgi savaşı, *network bilgi sistemlerinde bulunan veya İnternet vasıtasıyla iletmiş bilgisayar içerisindeki verilerin (dataların); bireyler ve ya örgütler tarafından belirli politik ve stratejik hedefleri doğrultusunda istismar edilmesi, yanıltılması imha edilmesini sağlayan savunma ya da saldırı amaçlı operasyonlardır.*[7]

B)Yeni Bir Tehdit: Bilgi Savaşı

Bilgi savaşı yöntemleri genel olarak bu ve bunları kullanacak olanların teknolojik kapasitelerine ve saiklerine bağlıdır.[8]

Ne yazık ki, siber dünyada bilgi sistemlerine yönelik ucuz, kullanılması ve erişilmesi kolay, geniş ve çeşitli saldırı yöntemleri bulunmaktadır. Bundan dolayı da çok basit düzeyde bilgisayar kullanabilen herkes eğer bir hacker ve siber terörist olma saiki, niyeti varsa İnternet üzerinde bu programlara ulaşabilmektedir.[9]

Özelliklede İnternetin sağladığı teknolojik avantaj hackerlerin tespit edilip, yakalanmasını zorlaştırmıştır.

Ayrıca artık günümüzde eğitim, ticaret sağlık ve askeri vb. insanoğlunun hayatta kalmasını sağlayan temel altyapılar bilgisayar tabanlı bilgi sistemleriyle kontrol edilmektedir.[10]

Bu durum, insanoğlunu çok yakın zamanda büyük bir tehditle karşı karşıya bırakmaktadır. Bu tehdit de bilgi savaşıdır. Bu tehdidi insanlığa karşı kullananlar kimlerdir?

---

[7] Rıchard Szafranki, "An İnformation Warfare", İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s120

[8] Wınn Schwartau, **"The Econo-Politics of İnformation Warfare"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.49

[9] İbid., s.50

[10] Anthony H &. Justin G Cordesman,. s.60

Bunlar dört başlık altında toplanabilir :

Hackerlar :

Bu kişiler, bireysel ekonomik çıkarlar elde etmek veya politik siyasi görüşlerini yaymak için bu yöntemleri kullanırlar.[11]

Sivil toplum örgütleri ve muhalif gruplar :

Bunlar görüşlerini yaymak, destekçileriyle temasa geçmek, karşı oldukları politik görüşleri temsil ettiklerini düşündükleri kurum ve kuruluşlara saldırmak amacıyla bilgi savaşı yöntemlerini kullanırlar.[12] Bunlara örnek olarak Burma da demokrasi mücadelesi yapan sivil toplum örgütleri verilebilir.[13]

Terörist örgütler:

Terörist amaçlarını gerçekleştirmek ve propagandalarını yapmak için bu yöntemleri kullanırlar.[14]

Devletler ve uluslararası kuruluşlar:

Bunlar siyasi ve ekonomik rakiplerine karşı bilgi savaşı yöntemlerini kullanırlar.

Yukarıda belirttiğim gruplara ve kişilere veya onların hedeflerine göre bilgi savaşı türleri oluşur. Bunlar bireysel, şirketler arası ve uluslararası bilgi savaşları diye üç gruba ayrılmaktadır.

---

[11] Pekka Himanen, **The Hacker Ethic**,RandonHouse Trade Paperback,Newyork, 2001,s.3

[12] John P. Sullivan, **"Gangs, Hooligans,And Anarchists- The VanGuard Of Netwarsİn The Streets"**, Networks And Netwars, ed:John Arquilla, David RonFeldt,Santa Monica, Rand, 2001, s.105

[13] Tiffany Danitz, WarrenP.Strobel, **"Networking Dissent:Cyber Activists The İnternet To Promote Democracy İn Burma"** Networks And Netwars, ed:John Arquilla, David RonFeldt,Santa Monica, Rand, 2001s.129

[14] DavidRonFelt,JohnArquilla, **"Emergence and Influence Zapatista"** Networks And Netwars, ed:John Arquilla, David RonFeldt,Santa Monica, Rand, 2001,s171

C)Bilgi Savaşları Türleri

1)Bireysel Bilgi Savaşları

Bu grupta yer alan saldırılar 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.[15]

Ortalama bir bilgisayar kullanıcısının sakladığı bilgi üzerindeki kontrolü ne yazık ki çok fazla değildir. [16]

Biz kendimize ait bilgilerin tamamını kontrol edememekteyiz. ABD'de yapılan bir araştırmaya göre, bilgisayar kullanıcılarının %78'i böyle bir saldırı sonucu bilgi kaybına uğramıştır.[17]

Geçmişte, bir kişi hakkında bilgi almak için çalışan bir ajan, minyatür kamera ya da mikrofon kullanmak zorundaydı.[18]

Günümüz ajanları ise, o cihazların daha da geliştirilmiş 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 şeyi öğrenmek mümkündür. [19]

Hakkımızdaki bilgilerin, çevreye yayılmasından endişe duyuyor muyuz? Tabii ki hiçbirimiz kredi kartı borçlarımızın, banka hesap numaralarımızın, finansal

---

[15] **Class 1: Personal İnformation Warfare,** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.473

[16] Liz Weise **"No privacy"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.487

[17] İbid.

[18] Beth Givens, **"İnformation Warfare: The Personal Front"**, İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.494

[19] İbid.

yatırımlarımızın, tıbbi kayıtlarımızın, sabıka kaydımızın, mahkeme kayıtlarımızın ya da herhangi bir kişisel bilgimizin gazetede, İnternette yayınlanmasını istemeyiz.[20]

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.[21]

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.

Özelliklede bu günlerde e- devlete geçmeye çalışan ve kişisel kayıtların güvenirliği tartışmalı olan Türkiye gibi ülkelerde " Yaşar Ne Yaşar Ne Yaşamaz" durumu her an başımızı gelebilir. Bu örnekler çoğaltılabilir. Özetle;

- 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 insanın hayatını mahvedebilir.

---

[20] MarkAldrich, **"Personal İnformation Warfare"**, İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.490

[21] Liz Weise, s.488

2)Şirketler Arası Bilgi Savaşları

Bu grup savaşlar, uluslararası şirketlerin veya devletlerin ekonomik ve siyasi rekabetinden doğmaktadır.[22]

Bu nedenle bu savaşların ana unsuru rekabettir.

Aynı kurum içerisindeki rakip birimlerin birbirlerine yaptıkları saldırılar da bu gruba girmektedir.

Bir milyon dolarlık yatırım yapacak olan bir şirketin, rakibinin sistemini kırarak, on beş milyon dolar değerindeki projesini ele geçirmesi veya rakibini ortadan kaldırması mümkündür. [23]

Ayrıca, rakibinin projesini ele geçirmekle kalmayıp, kaza ya da virüs süsü vererek, rakip şirketin konuyla ilgili tüm verilerini de yok edebilir. [24]

Bu tarz savaşlar aslında yeni değildir Geçmişi Amerika-Rusya arasındaki soğuk savaş dönemine kadar uzanmaktadır. O dönemki ajanların bilgi toplama çalışmalarına benzemektedir.[25]

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.[26]

---

[22] **Class 2: Corparete İnformation Warfare,** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,NewYork,Thunder's Mouth, 1996, s.513

[23] Ira Wınkler , **"Dairy of Industrial Spy"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,NewYork,Thunder's Mouth, 1996,s.538

[24] İbid.

[25] Class 2, s.514

3)Uluslararası Bilgi Savaşları

Bu grupta yer alan saldırı türleri, endüstri, global ekonomi güçlerini, tüm ülke ve devletleri hedef almaktadır.[27]

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.

Bu grubun içerisinde bu çalışmanın konusunu oluşturan siber terörde yer almaktadır.[28]

Artık konu para kaybı ya da kişisel bilgi kaybından öte tüm dünyayı etkileyecek zararları içermektedir.

Çünkü 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 çökertip, Wall Street'i yok edebilir. Ya da aşırı milliyetçi bir grup belli bir etnik kökenli insanların yerleştiği bir bölgedeki doğal gaz sistemine girip onu aşırı yükleme sonucunda havaya uçurabilir.

Bilgi savaşları türleri bu şekilde incelendikten sonra bu türlerin oluşumu ve tarihsel sürecin gelişimi irdelenecektir.

Bilgi savaşlarının tarihsel süreci; aslında insanoğlunun teknolojik evrimiyle paralel gitmektedir. Çünkü teknoloji geliştikçe insanoğlunun bilgiyi kullanabilme kapasitesi de artmıştır.

Bu artışla beraber; ne yazık ki bu bilimsel bilgi birikimini, devletler insanlığın iyiliği için değil, kendi politik çıkarları doğrultusunda kullanmışlardır.

---

[26] Stewart A. Baker, **"Should Spies Be Cops"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,NewYork,Thunder's Mouth, 1996,s.410

[27] **Class 3 : Global İnformation** Warfare İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996, s.540

[28] Matthew J. Littleton, s.6

Buna örnek olarak atom devriminin, Atom Bombasını yaratmasını, Hitler'in biyolojik araştırmalarının bugünkü biyolojik terörün temellerini oluşturmasını ve de bilgi teknolojisinin siber terörü yaratması verilebilir.

Bilgi savaşlarının tarihsel gelişimi üç ana başlıkta toplanabilir.

Bunlar, tarım, sanayi ve bilgi devrimidir.[29]

D)BİLGİ SAVAŞLARI TARİHİ

1)Tarım Devrimi

Tarım devrimi, dünya tarihini değiştiren ilk devrim olarak adlandırılabilir. Çünkü günümüz kapitalist toplumunun temelini oluşturan üretim ilişkileri o dönemde ortaya çıkmıştır.

Tarım, insanların üretime yönelmesine, ekonominin oluşmasına ve ilk ekonomik savaşların yapılmasına yol açmıştır. İnsanlığın ilk dönemlerinden beri süregelen toprak ve savaş ilişkisi bunun bir sonucudur.

İnsanlar, yönetici sınıf tarafından özellikle bilgisiz bırakılarak yüzyıllar boyu sadece, tarım ve toprakla ilgilenmelerini sağlamıştır.

Askerler yılın büyük bir kısmını çiftçilik yaparak geçirirlerdi. Gönüllü birlikler genellikle kışın çalışmayan çiftçilerden kurulurdu. Bu askerlere ödeme paradan çok, mal olarak yapılırdı. Pek çok ülkede ödeme küçük bir toprak şeklindeydi.

2) Sanayi Devrimi

Sanayi Devrimi savaş şekillerini tamamen değiştirdi. Seri üretim, seri ölüm silahlarını (nükleer ve kimyasal) yarattı. Sanayi askerlere, binlerce süngü, silah, el bombası ve her türlü ekipman üretmeye başladı.

İkinci Dünya Savaşı sırasında, hızla tırmanan endüstriyel savaş, milyonlarca insanın ölümüyle noktalandı. Naziler, Yahudi'leri ölüm fabrikalarına gönderdi.

Amerika, bugün bile olumsuz etkileri devam eden dünyanın ilk nükleer bombasını patlatarak Hiroşima'yı yok etti.

İkinci Dünya Savaşı sonrası, "Kitle Ölüm Teorileri Dönemi" olarak adlandırılmaktadır. Bu dönemde, savaşı kazanmak için her şeyi yok etme teorileri geliştirilmekteydi.

3) Bilgi Devrimi

1970'lerin sonu ve 1980'lerin başından itibaren, bilgi devrimi yaşanmaya başlandı. Bu devrimle kitle toplumları yavaş yavaş iletişim toplumlarına dönüştüler Bu evrimle beraber askeri doktrinler de değişmeye başladı.

Bir taraftan İkinci Dünya Savaşında olduğu gibi, hava bombardımanları devam ederken, dünyanın bilgi güçleri, hedefi tamamen yok edecek ileri teknolojiyle üretilen savaş makineleri üzerine çalışmaya başladılar.

Bu silahlar kullanılmadığı halde, düşmanın moralini bozmaya yeterli oluyordu. Vietnam'da ya da Körfez Savaşı'nda, bilgi devriminin sonucunda üretilmiş, ileri teknoloji silahları, Amerika tarafından moral bozma aracı olarak kullanıldı.

Bilgi devrimi yaygınlaştıkça, edinilen bilgiler, geleneksel silahları daha akıllı hale getirmenin ötesinde onları tamamen ortadan kaldıracak ve dünya askersiz savaşlara doğru gidecektir.

Kaldı ki bilgi devrimiyle beraber bilgi savaşlarının coğrafyası da genişlemiştir Artık bilgi savaşları sadece savaş alanlarında değil siber dünyada yani telefon kablolarının uzandığı her yerde cereyan etmektedir.

Tarihsel gelişim bu şekilde ortaya konulduktan sonra hangi alanlarda ne tür bilgi savaşı yöntemleri kullanıldığı bulunabilir. Bilgi savaşlarının yapıldığı ilk alan askeri teknolojidir. Bu nedenle öncelikle bilgi savaşlarının askeri boyutu değerlendirilmelidir.

---

[29] Wınn Schwartau, **"The Econo-Politics Of İnformation Warfare"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.46

E) BİLGİ SAVAŞLARININ ASKERİ BOYUTU

1)Yeni Silah Sistemleri

Bilgi Savaşı bugün sürekli gündemde olan bir konu. Hemen her gün gazetelerde yeni geliştirilen minyatür silahlar hakkında yazılar okumaktayız.

2010 yılına kadar gelişmiş ülkeler, savaş meydanlarını dijital ortama taşımayı ve askerlerini kablosuz silah sistemlerine bağlamayı planlamaktadırlar.[30]

Yirmi birinci yüzyıl askerleri, "Siber savaşçı" olarak adlandırılan yeni savaş teçhizatlarıyla donatılacak. "Siber savaşçı"lar, üst kısmında gece algılayıcılı, bir video paneli (aktif ses özelliği de olan) monte edilmiş hafif ağırlıkta bir miğfer, içinde bilgisayar yeri de bulunan bir zırh giyecekler.[31]

Zırhlarının içinde bulunan bilgisayar sayesinde, mayın ve kimyasal madde taraması yapabilecek, karşılarına çıkacak insanların dost ya da düşman olduğunu anlayabilecekler. Kısacası, bilgisayar teknolojisiyle, kendi beş duyularına gerek kalmadan etraflarını algılayabilecek, hatta gözleriyle göremeyecekleri tehlikelerden de korunacaklar. Miğferlerinin içindeki monitör sayesinde, vücutlarını düşmana doğrultmadan hedefi belirleyip, onu yok edebilecekler.[32]

Bütün bunlar "Yıldız Savaşları" filmini hatırlatmakla birlikte, hiçbirinin hayali olmadığı şu anda bu teknolojiye sahip olunduğu ve kısa gelecekteki savaşlarda benzeri ekipmanların kullanılacağı bir gerçektir.[33]

Bu sayede, bilgi ve teknolojiye en çok sahip olan ülkeler savaşlardan daha az zararla ayrılacakları kesindir.

---

[30] Wınn Schwartau, **Cyber Shock**, NewYork,Thunder's Mouth,2000,s.286
[31] John M.DEutch, **"Nonlethal Weapons"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.460
[32] İbid.
[33] John M. Deutch, **"Worldwide Threat Assesment"** İnformatin Warfare, ed Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996, s,437

Ancak bunların hiçbiri bilgi savaşının bir parçası olarak adlandırılamaz. Çünkü bilgi savaşı, tank kullanmayı değil, daha akıllı tanklar yapmayı hedef alan bir savaştır.

Tamamen bilgi üretimine ve bu bilgilerin güç savaşlarında hayata geçirilmesi üzerine kurgulanır, bilgi savaşları.

Bilgi Savaşları günümüz silah teknolojilerinin büyük bir kısmını kapsamakla birlikte, teknoloji hiçbir askerin fiziksel olarak katılmayacağı savaşlara doğru hızla ilerlemektedir.

2) C3I

Bilgi ordusunun en tepesinde C3I bulunmaktadır.

C3I; Kumanda, Kontrol, İletişim ve Zeka anlamına gelmektedir (Command, Control, Communications, Intelligence). C3I, bilgi savaşı kararlarını alır ve para akışını kontrol eder. C3I her konunun uzmanlarından oluşan küçük gruplardır.[34]

3) Düşük Yoğunluklu Savaşlar

Düşük yoğunluklu savaşlar, global bilgi savaşları içinde bir alt başlıktır. Amacı, düşmana karşı bilgi üstünlüğü sağlamaktan öte düşmanı yanlış ya da uydurma bilgilerle kendi isteği doğrultusunda yönetmektir.[35]

Örneğin, televizyon bir başka ulusu yanıltmakta en rahat kullanılan araçtır.

Düşman ülkenin lideri ya da siyasetçileri hakkında programlar yaparak, o kişileri hem kendi ülkelerinde hem de dışarıda yıpratmalı mümkündür.

Düşük yoğunluklu savaş teknikleri ayrıca, bir ülkenin kendi içinde de kullanılmaktadır. Bunun en açık örneği, kontrol altında tutulan bir medyadır. Körfez Savaşı sırasında CNN, bu amaçla kullanılmış ve geniş çaplı yönlendirmeler yapmıştır.[36]

---

[34] Matthew J. Littleton,
[35] Winn Schwartau, The Econo-Politics Of İnf. War.,s71
[36] İbid.

Bilgi teknolojisinin savaş alanlarına getirdiği bu yenliliklerin yanında bilgi savaşlarının sınırlarını da savaş meydanlarının ötesine evlerimizin içine kadar genişletmiştir.

İşte bu durum bilgi savaşının bu yeni boyutunu başka bir ifadeyle siber savaşları ortaya çıkarmıştır.

Siber savaşlarda, bütün savaşlar gibi silahlarla yapılmaktadır.

Ancak bu bilgi savaşlarının silahları da kendisi gibi yeni bir olgudur.

Nedenle şimdi bu yeni silahları incelenecektir. Bu silahlar dokuz başlık altında toparlanabilir. Bunlar bilgisayar virüsleri, kurtlar, truva atları mantık bombası, tuzak kapıları, mikroçipler, nano makineleri ve mikroplar, elektronik sıkışıklık, HERF Silahları ve EMP Bombalardır[37].

F) VAROLAN ve OLASI BİLGİ SAVAŞI SİLAHLARI

1)Virüs

Virüs, kendisini daha geniş programların içine kopya edebilen, ve bu programı değiştirilebilen parçalı bir koddur. [38]

Virüs ancak içinde bulunduğu program çalışınca, aktif hale geçer. Program çalışınca, virüs kendisini tekrar etmeye başlar ve başka programlara da yayılarak onları da kontrol altına alır.[39]

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 edildiğinden, ana vericiye virüs yollamak herhangi bir bilgisayara virüs yollamak kadar kolaydır.

---

[37] http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/TheLaw.html
[38] Rohas Nagpel. **"Cyber terrorism İnThe Context Of Glabalization"** (Çevrimiçi) http://www.asianlaws.org/cyberlaw/library/cc/rn_ct.htm#21 23 Mayıs 2004
[39] İbid.

2)Kurtlar(Worms)

Kurt (worm) bağımsız bir programdır. Kendi kendine çoğalarak, bir bilgisayardan ötekine kopyalanır, genellikle de bir network sistemine yayılır. [40]

Virüslerden farklı olarak, diğer programlara sıçramazlar. Kurtlar, veri yok etmemekle birlikte, network içinde dolaşarak, iletişimi yok edebilir. Ancak, bir kurt veri yok edicisine de dönüştürülebilir.[41]

Örneğin, bir bankanın network sistemine yerleşen bir kurt, o bankanın şubeleriyle olan tüm iletişimini kesebilir.

3)Truva Atı

Truva atı, bir program içinde gizlenen ve gizli bir işlev yapan parçalı bir koddur.[42] 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.

---

[40] http://www.bilgisayardershanesi.com/virus.htm
[41] Dorothy E. Denning **"Is Cyber Terror Next?"**, (Çevrim içi) http://www.ssrc.org/sept11/essays/denning.htm 12 Aralık 2003
[42] http://www.po.metu.edu.tr/links/inf/css25/bolum14.html#7

4) Mantık Bombası

Mantık Bombası, virüs, kurt ya da başka bir sistemi yaymak için kullanılan bir truva atı türüdür.[43] Bağımsız bir program ya da bir sistem programcısı tarafından yazılmış, bir kod da olabilir.

Dışarıdan çalıştırılması mümkün olan mantık bombası, bir bilgisayarın hard disk ya da posta dokümanlarının formatını etkileyebilir. Günümüzde büyük yoğunlukla Amerikan yazılımlarında kullanılmaktadır.[44]

Örneğin CIA, dünyanın her yerinden bilgisayar sistemlerine bağlanarak, istediği her bilgiyi alabilecektir. Mantık bombalarında olduğu gibi, tüm sistem üreticilerinin böyle bir mekanizmayı başka ülkelere ihraç ettikleri yazılımların içine yerleştirdiklerini düşünün.

Bu belki de, stratejik planlar ve uygulamalar için en kullanışlı yol olacaktır. En canlı istihbaratlar bu şekilde yapılacaktır.

5)Tuzak kapısı

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.[45]

Mantık Bombalarında olduğu gibi, tüm sistem üreticilerinin böyle bir mekanizmayı başka ülkelere ihraç ettikleri yazılımların içine yerleştirebilirler.

Böylece tüm bilgi savaşı ajanları, istedikleri her bilgiye elleriyle koymuş gibi ulaşabileceklerdir.

---

[43] http://www.webopedia.com/TERM/l/logic_bomb.html
[44] İbid.
[45] Fehime Tüfekçioğlu, **"Zarar Verici Lojik"**, (Çevrimiçi) www.ce.itu.edu.tr/lisansustu/dersler/blg510/2003/sunumlar/504031511_rapor.pdf 09 Mayıs 2004

6) Mikroçipler

Mikroçipler küçük silikon yonga plakalarının yüzeylerine "basılmış" elektronik aygıtlardır. Genel olarak mikroçipler, hepsi gerekli elemanların bir "maske" yoluyla silikona "püskürtüldüğü" özel toplu üretim işlemleri ile üretilen binlerce transistör, direnç ve diğer devre elementlerini içerir.[46]

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.[47] 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.

7) Nano Makineleri ve Mikroplar

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.[48] 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.

---

[46] http://www.daghanoves.netfirms.com/bilim/bilim2.htm
[47] İbid.
[48] Zuhal Özer **"Nanoteknoloji"**, Bilim Çocuk (Çevrimiçi)
www.biltek.tubitak.gov.tr/cocuk/01/eylul/**nano**.pdf - 12 Mayıs 2004

Donanımı yok etmenin başka bir yolu da özel üretilmiş mikroplardır. Bu mikroplar bildiğimiz kadarıyla yağ yemektedirler. Ya silisyum yiyenleri geliştirilirse?[49] Bir bilgisayar laboratuarındaki tüm entegre devreleri, bir siteyi, bir binayı hatta bir şehri yiyip yok edebilirler.

8) HERF Silahları ve EMP Bombaları

HERF (High Energy Radio Frequency) Yüksek Enerji Radyo Frekansının kısaltmasıdır.[50] HERF silahları, elektronik bir hedefi, yüksek radyo frekansıyla vurarak, onu saf dışı bırakır.[51] 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.[52]

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.[53] Bütün bu silahlar bilgi savaşı yöntemlerinin hepsinde kullanılır.

Bilgi savaşı silahlarının özelikleri ve karakteristik yapısı genel olarak açıklandıktan sonra bir Bilgi Savaşı yöntemi olan Siber Terör incelenebilir.

---

[49] İbid.
[50] "Wınn Schwartau, **"More About HERF"** İnformatin Warfare, ed:Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.270
[51] İbid
[52] Carlo Copp ," **The E-bomb"** İnformatin Warfare, ed :Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.270

II. BİR BİLGİ SAVAŞI YÖNTEMİ: SİBER TERÖR

A)Siber Terör Nedir?

Siber terörü tanımlamak için önce terör kavramını incelemek gerekmektedir.

Terör ve terörle ilgili kavramları tam olarak tanımlamak, yada genel geçer bir tanımdan bahsetmek imkansızdır. Çünkü terör kavramının tanımı; kişiden kişiye, toplumdan topluma, devletten devlete değişmektedir.[54] Bunun nedeni; ne yazık ki terör kavramının siyasal içeriğinin zaman, mekana ve kişilere göre değişmesidir. Terör TDK Türkçe Sözlüğünün genişletilmiş 7. baskısında:

" Yıldırma, korkutma tedhiş" olarak tanımlanmıştır. Türkçe'ye Fransızca'dan geçen terör kelimesinin etimolojik kökeni, Latince anlamı korkutmak, sindirmek ve ürkütmek olan ***"terrere"*** kelimesinden gelmektedir.[55]

Ayrıca terör kelimesinin Fransızca'dan Türkçe'ye geçmesi bir tesadüf olmayıp Fransız Devriminde Jakobenlerin eylemleri terör kelimesi ile tanımlanmıştır.[56]

Terör kelimesin anlamını belirginleştirmek için birkaç tane tanım vermek gerekmektedir:

Title 22 of the United States Code, Section 2656f(d)

"Terör, Sivillere karşı politik motivasyonla tasarlanmış yasa dışı şiddet eylemidir"[57]

---

[53] İbid.
[54] Faruk Örgün,**Küresel terör**,İstanbul,Okumuş Adam,2001,s.11
[55] İbid.
[56] Prof. Dr. Yılmaz Altuğ, Terörün Anatomisi,İstanbul,Altın Kitaplar,1995s,.19
[57] **"Patterns of Global Terrorism: 1998"** çervim içi
http:www.state.gov/www/global/terrorism/1998Report/review.html 30 Haziran 2004

➢ FBI terörü şu tanımlamaktadır.

"Terör, politik ve sosyal amaçları gerçekleştirmek için kişilere veya mülkiyete karşı yasadışı güç veya şiddetin kullanılması veya kullanma tehdidi ile hükümete, halka veya onun bir bölümüne korkutmak veya baskı yapmaktır."[58]

Bu tanımlar arasında önemli farklılık, yukarıdaki tanımda "mülkiyet" kavramına atıf yokken, FBI tanımında mülkiyete yapılan saldırıların ve tehditlerin terör eylemi olarak tanımlanması, terör kavramının yeni boyutunu göz önüne sermektedir. Terör kavramının bu boyutu özellikle de siber terörün açıklanmasında, faydalı olacaktır.

Yukarıda verilen iki tanımı birleştiren bir tanım da DoD (Department of Defense) yapmaktadır.

➢ DoD terörü şu şekilde tanımlamaktadır :

"Terör, dinsel, politik ve ideolojik hedeflere ulaşmak için kişilere veya mülkiyete karşı yasadışı güç veya şiddetin kullanılması veya kullanma tehdidi ile hükümete, halka veya onun bir bölümüne korku aşılamayı, gözdağı vermeyi veya baskı yapmayı tasarlamaktır."[59]

Bu tanımlardan yola çıkarak Chomsky, terörü şu şekilde tanımlamıştır.

"Terör eylemi; (A) Birleşik Devletler'in yada herhangi bir Eyaletin ceza yasalarını çiğneyen ya da Birleşik Devletlerin yada herhangi bir eyaletin yargılama alanı içinde işlendiğinde ceza gerektirecek ihlal oluşturan bir şiddet eylemi yada insan yaşamı için tehlike oluşturan bir eylem içeren bir etkinlik;

---

[58] **"Terörrism in USA 1999"** 21st Century Guide to FBI

[59] **"White paper: Cyberterror Prospects and Implications"** (Çevrim içi) http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf 05 Şubat 2003

(B) (i) sivil nüfusa bir gözdağı verme yada baskı yapma (ii) gözdağı ya da baskı yoluyla bir hükümetin siyasetini etkileme;(iii)suikast yada adam kaçırma yoluyla bir hükümetin davranışına etki amacını güttüğü ortaya çıkan bir etkinlik demektir. "[60]

➢ 12.04.1991 tarih ve 3713 sayılı Terörle Mücadele Kanunu ise terörü *şöyle tanımlamaktadır"Terör, baskı, cebir, şiddet, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, devletin ülkesi ve milleti ile bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyeti'nin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü eylemlerdir."*

Terör kavramanın tanımında değişik ifade biçimleri kullanılmış olsa da, terör genel olarak şu şekilde tanımlanabilir.

"Terör, dinsel, politik ve ideolojik hedeflere ulaşmak için kişilere veya mülkiyete karşı yasadışı güç veya şiddetin kullanılması veya kullanma tehdidi ile hükümete, halka veya onun bir parçasına korku aşılamayı, gözdağı vermeyi veya baskı yapmayı tasarlamaktır".[61]

Siber terör, bu terör tanımının üzerine yeni bir unsur ekler. Siber terör, teröristlerin bilgisayar teknolojisini kullanmasıdır.[62]

Terörün bir alt kümesi olarak siber terör, terörist amaçları gerçekleştirmek için bilgisayarların, bir silah, bir yöntem veya hedef olarak kullanılmasıdır.[63] Siber

---

[60] NoamChomsky, **"Uluslararası Terörizm : Görünüş ve Gerçek"** Chomsky, Noam, vd ed Terörizm Efsanesi, çev:Bahadır Sına Şener Ankara,Ayraç,1999,s.10

[61] http://www.-cs.etsu.edu/gotterbarn/stdtppr.htm (Çevrim İçi) 20 Ocak.2002

[62] Barry C. Collin, **" CyberTerrorism From Virtual Darkness: New Weapons in a Timeless Battle"**, (Çevrim içi)
hhtp://www.nici.org/Research/Pubs/98-5.htm 13 Kasım 2001

[63] Noam Chomsky vd ed., **Terörizm Efsanesi,** çev:Bahadır Sına Şener, Ankara,Ayraç,1999

terör, siber dünyada gerçekleşen ve bilgisayarlara, bilgisayar ve bilgi sistemlerine fiziksel zarar vermesini hedefleyen eylemlerdir.[64]

Bu açıklamalardan sonra Siber terörizm şu şekilde tanımlanabilir:

"Siber terör, teröristlerin dinsel, politik ve sosyal hedeflerine ulaşmak amacıyla toplumları veya devletleri yıldırmak ve baskı altına almak için dijital mülkiyete yasa dışı zarar verilmesidir."[65]

İngiltere Terörizm Yasası 2000'de siber terörizm "Hükümeti etkilemek ya da toplumu korkutmak amacıyla elektronik sistemlerin içine izinsiz girmek veya bu sistemleri bozmak" olarak tanımlanmaktadır.[66]

Ayrıca doktrinde siber terörizmle ilgili şu tanımlar da bulunmaktadır:

- Mark M .Pollitt göre "Siber Terör bilgisayar ve bilgi sistemlerine, bilgisayar programları ve verilerine önceden tasarlanmış politik saldırılardır".[67]

- Barry Collins de "siber dünyayla terörizm birleşmesi sonucunda siber terör ortaya çıktığını ileri sürmektedir".[68]

- Dorothy E. Denning ise siber terörizmi "Bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinlikler" olarak tanımlamaktadır.[69]

---

[64] White paper, s.9
[65] İbid.
[66] Mehmet Özcan, **"Yeni Milenyım Yeni Tehdit: Siber Terör"** Polis Dergisi ,Sayı:34 s.171
[67] Mark M. Pollitt, **" CYBERTERRORISM - Fact or Fancy?"**, (Çevrim içi) http://www.cs.georgetown.edu/%7Edenning/infosec/pollitt.html 08 Haziran 2004
[68] Barry C. Collin, **"The Future of CyberTerrorism:Where the Physical and Virtual Worlds Converge"**(Çevrimiçi) http://afgen.com/terrorism1.html 15 Mayıs 2004
[69] Dorothy E. Denning, **"CYBERTERRORISM"** (Çevrim içi) http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html 03 Nisan 2004

Yukarıda açıklanan siber terörizmin iki türü vardır.[70] Bunlar:

Siber terör destek ve siber terör saldırı eylemleridir.

Siber terör saldırısı, terör örgütlerinin hedeflerine ulaşmak adına direk topluma zarar vermek için bilgi teknolojisini kullanılması iken, siber terör destek ise hedeflenen terör eyleminin gerçekleşebilmesi bilgi sistemlerinden faydalanılmasıdır.

Bu yüzden terör eyleminin yapılmasına yardımcı olan, onu destekleyen siber terör eylemleriyle; klasik terör eylemlerinin yerini alabilecek siber terör saldırı arasındaki ayrımı belirginleştirmek gereklidir.

B) Siber Terör Destek: Klasik Terör Eylemlerini Destekleyen Siber Terör Faaliyetleri

Bombalama, soygun ve adam kaçırma gibi klasik terör eylemlerine destek sağlamak amacıyla yapılan siber terör faaliyetleri siber terör destek olarak adlandırılır.

Buna göre siber terör destek:

Terör örgütlerinin, diğer terör eylemlerini gerçekleştirmek, geliştirmek veya etkisini artırmak için bilgi sistemlerinin, direkt bir tehdit unsuru ve zarar amacı olmadan yasa dışı kullanımıdır.[71]

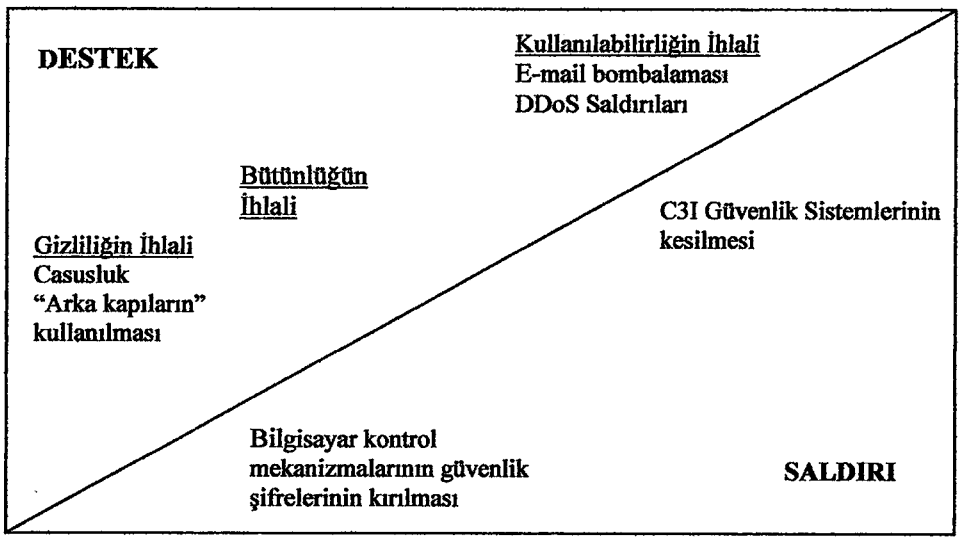
Ancak terör örgütlerinin haberleşmek ve istihbarat toplamak için İnternet gibi, bilgi sistemlerini yasal sınırlar içerisinde kullanması siber terör destek değildir.[72]

Siber terör destek eylemelerinin üç biçimi vardır Bunlar, Gizliliğin Bütünlüğün ve Kullanabilirliğin ihlalidir. [73]

---

[70] White paper s.9
[71] İbid.,s.10
[72] İbid.
[73] İbid.

Tablo 1: Siber Terör Destek Ve Saldırı Eylemleri Şeması



1) Gizliliğin İhlali:

Gizlilik ihlalli yetkisiz kişinin, bilgiyi izinsiz elde etmesidir.[74] Bunun klasik örneği başka bir şahsa ait şifreyi kullanarak bilgi edinilmesidir. Bu eylem biçimi; terör örgütünün eylemlerinde kullanacakları gizli bilgilere ulaşabilmek için bu bilgileri kullanabilme yetkisi olan şahısların şifrelerinin elde edilmesi ve bunların kullanılmasından ibarettir.

2) Bütünlüğün İhlali:

Bütünlüğün ihlali, bilgi sisteminin onun programlarının, verilerinin veya talimatlarının modifikasyonudur.[75] Bu modifikasyon, sistemdeki verinin tamamen yok edilmesini veya değiştirilmesini kapsar.[76]

Ancak bütünlüğün ihlali hem bir siber terör destek eylemi hem de bir siber terör saldırısı olabilir. Bir kullanıcının hesabının gizlice değiştirilmesi sonucunda bilgi sistemine girilmesi bir siber terör destek eylemi olurken; diğer taraftan hava

[74] İbid., s. 11
[75] İbid
[76] İbid.

kontrol sistemlerine girerek uçakların rotasının değiştirilmesi sonucunda havada uçakların çarpışmasını sağlamak bir siber terör saldırısıdır.[77]

3) Kullanabilirliğin İhlali

Kullanabilirlik, web sitelerine ve bilgi sistemlerine yasal girişlerin yapılabilmesi demektir.[78] Kullanabilirliğin ihlali ise bilgi sistemlerine yasal girişlerin engellenmesidir.[79] Genellikle bu eylemler Dos saldırısı biçiminde yapılır. Kullanabilirliğin ihlali, bütünlüğün ihlali, gibi aynı zamanda bir siber terör destek eylemi veya bir siber terör saldırısı olabilir.

Buna örnek olarak; bir devlet binasının güvenlik sisteminin kullanılmasını engelleyerek, binaya giriş yapılmasını engellemek bir siber terör destek eylemidir; fakat metro kontrol sistemlerinin kullanılmasını engellemeye çalışmak bir siber terör saldırısıdır.

Sonuçta her siber terör eylemi, gizliliğin, bütünlüğün ve kullanabilirliğin ihlali olsa da bu üç suçun işlenmesi her zaman bir siber terör eylemi olmaz.

Bu noktada karşımıza yeni bir sorun çıkmaktadır. Bu sorunda siber suçla siber terör arasındaki ayrımın ortaya konmasıdır.

C) Siber Suçla Siber Terörün Ayrımı

Bir eylemin siber terör olarak adlandırılması için o eylemin öncelikle bir terör eylemi olması şarttır. Yukarıda değinildiği üzere terör, toplumları veya devletleri korkutmak, yıldırmak ve zarar vermek tehdidi ile teröristlerin politik hedeflerini gerçekleştirmek için yaptıkları eylemlere denir.

Özetle terörizm, politik amaçları gerçekleştirmek için yapılan yasa dışı hareketlerdir. Bu nedenle bilgi teknolojisini kullanarak siber dünyada gerçekleşen; ancak siyasi ve politik bir kastla işlenmeyen tüm suçlar siber suç olarak ifade edilmektedir.

---

[77] R.J. Pınerıo,Cyber Teror,NewYork, Forge, 2003, s17
[78] Wihte paper, s.11
[79] İbid

TCK'da Bilişim Suçları altında düzenlenen siber suç tipleri bilgi teknolojisinin yasa dışı kullanımıyla ortaya çıkan yeni suçlar ve klasik suçlarda bilgi teknolojileri kullanılması sonucunda ortaya çıkan suçlar olarak ikiye ayrılır.[80]

Buna göre

1)Bilgi Teknolojisinin Yasa Dışı Kullanımıyla Ortaya Çıkan Yeni Suçlar

a)Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme

Günümüzde daha modern bir yapıya ulaşan iletişim kavramı artık bilgisayarlar üzerinden yapılmakta ve hatta kişilere ait önemli bilgiler bu ortamda iletilebilmektedir.[81]

Kişilerin, bankaların, hastanelerin, hatta güvenlik ve istihbarat birimlerinin tutmuş olduğu bilgiler bilgisayarlarda saklanmaktadır.

Bu bilgilere ulaşmakta yine bilgisayar teknolojileri kullanılarak yapılmaktadır. İşte bu noktada gizlilik gerektiren bilgilere yetkilisi haricinde yapılan erişimler bu suç tipine girmektedir.

Erişim haricinde haberleşme amacıyla kurulu iki bilgisayar sisteminin iletişiminin dinlenmesi de aynı şekilde değerlendirilmektedir.[82]

İletişimin dinlenmesi; sadece bilgisayar başındaki iki kişinin birbiri ile görüşmesi olarak düşünülmemelidir. Birbirine bilgi gönderen ve uyum içinde çalışan bilgisayarların network içinde göndermiş oldukları bilgilerin dinlenmesi de dinleme olarak değerlendirilmelidir.

---

[80]Ayhan ÇANKAYA, **"BİLİŞİM SUÇLARI"** (Çevrim içi) www.egm.gov.tr/sempozyum2003/ Bildiriler/Bilisim_Suclari.pdf 05.Nisan 2004,s.2

[81] Yrd.Doc. İsmail Güneş **"İnternette Güvenlik ve Denetim: Masumiyet Yitiriliyor mu?"** (Çevrimiçi), http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=243, 08 Haziran 2004.s,3

[82] www.emniyet.gov.tr/docs/RAPOR1.pdf (Çevrim içi) 09 Temmuz 2004

b) Bilgisayar Sabotajı:

Bilgisayar Sabotajı yetkisiz erişimin ikinci aşaması olarak değerlendirilebilir.[83]

Çünkü; Yetkisiz erişimde bulunan kişi sadece pasif bir davranışta bulunarak özel hayatın gizliliğini bozmuş olur.[84]

Ancak Bilgisayar Sabotajı, erişimden sonra elde ettiği bilgilerin silinmesini ve değiştirilmesini içerir. Bu suç tipi iki şekilde karşımıza çıkmaktadır. Birincisi; yine bilgisayar teknolojileri kullanılarak erişilen bilgilerin silinmesi, yok edilmesi ve değiştirilmesidir.

İkincisi ise bilgisayar teknolojileri kullanılmadan direk olarak bilgilerin tutulduğu bilgisayarı ve/veya bilgisayarları fiziksel olarak zarara uğratmaktır. Burada önemli olan, eylemi mala karşı değil de, bilgisayarın içindeki bilgilere karşı yapılmış bir hareket olarak algılamak lazımdır. Çünkü bu bilgiler bilgisayarın kendisinden daha değerli olabilir.

2)Klasik Suçlarda Bilgi Teknolojilerinin Kullanılması Sonucunda Ortaya Çıkan Suçlar

a)Bilgisayar Yoluyla Dolandırıcılık

Klasik olarak bildiğimiz ve karşılaştığımız dolandırıcılık suçunun bilgisayar ve iletişim ortamları üzerinden yapılıyor olmasıdır. Bilgisayar Yoluyla Dolandırıcılık en çok kredi kartlarının kullanımıyla yapılmaktadır. [85]

b)Bilgisayar Yoluyla Sahtecilik

Yine klasik olarak bilinen sahtecilik suçunun, yüksek teknoloji ürünü cihazlar kullanılarak yapılmasıdır.[86] Bilgisayar Suçlarının tanımı içerisinde bu suçlara

---

[83] İsmail Güneş,s3
[84] İbid.
[85] Rapor 1
[86] İbid

bakıldığında diğer sahtecilik suçlarından ayırt edebilmek için Bilgisayar Yoluyla Sahteciliği ayrı olarak ele almak gerekmektedir.

Çünkü; bilgisayar kullanımı ile üretilmiş sahte para suçunda, olay yerinde delil niteliği teşkil edecek bilgilerin bulunması çok zordur ve bu delillerin toplanması ve soruşturulması teknik bir olay olarak karşımıza çıkmaktadır.

c)Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

Fikir ve Sanat Eserleri Kanununda eser olarak kabul edilen bilgisayar yazılımlarının lisans haklarına aykırı olarak kullanılmasıdır.[87]

d)Yasadışı yayınlar

Bunlar karşımıza iki şekilde çıkmaktadır. Bunlardan birincisi; vatanın bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli Internet sayfalarıdır. İkincisi genel ahlaka aykırı pornografik görüntülerdir.[88]

Yukarıda ayrıntılı şekilde suç tipleri açıklanan siber suçlar,

Özetle bilgisayarla işlenen, bir terör eylemi olmayan tüm suçlardır.[89]

Bu suçları şu başlıklar altında sıralanabilir.[90]

- Telekomünikasyon Hizmetleri Hırsızlığı,
- Bilgisayar Sistemlerinin Başka Suç İşlemek için Kullanılması,
- Bilgi Korsanlığı, Sahtecilik ve Kalpazanlık,
- Kötü, Çirkin Görüntü ve Kayıtların Yayılması,
- Tehdit ve Gasp tır.

---

[87] İsmail Güneş S.4
[88] Rapor 1
[89] **Computer Crime and Intellectual Property Section of the Criminal Division of the U.S.** (Çevrim içi) Departmentof Justice, http://www.cybercrime.gov. 08 temmuz 2004
[90] Mehmet Özcan, s.4,5

Ne var ki bilgi ve network sistemlerini kullanarak işlenen siber suçlarla, siber terör arasında çok ince bir çizgi vardır.

Bu çizgi; ancak bu suçların işlenmesindeki amaçları ortaya çıkartarak belirginleştirebilir. Siber suçta faillerin amacı bireysel kazanç elde etmek iken; siber terörde ise hedeflenen politik bir başarı kazanmaktır.

Bu fark şu örnekle açıklanabilir:

Bir havayolu şirketinin bilgisayar sistemine girerek kaçak veya sahte bilet satmak siber suçtur. Fakat havalimanı güvenlik sisteminin çalışmasını engelleyerek uçak kaçırmak için gerekli patlayıcı ve ateşli silahları uçağa sokmak bir siber terör destek eylemi, hava trafik kontrol sistemlerine girerek uçakların rotalarını değiştirilmesi sonucunda uçakların havada çarpışmasına neden olmak bir siber terör saldırısıdır.[91]

Yukarıdaki örnekte de görüldüğü gibi,

Siber suç, bireysel kazanç sağlamak için bilgi teknolojisini kullanarak suç işlemektir. Bunun yanı sıra siber terör destek ise ya klasik terör eyleminin yada bir siber terör saldırısının gerçekleşmesini sağlamak için direk bir tehlike oluşturmayan bilgi teknolojisinin yasa dışı kullanımıdır. Siber terör saldırısı ise terör örgütlerinin hedeflerine ulaşmak adına topluma doğrudan zarar vermek için bilgi teknolojisini kullanmasıdır.

Siber terör eylemi ile siber suç arasındaki farklılıkların belirlenmesinden sonraki aşama siber terör eylemin düzeyinin ve derecesinin tespit edilmesidir.

D)Siber Terör Eylemlerinin Dereceleri

Bir siber terör eylemi, ister siber terör destek eylemi, ister siber terör saldırısı olsun; bu eylemin belli özelliklerine göre eylemin şiddeti yani derecesi değişmektedir.

---

[91] R.J. Pinerio, s.170

Bundan dolayı siber terör eyleminin düzeyini, derecesini belirleyebilmek için bazı kriterler kullanılmaktadır.

Nedenle siber terörün dereceleri açıklanmadan önce bu dereceleri belirleyen kriterleri tespit etmek gereklidir.

Bu kriterler, teknoloji kullanma yeteneği, hedef analiz düzeyi ve örgütsel kapasitedir.[92]

- **Teknoloji Kullanma Yeteneği**

Teknoloji kullanma yeteneği, terör örgütünün hedef aldığı network sistemine müdahale etmek için gerek duyduğu donanım ve yazılım teknolojisine sahip olabilmesini ve de bu teknolojik birikimini eylemini gerçekleştirirken karşılaşacağı problemleri aşmak için kullanabilmesini ifade eder.[93]

- **Hedef Analiz Düzeyi**

Bir terör örgütünün, siber terör eyleminden önce hedef aldığı network sisteminin zayıf noktalarını tespit etmesi ve bu noktaları nasıl kullanabileceğini bulmakta ki ulaştığı seviye o örgüttün hedef analiz düzeyidir.[94]

- **Örgütsel Kapasitesi**

Örgütsel kapasite, terör örgütünün emir ve kontrol zincirinde ve istihbarat toplamakta geldiği düzeyi ifade etmektedir.[95]

Terör örgütlerinin bu üç kriterden, hangisine ve ne kadar sahip oldukları, bu örgütlerin ne derece de etkin bir siber terör eylemi gerçekleştirebileceğini belirler.

Bundan dolayı da örgütler üç ayrı düzey ve derece de siber terör eylemi yapabilir Bunları Basit Yapılandırılmamış, İleri Düzeyde Yapılandırılmış ve Karmaşık Koordinasyonlu eylemlerdir.[96]

---

[92] White Paper, s.76
[93] İbid. s.77
[94] İbid.
[95] İbid.
[96] İbid. s.36

Bunların irdelenmesi; bir anlamda da bir siber terör eyleminin ve siber teröristlerin en alt düzeyden, en üst düzey geçerken geçirdiği evrimi göstermesi bakımından önem arz eder.

Nedenle ilk önce siber terör eyleminin en basit formu olan basit yapılandırılmamış siber terör eylemini irdelenmelidir.

Tablo 2 : Siber Terör Eylemlerinin Dereceleri

Siber Terör Dereceleri	**Hedef**	**Hedef Analizi**	**Eylemin Sonuçları**	**Teknoloji Kullanma Kapasitesi**	**Araçları**
Basit Yapılandırılmamış	Basit bilgi ve network sistemleri	Yok	Odaklanılmamış	Basit	Var olan siber terör araçları
İleri Düzeyde Yapılandırılmış	Çoklu bilgi ve network sistemleri	Başlangıç düzeyinde	Odaklanılmış	Gelişmiş	Modife edilmiş
Karmaşık Koordinasyonlu	Çoklu network sistemleri	İleri düzeyde	İstenilen ve Ölçülebilen sonuçlar	İleri düzeyde	Hedefe göre yaratılmış

1) Basit Yapılandırılmamış Eylem :

Basit yapılandırılmamış eylemler, başkaları tarafından yaratılmış programları ve aletleri kullanarak kişisel sistemlere karşı yapılmış basit düzeydeki siber terör eylemleridir.[97]

Bu eylemleri gerçekleştiren kişiler veya örgütler henüz hedef analizi, emir, kontrol ve öğrenme kapasitesine sahip değillerdir.[98]

---

[97] İbid. s.77
[98] İbid.

Bu düzeyde ki siber terör saldırılılarını gerçekleştirebilmek için çok basit derece de bilgisayar kullanabilmek yeterlidir. Ayrıca bu düzey için gerekli olan temel teknolojik donamın sadece bir bilgisayardan ve bir İnternet kablosundan ibarettir.[99]

Çünkü bu düzey için gerekli olan bilgisayar programları chat odalarında ve İnternette bulunan hacker sitelerinden kolaylıkla indirilebilmektedir. Bu nedenle basit ve yapılandırılmamış siber terör eylemini, tek bir kişi veya amatör bir grup da rahatlıkla gerçekleştirebilir.

Bu durumda, bu eylemi yapan kişilerin veya örgütlerin emir, kontrol ve örgütlenme kapasiteleri çok alt düzeydir. Ayrıca bu kişilerin ve örgütlerinin teknolojik bilgileri ve bunu kullanma kabiliyetleri çok sınırlı olduğu için bunların bir hedef analizi yapma yetenekleri de yoktur.

Basit yapılandırılmamış siber terör eylemlerine örnek olarak Smurf bilgisayar programıyla bazı hükümet sitelerine saldırılması verilebilir. Smurf bilgisayar programının kullanılmasıyla yapılan bir terör eylemi özetle rasgele seçilen bir web sayfasından hedef alınan web sitesine gönderilen mesajlarla, hedef alınan kurumun haberleşme sistemlerinin engellenmesidir.[100]

Özetle bu eylem siber terörün en basit düzeyidir. Bundan sonra teknolojik bilgisini geliştiren hacker daha sonraki aşama olan ileri düzeyde yapılandırılmış eylem formuna geçmektedir.

2)İleri Düzeyde Yapılandırılmış Eylem

İleri düzeyde yapılandırılmış eylemler, çoklu veya network sistemlerine düzenlenen daha gelişmiş siber terör eylemleridir.[101]

Bu eylemleri yapanlar basit hacker programları ve aletleri yapabilecek teknolojik yeteneğe sahip olmanın yanı sıra bu örgütler başlangıç düzeyinde de olsa hedef analizi, emir kontrol ve öğrenme kapasitesine sahiptirler.[102]

---

[99] İbid., s.79
[100] İbid., s.78
[101] İbid., s.80

İleri düzeyde yapılandırılmış siber terör eylemi yapabilmek için şu özelliklerin bulunması gerekmektedir.

Bunlar şu şekilde sıralanabilir:[103]

- İleri düzeyde bilgisayar programcılığı bilgisi,
- Güvenlik sistemlerinin mekanik yapısını anlayabilmek,
- TCP/IP protokolü hakkında detaylı bilgiye sahip olmak,
- En az bir işletim sistemi konusunda uzman olmak,
- Sistem ve network mühendisliği hakkında detaylı bilgiye sahip olmak,
- Telekomünikasyon sistemleri ve veri tabanları hakkında bilgi sahibi olmaktır.

Bütün bu özellikler basit bir düzeyde bir bilgisayar kullanıcısının sahip olmadığı yeteneklerdir. Bu yeteneklerden bir veya kaç tanesine sahip olmak bile aylarca çalışmayı gerektirdiğinden, ileri düzeyde yapılandırılmış bir terör eylemi gerçekleştirmek için uzun bir hazırlık sürecine ihtiyaç vardır.

Bu saldırıların hedefi network ve çoklu bilgisayar sistemleri olduğu için, başlangıç düzeyinde bile olsa, bir hedef analizi yapılması şarttır.

İş bu hedef analizi yapabilmek için en azından hedef alınan sisteme benzer sistemlerin kurulması ve üzerinde çalışması gerekmektedir. Bundan dolayı da teknolojik bir altyapıya ve bu teknolojik altyapıyı sağlayacak örgütsel kapasiteye gerek vardır.

Sonuçta ileri düzeyde yapılandırılmış siber terör eylemi basit yapılandırılmamış siber terör eylemi arasındaki temel fark bilgisayar teknolojisine hakimiyettir. [104]

---

[102] İbid.
[103] İbid.

Bundan sonraki aşama siber terörün ulaşabileceği en son nokta olan karmaşık koordinasyonlu eylemlerdir.

3)Karmaşık Koordinasyonlu Eylemler

Karmaşık koordinasyonlu siber terör eylemlerini gerçekleştirmek için gerekli özellikleri şöyle sıralanabilir.[105]

- Uzman düzeyde program bilgisi,
- Çeşitli işletim sistemleri konusunda uzman olmak,
- Sanayide kullanılan bilgisayar alt yapı sistemleri hakkında detaylı bilgiye sahip olmak,
- Telekomünikasyon sistemleri konusunda uzman olmaktır

Bu düzeydeki siber terör eylemleri; aslında gerçek, saf siber terördür. Çünkü bu aşamadaki siber terör eylemleri yüksek oranda mal ve can kaybına neden olabilecek enerji, askeri ve sağlık gibi kritik alt yapı sitemlerini hedef alır.

Bu güce sahip karmaşık koordinasyonlu siber terör saldırıları yapabilmek için aynı hedefe farklı yerlerden eş zamanlı saldırı yöneltebilecek aynı zamanda şifreleme gibi karşı koruma tedbirlerini kırabilecek teknolojiye sahip olmak lazımdır.[106]

Ayrıca geliştirilecek yeni koruma tedbirlerinin kırılabilmesi için hedefin yeni zayıf noktalarını keşfedebilecek hedef analiz kapasitesine ulaşmak gereklidir.[107]

Kaldı ki bu teknolojik ve hedef analiz kapasitesini koordinasyonlu bir şekilde yürütebilecek örgütsel yapıya da ihtiyaç vardır.[108]

---

[104] İbid., s. 85
[105] İbid., s. 90
[106] Douglas Hayward, **"Hacker's Dark Side Gets Even Darker"** *TechWire.*. (Çevrim içi) http://www.techwire.com/,01 Mart 2003
[107]Tom Bearden, "Hacking Around" transcript of *The NewsHour with Jim Lehrer,* (Çevrim içi) http://www.pbs.org/newshour 08 Mart 2003
[108] DorothyDenning, **Information Warfare and Security** (Çevrim içi) http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html 02 Nisan 2003)p. 51.

Çünkü bu derecedeki siber terör eylemleri aynı anda birçok eş zamanlı saldırılardan meydana gelir. Bu tarz büyük eylemleri gerçekleştirmek için kurumsallaşmış bir örgüt yapısını da gerekli kılmaktadır.

Yukarıdaki özelliklere sıradan bir muhalif grubun veya anarşist hacker topluluğunun ulaşabilmesi çok zordur.

Nedenle bu düzeydeki; yani gerçek anlamda siber terör ya El Kaide gibi profesyonel uluslararası terör örgütleri yada İsrail, Amerika Birleşik Devletler gibi, büyük devletleri kendi varlığına karşı tehdit gören Kuzey Kore gibi ülkelerin istihbarat birimlerince yapılabilmesi teorik olarak mümkündür.

Ancak karmaşık koordinasyonlu düzeydeki siber terör saldırıları şu an için sadece teorik bir varsayımdır. Literatürde bu düzeyde yapılmış siber terör saldırısı bulunmamaktadır.

Fakat şu an yakın bir tehdit olmayan siber terörün bu derecesi, teknolojinin gelişme ve yayılma hızının her gün daha da artmasıyla kısa bir zaman sonra insanlığın en büyük kabusu olabilir.

Bundan dolayı Amerika Birleşik Devletleri'nde siber terör özellikle de kritik altyapıların korunmasıyla ilgili teknik ve yasal hazırlıklar yapılmaktadır.

Siber terör eylem düzeyleri bu şekilde incelendikten sonra şimdi de siber teröristlerin hedef aldığı yerler ve bu yerleri belirlerken kullandıkları kriterler açıklanacaktır.

E)Siber Terör Eylemlerinin Hedefleri ve Bunların Seçilmesinde Kullanılan Kriterler

1) Siber Terör Eylemlerinin Hedefleri

Siber terör, siber dünyada gerçekleşmesinden dolayı siber terör tehdidi ile ilgili çalışmalarda coğrafya sınırsız ve de bir o kadarda önemsiz bir kavram haline girer. Bu yüzden de siber terörün nerede meydana geldiğinden bahsedildiğinde, belirli bir fiziksel yer söz konusu edilemez.

O zaman sistemlerin saldırıya uğradığı en olası yer, bizim en korumasız olduğumuz yer olan sanal ve gerçek dünyanın birleştiği noktadır. Bu noktayı daha iyi anlayabilmek için bu iki dünyayı tanımlamak lazımdır.

Fiziki dünya: Çalışılan ve yaşanılan fiziki yer.

Siber dünya : Sembolik sıfır ve birlerden oluşan bilgi sistemlerin dünyası.

Bu iki dünya doğal olarak ayrı dünyalardır. Bununla birlikte bu iki dünyanın kesiştiği, birleştiği nokta siber terörist eylemin gerçekleştiği en olası yerdir.

Bu noktada tehdit altında olan fiziki dünyada yaşamsal önem taşıyan altyapı sistemleridir.

Bunlar şu başlıklar altında toplanabilir.[109]

- Beslenme ve Sağlık Sistemleri
- Alt Yapı Sistemleri
- Finansal Sistemler
- Ulaşım Sistemleri
- Kamu Güvenliği ve Acil Servis Sistemleri
- Haberleşme ve Çevre Sistemleri
- Askeri Sistemler

Siber terör yukarda belirtilen ve sanal dünyayla fiziki dünyanı birleştiği, düzen içerisinde en çok bağımlı olunan ve güvenilen sistemlerde, başka bir ifadeyle en korunmasız olunan noktada meydana gelmektedir.

2) Hedeflerin Seçilmesinde Kullanılan Kriterler

a)Hedefin Taşıdığı Değer Ve Görünebilirliği (Visibility) :

Siber terörist bir hedefi seçerken, o hedefin hükümet ve halk için ne kadar değerli olduğunu veya o hedefe saldırmanın ne kadar ses getireceğini göz önüne alır.

b)Hedefin Savunmasızlığı :

Siber teröristlerin kolayca zarar verebildiği sistemler, girilmesi zor olan sistemlere göre daha fazla saldırının hedefini oluşturur.[110]

c)Hedefin Uzaklığı :

Siber teröristler, daha yakında olan ve kolay ulaşabilecekleri hedefleri seçerler.

d)Toplumun Hedefe Karşı Duyduğu Güven ve Bağımlılığı :

Siber terörist için bir hedefi çekici kılan diğer bir etken ise ister duygusal ister psikolojik veya yaşamsal nedenlerden kaynaklansın toplumun hedefe duyduğu ihtiyaç veya güvendir.

e) Saldırının Ölçeği :

Siber terörist eylemin büyüklüğü kadar medyada yer alması için daha çok ses getirebilecek olan hedefler seçmeye çalışır.

f) Başarı Olasılığı :

Eylemin başarılı olma olasılığı seçilen hedefe doğrudan bağlı olduğu için başarma şansları daha yüksek olan hedefler seçilir.

---

[109] hhtp://www.nici.org/Research/Pubs/98-5.htm (Çevrim içi)12 Eylül 2003

g) Eylemin Gerektirdiği Teknoloji :

Siber teröristlerin eylemlerini gerçekleştirmek için; basit bir bilgisayar, bir modem ve telefon hattı yeterlidir. Ancak hedefin zorluğuna göre gereken teknolojinin derecesi de yükselebileceğinden bu da siber teröristlerin aradığı kriterlerden birisidir.

Siber terörist hedefi seçerken yukarıda açıklanan tüm faktörleri dengeli bir şekilde bir araya getirmeye ihtiyaç duyar.

Ancak insanların her geçen gün sanal dünyayla fiziki dünya arasındaki birleşim noktalarında bulunan altyapı sistemlerine olan bağımlılığı arttığı için potansiyel hedeflerin sayısı da artmaktadır.

Bu durum da bizleri daha çok güvenlik duvarı inşa etmek ve de bilgi sistemlerine izinsiz girişleri engellemek için daha çok çaba harcamak zorunda bırakmaktadır.

Yukarıda belirtilen hedefler ve bu hedeflerin seçilmesinde kullanılan kriterler tekrar incelendiğinde görülecektir ki bütün bu hedefler klasik terör eylemleri ile gerçekleştirebilecek saldırılara da konu olabilir.

Bu yüzden teröristlerin bu hedeflere saldırmak için neden klasik terör yöntemleri değil de; siber terör yöntemlerini tercih ettiklerinin ortaya konulması gerekmektedir.

Aşağıda siber terörün; teröristlere sağladığı avantajlar ve getirdiği yenilikler açıklanacaktır.

F) Siber Terörün Tercih Edilmesini Sağlayan Faktörler

Bu faktörler genel olarak bilgi devriminin sağladığı teknolojik ortamın teröristlere getirdiği yenilikler ve kolaylıklardır.

---

[110]hhtp://www.nici.org/Research/Pubs/98-5.htm

Ayrıca siber terör, bir bilgi devriminin karanlık yüzü olarak ifade edebileceğinden, bu faktörler teknolojinin kötü amaçlar için kullanılması olarak ta tarif edilebilir.

Siber terörün tercih edilmesini sağlayan faktörler dört başlık altında toplanabilir.[111]

Bunlar; küresel bağlanabilirlik, teknolojiye olan bağımlılık, hukuksal bütünlüğün olmaması ve düşük maliyettir.

1)Küresel Bağlanabilirlik (Global Connectivity)

Küresel bağlanabilirlik, İnternetle beraber teröristlerin coğrafi sınırlara bağlı kalmadan hareket edebilmeleri demektir.[112]

Küresel düzeyde sınırsız bağlanabilirliğin sağladığı avantajlar şunlardır :[113]

- İnternetle sınırlı olmayan çeşitli sistemleri kullanabilmesi ve saldırabilmesi,
- Saldırıların tespit edebilmesinin zorlaşması,
- Altyapı sistemlerini ve ulaşabilirliklerini değiştirebilme düzeyi,
- Hedeflerin sayısının çeşitlendirmesi ve artırması,
- Emir ve kontrol sistemlerinin ve de propagandanın yaygınlaştırılmasını basitleştirmesi ve ucuzlattırması,
- Terörist eylemlerinin izleyici sayısını ve izlenebilme oranını yükseltmesi,
- Uluslararası propaganda yapabilmek için yeni olanaklar sağlamasıdır.

Küresel bağlanabilirliği meydana getiren şey, tüm dünyanın telefon kablolarıyla sarılmış olmasıdır.

---

[111] White Paper, s.24-34
[112] İbid., s.24
[113] İbid

Bu durum da siber terör eylemlerinin hedeflerini, sayısını ve eylemlerin etkinliğini artırmıştır. Özelliklede telekomünikasyon sistemlerine olan bağımlılığı düşünürsek, bu sistemlere yönelik saldırıların günlük hayata olan etkisinin yüksek düzeyde olacağı konusunda hiçbir şüphe yoktur.

Ancak, bu bağımlılık sanayileşmiş toplumlar daha yüksek orandadır. Örneğin ABD nüfusunun yaklaşık %52 si internet kullanıcısıdır.[114] Ayrıca Dünya çapında İnternet kullanıcılarının % 56 sı Kuzey Amerika da %22 si Avrupa da %17 si Asya da bulunmaktadır.[115]

Ayrıca küresel bağlanabilirlik, propaganda ve haberleşme yöntemlerini sayısını inanılmaz ölçüde artırarak, coğrafi sınırları kaldırmıştır.

Buna örnek olarak Tupac Amura gerillalarının Peru'da ki Japon Elçiliği baskınını İnternet aracılığıyla bunu tüm dünyaya duyurması verilebilir.

Küresel bağlanabilirlik aynı zaman da teknolojiye olan bağımlılığı da arttırmaktadır .

Nedenle siber terörün tercih edilmesini sağlayan bir diğer faktör de bilgi teknolojisine olan bağımlılığın artmasıdır.

2) Teknolojiye Olan Bağımlılığın Artması

Bilgi teknolojisine bağımlılığın artmasının, sonuçları şu şekilde sıralanabilir.[116]

- Amerika Birleşik Devletler ve diğer sanayileşmiş ülkeler de bilgi teknolojisinin kullanımının yüksek düzeyde olması,
- Bunun yeni zayıf noktalar yaratması,

---

[114] **Computer Industry Almanac as quoted in the CyberAtlas web site.**(Çevrim içi)http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_150591,00.html 24Mayıs2004

[115] Organization for Economic Co-operation and Development, Working Party on Telecommunication and Information Services Policies, Internet Infrastructure Indicators, (Çevrim içi) http://www.oecd.org/dsti/. 24Mayıs2004

[116] White paper, s.27

- Siber terör saldırılarının sonuçlarının etkisinin artırması,
- Finansal destek potansiyelini artırmasıdır.

Özelilikle de Amerika Birleşik Devletlerinin savunma, eğitim, sağlık ve ticaret gibi kritik altyapı sistemlerinde bilgi teknolojisine olan bağımlığı üst düzeye ulaşmıştır.[117]

Bu durum da siber terör saldırıları için uygun bir ortam ve geniş bir hedef çeşitliliği sağlamaktadır.

Ayrıca bilgi teknolojisine bağımlılık, bu sistemlerin içerisinde yeni zayıf noktalar yaratmaktadır.

Örneğin bilgi devriminden önce askeri üssün etrafını dikenli tellerle ve mayın tarlalarıyla çevirmek oraya izinsiz girişi engellemek için yeterli iken; şimdi tamamen elektronik sitemlerle korunan askeri üstler, bu elektronik sistemlerdeki en ufak bir arızada veya bu elektronik sistemlerin kırılmasında tamamen korunmasız kalabilir.

Bu yüzden de Amerika Birleşik Devletleri kritik altyapıların korunması için önemli adımlar atmıştır.

Bu adımların başında Homelend Security Act ile NİPC'nin kurulması gelmektedir.[118]

Teknolojik bağımlılığın artmasının yanı sıra; bilgi teknolojisini kullanarak işlenen suçlarla ilgili hukuksal bir bütünlüğün ve uluslararası işbirliğinin olmaması bu suçların işlenmesi için teşvik edici bir durum yaratmaktadır.

Bunun içinde küresel düzeyde hukuksal bir bütünlüğün oluşturulmamasının siber teröristlere sağladığı avantajlar incelenecektir.

---

[117] National Strategy To Secure Cyberspace, (Çevrim içi) www.dhs.gov/interweb/assetlibrary/ National_Cyberspace_Strategy.pdf 11 Mart2004 s.2
[118] www.nipc.gov

3) Hukuksal Bütünlüğün Olmaması

Hukuksal bütünlüğün ve işbirliğinin olmamasının nedenleri: [119]

- Çok sayıda uluslararası terörle mücadele anlaşmaları olmasına rağmen bunların hiçbirinde bilgi sistemlerine yönelik saldırılarla ilgili açık düzenlemelerin bulunmamasının yarattığı uluslararası platformda oluşan yasal boşluk,
- Bu suçlarda suçlunun kesin olarak tespit edilmesindeki zorluk,
- Siber terörle ilgili ulusları bir konsensüsün henüz oluşmamasıdır.

Özellikle siber terörün teknik özelliklerinden dolayı, siber terörü ulusal ceza politikalarıyla engellemek mümkün değildir.

Bu nedenle bu suçların, tespit edilmesi ve suçluların yakalanması için küresel işbirliği ve uluslararası anlaşmaların yapılması zorunludur. Ancak bugün siber terörle ilgili böyle bir uluslararası anlaşma bulunmamaktadır.

Ancak siber suçlarla ilgili yapılan çalışmalar, özellikle 2001 yılında yapılan "Avrupa Siber Suç Sözleşmesi" bilgi teknolojilerinin yasadışı kullanımlarıyla ilgili uluslararası bir ceza hukukunu yaratmasıyla ilgili umut verici gelişmelerdir.

Öte yandan siber terörün, siyasal boyutu, uluslararası politik dengelere bağımlı olduğundan, bu konuda uluslararası bir görüş birliğinin sağlamasını zorlaştırmaktadır.

Bu zorluk ta siber teröristler için rahatça hareket edebilecekleri bir ortam sağlamaktadır. Bu uygun ortamın yanında bu ortamdan faydalanmasını sağlayacak teknolojik donamının kolay ve ucuz elde edilebilir olması, siber terörün tercih edilmesini sağlayan diğer bir faktördür.

---

[119] White paper, s.29

4) Düşük Maliyet

Bir siber terör eyleminin az bütçeyle yapılmasını sağlayan unsurlar:[120]

- Bilgisayar donanımlarının fiyatlarının ucuzlaması,
- Gelişmiş hacker programlarının İnternet üzerinden ücretsiz olarak kullanılabilmesi ,
- Ulaşmak istediğin hedef için gerekli teknolojik yatırımı yapmanın yeterli olmasıdır.

Siber terör eylemin düşük maliyeti özellikle de küçük anarşist grupların ve kişilerin siber terör saldırılarını gerçekleştirmeye iten nedenlerin başında gelmektedir.

Ancak karmaşık koordinasyon düzeyindeki siber terör saldırıları için düşük maliyet söz konusu değildir. Nedenle düşük maliyet sadece basit ve yapılandırılmış siber terör saldırıları için geçerlidir.

Bu nedenlerle tercih edilen bir siber terör eylemi bilgi sistemlerine üç çeşit saldırıda bulunabilir. Bu saldırıları gerçekleştirirken çok çeşitli araçlar kullanılmaktadır. Bunların bir kısmını bilgi savaşları silahları başlığı altında incelenmiştir.

Ancak burada bir siber terör saldırı aracı olarak bunlar daha ayrıntılı olarak açıklanacaktır.

---

[120] İbid. s.30

G) Siber Terör Saldırı Çeşitleri ve Bunların Araçları

1)Siber Terör Saldırıları

Siber terör saldırılarının üç çeşidi vardır. Bunlar fiziksel, sözdizimsel (syntactic), ve semantik (semantic) saldırılardır.[121]

Fiziksel saldırı: Bilgi sistemlerine klasik yöntemleri gibi maddi açıdan zarar verir.

Sözdizimsel (syntactic) saldırılar: Bunlar bilgi sistemlerinin mantıksal yapısını değiştirerek, sistem de gecikmeler ve belirsizlikler yaratır.[122]Bu saldırı biçiminde virüs, kurtçuklar ve truva atları kullanılmaktadır.

Semantik (Semantic) Saldırılar: Bu saldırılar sistem kullanıcısının sisteme duyduğu güveni istismar etmeyi amaçlar Saldırı biçimlerindeki en tehlikeli olanıdır. Çünkü saldırılar kullanıcının haberi olmadan sisteme giren veya çıkan verileri değiştirerek sistemde arızaların meydana gelmesine neden olur.[123]

Siber teröristler bu saldırıları gerçekleştirmek için bazı aletler yaratırlar ve kullanırlar Bunlar virüsler, kurtlar, truva atları, zombiler ve DDos, arka kapılar ve mantık bombaları ve e- mail bombardımanıdır.[124]

Bu araçlar, bilgi savaşı silahları incelenirken de açıklanmıştı. Ancak siber teröristlerin en çok kullandıkları bu araçların ayrıntılarını ortaya koyarken aynı zamanda bunların kullanılmasının yarattığı suçlar ve hukuki durumu da incelenecektir.

Siber teröristlerin en çok kullandıkları araçlar, virüsler, kurtlar, truva atları, zombile ve DDoslardır

---

[121] **Pratik Sonwale, Sulejemen Mehmedagic, Computersve Society,**(Çevim içi) http://www.iit.edu/~mehmsul/projects/cs484/ 02.Nisan 2003
[122] İbid.
[123] İbid.
[124]http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/TheLaw.htl

2)Siber Terör Saldırı Araçları

a)Virüsler

(1) Tanımı:

Virüs, konuk programın özüne yüklenmiş, yeni bir çalıştırılabilir dosyaya nüfuz ederek kendi kendini çoğaltma yeteneğine sahip bir kod parçasıdır.[125]

Virüsler yetmişli yıllarda, o dönemin programcıları *"core war"* adı verilen oyunu oynarken ortaya çıkmıştır.[126]

(2)Çeşitleri

Farklı üretici ve araştırmacıların, farklı sınıflandırma önerileri olmakla beraber, bazı temel türlerden bahsetmek mümkündür. Bunlar:

i) Dosya Virüsleri:

Virüslü bir dosyanın sisteme kopyalanması (Internet'ten indirilen programlar, disket/CD değişimi, program kopyalama, vb.) ile bulaşan, dosya çalıştırıldığında üreyen ve zarar verebilen virüslerdir.[127]

ii) Makro Virüsleri:

Virüslü bir belgenin kullanılması (örn. Word ve Excel dosyaları) ile aktif hale geçen, bulaşan, zarar verebilen virüslerdir.[128]

iii)Karma Virüsler:

Karma olarak nitelendirilebilecek bu virüsler, farklı yöntemleri bir arada kullanabilirler. Örneğin paylaşılmış dizinlerde dosya aktarımı, ortamda zaaf sahibi web sunucuların bulunması ve bunlara bulaşılması, e-mail gönderimi, vb. dır.[129]

---

[125] Christophe Blaeses **"Virüsler: herkesi endişelendiren konu"**, çev. Hüseyin Kaya,Gülşen Taşkın,Sevda Üsküplü, D. Melih Naim (Çevrim içi) www.linuxfocus.org/Turkce/ September2002/article255.shtml (Çevrimiçi) 25 Temmuz 2004

[126] İbid.

[127] Barış Arkış **"Vüristen Koruma Yolları"** (Çevrim içi) http://www.barisarkis.com/tyorum/tyorumfiles/BarisArkis_Virusten_Korunma.pdf 27 Temmuz 2004

[128] İbid.

iv)Virüs Söylentileri:

"Hoax" olarak bilinen bu grup, aslında olmayan bir virüs, tehdit veya fırsat hakkında yayılan e-posta mesajlarını tanımlamaktadır. Bu tür mesajlar, hem sistemlere gereksiz yük getirmekte, hem de pek çok kullanıcının e-mail adresinin üçüncü şahıslarca toplanarak ticari veya kötü niyetli biçimde kullanımına imkan vermektedir.[130]

(3) Örnekler:

Bütün dünyayı etkilemiş bir kaç tane ünlü virüs vardır.[131]

i) Çernobil

ii) I love you

iii)Mellisa

b) Kurtlar (Worms)

(1) Tanımı:

Genellikle e-mail iletileri ile çoğalan, kendi kendilerine de e-mail gönderen, hatta sahte gönderici adresleri kullanabilen virüslerdir.[132]

Kurtlarda virüsler ile aynı prensipten gelir. Kendilerini kopyalama yöntemi ile çoğalmayı hedeflerler. [133]

Virüsler ile kurtlar arasındaki en önemli fark, Kurtların virüsler gibi bir yayılma aracı olarak programları kullanmaması, bunun yerine ağ içinde kullanılan e mail gibi servisleri yayılma aracı olarak kullanmalarıdır.[134]

---

[129] İbid.
[130] İbid.
[131] http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/TheLaw.htm
[132] Barış Arkış
[133] Av.Ali Osman Özdilek " **KURTLAR VE ZOMBİLER: Worm'ların ve DDoS Ataklarının Hukuki İncelemesi"** (Çevrim içi) http://www.hukukcu.com/bilimsel/kitaplar/wormlarhukuki.ht 12 Haziran 2004

(2) Örnekler

i) Morris Wormu

Tespit edilen ilk kurttur. İsmi yaratıcısı Robert Tappan Morris'den gelmektedir.[135]

ii) 2001 yılındaki kurt salgını[136]

c)Truva atları

(1) Tanımı:

Truva Atı, bir program içinde gizlenen ve gizli bir işlev yapan parçalı bir koddur. Virüsleri yada kurtları saklamak için sıklıkla kullanılan bir mekanizmadır.[137]

Truva atlarının özellikleri şunlardır.[138]

- Zararsız programlar gibi gözükürler,
- Etkilediği programlar normal çalışmaya devam eder,
- Yapacağı işleri sistemi arka planında gerçekleştirilirler,
- Fark edilmeleri çok zordur.

(2) Örnekler

Truva atlarına somut örnek vermek çok zordur. Çünkü İnternet ortamında her program ve e-mail truva atı olarak kullanılabilir. Ancak en yaygın Truva atları bugünlerde çok klasik olarak görünse de ekran koruyuculardır.[139]

Aslında hem kurtlar hem de truva atları bir tür virüstür. Bundan dolayı virüslerin, kurtların ve truva atlarının kullanılmasının ihlal ettiği hukuki değer

---

[134] Christophe Blaeses
[135] Av.Ali Osman Özdilek
[136] http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/TheLaw.htm
[137] AyhanÇankaya , s.3
[138] Korhan Güler **"İnternete Bireysel Güvenlik"** (Çevrimi içi)
- seminer.linux.org.tr/seminer-notlari/ senlik-2002/ankara-bireysel.ppt18 Ağustos 2004
[139] Christophe Blaeses

aynıdır. Bu nedenle Bu üç siber terör yönteminin kullanılmasının yarattığı hukuki sonuçlar aynıdır.

d) Hukuki Sonuçları

Virüsler, wormlar ve truva atları gibi kötü amaçlı olarak yazılmış kodlar hukukun çeşitli alanlarının inceleme sahasına girmektir. Ancak bu çalışmada bunlar ceza hukuku açısından irdelenecektir.

Bu kodların ceza hukukunda incelenmesinde öncelikle sorulması gereken soru; sadece kötü niyetli bir kodun yazılmış olmasının yazarı için cezai sorumluluk doğurup doğurmayacağı sorusudur.

Bu sorunun cevabı; sadece kötü niyetli kod yazımının suç olmaması gerektiğidir. Çünkü bunların yazılmış olması bunların bir siber terör eylemi için kullanılacağı anlamına gelmez. Burada sadece bir saikten söz edilebilir..

Ancak bu nokta da başka bir soru çıkmaktadır. Bu soruda sadece kötü niyetli kod kullanımının bir tehlike suçu oluşturup oluşturmadığıdır.[140]

Sadece kötü niyetli kod yazımı bir tehlike suçu meydana getirmez. Bir tehlike suçundan bahsedebilmek için objektif olarak bir hareketin yapılması ve bu hareketin sonucunda ceza hukuku açısından bir neticenin meydana gelme ihtimalinin kuvvetli olması gerekir.[141]

Yukarıda da belirtildiği gibi sadece kod yazımı bir saikten öte anlam ifade etmemelidir.

Fakat yazılan bu kodun sonuçlarını doğurmaya elverişli bir halde sunulması örneğin halen görüldüğü gibi bir hack web sitesinde kullanılmaya elverişli şekilde yer alması durumunda artık bir tehlike suçunun varlığından söz edilebilecektir. Çünkü virüs kodları artık bir saik olmaktan çıkmış ve suç yolunda elverişli bir araç haline dönüşmüştür.

---

[140] Av.Ali Osman Özdilek, s.3
[141] Ayhan Çankaya

aynıdır. Bu nedenle Bu üç siber terör yönteminin kullanılmasının yarattığı hukuki sonuçlar aynıdır.

d) Hukuki Sonuçları

Virüsler, wormlar ve truva atları gibi kötü amaçlı olarak yazılmış kodlar hukukun çeşitli alanlarının inceleme sahasına girmektir. Ancak bu çalışmada bunlar ceza hukuku açısından irdelenecektir.

Bu kodların ceza hukukunda incelenmesinde öncelikle sorulması gereken soru; sadece kötü niyetli bir kodun yazılmış olmasının yazarı için cezai sorumluluk doğurup doğurmayacağı sorusudur.

Bu sorunun cevabı; sadece kötü niyetli kod yazımının suç olmaması gerektiğidir. Çünkü bunların yazılmış olması bunların bir siber terör eylemi için kullanılacağı anlamına gelmez. Burada sadece bir saikten söz edilebilir..

Ancak bu nokta da başka bir soru çıkmaktadır. Bu soruda sadece kötü niyetli kod kullanımının bir tehlike suçu oluşturup oluşturmadığıdır.[140]

Sadece kötü niyetli kod yazımı bir tehlike suçu meydana getirmez. Bir tehlike suçundan bahsedebilmek için objektif olarak bir hareketin yapılması ve bu hareketin sonucunda ceza hukuku açısından bir neticenin meydana gelme ihtimalinin kuvvetli olması gerekir.[141]

Yukarıda da belirtildiği gibi sadece kod yazımı bir saikten öte anlam ifade etmemelidir.

Fakat yazılan bu kodun sonuçlarını doğurmaya elverişli bir halde sunulması örneğin halen görüldüğü gibi bir hack web sitesinde kullanılmaya elverişli şekilde yer alması durumunda artık bir tehlike suçunun varlığından söz edilebilecektir. Çünkü virüs kodları artık bir saik olmaktan çıkmış ve suç yolunda elverişli bir araç haline dönüşmüştür.

---

[140] Av.Ali Osman Özdilek, s.3
[141] Ayhan Çankaya

Mevzuatımızda kötü niyetli kod yazma ve bunu yaymaya ilişkin açık bir hüküm bulunmamaktadır. Kötü niyetli kodlarla bir bilgisayar sistemine zarar verme doktrinde genellikle "sistem ve unsurlarına yönelik nas-ı ızrar suçu" olarak adlandırılmaktadır.[142]

Fakat bu suçu nas-ı ızrar suçu olarak tanımlamak bu suçun niteliğini ve kapsamını açıklamaya yetmez. Çünkü virüsler daha çok bir sistemde mevcut programlara zarar verirler. Bir bilgisayar sisteminin standart olarak belirlenen fonksiyonlarının, kendisine yükletilen şekilde yerine getirmesine engel olurlar.[143]

Hukukumuzda TCK m.525/b.1 ile kötü amaçlı kod kullanarak bilgisayar sistemine zarar verme suçunu karşılayabilecek bir hüküm olduğu iddia edilmektedir.[144]

Bu kötü niyetli kod yazılımlarının yanı sıra siber teröristler Denial of service veya Distributed Denial Service (Dos veya DDos) saldırıda yapmaktadırlar.

e)Dos veya DDos

(1) Tanımı:

Dos saldırısı bilgisayar ağlarını zor duruma düşürmek ve sistemleri yavaşlatacak düzeyde büyük çapta ağ trafiği yaratmaktır. DDoS (Distributed Denial of Service) saldırısı ise dağıtılmış yani birkaç yönden gelen DoS saldırısıdır.

DDoS saldırılarının amacı hedef sistemi işlemez hale getirmektir. Bazı DDoS atakları hedef sistemi iflas ettirmek için tasarlanmışken diğer bazıları da hedef sistemi meşgul edip normal işleyişini yavaşlatmak için oluşturulmuştur.[145]

---

[142] Av.Ali Osman Özdilek,s.3
[143] İbid
[144] İbid.
[145] Taccettin Karadeniz " **Dos**" (Çervim içi) 08 Ağustos 2003
http://www.olympos.org/article/articleview/403/1/10

(2) Saldırının düzenleniş şekli:

Saldırı anında kişi, kendini gizlemek için önceden sızdığı bilgisayarlara 'zombi' adı verilen küçük programcıkları yerleştiriyor. Saldırılar bu "zombi"ler üzerinden yapılarak birden fazla bilgisayar ve istenilen hedefler üzerine veri bombardımanı gerçekleştiriyor.

Olympos Security'de yer alan bilgilere göre, binlerce bilgisayarlara yerleştirilen zombiler, bilgisayarlara uzaktan kontrol (remote) imkanı vererek, bu bilgisayarlar üzerinden istenilen sunucuya çok sayıda veri göndererek, sunucuyu devre dışı bırakma imkanı sağlıyor. Böylece saldırganlar, saldırıları başka insanların bilgisayarları üzerinden gerçekleştirdiği için tespit edilmeleri zorlaşıyor.[146]

(3) DDoS saldırısı araçları:[147]

- The Tribe Flood Network (TFN)
- Stacheldraht
- Trinity
- Shaft Tribe Flood Network 2K(TFN2K)
- MStream
- Trinoo(Trin00)

DDos saldırı incelenken karşımıza Zombi denilen yeni bir kavram çıkmaktadır.

f) Zombiler

(1) Tanımı:

DDos saldırısı düzenleyen kişiler kimliklerini ele vermemek için kullandıkları bilgisayarlara denir.[148]

---

[146] Av.Ali Osman Özdilek,s.3
[147] RohasNagbel

Böylece siber terörist aynı anda bir çok bilgisayarın hedefe saldırmasını sağlayarak kimliğini gizlemeyi başarır.

Zombiler saldırgan tarafından ele geçirilen sistemlere yerleştirilirler. Ele geçirilen sisteme yerleştirilen zombiler kendi bünyesindeki daemonlar vasıtasıyla belirli bir porttan gelecek olan DDoS isteklerini gerçekleştirirler.

g) Hukuki Sonuçları:

Bu suçu incelerken suçun oluşabilmesi için geçilmesi gereken teknik aşamalar da göz önüne alınmalıdır. Çünkü tek bir mağdura karşı yapılan tek bir eylem yoktur.

Failin ilk eylemi herhangi bir kullanıcının bilgisayarını zombi bilgisayar haline getirmektir. Bunun için de bu bilgisayara yetkisiz giriş yaparak amacını gerçekleştirebileceği programı bu bilgisayara kurar. Bu sayede dilediği zaman bu bilgisayarın kendi yüklediği program sayesinde belirli bir fonksiyonu yerine getirmesini sağlar yani sistemin işleyişini değiştirir.[149]

Fail bundan sonra zombi bilgisayarlara bir emir vererek hedef sunucuya çok yoğun biçimde talep göndermeye başlar. Bunun sonucunda bu yükü kaldıramayan sunucu ya çöker ya da işleyişi yavaşlar.

Suçun oluşabilmesi için sunucuyu işletenin bundan maddi olarak bir zarar görmesi gerekmez. Sunucularının kapasitesi yüksek olup ta bu eyleme maruz kalan bir işleten bu eylemden dolayı hiçbir zarara uğramasa da suç meydana gelir.

Bu suç ancak kastla işlenebilir. Suç teşebbüse elverişlidir. Zombi bilgisayar kullanıcılarının durumu fark etmesi ile bilgisayarlarını kapatmaları, sunucuyu işletenin güvenlik biriminin durumu başından fark edip gerekli tedbirleri alması gibi durumlarda suç teşebbüs derecesinde kalabilir.

---

[148] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html
[149] Av.Ali Osman Özdilek

Teşebbüsün türü somut olayın şartlarına göre değerlendirilmelidir. Burada zombi bilgisayar kullanıcılarına cezai bir sorumluluk yükletmek mümkün değildir meğer ki saldırganla işbirliği yaptıkları tespit edilmiş olsun.

Sonuçta suç, zombi bilgisayarlardan sunucuya taleplerin yöneltilmeye başlamasıyla birlikte gerçekleşmiş olur. Suçun işlendiği yer olarak hedef sunucunun bulunduğu yer kabul edilmelidir.

Bu suçta da TCK'nin 525/b maddesinin uygulanabileceği ileri sürülmektedir.[150] Bu saldırı biçimleri açıklandıktan sonra şimdi de bu saldırılara karşı alınması gereken tedbirler ve karşı korunma yöntemleri incelenecektir.

Bu koruma yöntemleri; teknolojik tedbirler ve bilgi teknolojilerinin yasadışı kullanımıyla ilgili hukuki düzenlemelerdir.

H)Teknolojik Tedbirler

Bunlar, Şifreleme, Firewalls (Güvenlik Duvarları) ve Proxy Severs (Vekil sunucuları), Anti Virüs Programları, Biyometri dır.

1) Şifreleme

Şifreleme, matematiksel bir algoritma ve bir şifreleme anahtarı kullanılarak bir bilginin alıcı dışında başka bir kişi tarafından okunamayacağı biçimde kodlanmasıdır.[151]

2) Güvenlik Duvarları (Firewalls)

Bir güvenlik duvarı, bilgisayara ve ağa veri geçişini denetleyen, belirli kriterlere uymayan paketleri geçirmeyen bir yazılım programı veya donanım parçasıdır.[152]

---

[150]Av.Ali Osman Özdilek s.7
[151] http://www.ykb.com/hizmetler/e_ticaret/sorular.html#18
[152] Yalçın Tosun **"AĞ GÜVENLİĞİ PROJE I VEKİL SUNUCULAR VE GÜVENLİK DUVARLARI"** (Çevrim içi)www.cs.itu.edu.tr/~orencik/Vekil Sunucular ve Guvenlik Duvarlari.ppt 23 Haziran 2044

Kullanılan güvenlik duvarının tipine göre bu işlem, verinin kaynağıyla işlemci bilgisayar arasında olabilir veya bilgisayarda bir uygulama olabilir. Ama yapılan temel işlem tüm güvenlik duvarları için aynıdır.[153]

3) Anti Virüs Programları:

Bunlar Nortan Anti Virüs, McAFee gibi programlar olup bilgisayarlara giren virüsleri tespit edip onları zararsız hale getirirler.

4) Biyometri

Sisteme giriş için kişileri biyolojik özellikleri aracılığıyla tanımlamaktır. Artan güvenlik ihtiyacının şifrelerle karşılanamayacağı görüldüğü için biyometrik sistemlerin geliştirilmesi kaçınılmaz olmuştur.[154]

Teknolojik olarak alınabilecek bu önlemlerin yanısıra bir suç olan siber terörü önlemek için bilgi teknolojilerinin yasadışı kullanımını hususunda yasal düzenlemelerin yapılması da bir zorunluluktur.

---

[153]İbid.

[154] http://www.sj.k12.tr/html/konu/biyometri/tr/menu.html

[154]http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/TheLaw.htm

III.BİLGİ SİTEMLERİNİN YASADIŞI KULLANIMIYLA İLGİLİ YASAL DÜZENLEMELER

Dünyada ve Türkiye'de bilgi teknolojilerinin yasa dışı kullanımının hukuk sistemlerinde yerini alması çok yeni bir olgudur.

Özellikle gelişmiş ülkelerde günlük hayattaki birçok işlemin bilgi teknolojilerini kullanarak yapılmaya başlanmasıyla doğru orantılı olarak bilgi teknolojilerinin yasa dışı kullanımı da artmıştır. Son yıllarda Amerika Birleşik Devleri ve Kara Avrupa'sında bilgi teknolojilerinin kullanılmasına dair kanunlar yapılmıştır.

Fakat bu kanunlar siber suçların tespit edilmesi ve cezalandırılmasıyla ilgilidir. Bu yüzden siber terör ile ilgili ne ulusal bazda ne de uluslararası platforma yasal bir düzenleme henüz mevcut değildir.

Ancak başta Amerika Birleşik Devletleri olmak üzere sanayileşmiş ülkelerde özellikle kritik altyapılarının korunması ile ilgili yasal düzenleme yapılmaya başlanmıştır. Fakat bu düzenlemeler henüz yeterli değildir.

Bu nedenle siber terörle ilgili yasal düzenlemelerin hukuksal karakterini resmedebilmek için temel olarak anti terör yasaları ve siber suçlarla ilgili düzenlemeler ele alınacaktır.

Bu yasaları temel almak ta ki, amaç ilk önce bilgi teknolojilerinin yasa dışı kullanımlarıyla ilgili yasal düzenlemelerin genel özelliklerini tespit etmek ve de bu özellikleri terörle mücadele çerçevesinde değerlendirmektir.

Bu değerlendirmeler için öncelikle:[155] Amerika Birleşik Devletlerindeki, Uluslararası Örgütlerin İlgili Kararları, Türkiye ve diğer ülkelerdeki yasal düzenlemeler incelenecektir.

A)Amerika Birleşik Devletlerindeki Yasal Düzenlemeler

Bu düzenlemeler: [156] Yasalar ve Başkanın İdari düzenlemeleri olmak üzere iki ana gruptur.

1) Yasalar

Bunlar beş tanedir.[157]

a) Bilgisayar Bağlantılı Dolandırıcılık, Hile ve İlgili Faaliyetler (18 U.S.C §1030 "Fraud and Related Activity in Connection with Computers"): [158]

b)Anavatan Güvenlik Yasası (Homeland Security Act 2002)[159]

c)Terör Suçları Cezayı Müeyyideler (18 U.S.C §2332 "Criminal Penalties for Terrorism") [160]

d) Ulusal Sınırları Dışında Yapılan Terör Eylemleriyle İlgili Yasalar (18 U.S.C §2332 (b) "Acts of Terrorism transcending national boundaries")[161]

e) USA Patriot Act (2001)[162]

---

[156] İbid.
[157] İbid
[158] http://www.usdoj.gov/criminal/cybercrime/1030NEW.html
[159] www.whitehouse.gov/deptofhomeland/bill/
[160] http://www4.law.cornell.edu/uscode/18/2332.html
[161] http://www4.law.cornell.edu/uscode/18/2332b.html
[162] www.epic.org/privacy/terrorism/hr3162.html

a) Bilgisayar Bağlantılı Hile, Dolandırıcılık ve İlgili Faaliyetler (18 U.S.C §1030 "Fraud and Related Activity in Connection with Computers"):

Bu yasada siber suçlar tanımlanmış ve cezaları belirlenmiştir.Buna göre bu yasa hacking, cracking ve virüs yayma gibi suçların çeşitli tipleri tanımlanarak yasaklamıştır.[163]

Bu yasa siber suçları sıralamıştır.[164]

(1)Yetkisiz Erişim ve Bildirim:

Bilgisayarlara izinsiz erişerek veya izinli girişi aşarak Amerika Birleşik Devletleri'ne dezavantaj oluşturabilecek bilgileri bilerek elde etmek ve yetkisiz kişilere bildirmek.[165]

(2)Federal Hükümetin Bilgisayarlarını Yetkisiz Kullanım:

Sadece federal hükümet tarafından kullanılan veya onları etkileyebilecek bilgisayarları kasten yetkisiz kullanmaktır.[166]

Bu suçların müeyyideleri 1 ile 20 yıl arasında hapis cezası olarak ve daha önceki işlenmiş suç ve suçlara göre değişmektedir.[167]

b) Anavatan Güvenlik Yasası (Homeland Security Act 2002)

Bu yasanın, 225. bölümüyle 18. U.S.C§ 1030'da düzenlenmiş siber suçlara yeni suçlar eklenip ve bu suçlarla ilgili cezalar artırılmıştır.

Ayrıca bu yasanın 225. bölümü Cyber Security Enhancement Act (Siber Güvenliği Artırma Yasası) olarak adlandırılmaktadır.[168]

---

[163]http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/USLaw.html
[164]http://www.usdoj.gov/criminal/cybercrime/1030NEW.html
[165]http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/USLaw.html
[166]İbid.
[167]İbid
[168]www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm -

Bu yasa, 18. U.S.C§ 1030 da sayılmış suçlara, kastla veya taksir yapılmış olmasına bakılmaksın ölüm veya yararlanmaya neden olan suçları eklemiştir. Buna bağlı olarak cezalarda müebbet hapis cezasına varan önemli artırımlara gidilmiştir.

Ancak siber suçlar, insanlara fiziksel zarar verebilecek bir suç tipi olmadığından söz konusu yasayla eklenen suçların aslında siber terör suçları olduğunu söylemek yanlış bir yorum olmayacaktır.

Homelend Security Act diğer bölümlerinde

Department of Homeland Security (Anavatan Güvenlik Departmanı) kurulmuştur. Bu departmanın görevi Amerika Birleşik Devletlerine yönelik terörist saldırıları engellemek veya etkisini azaltmaktır.[169]

c) Terör Suçları Cezayı Müeyyideler (18 U.S.C §2332 "Criminal Penalties for Terrorism")

(1)Maddenin Özeti:

Her kimse,

Bir Amerika vatandaşına, bu kişi Birleşik Devletlerin dışındayken, karşı ciddi bir fiziksel yaralama niyetiyle fiziksel şiddet kullanırsa yada

Şiddet eylemi Amerika Vatandaşlarının ciddi derece yararlanmasına sebebiyet vermişse, bu kanundaki cezayı müeyyide veya on yılı kadar hapis cezası veya ikisi birden verilir

(2)Siber Teröre Uyarlanması:

Bazı siber terör saldırıları, özelliklede karmaşık koordinasyon derecesindeki saldırılar büyük miktarda insanın ölümüne neden olabilir.[170]

Örneğin; Amerika'da yaşayan bir terörist, belli bir coğrafi sınıra bağlı kalmadan, Türkiye'deki hava kontrol sistemlerine girerek havada uçakların

---

[169]http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/USLaw.html
[170] İbid.

çarpışmasını veya doğal gaz sistemlerine aşırı yükleme yaparak havaya uçmasını sağlaması gibi.

İste bu siber terör saldırıları da bu madde kapsamında değerlendirilmesi mümkündür.

d) Ulusal Sınırları Dışında Yapılan Terör Eylemleriyle İlgili Yasalar (18 U.S.C §2332 (b) "Acts of Terrorism transcending national boundaries")

(1)Maddenin Özeti:

Her kim, ulusal sınırların dışında yapılan ve dış veya iç ticareti engelleyecek veya ABD sınırları dahilinde bir mülkiyeti veya bir alt yapıyı imha veya zarar vererek insanların can güvenliğine dair ciddi tehlike yaratan veya buna teşebbüs eden bir eyleme iştirak ederse ağırlaştırılmış hürriyeti bağlayıcı cezalar alır.

Bu ağırlaştırılmış cezalar;

Adam Öldürme: idam dahil her türlü hürriyeti bağlıyıcı ceza.

Adam Yaralama: 35 yıla kadar hapis cezası.

Adam Kaçırma: müebbet hapis cezası.

(2)Siber Teröre Uyarlanması:

Siber terör ulusal sınırla bağlı kalmadan işlenebilecek suçlardandır. Ayrıca siber teröristlerin en çok e- ticareti ve Çok Uluslu Şirketleri hedef alırlar. Bu nedenle siber terör suçları da bu madde içerisinde değerlendirebilir.[171]

e) USA Patriot Act (2001)

Bu yasa özellikle 11 Eylül saldırılarından sonra Amerika Birleşik Devletlerinin terör karşı savaşının yasal sonucudur . Bu yasayla getirilen yenilikleri şunlardır:[172]

- Bu yasanın 814. bölümüyle ilk defa siber terörle ilgili düzenlemeler yapılmıştır.
- Toplu Ulaşım Araçlarına yönelik saldırılar gibi yeni suçlar tanımlamıştır.
- Cezalar artırılmıştır.
- Teröristler ve onların eylemleri hakkında güvenlik güçlerine bilgi verenlerin ödülleri artırılmıştır.
- Güvenlik güçlerine, elektronik izleme yetkisi verilmiştir.
- Bu suçlar için yakalama, arama gibi yasal izinler tüm eyaletler de geçerli hale getirilmiştir.

2) İdari Düzenlemeler

Bunlar iki tanedir.[173]

a) Başkanın İdari Emri 13010 (Presidental Executive Order 13010)

Bu düzenlemedeki amaç özel sektörün siber terör ile ilgili önlemler almasını ve kritik alt yapı sistemlerinin korunmasıyla ilgili hükümetle işbirliğini geliştirmesini sağlamaktır.

---

[171] http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/USLaw.html
[172] İbid.
[173] İbid

b)Siber Uzayı Ulusal Koruma Stratejisi (National Strategy To Secure Cyber Space)

Bu planın amacı Amerika Birleşik Devletleri vatandaşlarının kullandıkları ve kontrol ettikleri siber uzay parçasını (e-mail adresleri, web sayfaları vb.) korumaları için sorumluk vermek ve yetkilendirmektir.

Bu amacı gerçekleştirmek için Federal Hükümet beş tane ulusal öncelik belirlemiştir.[174]

- Ulusal siber uzay güvenlik cevap sistemi yaratılması,
- Ulusal siber uzay güvenlik zaaflarını ve tehditlerini azaltma programının kurulması,
- Ulusal siber uzay güvenlik erken uyarı programının kurulması
- Kamusal siber uzayın korunması,
- Ulusal ve uluslararası güvenlik kurumları arasındaki işbirliğinin artırılmasıdır.

Amerika Birleşik Devletleri'ndeki yasal düzenlemelerin temel ilkeleri genel olarak belirlendikten sonra Birleşmiş Milletler ve Avrupa Konseyi gibi uluslararası örgütlerin uluslar arası terörle ilgili aldığı kararlardan yola çıkararak bunların siber teröre karşı duruşları incelenecektir.

B) Uluslararası Örgütlerin Uluslararası Terörle İlgili Kararları

Daha öncede ifade edildiği gibi, siber terör ulusal sınırların çok ötesinde etkiler doğurmaktadır. Bundan dolayı siber terörle mücadelede uluslararası işbirliği çok önemlidir. Ancak siber terörle ilgili uluslararası bir anlaşma yoktur. Bu nedenle uluslararası topluluğun siber teröre karşı tavrını ortaya koymak için uluslararası kuruluşların uluslararası terörle ilgili kararlar belirlenmiş ilke ve kararları siber teröre uyarlanmaya çalışılacaktır. Bunun içinde Birleşmiş Milletler ve Avrupa Konseyi kararları incelenecektir.

1) Birleşmiş Milletler Kararlarında Terörizm

BM, terörle mücadele konusunda ilk defa 1937 tarihli Cenevre Sözleşmesine atıfta bulunarak "Devletler arasında BM şartlarına uygun bir şekilde Dostane Münasebetler Kurma ve İşbirliği Yapılmasına Dair Milletlerarası Hukuk İlkeleri Hakkında Bildiri" ile kimsenin teröre destek olmamasını istemiştir.

Birleşmiş Milletler kurulduğu günden bugüne kadar, terör eylemlerine karşı uluslararası sözleşmeler ya da bildiriler hazırlayarak, üye ülkelerin imza ve onayına sunmaktadır. Terörle mücadelede demokratik ülkelerin normlarını oluşturan bu sözleşmelerden bazıları şunlardır:[175]

- 14 Eylül 1963 tarihinde Tokyo'da imzalanan, "Uçak içinde işlenen suçlar ve diğer eylemler hakkında sözleşme",
- 16 Aralık 1970 tarihinde Lahey'de imzalanan "Uçağın hukuka aykırı olarak ele geçirilmesinin ortadan kaldırılması hakkında sözleşme"
- 23 Eylül 1971 tarihinde Montreal'de imzalanan "Sivil havacılık güvenliğine karşı eylemler sözleşmesi" ve buna ek 24 Şubat 1988 tarihli protokol,
- 14 Aralık 1973 tarihinde New York'ta imzalanan "Diplomatik görevliler dahil uluslararası alanda koruma altındaki kimselere karşı işlenen suçların önlenmesi ve cezalandırılması hakkında sözleşme",
- 17 Aralık 1979 tarihinde New York'ta imzalanan "Rehin almaya karşı sözleşme",
- 10 Mart 1988 tarihinde Roma'da imzalanan "Güvenli deniz taşımacılığında yasaya aykırı eylemlerin ortadan kaldırılması hakkında sözleşme",

---

[174] İbid.
[175] http://www.egm.gov.tr/temuh/terorizm7.htm

- 1 Mart 1991 tarihinde Roma'da imzalanan "Kıta sahanlığı üzerine yerleştirilmiş sabit platformların güvenliğine karşı hukuk dışı eylemlerin kaldırılması hakkında protokol",
- 1 Mart 1991 tarihinde Montreal'de imzalanan "Arama amaçlı plastik patlayıcıların markalanması hakkında sözleşme",
- 9 Aralık 1994 tarihinde "Uluslararası Terörizmi Ortadan Kaldırmak İçin Alınacak Önlemler" başlıklı bir bildirge.
- Genel Kurul'un, Güvenlik Konseyi'nin 13 Ağustos 1998 gün ve 1189 (1998) sayılı kararı ile de tekrar edilen, Ekim 1970 tarih ve 2625 (XXV) sayılı kararı
- 11 Eylül 2001 tarihinde ABD'de meydana gelen terör saldırısından sonra ise 1373 sayılı BM Güvenlik Konseyi kararıdır.

Özelikle de Genel Kurul'un Ekim 1970 tarih ve 2625 sayılı kararını tekrar eden Güvenlik Konseyi'nin 1198 sayılı 1373 sayılı kararları uluslararası terörle ilgili genel ilkeler ortaya koymaktadır.

Buna göre;[176]

- Terörizmin uluslararası barış ve güvenliğe tehdit oluşturduğu açıkça ortaya konulmakta,
- Terörizme karşı bireysel veya toplu olarak meşru savunma hakkı tanınmakta,
- Terörizmle ilgili uluslararası sözleşmelerin tam olarak uygulanmalarının önemine değinilmekte,
- Bütün devletlerin terörizmin finansmanını önlemeye yönelik tedbirler almaları öngörülmekte,

---

[176] http://www.teror.gen.tr/turkce/makaleler/el_kaide_1.html2(çevrim içi) 12 Ağustos 2004

- Devletlere, terörizmin finansmanının suç teşkil etmesi, buna yönelik her türlü malvarlığının dondurulması, her türlü malvarlığı ve ekonomik değerin terörizme kaynaklık etmek üzere tedarikinin yasaklanması amacına yönelik yasal düzenlemeler yapmaları önerilmekte,

- Devletlere, teröristlere aktif veya pasif biçimde destek sağlamaktan kaçınmaları bildirilmekte,

- Teröristlere koruma sağlanmayacağı belirtilmekte,

- Terör eylemlerini işleyenlerin adalete teslimi öngörülmekte,

- Devletlerin, 1999 tarihli Terörizmin Finansmanının Önlenmesi Sözleşmesi dahil olmak üzere, ilgili bütün uluslararası antlaşmalara taraf olmaları tavsiye olunmakta,

- Sığınmacı statüsü tanınırken önce sığınma isteminde bulunan kişinin terör eylemlerine karışıp karışmadığının araştırılması gerektiği vurgulanmakta,

- Siyasî amaçlarla eylem yapmış olma gerekçesinin, terör sanıklarının iadesi talebinin reddine neden olmayacağı bildirilmekte,

- Güvenlik Konseyi çerçevesinde bir İzleme Komitesi kurulmakta ve devletlerin bu karar çerçevesinde aldıkları önlemleri kararın kabulünden itibaren 90 gün içinde Komiteye bildirmeleri ifade edilmektedir.

Yukarıda sayılan ilkeler terörizme karşı uluslararası topluluğun aldığı tedbirlerin boyutunu göstermektedir. Siber terör, küresel terörün alt kümesi olarak değerlendirilirse; bütün bu tedbirlerin siber terör eylemleri için geçerli olabileceği iddia edilebilir.

Birleşmiş Milletlerin terör ile ilgili kararlarını ve bu kararların siber terörle bağlantısını ortaya koyduktan sonra Avrupa Konseyi'nin terör ile ilgili aldığı karar ve bu kararların ortaya koyduğu ilkeleri inceleyebiliriz.

2)Avrupa Konseyi Kararlarında

a) Terörizmle ilgili kararları[177]

Avrupa Konseyi, kararları ile teröre karşı uluslararası önlemler alan etkin bir bölgesel kuruluştur. Avrupa Konseyi Danışma Meclisi, 1973'de aldığı 703 sayılı kararıyla uluslararası terörün bir suç olduğunu belirtmiş ve "teröriste ya ceza ver, ya da iade et" kuralı desteklenmiştir.

Konseyin 1974 tarihli 3 sayılı tavsiye kararı, uluslararası terörizm konusunda önem taşımaktadır.

27.01.1977'de, "Terörün Önlenmesi Hakkında Avrupa Sözleşmesi" de kapsamlı ve tek bir metin oluşturularak imzalanmış ve 1978'de yürürlüğe girmiştir. Strasbourg'da Türkiye dahil 17 ülke tarafından onaylanmış bulunan bu belgeyi, sadece Malta ve İrlanda tasdik etmemiştir. Sözleşmenin amacı, terör eylemlerini yapanların ceza almalarını sağlamaktır. Bu amaçla sözleşme, suçluların iadesi konusuna ağırlık vermektedir.

Ayrıca, Bakanlar Komitesi'nin 15.01.1982 tarih, 1 sayılı tavsiye kararı ile terör fiillerinin kovuşturulması ve cezalandırılması ile ilgili tavsiye kararı,

28.04.1982 tarih ve 941 sayılı tavsiye kararı,

Avrupa Konseyi İstişare Asamblesi'nin 1984'de benimsediği "Avrupa'da Terörizme Karşı Demokrasinin Savunulması" konusundaki 1982 sayılı kararı,

1984'de Madrit'te toplanan Adalet Bakanları 14. Konferansında ele alınan "Terörizm ve Uluslararası Organize Suçlara Karşı Mücadele İşbirliği"ne ilişkin 4 nolu karar önem taşımaktadır.

b) Avrupa Konseyi tarafından hazırlanan 23 Kasım 2001 tarihli Siber Suçlar Sözleşmesi:

Bu sözleşme "siber suçlar" sözleşmesi olmasına rağmen, bu sözleşme, daha çok sisteme yönelik haksız müdahaleleri suç olarak tanımlamıştır. Sözleşmenin II. Bölümü "Ulusal düzeyde alınabilecek önlemler" başlığını taşımakta ve bu önlemleri de maddi ceza hukuku ve ceza muhakemesi hukuku bakımından ikiye ayırmaktadır.[178]

II. Bölümün 1. Kısmı, ceza hukuku alanında yapılacak düzenlemelere ayrılmıştır. Suç olarak belirlenen fiiller dört alt başlık altında düzenlenmiştir. Bunlar sırasıyla; [179]

- Bilgisayar veri ve sistemlerinin gizliliğine, doğruluğuna ve elde edilebilirliğine karşı suçlar,
- Bilgisayarla ilgili suçlar (Computer-related offences),
- İçerikle ilgili suçlar,
- Telif hakları ve bağlantılı hakların ihlali ile ilgili suçlar şeklinde tasnif edilmiştir. Birinci kategoriyi oluşturan suçlar ise,
- 2.Madde : Yasadışı Erişim
- 3.Madde : Yasadışı Araya Girme
- 4.Madde : Verilere Müdahale
- 5.Madde : Sisteme müdahale
- 6. Madde : Cihazların Kötüye Kullanılması

Bu kategoriyi oluşturan suçlar, bilgisayarın kullanımıyla ortaya çıkan yeni suçlar oldukları için teknik özellikleri bakımından siber terörle ortak yönler taşırlar.

---

[177] http://www.bilecik.pol.tr/teroruluslararasiantlasmalardaterorizm.htm
[178] Ayhan Çankaya, s.5
[179] İbid.

Ayrıca aşağıda daha ayrıntılı olarak açıklanacağı üzere siber terör eylemlerinin maddi ceza hukuku ihlallerini kapsamaktadır.

Diğer kategorilerdeki suçlar ise, Bilgisayarla İlgili Dolandırıcılık ve İçerikle ilgili suçlardan ibarettir.

Ancak bu suçlar klasik suçların bilgisayar aracılığıyla işlenmesi sonucu meydana geldiklerinde siber terörle fazla ortak özellikleri yoktur. Nedenle de bu çalışmanın dışında kalmaktadır.

C)Türkiye Ve Diğer Ülkelerdeki Yasal Düzenlemeler

Bu bölümde ilk önce belli başlı sanayileşmiş ülkelerin bilgi teknolojilerinin yasadışı kullanımıyla ilgili yaptıkları yasal düzenlemeler özetlendikten sonra Türkiye de bu suçlarla ilişkin düzenlemeler incelenecektir.

Diğer ülkeler başlığı altında; İsrail, İtalya, Kanada ve Hindistan İnternetin yasadışı kullanımıyla ilgili yasal düzenlemeleri özet olarak verilecektir.

İsrail, Kanada ve Hindistan bilgi teknolojileri konusunda gelişmiş ülkeler olmaları nedeniyle; İtalya ise Türk Ceza Hukuku Geleneğine olan etkilerinden dolayı seçilmiştir.

Diğer Avrupa ülkelerinin bu çalışmada konu edilmemesinin nedeni bu ülkelerin konuyla ilgili düzenlemelerinin Siber Suçlar Sözleşmesiyle paralellik taşımasıdır.[180]

1) Diğer Ülkeler

a) İsrail

İsrail Emniyet Müdürlüğü, bilgisayar üzerinden işlenen suçlar konusuyla 1996 yılından itibaren ilgilenmeye başlamıştır.[181] Bu yılın başında, Sahtekarlık bünyesinde Bilgisayar Suçları Bölümü kurulmuştur. Anılan bölümdeki görevliler, esasen polis olup bilgisayar konusunda eğitimden geçirilmişlerdir. Bu birim, 1995 yılında

---

[180] İsmail Güneş, s.7

[181] www.emniyet.gov.tr/docs/RAPOR2.pdf (çevrim içi) 09 Temmuz 2004

yürürlüğe giren Bilgisayar Yasası ve polis soruşturma ve tutuklama kanunu çerçevesinde görev yapmaktadır. Gerektiğinde diğer polis birimlerince yürütülen soruşturmalara yardımcı olmaktadır.

Bilgisayar üzerinden işlenen suçlara karşı polis tarafından teknik önlemler alınması söz konusu değildir. Bu alanda diğer devlet kuruluşları ve özel şirketlere yardımcı olunmamaktadır. Söz konusu kuruluşlar kendi imkanları ile korunma sistemlerini oluşturmakta ve işletmektedirler.

İsrail hükümeti, bilgisayar suçları ile mücadele konusunda başta ABD olmak üzere, birçok Avrupa ülkesiyle işbirliği anlaşması imzalanmış bulunmaktadır.

b)İtalya

Bilgisayar suçları konusunda en son yasal düzenleme 23 Aralık 1993 tarihinde 547 sayılı kanun ile yapılmıştır.

İtalya da bilgi teknolojilerinin yasadışı kullanımıyla ilgili maddeler şöyledir:[182]

Yazılımları kısmen veya tamamen tahrip eden, değiştiren, bilgi veya iletişim sistemlerinin doğru çalışmasını engelleyen programlarla saldırıda bulunmaya 1 milyon liret, "500$" kadar para cezası verilir. Kamu yararına kullanılan tesislerin, bilgi sistemlerinin, veri, bilgi ve yazılımlarının içeriklerini tahrip etmek ve çalışmasını kesintiye uğratmaya 1 yıldan 4 yıla kadar hapis cezası verilir.

Bilgi veya iletişim sistemlerine fiziki olarak veya yazılım aracılığıyla yetkisiz olarak girmek, bilgi almak, alınan bilgileri yaymak, kayıtlar üzerinde tahribat yapmak veya sisteme maksatlı olarak yeni bilgiler ilave etmeye 3 yıla kadar hapis ve 10 milyon liret "5000$" kadar para cezası verilir.

Her türlü iletişimin engellenmesi, mahremiyetini, ihlal edilmesi, bu amaçla çeşitli cihaz ve sistemlerin kurularak enformatik ve telematik haberleşmenin kesintiye uğratılması, araya girilmesi veya iletişimin içeriğinin değiştirilmesi,

---

[182] İbid.

Gizli dokümanların içeriğinin açıklanması, gizli kalması gereken kamu veya özel dokümanların içeriğinin yasadışı olarak ele geçirilmesi ve açıklanmasına 3 yıla kadar hapis ve 2 milyon lirete kadar para cezası verilir.

c)Kanada[183]

Kanada'da siber terörizm ve benzeri teknolojik suçlar halen mevcut ceza kanunu kapsamında işlem görmektedir. Ceza kanununun 1985 yılından itibaren yapılan değişikliklerle bu tür faaliyetler de suç kapsamına alınmıştır. Ceza kanununun 342. maddesi uyarınca hakkı olmadan ve sahtekarlık yoluyla elektromanyetik, akustik, mekanik veya başka bir cihaz yoluyla bir bilgisayar sistemini dolaylı veya doğrudan kesintiye uğratan herkes cezai müeyyideyi gerektiren bir suçun faili durumundadır.

d)Hindistan[184]

Siber terörizm ve benzeri teknolojik suçlarla mücadele hususunda Hindistan Bilgi ve Teknoloji Bakanlığı tarafından yapılan çalışmalarda üç aşamalı bir yaklaşım izlenmiştir.

Birinci aşamada, bu tür suçların önlenmesi için gerekli fiziki tedbirler belirlenmiş ve kullanıcıların istifadesi için güvenlik rehberi hizmeti verilmeye başlanmıştır.

İkinci aşamada, başta savunma, dışişleri, içişleri bakanlıkları olmak üzere, hassas bilgilere ve teknolojilere sahip bakanlık ve kuruluşları, siber terörizm ve teknolojik suçların yaratabileceği tehlikeler ve bunlara karşı alınacak tedbirler hakkında bilgilendirme çalışmaları başlatılmış ve müteakip aşamada oluşturulacak yasal çerçeve için söz konusu kurulların destek ve deneyimlerine başvurulmuştur.

Son aşama yasal çerçevenin hazırlanmasıdır. Bu amaçla aralık 1999'da parlamentoya sunulan yasa tasarısı bahse konu suçların önlenmesi ve bu suçları yasal

---

[183] İbid.
[184] İbid.

bir çerçeveye oturtmayı ve devletin bu alandaki kontrol zafiyetini gidermeyi amaçlamaktadır.

2) Türkiye'deki yasal düzenlemeler

Bu bölümde öncelikle siber terör eylemleriyle ortak özellikler taşıyan bilgi sistemlerinin yasa dışı kullanımıyla meydana gelen suçlar incelenecektir.

Türkiye de bilgi sistemlerinin yasa dışı kullanımıyla oluşan suçlar Bilişim suçları olarak ifade edilir

Bilişim suçu kavramı Türk Ceza Hukukuna ilk defa 1991 yılında 3756 sayılı Kanunla girmiş olup Bilişim Alanında Suçlar başlığı altında Türk Ceza Kanunu'nun 525 inci maddesinin (a-b-c-d) bentlerindeki düzenlemeleri yapan Yasa koyucumuzun bilişim alanı ihlallerini bilişim suçu olarak isimlendirmeyi tercih ettiği görülmektedir.

525 inci maddenin (d) bendi, bilişim suçu işleyenler hakkında verilmesi gereken (kamu hizmetinden veya meslek veya sanat veya ticaretten muayyen bir süre yasaklanma) şeklindeki fer'i ceza ile ilgili olup (a),(b) ve (c) bentlerinde tarifi yapılıp müeyyideleri gösterilen beş ayrı suç tipinden bahsetmek mümkündür.[185]

Ancak 525inci maddenin (a) ve (b) bentleri bilgisayar aracılığıyla işlenen yeni suçları düzenlemektedir. Bu suçlar teknik özellikleri bakımından siber terör eylemleriyle paralellik gösterirler. Bu suçlar veri bütünlüğünü, yasal erişimi ve ağların kullanabilirliğini ihlal eden eylemlerdir.

---

[185] Cevat Özel **"Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı"** (Çevrim içi) www.hukukcu.com/bilimsel/ kitaplar/bilisimsuclari_TCKtasarisi.htm - 96k 16 Temmuz 2004

Buna göre.

- 525(a) Başkasına zarar vermek için sistemde bulunan bilgileri kullanmak, nakletmek, çoğaltmak suçunu düzenler
- 525(b) Sistemi, verileri tahrip etmeyi kapsamaktadır.[186]

Şu an yürürlükte olan TCK bilgisayar kullanılarak oluşan yeni suçlarları bu şekilde düzenlemiştir.

Bu düzenlemenin yanısıra yakında yasalaşacak olan Türk Ceza Kanunu Tasarısının İkinci Kitabının İkinci Kısmının Dokuzuncu Bölümü "Bilişim Alanında Suçlar" başlığını taşımakta olup bu bölümde 346 inci madde ile başlayıp 351 inci madde ile sona eren yedi ayrı madde mevcuttur.[187]

Ancak bu tasarının 346 ve 347 maddeleri de bilgisayar aracılıyla işlenen yeni suçları düzenlemektedir.Nedenle bu çalışma da sadece 346. ve 347 . maddelerin ayrıntılı açılımı yapılacaktır.

a) 346. madde

346. madde şöyledir:[188]

Bilişim Sistemine girme,verileri tahrip etme ve bozma

Madde 346- Bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve üç milyar liraya kadar ağır para cezası verilir

Bu fiil nedeniyle sistemin içerdiği verileri yok edilir veya değişirse faile iki yıldan dört yıla kadar hapis ve beş milyar liradan onbeş milyar liraya kadar ağır para cezası verilir.

Bu suçlara teşebbüs halinde tamamlanmış suç cezası verilir

Birinci fikra, ne maksatla olursa olsun hukuka aykırı olarak sisteme girilmesini suç olarak kabul ettiğinden sisteme haksız olarak genel kasıtla girilmesi

---

[186]Cevat Özel **"BİLİŞİM-İNTERNET SUÇLARI"** (Çevrim içi) www.hukukcu.com/bilimsel/ kitaplar/bilisimsuclari_TCKtasarisi.htm - 96k 16 Temmuz 2004
[187] İbid.
[188] http:// www.tbmm.gov.tr

suçun oluşması için yeterlidir.[189] Nedenle failin belirli ve özel bir saikle hareket etmesi aranmamaktadır.

İkinci fıkra, yeni bir suç türü ihdas etmemekle birlikte ilk fıkraya bağlı bir ağırlaştırıcı sebebi düzenlemektedir.Failin hangi nedenle olursa olsun sisteme haksız ve kasıtlı bir şekilde girmesi sonucu sistemde bulunan veriler imha edilir veya değiştirilirse sadece bu neticeden dolayı fail daha ağır bir ceza ile cezalandırılmaktadır.[190]

Burada failin sisteme girmesi ve bu girme sonucunda verilerin imha edilmesi ya da değiştirilmesi yeterli olup failin ayrıca bu neticeyi isteyip istememesi önemli değildir. Üçüncü fıkra, sisteme haksız olarak girmeye teşebbüs edilmesi halinde de faile suç tamamlanmış gibi ceza verilmesi söz konusudur.

b)347. madde:

347. madde şöyledir:[191]

Sistemi engelleme, bozma, haksız yere yarar sağlama

Madde 347- Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve üç milyar liradan onbeşmilyar liraya kadar ağır para cezası verilir

Bilişim sistemine hukuka aykırı olarak veriler sokan veya sistemin içerdiği verileri yok eden veya değiştiren kimseye üç yıldan altı yıla kadar hapis ve on milyar liradan otuz milyar liraya kadar ağır para cezası verilir iki yıldan altı yıla kadar hapis ve beş milyar liradan yirmi milyar liraya kadar ağır hapis cezası verilir

Yukarıdaki fıkrada belirtilen eylemlerle fail başkasının zararına ve kendisinin veya başkasının yararına haksız bir çıkar sağlarsa iki yıldan altı yıla kadar hapis ve beş milyardan yirmi milyara kadar ağır para cezasına hükmedilir

Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir

Birinci fıkra, bilişim sistemlerine yönelik olarak işlenen bozma, engelleme gibi ızrar fiillerini özel bir suç haline getirmektedir. [192]

---

[189] Cevat Özel, Türk Ceza Kanunu Tasarısı
[190] İbid.
[191] http:// www.tbmm.gov.tr

Burada koruma altına alınan şey, bilgi sisteminin diğer bir deyişle bilgisayarın fiziki varlığı ve sistemin işlemesini sağlayan bütün diğer unsurlardır.

İkinci fıkra, ise bilgi sistemine veri sokulması, verilerin yok edilmesi, değiştirilmesi suç haline getirilmiş olup bu fıkranın uygulanabilmesi için failin bu neticelerin gerçekleşmesine yönelik özel bir kasıtla hareket etmesi gerekmektedir.

Üçüncü fıkra, failin, yukarıdaki iki fıkrada sayılan eylemleri ile başkasının zararına, kendisinin veya başkasının yararına haksız maddi yarar elde etmek için bilgi sistemine girmesini cezalandırmaktadır.

347 nci maddenin ilk fıkrasındaki ceza miktarı bir yıldan üç yıla kadar hapis,bir milyar liradan beş milyar liraya kadar ağır para cezasıdır.

Bu fıkradaki eylemin üçüncü fıkraya uyması durumunda ağırlaştırıcı hal sebebi ile ceza miktarının iki yıldan altı yıla kadar hapis ve iki milyar liradan on milyar liraya kadar ağır para cezasına çıkarıldığı görülmektedir.

İkinci fıkradaki ceza miktarı ise üç yıldan altı yıla kadar hapis ve üç milyar liradan on milyar liraya kadar ağır para cezasıdır.

Ancak üçüncü fıkradaki haksız çıkar sağlama eyleminin ikinci fıkradaki hale uygun olarak işlenmesi ve ağırlaştırıcı sebebin gerçekleşmesi durumunda ikinci fıkrada öngörülenden daha az hapis ve ağır para cezasının üst sınır olarak belirlenmesi bir çelişki oluşturmaktadır.

Yukarıda da ifade edildiği gibi üçüncü fıkradaki hapis cezasının üst sınırı iki yıl, ağır para cezasının asgari haddi ise iki milyar liradır ve bu miktarlar ikinci fıkradaki üst sınırın da altındadır.

347 nci maddedeki suçlara teşebbüs halinde de faile suç tamamlanmış gibi ceza verilecektir.

---

[192] Cevat Özel, Türk Ceza Kanunu Tasarısı

Türk Ceza Mevzuatında bilgi sistemlerinin yasa dışı kullanımıyla ilgili yasal düzenlemelerdeki suçların siber terör eylemleriyle olan ortak özelliklerini inceledikten sonra şimdi siber terör eylemlerinin hukuksal boyutuna geçebiliriz.

D) SİBER TERÖR EYLEMLERİNİN HUKUKİ DEĞERLENDİRİLMESİ

1)Siber Terör Eylemlerinin Ceza Hukukundaki Düzenleme Alanları

Literatürde, siber terör eylemleri sonucunda meydana hukuki ihlaller; veri suçları, ağ suçları, erişim suçları ve ilgili suçlar şeklinde üçlü bir ayrıma tabi tutulmaktadır.

Bu ayrıma göre:[193]

a) Veri İhlali :

Veri, ham bilginin bilgi teknolojileri alanında kullanılabilecek şekilde işlenmesi sonucunda oluşmaktadır. Bilgi teknolojilerinin veri iletimi eksenli işleyişi, öncelikle maddi ceza hukuku normları ile verilere karşı gerçekleştirecek hukuka aykırı fiilleri müeyyide altına almayı gerekli kılmıştır. Verilere karşı gerçekleştirilecek ihlaller şu alt gruplar altında incelenmektedir:

(1) Verilere Müdahale Edilmesi (Data Interception) **:**

Bu ihlal, aktarım esnasında 3. kişiler tarafından yapılan hukuka aykırı müdahaleye maruz kalınmasıyla gerçekleşir. Bu müdahale verilerin aktarımının engellenmesi, aktarım rotalarının değiştirilmesi, verilerin aktarım sırasında 3.kişiler tarafından ele geçirilmesi şeklinde ortaya çıkmaktadır.[194]

---

[193] Mahmut KOCA **"Bilişim Teknolojileri ve Ceza Hukuku"** Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu Av. Gökçe ÜZEL ed., (Çevrim İçi) http:/www.taek.gov.tr/taek/bet/pdf/hukuk_cg_raporu.pdf s.50 23 Temmuz 2004

[194] Mehmet Emin BİLGE **"Bilişim Teknolojileri Alanındaki Suçlar ve Mevcut Durum"**, Türkiye Bilişim Şurasıhukuk Çalışma Grubu Raporu Av. Gökçe ÜZEL ed., (Çevrim İçi) http:/www.taek.gov.tr/taek/bet/pdf/hukuk_cg_raporu.pdf s.65 23 Temmuz 2004

Bu ihlalin gerçekleşebilmesi için, verilerin aktarım esnasında, daha açık bir deyişle verinin elde edildiği veya saklandığı kaynaktan gönderilmesiyle başlayıp belirlenen hedef noktaya ulaşması arasında geçen süreç içersinde, bir müdahaleye uğraması gerekmektedir.

(2)Verilerin Değiştirilmesi (Data Modification) **:**

Literatürde bu suç seçimlik hareketli bir ihlal olarak değerlendirilmektedir. Böylelikle verilerin değiştirilmesi, tahrip edilmesi veya silinmesi eylemleri cezai müeyyide altına alınmaktadır. [195]

Bu başlık altında incelenen eylemler yukarıda belirtilen verilere müdahale edilmesi ihlalinden, işlendiği ortamda bir sınırlama olmaması açısından kesin bir çizgiyle ayrılmaktadır.

Bu ihlalin oluşabilmesi için verilerin bulunduğu ortamın bir önemi yoktur. Verilerin depolanmış bir şekilde saklandığı bir ortamda veya verilerin iletimi sırasında yukarıdaki seçimlik hareketlerin her hangi birinin gerçekleştirilmesi ile bu suç oluşur. Buradan hareketle, aktarım sırasında verilere müdahale edilerek bu veriler değiştirilebilir veya tahrip edilebilir veya silinebilirler .

Bu durum aynı zamanda iki ayrı suçun işlenmesi sonucunu doğurur ve bu halde her iki suç içtima edilerek fail cezalandırılır.[196]

(3) Veri Hırsızlığı (*Data Theft*) :

Veri hırsızlığı başlığında verilerin alınması ve kopyalanması eylemleri cezalandırılmaktadır.

b)Ağ Sistemleri İhlali :

İkinci ihlal grubu ağ suçlarıdır. Ağ sistemi verilerin bir yerden bir yere iletilmesini sağlamaktadır. Ağ ihlalleri de iki ana başlık altında incelenmektedir.

---

[195] Mahmut KOCA, s.52
[196] İbid.

(1)Ağ Engellemesi (Network Interference) :

Bu ihlal grubunda ağın tamamına veya bir bölümüne diğer kişilerin erişiminin engellenmesi veya önlenmesi durumu ortaya çıkmaktadır. [197]

Bu ihlal çok değişik yöntemler kullanılarak gerçekleştirilebilir. En çok görülen şekli web siteleri ve ISS üzerine yağdırılan DDOS (distributed denial of service) saldırılarıdır.

Ağ engellemesi sistemin gayri fiziki bileşenlerine yönelmiş eylemleri bir araya getirilmektedir.

"Hacking", "cracking", DDOS bu ihlalin farklı formlarda işleniş şekilleridir . Kara Avrupa'sı Hukuk sisteminde Hacking, Cracking, DDOS gibi ihlaller ayrı birer suç tipi olarak değil, tek bir suç olarak tanımlanmıştır.

Ancak Anglo Amerikan ve Anglo Sakson Hukuk sistemlerinde ise sayılan ihlal biçimleri ayrı ayrı suç olarak kabul edilmesi yöntemi izlenmektedir.

Fakat bu iki farklı kanunlaştırma biçimi içerisinde doğru olan Kara Avrupa'sı sistemidir. Çünkü bu suçların tek tek belirlenmesi zorunluluğu ortadan kalkacaktır. Özellikle teknolojinin hızla gelişiyor olması çerçeve bir düzenlemeyi kaçınılmaz kılmaktadır. Eğer, tek tek bu ihlalleri sayarsanız, yarın ortaya çıkacak yeni ihlal biçiminin yaptırımsız kalması kaçınılmaz olacaktır.

Bu türün ikinci ihlali ise ağ sobatajdır.

(2) Ağ Sabotajı (Network Sabotage) :

Ağ sabotajı, ağın veya sistemin tahrip edilmesi yahut değişikliğe uğratılması sonucu ortaya çıkmaktadır. Burada daha çok sistemin fiziki bileşenlerine yönelmiş bir hareket vardır. Yani burada ortaya konulan suç ceza kanunumuzda düzenlenen nas' ızrar suçunun özel bir çeşidini oluşturmaktadır.[198]

---

[197] İbid.
[198] İbid., s53

c)Erişim İhlalleri :

Bu ihlal izinsiz veya yasadışı erişimden meydana gelir. Buna göre;

(1)Yetkisiz Erişim (Unauthorized Access) :

Yetkisiz erişim, yetkisiz kişilerin, sistem içersindeki verilere izinsiz ulaşması veya yetkisiz 3.şahısların bu verilere izinsiz ulaşmasına sağlamasıdır.[199]

Ancak bu ihlalin oluşabilmesi için özel bir kasta gerek vardır. Çünkü sırf merak amacıyla, hiçbir hukuka aykırı amacı olmadan, sisteme zarar vermeyen, hatta sadece sisteme girip hiçbir bilgiye erişmeyen kişileri sırf yetkisi olmadığından ötürü cezalandırmak, hakkaniyet ve ölçülülük ilkesine aykırıdır.

Ayrıca, özel bir kastın aranması, bilgi teknolojilerinin gelişiminde önemli rol oynayan, güvenlik ve test amaçlı sistem erişimlerinin suç kapsamı dışında bırakılması yararını da getirecektir.

(2)Virüs Yayımı (Virüs Dissemination) :

Virüs yayımı olarak belirlenen hareket, bilgi ve iletişim sistemlerinin donanımsal veya yazılımsal bileşenlerine zarar vermek amacıyla gerçekleştirilen ihlaldir.[200]

Virüs yayımı, küresel ölçekte büyük zararlara yol açması nedeniyle bir çok ülke yasalarında konuyla ilgili ayrı bir başlık altında düzenlemeye gidilmiştir. Ancak bu ihlalin esas düzenleme alanı, ağ sistemleri veya veri ihlalleri kapsayan suç tiplerinde olması uygun olacaktır.

Çünkü virüsü üreten ve bu virüsü kasten yayan kişilerin esas amacı verilere veya ağ sistemlerine zarar vermektir. Yoksa virüs yayımının müstakil bir suç teşkil etmesi bir zorunluluk değildir. Eğer virüs yayımı ile ilgili düzenlemeye gidilecek ise

---

[199] Cevat Özel, Türk Ceza Kanunu Tasarısı

virüs üretmeyi bir tehlike suçu olarak yaratıp, virüs sistemlere herhangi bir zarar vermese dahi virüsü kasten diğer sistemlere de yayan kişilerin cezalandırılmasına gidilmesi en akılcı yol olacaktır.[201]

Bu başlıklar altında incelenen siber terör eylemlerinin neden olduğu ihlallerde oluşabilecek iştirak teşebbüs vb. gibi, hususlarda şu an için hukuki bir boşluk olduğundan bu konuda ceza hukukunun genel hükümlerini uygulanması gereklidir.

Siber terör eylemlerinde siber suçlar gibi neticesi hareketle birleşik suçlardandır.[202] Nedenle siber terör eylemlerinde sadece eksik teşebbüs söz konusu olabilir.

2) Siber Terör Eylemlerinde Kişilerin Ve Özellikle İnternet Servis Sağlayıcıların Sorumluluk Rejimi

Ceza hukukunda asıl olan, bir kişinin kendi işlediği bir fiil sebebiyle sorumlu olmasıdır. Ancak toplumsal yaşamın getirdiği birliktelik gereği; ceza kanunlarında bireyin bulunduğu topluluğun başka bir üyesinin eylemi sebebiyle suçtan sorumlu olduğu durumlar yaratılmıştır.

İnternetin teknolojik üstünlüğünden dolayı klasik iletişim araçları için, mevcut kanunlarla düzenlenmiş sorumluluk rejimleri, İnternetle uyuşmamaktadır.[203]

Burada yapılması gereken, internetteki mevcut yapıların teknik anlamda nasıl işlediğini açıklıkla ortaya koyup, sorumluluk sahibi süjelerin objektif kriterlerle tespit edilmesidir.[204]

İnterneti kullanmamızı sağlayan İSS'lerdir. İSS'ler yani İnternet Servis Sağlayıcıları sanal ortamının en önemli kurumlarından biridir. Servis sağlayıcılar

---

[200] White paer s.45
[201] Mahmut Koca, s.52
[202] Hasan Sınar **İnternet ve Ceza Hukuku,** İstanbul, Beta,2001, s.129
[203] Mahmut Koca s.52
[204] İbid.

işlevleri "bireylerin ya da kurumların internete erişimlerini sağlama", "içerik hazırlama", "sunucu kiralama ve sunucu barındırma" olarak sayılabilir.[205]

Servis sağlayıcının ceza sorumluluğunun hangi koşullarda bulunacağı konusunda, Alman Tele Hizmetler Kanunu (Teledienstegesetz-TDG) örnek bir düzenleme yapmıştır. Bu kanuna göre, servis sağlayıcılar, sunucularında depoladığı başkalarına ait suç içerikli verilerden, ancak bu verilerin bu niteliğinden haberdar olmaları ve ayrıca bu verilerin İnternet üzerinden erişilebilir kılınmasını teknik olarak önleme olanağına sahip bulunmaları durumunda sorumlu tutulmaktadırlar.[206]

Ancak bu düzenleme siber terör eylemleri için geçerli olamaz.

Çünkü. siber teröristler, teknolojik üstünlüklerini sayesinde servis sağlayıcılarının işlevlerini; izinsiz kullanırlar veya İSS'lerin siber terör eylemlerine iştirak ettiklerinden haberleri bile olmaz.

Zaten İnternetin doğduğu yer olan Amerika Birleşik Devletlerinde ise İSS'lerin, bazı istisnalar dışında, ne hukuki ne de cezai sorumluluğu kabul edilmektedir. Bu ülkede İSS'lerin sorumlu tutulduğu yegane durum, İnternet üzerinden yapılan ve Fikri Mülkiyet Haklarını konu alan ihlallerdir.[207]

Siber terör eylemleri bilindiği gibi siber uzayda gerçekleştirilmektedir.Siber uzayda cezalandırma yetkisinin kime ait olduğu tartışmalıdır.Bu yüzden siber terör eylemlerinde uluslararası yetki sorunu ortaya çıkmaktadır

3) Uluslararası Yetki Sorunu

Siber Uzay (Cyberspace) denilen sanal ortamda ülkelerin cezalandırma yetkilerini belirlemek güç bir uğraştır.

Ülkelerin egemenlik yetkilerinin sınırını üç yüz yıl önce ortaya koyan Westphalia Sözleşmesi'nin ve yüzyılımızın başında uluslararası hukuk alanında kurallarını belirleyen Montevideo Konvansiyonu oluşturduğu ortak anlayış

---

[205] Mehmet Emin Bilge, s.70
[206] İbid.
[207] İbid

çerçevesinde şekillenen ilkeler, geleneksel anlamda devletin egemenlik alanının sınırlarını çizmektedir.[208]

Siber terör eylemlerinde hareketle, netice; ülkenin coğrafi sınırlarına ve vatandaşlık kriterlerine göre belirlenmiş farklı egemenlik alanlarında gerçekleşmektedir.

Doktrinde de bu tip suçlar mesafe suçu denilmektedir ve bu tür suçların nerede işlenmiş sayılacağı konusunda değişik fikirler bulunmaktadır.

Doktrinde ve bir çok ülke yasasında kabul edilen görüş ise, karma görüş olarak adlandırılan ve gerek hareketin yapıldığı ve gerekse ilk ve doğrudan neticenin doğduğu yerlerde suçun işlendiğini kabul eden görüştür. Yeni TCK Tasarısı da bu görüsü benimsemiştir.

Bu durumda siber terör eylemlerinde hareketin yapıldığı ve gerekse ilk ve doğrudan neticenin doğduğu gerçekleşmiş olacağından cezalandırma yetkisi hem hareketin hem de neticenin gerçekleştiği ülkede olacaktır.[209]

Sonuçta siber terör eylemlerinin yeni Ceza Kanunlarında düzenlenme zorunluluğu hukuksal bir gerçekliktir.

Çünkü bu başlık altında yapılan tüm değerlendirmeler aslında siber suçlarla ilgili düzenlemelerin kıyas yapılması sonucunda çıkmıştır.

Ancak Ceza Hukukunun Genel İlkelerine göre ceza hukukunda kıyasın yasak olması ve Suçta ve Cezada Kanunilik İlkesi; siber terörle ilgili yasal düzenlemeler yapılmasını kaçınılmaz kılmaktadır.

Fakat bu değerlendirmeler, sadece gerekli yasal düzenlemeler için, temel teşkil edebilir.

---

[208] Av. Yasin Beceni **"SİBER UZAYDA MAHREMİYET"**, II Türkiye Bilişim Şurası Hukuk Çalışma Grubu, (Çevrimiçi) 27 Temmuz 2004
http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf s3

[209] Hasan Sınar, s.127-129

SONUÇ

Giriş bölümünde de belirtildiği gibi şu an için siber terör varsayımsal olarak vardır.

Bu gün literatürde verilen tüm siber eylem örnekleri sonuç itibariyle ya terör örgütlerinin İnterneti yasal sınırları içinde kullanmaları yada siber terörün en alt düzeyi olan basit yapılandırılmamış siber terör eylemleridir.

Çünkü hiçbir terör örgütünün gerçek, saf siber terör eylemlerini gerçekleştirecek kapasitesi yoktur.

Ancak bu durum insanlık için bu tehlikenin geçtiği anlamına gelmez. Çünkü başta Amerika Birleşik Devletleri olmak üzere büyük devletlerin bu güce sahip olduğu bir gerçektir.

Eğer ilk atom bombasının Amerika Birleşik Devletleri tarafından atıldığı hatırlanırsa bu tehlikenin kapımızı çalmaya hazırlandığını kolayca kavrarız.

Ayrıca teknolojinin hızla ilerlemesi yakın bir gelecekte teröristlerinde bu güce sahip olabilme olasılığını yükseltmektedir.

Siber terörün varsayımsal bir kavram olmasının yansıması da kendisini hukuk dünyasında da göstermiştir. Siber terörle ilgili bir yasal düzenleme sadece Amerika Birleşik Devletlerinin Patriot yasasının 814. bölümünde yapılmıştır.

Ancak bu yasanında 11 Eylül saldırılarından sonra yapılmış olması, insanlığın bu büyük tehlikeden korunmasını sağlayacak olan uluslararası topluluğun harekete geçmesi için milyonlarca masum insanın ölmesini bekleyeceğimiz anlamına gelmektedir.

KAYNAKÇA

Altuğ, Yılmaz: **Terörün Anatomisi,**İstanbul,Altın Kitaplar,1999

Arkış, Barış: **"Vüristen Koruma Yolları"** (Çevrim içi) http://www.barisarkis.com/tyorum/tyorumfiles/BarisArkis_Virusten_Korunma.pdf 27 Temmuz 2004

Arquilla, John,, Ronfeldt, David ed.: **Networks And Netwars,** Santa Monica,,Rand,2001

Baker: Stewart A.: **"ShouldSpies Be Cops"** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,NewYork,Thunder's Mouth, 1996,s.408-420

Bearden, Tom: **"Hacking Around" transcript of The NewsHour with Jim Lehrer,** (Çevrim içi) http://www.pbs.org/newshour 08 Mart 2003

Beceni,Yasin:, **"SİBER UZAYDA MAHREMİYET",** II..Türkiye Bilişim Şurası Hukuk Çalışma Grubu, (Çevrimiçi) 27 Temmuz 2004 http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf

Beth Givens, **"İnformation Warfare: The Personal Front",** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.494-497

Bilge, Mehmet Emin: **"Bilişim Teknolojileri Alanındaki Suçlar ve Mevcut Durum",** Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu Av. Gökçe ÜZEL ed., (Çevrim İçi) http:/www.taek.gov.tr/taek/bet/pdf/hukuk_cg_raporu.pdf s.65 23 Temmuz 2004

Blaeses, Christophe: **"Virüsler: herkesi endişelendiren konu"**, çev. Hüseyin Kaya,Gülşen Taşkın,Sevda Üsküplü, D. Melih Naim (Çevrim içi) www.linuxfocus.org/Turkce/ September2002/article255.shtml 25 Temmuz 2004

Chomsky, Noam, vd ed: **Terörizm Efsanesi,** çev:Bahadır Sına Şener, Ankara,Ayraç,1999

Class 1: **Personal İnformation Warfare, İnformatin Warfare,** ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.473- 486

Class 2: **Corparete İnformation Warfare,** İnformatin Warfare, ed: Wınn Schwartau, İkinci baskı,NewYork,Thunder's Mouth, 1996, s.513-533

Class 3 **: Global İnformation Warfare İnformatin Warfare**, ed: Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996, s.540-561

Collin, Barry C.: **" Cyber Terrorism From Virtual Darkness: New Weapons in a Timeless Battle"**, (Çevrim içi) http://www.nici.org/Research/Pubs/98-5.htm 13 Kasım 2001

Collin, Barry C: **"The Future of CyberTerrorism:Where the Physical and Virtual Worlds Converge"**(Çevrim içi) http://afgen.com/terrorism1.html 15 Mayıs2004

Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. (Çevrim içi) Departmentof Justice, http://www.cybercrime.gov. 08 temmuz 2004

Copp, Carlo: **" The E-bomb"** Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.296-334

Cordesman,Anthony H., Cordesman, Justin G., **Cyber Threat,İnformation Warfare and Criticial İnfrastructure** Protection,Londan,Praeger

Çankaya, Ayhan: **"Bilişim Suçları",** (Çevrim içi) www.egm.gov.tr/sempozyum2003/ Bildiriler/Bilisim_Suclari.pdf 03 Temmuz.2004

Danitz Tiffany, WarrenP.Strobel: **"Networkıng Dıssent:Cyber Actıvısts The İnternet To Promote Democracy İn Burma"** Networks And Netwars, ed:John Arquilla, David RonFeldt,Santa Monica, Rand, 2001s.129-171

Denning, Dorothy E.: **"Is Cyber Terror Next?",** (Çevrim içi) http://www.ssrc.org/sept11/essays/denning.htm 12 Aralık 2003

Denning, Dorothy E.: , **"CYBERTERRORISM"** (Çevrim içi) http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html 03Nisan2004

Denning, Dorothy E.: **"Information Warfare and Security"** (Çevrim içi) http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html 02 Nisan 2003)

Deutch, John M.: **"Nonlethal Weapons"** Wınn Schwartau, İkinci baskı,NewYork,Thunder's Mouth, 1996,s.459-462

Deutch, John M.: **"Worldwide Threat Assesment"** Wınn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996, s,453-459

Güler, Korhan: **"İnternete Bireysel Güvenlik"** (Çevrimi içi)- seminer.linux.org.tr/seminer-notlari/ senlik-2002/ankara-bireysel.ppt18 Ağustos 2004

Güneş, İsmail: **"İnternette Güvenlik ve Denetim: Masumiyet Yitiriliyor mu?"** (Çevrimiçi), http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=243, 08 Haziran 2004.

Hayward,Douglas: **"Hacker's Dark Side Gets Even Darker."** (Çevrim içi) http://www.techwire.com/,01 Mart 2003

Hımanen, Pekka: **The Hacker Ethic**, Newyork Randon House Trade Paperback, , 2001

http:/www.taek.gov.tr/taek/bet/pdf/hukuk_cg_raporu.pdf 23 Temmuz 2004 s.64-72

Ira Winkler , **"Dairy of Industrial Spy"** İnformatin Warfare, ed: Winn Schwartau, İkinci baskı,NewYork,Thunder's Mouth, 1996,s.537-540

Karadeniz, Taccettin: **" Dos"** (Çevim içi)
08Ağustos.2003http://www.olympos.org/article/articleview/403/1/10

Koca, Mahmut: **"Bilişim Teknolojileri ve Ceza Hukuku"** Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu Av. Gökçe ÜZEL ed., (Çevrim içi)
http:/www.taek.gov.tr/taek/bet/pdf/hukuk_cg_raporu.pdf 23 Temmuz 2004 s 50-64

Littleton, Matthew J.:, **"İnformatıon Age Teroroism"**, (Çevrim içi)
http://www.fas.org/irp/threat/cyber/docs/npgs/app_a.htm#frmconve 04 Nisan 2004

MarkAldrich, **"Personal İnformation Warfare"**, İnformatin Warfare, ed: Winn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.488-494

Nagpel, Rohas: **"Cyber terrorism İnThe Context Of Glabalization"** (Çevrim içi)
http://www.asianlaws.org/cyberlaw/library/cc/rn_ct.htm#21 23 Mayıs 2002

Natıonal Strategy To Secure Cyberspace, (Çevrim içi)
www.dhs.gov/interweb/assetlibrary/ National_Cyberspace_Strategy.pdf 11 Mart2004

Örgün, Faruk: **Küresel Terör,** İstanbul,Okumuş Adam,2001

Özcan, Mehmet **"Yeni Milenyım Yeni Tehdit"**, Siber Terör Polis Dergisi ,Sayı:34 s.170-180

Özdilek, Ali Osman: **" KURTLAR VE ZOMBİLER:Worm'ların ve DDoS Ataklarının Hukuki İncelemesi"** (çevrim içi)
http://www.hukukcu.com/bilimsel/kitaplar/wormlarhukuki.ht 12 Haziran 2004

Özel, Cevat: **"Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı"** (Çevrim içi) www.hukukcu.com/bilimsel/
kitaplar/bilisimsuclari_TCKtasarisi.htm - 96k 16 Temmuz 2004

Özel, Cevat: **"BİLİŞİM-İNTERNET SUÇLARI"** (Çevrim içi)
www.hukukcu.com/bilimsel/ kitaplar/bilisimsuclari_TCKtasarisi.htm - 96k 16 Temmuz 2004

Özer Zuhal: **"Nanoteknoloji"**, Bilim Çocuk (Çevrimiçi)
www.biltek.tubitak.gov.tr/cocuk/01/eylul/**nano**.pdf - 12 Mayıs 2004

Patterns of Global Terrorism: 1997 (Çevrim içi)< 30 Haziran 2004

Pınerıo, R.J: **Cyber Teror**,NewYork, Forge, 2003

Pollitt, Mark M: **"CYBERTERRORISM - Fact or Fancy?** (Çevrim içi)
http://www.cs.georgetown.edu/%7Edenning/infosec/pollitt.html 08 Haziran 2004

RonFelt David,Arquilla John: **"Emergence and Influence Zapatista"** Networks And Netwars, ed:John Arquilla, David RonFeldt,Santa Monica, Rand, 2001,s.171-201

Schwartau, Winn: **"More About HERF"** Winn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.288-296

Schwartau, Winn: **"The Econo-Politics of İnformation Warfare"** İnformatin Warfare, ed: Winn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth,1996, s 49-71

Schwartau,Winn ed.: **İnformatin Warfare**, ed: İkinci baskı,"NewYork,Thunder's Mouth,

Schwartau,Winn: **"An İntroduction To İnformation Warfare"** İnformatin Warfare, ed: Winn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996, s 27-43

Schwartau,Winn: **Cyber Shock,** NewYork,Thunder's Mouth

Sınar, Hasan: **İnternet ve Ceza Hukuku,** İstanbul, Beta, 2001

Sonwale, Pratik Mehmedagic, Sulejemen: **"Computersve Society"**,(Çevrimiçi) http://www.iit.edu/~mehmsul/projects/cs484 02.Nisan 2003

Sullivan John P: **"Gangs, Hooligans,And Anarchısts- The VanGuard Of NetwarsİnThe Streets"**, Networks And Netwars, ed:John Arquilla, David RonFeldt,Santa Monica, Rand, 2001, s.99-129

Szafranki Richard: **"An İnformation Warfare", İnformatin Warfare**, ed: Winn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.115-125

Telecommunication and Information Services Policies, Internet Infrastructure Indicators, (Çevrim içi) http://www.oecd.org/dsti/. 24Mayıs2004

Terörrism in USA 1999 21st Century Guide to FBI

Tosun, Yalçın: **"Ağ Güvenliği Proje I Vekil Sunucular Ve Güvenlik Duvarları"** (Çevrim içi) www.cs.itu.edu.tr/~orencik/Vekil Sunucular ve Guvenlik Duvarlari.ppt 23 Haziran 2004

Tüfekçioğlu, Fehime: **"Zarar Verici Lojik"**, (Çevrimiçi) www.ce.itu.edu.tr/lisansustu/dersler/ blg510/2003/sunumlar/504031511_rapor.pdf 09 Mayıs 2004

Weise Liz: **"No privacy"** İnformatin Warfare, ed: Winn Schwartau, İkinci baskı,"NewYork,Thunder's Mouth, 1996,s.487

White paper: Cyberterror Prospects and Implications"(Çevrim içi) http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf 05 Şubat 2003

Zanini Michele,SeanJ.A. Edwards: **"Networking of Teror İn The İnformation Age"**, Networks And Netwars, ed: John Arquilla, David Ronfeldt,Santa Monica,,Rand,2001

WEB SİTELERİ

http://www.-cs.etsu.edu/gotterbarn/stdtppr.htm (Çevrim içi) 20 Ocak 2002

http:// www.nipc.gov

http://www.unc.edu/courses/2004spring/law/357c/001/projects/knouff/Cyberterrorism/TheLaw.html

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html

http://www.ykb.com/hizmetler/e_ticaret/sorular.html#18

http://www.sj.k12.tr/html/konu/biyometri/tr/menu.html

http://www.usdoj.gov/criminal/cybercrime/1030NEW.html

www.whitehouse.gov/deptofhomeland/bill/

http://www4.law.cornell.edu/uscode/18/2332.html

www.epic.org/privacy/terrorism/hr3162.html

http://www.usdoj.gov/criminal/cybercrime/1030NEW.html

http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm -

http://www4.law.cornell.edu/uscode/18/2332b.html.

http://www.emniyet.gov.tr/docs/RAPOR1.pdf (Çevrim içi) 09 Temmuz 2004

http://www.nici.org/Research/Pubs/98-5.htm (Çevrim içi) 12 Eylül 2003

http://www.egm.gov.tr/temuh/terorizm7.htm

http://www.teror.gen.tr/turkce/makaleler/el_kaide_1.html2 (Çevrim içi) 12 Ağustos 2004

http://www.bilecik.pol.tr/teroruluslararasiantlasmalardaterorizm.htm

http:/www.emniyet.gov.tr/docs/RAPOR2.pdf (Çevrim içi) 09 Temmuz 2004

http://www.bilgisayardershanesi.com/virus.htm

http://www.webopedia.com/TERM/l/logic_bomb.html

http://www.daghanoves.netfirms.com/bilim/bilim2.htm

http:// www.tbmm.gov.tr

http://www.po.metu.edu.tr/links/inf/css25/bolum14.html#7

Ekler

1) Bilgisayar Bağlantılı Hile, Dolandırıcılık ve İlgili Faaliyetler

2) Anavatan Güvenlik Yasası 225. Bölümü: Siber Güvenliği Artırma Yasası

3) Amerika Birleşik Devletlerinin Patriot Yassının 814. Bölümü: Siber Terörün Caydırılması ve Önlemesi Yasası

4)Terör Suçları Cezayı Müeyyideler

5) Ulusal Sınırları Dışında Yapılan Terör Eylemleriyle İlgili Yasalar

Ek 1: Bilgisayar Bağlantılı Hile, Dolandırıcılık ve İlgili Faaliyetler :

Başlık 18. Suçlar ve Cezai Prosedürleri

Konu 1- Suçlar

Bölüm 47- Hile ve Yalan Beyanlar

§ 1030 Hile ve Bilgisayarla bağlantılı ilişkili faaliyet

(a) Her kim ki

(1) bilerek, bir bilgisayara, yetkisiz olarak erişir veya yetki verilen erişimi aşar ve bu tür bir davranış yoluyla, yürütme kararı veya dış ilişkiler veya milli savunma nedeniyle yetkisiz ifşaya karşı koruma gerektirmek için tüzük doğrultusunda Birleşik Devletler Hükümeti tarafından belirlenmiş olan bilgileri veya Birleşik Devletlere zarar vermek için kullanılabilen bir şekilde bu bilgilerin elde edildiğine inanılacak şekilde 1954 tarihli Atom Enerji Yasasının 11. Kısmının y bölümünde tanımlandığı üzere herhangi bir sınırlı veriyi elde eder veya herhangi bir yabancı ulus lehine bilinçli olarak bunları, bunları almak için hakkı olmayan herhangi bir kişiye bildirir, teslim eder aktarır veya bildirmek, teslim etmek, aktarmak için çalışır veya bunların bildirilmesini, teslim edilmesini veya aktarılmasını sağlar veya bunları bilinçli olarak elde tutar ve bunu elde etmek için hakkı bulunan Birleşik Devletler görevli veya çalışanlarına bunu teslim etmez
(2) bilinçli olarak bir bilgisayara, yetkisiz olarak erişir veya yetki verilen erişimi aşar ve böylece de aşağıdakileri elde eder

(A) Mali bir kurumun veya Kısım 15.in 1602(n) bölümünde tarif olunduğu üzere bir kart tanzim eden firmanın mali kayıtlarında yer verilen bilgiler veya Adil Kredi Raporlama Kanununda tanımlanmış koşullarda (15 U.S.C 1681 ve devamı), bir müşteri hakkında müşteri bildirim acentesinin dosyasında yer verilen bilgiler
(B) Birleşik Devletlerin herhangi bir bölümü veya kısmından bilgiler veya

(C) Eğer bir devletler arası veya yabancı iletişimle ilgili işlem olursa, herhangi bir korumalı bilgisayardan bilgiler

(3) Planlı bir şekilde, Birleşik Devletlerin bir bölümü veya kısmın kamuya açık olmayan herhangi bir bilgisayarına yetkisi olmadan, münhasıran Birleşik Devletler Hükümetinin kullanımı için olan bu bölüm veya kısmın bu tür bir bilgisayarına erişir veya bu tür bir kullanım için münhasır olmayan bir bilgisayar durumunda, Birleşik Devletler Hükümeti tarafından veya onun için kullanılanlar durumunda ve bu tür bir işlemin Birleşik Devletler Hükümeti tarafından veya onun için kullanımları etkiler

(4) hilenin nesnesi ve elde edilen şeyin sadece bilgisayarın kullanımından oluşmaması halinde ve bu tür bir kullanım, herhangi bir 1 yıllık dönem içinde $ 5,000 den fazla olmaması halinde, bilerek ve yanıltma niyetli olarak, korumalı bir

bilgisayara yetkisiz olarak erişir veya yetki verilen erişimi aşar ve bu tür bir davranış yoluyla, planlanan niyeti ileri götürür ve değerle herhangi bir şeyi elde eder

(5)(A)(i) bilerek bir programın, bilginin, kodun veya komutun iletimine sebep olup, bu ileti sonucu korumalı bir bilgisayara izinsiz şekilde isteyerek zarar verme,

(ii) korumalı bir bilgisayara isteyerek izinsiz erişip ve sonucunda dikkatsizlikle zarara sebep olma; veya

(iii) korumalı bir bilgisayara isteyerek izinsiz erişip sonucunda zarara sebep olma ; ve

(B) (A) alt bölümün (i),(ii) veya (iii) fikralarında tarif edilen fillerin yol açtığı (veya bir suç durumunda, olacaksa, eğer tamamlanmışsa, sebep olunduysa)

(i) 1 veya birden fazla kişiye 1 senelik periyot esnasında toplam en az 5000 dolar değerinde zarar (ve bir araştırma, kovuşturma veya yalnızca Birleşik Devletler tarafından getirilmiş diğer bir tatbikat maksatları için, ilgili iletinin gidisinden doğan zarar diğer 1 veya birden fazla bilgisayarı etkiliyorsa);

(ii) 1 veya daha fazla kişinin tıbbi incelemesi, teşhisi, tedavisi veya bakımının değişme veya zarar verirse veya potansiyel değişiklik veya zara verirse;

(iii) herhangi birine fiziksel zarar;

(iv) halk sağlığına veya emniyetine bir tehdit; veya

(v) milli güvenlik, milli savunma, adalet yönetimi tarafından veya hükümetin bundan başka ayrı bir bölümü için kullanılan bir bilgisayar sistemini etkilenmesi;

(6) bilerek ve dolandırıcılık kastıyla, herhangi bir parola veya izinsiz erişile bilinen bir bilgisayardan alınan benzer bilginin ticareti yapılması (bölüm 1029 da tarif edildiği gibi); eğer

(A) söz konusu işlemler dış veya devletler arası ticareti etkilerse; veya
söz konusu bilgisayar Birleşik Devletler hükümeti tarafından veya için kullanılıyorsa;

(7) korumalı bir bilgisayara zarar verecek herhangi bir tehdit içeren, birinden para veya herhangi başka kıymetli bir şey sızdırmak kastiyle devletler arası veya dış ticarette yapılan herhangi bir haberleşme,bu bölümün (c) altbölümünde tarif edildiği gibi cezalandırılır.

(b) herkim bu bölümün (a) altbölümüne tabi bir suç işleme teşebbüsünde bulunursa, bu bölümün (c) altbölümlerindeki şartlarla cezalandırılır.

(c) bu bölümün (a) veya (b) altbölümlerine tabi bir suç için ceza ---

(1)(A) bu babın (a)(1) altbölümlerine tabi, bu bölümdeki başka bir suç için bir mahkumiyetten sonra vuku bulmayan bir suç veya bu alt bölümdeki cezayı gerektiren bir suç işleme durumunda bu başlık altında bir para cezası, veya 10 yıla kadar hapis veya her ikisi de ; ve

(B) bölümün (a)(1) alt bölümünde, bu bölüme tabi başka bir suç için mahkumiyet olduktan sonra vuku bulan bir suç veya bu alt paragrafta cezayı gerektiren bir suç işleme teşebbüsü durumunda bu başlık altında para cezası ve 20 yıla kadar hapis veya her ikisi de;

(2)(A) alt paragraf (B) de belirtilen şart hariç, bu bölümün (a)(2),(a)(3), (a)(5)(A)(iii) veya (a)(6) altbölümlerine tabi bu bölümdeki başka bir suç için bir mahkumiyetten sonra vuku bulmayan bir suç veya bu alt paragraftaki cezayı gerektiren bir suç işleme teşebbüsü durumunda, bu başlık altında bir para cezası veya 1 yıla kadar hapis veya her ikisi de,

(B) (a)(2) altbölümündeki bir suçun işlenmesi veya bu alt paragraftaki cezayı gerektiren bir suç işleme teşebbüsünde, bu başlık altında bir para cezası veya 5 yıla kadar hapis veya her ikisi de, eğer--

(i) suç ticari avantaj ve özel finansal kazanç amacıyla işlendiyse,

(ii) suc, herhangi bir devletin (eyaletin) veya Birleşik Devletlerin anayasası ve yasalarına yönelik herhangi bir suç veya tecavüz teşkil eder veya ayrıca, herhangi bir davranışla ihlaline yönelik işlenir; veya

(ii) elde edilmiş bilginin değeri 5000 dolar dan fazlaysa;

(C) bu bölümün (a)(2), (a)(3) veya (a)(6) altbölümlerine tabi, bu bölümdeki başka bir suç için bir mahkumiyetten sonra vuku bulan bir suç veya bu alt paragraftaki cezayı gerektiren bir suç işleme durumunda, bu başlık altında bir para cezası veya 10 yıla kadar hapis veya her ikisi de; ve bu bölümün(a)(4) veya (a)(7) altbölümlerine tabi, bu bölümdeki başka suç için mahkumiyetten sonra olmayan bir suç işleme teşebbüsü durumunda, bu başlık altında bir para cezası ve 5 yıla kadar hapis veya her ikisi de; ve

(B) bu bölümdeki başka suç için mahkumiyetten sonra olan, bu bölümün (a)(4), (a)(5) (A)(iii), veya (a)(7) alt bölümlerine tabi bir suç veya bu alt paragraftaki cezayı

gerektiren bir suçu işleme teşebbüsü, bu başlık altında bir para cezası ve 10 yıla kadar hapis veya her ikisi de ; ve

(4)(A) (a)(5)(A)(i) altbölümüne tabi bir suçu işleme veya o bölümdeki cezayı gerektiren bir suçu işleme teşebbüsü durumunda bu başlık altında bir para cezası ve 10 yıla kadar hapis veya her ikisi de;

(B) (a)(5)(A)(ii) altbölümlerine tabi bir suçu işleme veya o bölümdeki cezayı gerektirecek bir suçun teşebbüsünde, bu başlık altında bir para cezası, 5 yıla kadar hapis veya her ikisi de;

(C) (a)(5)(A)(i) veya (a)(5)(A)(ii) bölümlerine tabii bir suç veya bu bölümdeki başka bir suç için mahkumiyetten sonra olmayan veya her iki altbölümdeki cezayı gerektiren bir suç işleme teşebbüsü bu başlık altında bir para cezası 20 yılda kadar hapis veya her ikisi de.

d)(1) Birleşik Devletlerin gizli servisi bu bölümdeki suçları soruşturmada ayrıca diğer devlet organlarının yetkili olduğu gibi yetkilidir.

(2) Federal soruşturma bürosu, bu başlığın 3056(a) bölümüne uygun olarak, Birleşik Devletler gizli servisinin görevlerini Etkileyen suçlar dışında, casusluk, yabancı karşı istihbarat, milli savunma veya dış ilişkiler nedenlerinden dolayı korunan bilgilerin izinsiz açığa çıkarılmasıyla ve sınırlandırılmış bilgilerle (1954 atomik enerji kanununda bölüm 11 y de tarif edildiği gibi (42 U.S.C. 2014(y)), ilgili durumlarda alt bölüm (a)(1) e tabi suçları araştırmada asıl yetkilidir.

(3) bu yetki Hazine Sekreterliği ve Başsavcı tarafından girişilecek bir anlaşmaya uygun olarak kullanılır.

(e) bu bölümde kullanılan

(I) bilgisayar; elektronik, manyetik, optik, elektro kimyasal veya diğer yüksek hızda veri işleyen, mantık, aritmetik, veya depolama fonksiyonları çalışan ve herhangi bir bilgi depolama kolaylığı veya birlikte çalışan başka bir benzer aygıtla haberleşme özelliği olan aygıt anlamındadır. Bu kavram otomatik daktilo, veya dizgi makinesini, taşına bilinir el hesap makinesini ve benzer aygıtları içermez.

(2) "korumalı bilgisayar" herhangi bir bilgisayar anlamındadır.

(A) Birleşik Devletlerin hükümeti veya finansal bir kurumda münhasıran kullanım için veya Birleşik Devletler Hükümeti veya finansal bir Kurum tarafından veya için kullanımın münhasıran olmaması durumunda ve finansal kurum veya Birleşik Devletler hükümeti tarafından veya için kullanılan bir bilgisayarı etkiler suç oluşturan davranış; veya

(B) Birleşik Devletlerin dışında kullanılan bir bilgisayar dahil, devletler arası veya dış ticarette veya haberleşmede kullanılan, Birleşik Devletlerin devletler arası veya dış ticaretini veya haberleşmesini etkileyen şekilde kullanılan,

(3) Devlet kavramı, Colombia bölgesini, Puerto Rico ulusunu ve Birleşik Devletlerin sahip olduğu diğer topraklarını ve mülkünü içerir.

(4) Finansal kurumun anlamı

(A) Federal Mevduat Sigortası tarafından sigortalanmış bir mevduat kurumu;

(B) herhangi bir Federal Merkez bankası dahil Federal Merkez üyesi olan Federal merkez;

(C) Ulusal Kredi birliği İdaresi tarafından sigortalanmış bir kredi sandığı;

(D) Federal Mesken Bankası sisteminin bir üyesi ve herhangi bir mesken bankası;

(E) 1971 Tarımsal Kredi Kanunu altında herhangi bir tarımsal kredi sistemi kurumu;

(F) 1934 Menkul Kıymetler Borsası kanununun 15 inci bölümüne uygun, Menkul kıymetler Borsasına kayıtlı olan bir borsa acentesi-satıcı ;

(G) Menkul sermayeler Yatırımcısını Koruma Kurumu,

(H) bir yabancı bankanın acentesi veya şubesi (1978 Uluslar arası bankacılık kanununun 1 (b) bölümünün (1) ve (3) paragraflarında tarif edildiği gibi) ve;

(I) Federal ihtiyat kanununun 25 veya 25 (a) bölümüne tabi bir organizasyon işlemi;

(5) "finansal kayıt" ın anlamı, bir finansal kurumun bir müşterinin finansal kurum ile ilişkisiyle ilgili tuttuğu herhangi bir kayıttan sağlanmış bilgidir;

(6) "yetkili erişim ile girme" nin anlamı, erişime ve değiştirmeye hakkı olmayan bir erişimcinin bir bilgisayara izinle girip, elde ettiği erişimi bilgisayardaki bilgileri almak veya değiştirmek için kullanmasıdır;

(7) "Birleşik Devletler Departmanı" nın anlamı, hükümetin yasamayla veya yargıyla ilgili bir dairesi veya
başlık 5 bölüm 101 de sıralı olan icracı dairelerinden biridir;

(8) "hasar" ın anlamı, bir program, bir sistem, bir data veya bir bilginin bütünlüğünde veya elde edilebilmesinde herhangi bir zarardır;

(9) "devletin müstakil bir bolümü " kavramı, Birleşik Devletler Hükümetini, Birleşik Devletlerin herhangi bir resmi veya politik alt bölümünü, ve herhangi bir yabancı ülke, ve herhangi bir eyalet, vilayet, belediye, veya yabancı bir ülkedeki diğer politik alt bölümlerini içerir;

(10) "mahkumiyet" in anlamı, bir bilgisayara izinli erişimle tecavüz veya yetkisiz erişim esasıyla, herhangi bir eyaletin yasasına tabi 1 seneden fazla hapis ile cezalandırılabilir bir suç için mahkumiyeti içerecek;

(11) "kayıp" ın anlamı, bir suçu telafi edecek bedel, bir zararın telafi edilmesi ve data, program, sistem veya bilginin suç işlenmeden önceki şartlara getirilmesi ve herhangi bir gelir kaybı, zorunlu yapılan masraf, veya hizmetin kesilmesinden dolayı sonuçta maruz kalınan zararlar dahil, bir kurbana orta derecede maliyetidir.

(12) "şahıs" ın anlamı herhangi bir münferit şahıs, firma, korporasyon (dernek, şirket,zümre), eğitim müessesesi, finansal kurum, devlet dairesi, veya tüzel kişi veya diğer müstakil işletmelerdir;

(f) Bu bölüm, Birleşik Devletlerin bir yasa uygulama dairesinin, bir eyaletin, veya bir eyaletin bir politik alt şubesinin veya Birleşik Devletlerin istihbarat servisinin, yasal yetkili inceleme, koruma veya istihbarat aktivitesini men etmez.

(g) Bu bölümdeki herhangi bir ihlal sebebiyle kayıp ve zarara uğrayan herhangi bir kişi, zararlarını karşılayan tazminatı almak, ve mahkemece verilen emirle mağduriyetinin giderilmesi veya başka adil bir telafi için, ihlali yapana karşı bir hukuk davası ile hakkını savunabilir. Eğer hareketin tavrı, sadece alt bölüm (a)(5)(B) nin (i), (ii), (iii), (iv) veya (v) şartlarını ifade eden faktörlerden birini kapsıyorsa, bu bölümdeki ihlallerden birisi için hukuk davası getirilebilir. Sadece altbölüm (a)(5)(B)(i) de tanımlanan icraatı kapsayan bir ihlalin zararları ekonomik zararlar ile sınırlıdır. Söz konusu dava zararın keşif tarihinden veya şikayet edilen davranış tarihinden sonraki 2 sene içinde başlatılmazsa bu bölüm altında dava açılmaz. Kusurlu tasarım veya bilgisayar donanımı, bilgisayar yazılımı, veya aygıt yazılımı için bu alt başlığa tabi dava açılmaz.

(h) Başsavcı ve Hazine Vekili (a)(5) alt bölümüne tabi kanuni tatbikatlar ve tahkikler hakkında,
bu alt bölümdeki kanunun yürürlüğe giriş tarihini takip eden ilk 3 yıl Kongreye yıllık rapor verecekler.

Ek 2: Anavatan Güvenlik Yasası 225. Bölümü: Siber Güvenliği Artırma Yasası

Bölüm. 101...Belli Bilgisayar Suçlarıyla İlgili Karar Ana Hatlarında Değişim.

(a) US KARAR KOMİSYONUNA DİREKTİF.Başlık 28 bölüm 994(p) altındaki US yasasına tabi

yetkisine göre ve bu bölüm gereğince US karar komisyonu tekrar gözden geçirecek ve eğer yerindeyse ana hatlarını ve politik hedeflerini başlık 18, bölüm 1030 US yasasına tabi bir suçtan mahkum kişilere uygulanabilir şekilde değiştirecek.

(b) İSTEKLER.

Bu bölümün sürdürülmesi bakımından, karar komisyonu

(1) kararların ana hatlarının ve politik hedeflerinin, alt bölüm (a) da tarif edilen bu suçların tehlikeli doğasını, bu suçların karşılıklarını arttırmayı, bu suçları önlemek için etkili bir caydırıcı ve uygun cezalandırma gereksinimini yansıtmasını sağlayacak.

(2) aşağıdaki faktörler ve ana hatların bunlara cevap verip veremeyeceği boyutu göz önüne alındığında----

(A) suçun neticesinde potansiyel ve gerçek bir kayıp;

(B) suça karışan sofistikasyon ve planlamanın düzeyi

(C) suçun özel maddi menfaat veya ticari avantaj amaçları için işlenip işlenmediği;

(D) suçun işlenmesinde sanığın kötü niyetle zarara sebep olmak kastıyla davranıp davranmadığı;

(E) suçun, zarar gören insanların özel haklarını ihlal eden boyutu;

(F) suçun, devletin adalet yönetimi, ulusal güvenlik ve ulusal savunma için kullandığı bir bilgisayara bulaştırılıp bulaştırılmadığı;

(G) ihlalin, önemli bir engelleme ve kritik bir altyapının alt üst olmasına yol açmak niyeti taşıyıp taşımadığı veya etkisi olup olmadığı; ve

(H)ihlalin, halk sağlığı ve emniyeti için bir tehdit veya herhangi birine zarar verme niyeti taşıyıp taşımadığı veya etkisi olup olmadığı;

(3) konuyla ilgili diğer direktifler ve diğer karar ana hatları ile makul tutarlılığı temin etme;-

(4) kanıtlama istisnaları olabilen ilave edilmiş ağırlaştırıcı veya hafifletici koşullar için genellikle başvurulabilen karar serilerine göre açıklama

(5) karar ana hatlarına uyan gerekli değişiklikleri yapma; ve

(6) (6) ana hatların, başlık 18 bölüm 3553(a)(2) US yasası içindeki ifade edilen kararların amaçlarına yeterli derecede uygun olmasını (çakışmasını) temin etme.

BÖLÜM 101A. BİLGİSAYAR SUÇLARI HAKKINDA ARAŞTIRMA (ÇALIŞMA) VE SUNUM.

1 Mayıs 2003 den önce Birleşik Devletler Karar Komisyonu, Kongreye Karar Komisyonu tarafından bu yasaya karşılık yapılan işlemleri izah eden, Başlık 18 bölüm 1030 altındaki suçlar için kanunla yapılmış cezalara ilişkin, komisyonun önerilerini de içerebilecek bir brifing sunacak.

BÖLÜM 102. OLAĞANÜSTÜ TEHLİKELİ DURUM AÇIKLAMA BEKLENTİSİ.

(a) GENELDE.---- Başlık 18 bölüm 2702(b) Birleşik Devler Yasası değiştirilmiştir.

(1) paragraf (5) in sonundaki "veya" nın çıkarılması;

(2) paragraf (6) nın (C) alt paragrafının çıkarılması; ve

(3) Paragraf (6) da, alt paragraf (B) nin sonundaki "veya" nın çıkarılması ve alt paragraf (A) nın sonuna

"veya" nın konulması;

(4) paragraf (6) nın sonundaki aranın çıkarılıp "veya" eklenmesi; ve

(5) paragraf (6) dan sonra aşağıdakinin eklenmesi:

"(7)İyi niyetle herhangi birisine ciddi bir fiziksel hasar veya ölüm tehlikesi içeren bir olağanüstü tehlikeli durum olduğuna inanan kimsenin acil durumla ilgili bildirimi geciktirmeden bir Federal, Devlet veya lokal idari varlığa açıklaması zorunludur.

(b) AÇIKLAMALARIN BİLDİRİLMESİ.---- Bu bölüm altında bir açıklama alan devlet varlığı,

yapılan açıklamanın tabi olduğu alt paragraf , tarihi, yapıldığı bölüm, eğer açıklamada varsa, açıklamanın enformasyonunu alan kişiye ilişkin müşterilerin ve taraftarların sayısı ile haberleşmelerin miktarını, açıklamadan sonraki 90 gün içinde savcıya bildirmek için dosyalayacak. Savcı bütün bu raporları, tasarının yasalaşmasından bir sene sonra Kongreye sunulacak şekilde bir raporda birleştirecek.

BÖLÜM 103. İYİ NİYET BEKLENTİSİ.

Başlık 18 bölüm 2520(d)(3) Birleşik Devletler Yasası "2511(3)" den sonra "veya 2511(2)(i)" konulmasıyla değiştirilmiştir.

BÖLÜM 104. ULUSAL ALTYAPI KORUMA MERKEZİ

(a) GENELDE.--- Savcı, bir tehdit değerlendirmesi, uyarı, soruşturma ve ulusun kritik altyapısına maddi veya siber kaynaklı saldırılara cevap vermek için ulusal bir odak noktası olarak hizmet edecek bir Ulusal Altyapı Koruma Merkezi (bu bölümde bundan sonra merkez olarak geçecek) kuracak ve yürütecek

(b) ÖDENEKLER İZNİ.----- Bu bölümü sürdürmek için 2003 mali yılı için kendilerine 125 milyon dolar mal etmeye yetkileri vardır.

BÖLÜM 105. YASAL OLMAYAN YÖNTEMLERİN İNTERNETTE İLANI.

Başlık 18 in 2512(1)(c) bölümü Birleşik Devletler Yasası değiştirilmiştir.

(1) "veya başka yayın" dan sonra "veya elektronik araçlar ile yayılır" konulmasıyla; ve

(2) "bilgisi olmak veya bilmek için sebebi olmak " tan önce "ilanın içeriğini bilmek" konulmasıyla.

Bölüm 106 Cezaların Güçlendirilmesi.

Başlık 18 Bölüm 1030(c) Birleşik Devletler Yasası değiştirilmiştir.

(1) paragraf (3) ün sonundaki "ve" nin çıkarılmasıyla;

(2) Paragraf (4) ün alt paragrafları (A) ve (C) nin her birinin içinde " bu bölüme tabi bir para cezası" ndan önce "paragraf (5) de bulunan hariç"

(2) paragraf (4)(C) nin sonundaki sürenin çıkarılması ve "ve" konulmasıyla; ve

(3) sonuna aşağıdakilerin eklenmesiyle:

"**(5)(A)** eğer suçlu bilerek veya dikkatsizlik sebepleriyle ciddi bir bedensel hasara sebebiyet verir veya teşebbüs ederse, altbölüm (a)(5)(A)(i) yi ihlali içinde tavrı hareketten, bu başlık altında bir para cezası veya 20 yıla kadar hapis veya her ikisi de" veya

"**(B)** eğer suçlu bilerek veya dikkatsizlik sebepleriyle ölüme sebebiyet verir veya teşebbüs ederse, altbölüm (a)(5)(A)(i) nin ihlali içinde tavrı hareketten bu başlık altında bir para cezası veya yıllar süreli veya hayat boyu hapis veya her ikisi de."

Bölüm 108. Yardım Sağlayan Kimse

(a) BÖLÜM 2703. Başlık 18 bölüm 2703(e) Birleşik Devletler Yasası "celpname"den sonra "kanuna uygun yetki" konularak değiştirilmiştir.

(b) BÖLÜM 2511. Başlık 18 bölüm 2511(2)(a)(ii)Birleşik Devletler Yasası en son gözüktüğü yerdeki "mahkeme emri" nden sonra "kanuna uygun yetki" konularak değiştirilmiştir.

Bölüm 108. KRİTİK DURUMLAR.

Başlık 18 Bölüm 3125(a)(1) Birleşik Devletler Yasası değiştirilmiştir

(1) alt paragraf (a) nın sonunda "veya" nın çıkarılmasıyla

(2) alt paragraf (b) nin sonunda virgülün çıkarılıp, noktalı virgül konulmasıyla; ve

(3) sonuna aşağıdakinin eklenmesiyle

"**(C)** ulusal güvenlikle alakalı hazır bir tehdit; veya

"**(D)** korumalı bir bilgisayara devam eden bir saldırı (bölüm 1030 da tanımlandığı gibi) bir seneden fazla olmayan hapisle cezalandırılabilir bir suçu oluşturur.

Bölüm 109 Gizliliğin Korunması.

(a) BÖLÜM 2511.---Başlık 18 in 2511(4) bölümü. Birleşik Devletler Yasası değiştirilmiştir.

(1) paragraf (b) nin iptali: ve

(2) paragraf (c) nin paragraf (b) gibi belirtilmesi.

(b) BÖLÜM 2701.----başlık 18 in 2701(b) bölümü. Birleşik Devletlerin yasası değiştirilmiştir.

(1) paragraf (1) de "ticari menfaat" ten sonra "veya US veya bir devletin yasalarının veya anayasanın ihlalinde herhangi bir kriminal veya zararlı eylemin ilerlemesini sağlamada" nın eklenmesiyle:

(2) paragraf (1)(A) da "bir sene" nin çıkarılıp"5 sene" nin konmasıyla:

(3) paragraf (1)(B) de "iki sene" nin çıkarılıp "10 sene" nin konmasıyla: ve

(4) böylece paragraf (2) aşağıdaki şekilde okunur:

"**(2)** herhangi başka bir durumda

"**(A)** bu paragraf altındaki suçu ilk defa işleme durumunda bu başlık altında bir para cezası veya bir seneden çok olmayan hapis veya her ikisi de: veya

(B) bu alt paragrafa tabi bu bölüm altındaki başka bir suçtan mahkumiyetten sonra meydana gelen bir suç durumunda, bu başlık altında bir para cezası veya 5 seneden çok olmayan hapis."

(c) Görevli Memurun Varlığı Ve Müşteri Kayıtları Ve Haberleşmeler İçin Verilen Yetkinin İcrası. Başlık 18 in 3105. Birleşik Devletler yasası sonuna aşağıdakini eklemek suretiyle değiştirilmiştir: Yetki istenen istihbaratı elektronik haberleşme servisi veya uzaktan hesaplama servisini teçhiz eden kimse verdiğinde bölüm 2703de bir yetkinin icrası veya bir görevli memurun varlığına ihtiyaç duyulmaz

Ek 3 : BÖLÜM 814. SİBER TERÖRÜN CAYDIRILMASI VE ÖNLENMESİ DAİR YASA

BAŞLIK 18 BÖLÜM 1030 (a)(5) Birleşik Devletler yasası değiştirilmiştir.

(1) (A) dan sonra (i) konulmasıyla

(2) sırasıyla, alt paragraflar (B) ve (C) nin (ii) ve (iii) maddelerine göre yeniden belirtilmesiyle,

(3) madde (iii) nin sonuna "ve" katılmasıyla

(4) aşağıdakilerin sonuna eklenmesiyle

"**(B)** (A) alt paragrafının (i), (ii), (iii) maddelerinde tanımlanan davranış vasıtasıyla,

sebebiyet vermiş (veya bir suç teşebbüsü halinde, eğer olsaydı, tamamlandıysa, sebep olduysa)

"**(i)** 1 veya 1 den fazla kişiye 1 senelik dönem içinde toplam en az 5000 dolar değerinde zarar

(ve yalnız US tarafından getirilmiş bir araştırma, kovuşturma veya diğer kanuni tatbikat maksadı için, ilgili

iletinin gönderilmesinden doğan zarar 1 veya 1 den fazla bilgisayarı etkiliyorsa);

"**(ii)** 1 veya daha fazla kişinin tıbbi incelemesi teşhisi tedavisi veya bakımının değişmesi veya eksilmesi veya potansiyel değişiklik veya eksiklikler;

"**(iii)** herhangi birine fiziksel zarar verme;

"**(ıv)** halk sağlığına, emniyetine bir tehdit, veya;

"**(v)** milli güvenlik, milli savunma, adalet yönetimi tarafından veya hükümetin bundan ayrı bir bölümü için kullanılan bir bilgisayarın etkilenmesi.

(b) DOLANDIRICILIKTAN KORUNMA.------ Başlık 18, bölüm 1030(a)(7) US yasası " firma, birlik, eğitim kurumu, finans kurumu, hükümet bölümü veya başka yasal bölümler. (daireler)" in çıkarılmasıyla değiştirildi.

(1) paragraf (2) ----

(A) alt paragraf (A) da-----

(i) "bir para cezası"ndan önce, "alt paragraf (B) deki şart hariç" konulmasıyla;

(ii) "(a)(5)(C)" nin çıkarılması ve (a)(5)(A)(iii)" nin konulması; ve

(iii) sonundaki "ve" nin çıkarılması

(B) alt paragraf (B) ye "alt bölüm (a)(2)" den sonra madde (i) den önceki konuda "veya bu alt paragrafa tabi cezalandırılabilecek bir suçu işleme teşebbüsü " konulmasıyla; ve

(C) alt paragraf (C), sonundaki "ve" nin çıkarılmasıyla,

(2) paragraf (3)

(A) "(a)(5)(A), (a)(5)(B) nin gözüktükleri yerlerden çıkarılması; ve

(B) (a)(5)(C) nin çıkarılması ve (a)(5)(A)(iii) konulması; ve

(3) aşağıdakilerin sonuna eklenmesi;

"altbölüm (a)(5)(A)(i) e tabi bir suç işleme veya bu alt bölümde cezalandırılabilir bir suç işleme teşebbüsü durumunda bu başlığa tabi (4)(A) bir para cezası, 10 yıldan çok olmayan hapis veya her ikisi de;

"(a)(5)(A)(ii) alt bölümüne tabi bir suç işlenmesi veya bu alt bölümde cezalandırılabilecek bir suç işleme teşebbüsü durumunda bu başlığa (B) tabi bir para cezası, 5 yıla kadar hapis veya her ikisi de ;

a)(5)(A)(i) veya (a)(5)(A)(ii) altbölümlerine tabi, bu bölüme tabi başka bir suçtan olan bir mahkumiyetten sonra işlenen bir suç veya her ikisine de tabi bir suç işleme teşebbüsü durumunda bu başlık altında (C) bir para cezası, 20 yıla kadar hapis veya her ikisi de;

(d) NİTELENDİRME

Başlık 18, Bölüm 1030(e) , Birleşik Devletler Yasası değiştirilmiştir

(1) paragraf (2)(B) ye noktalı virgülden önce Birleşik Devletlerin dışında bulunan Birleşik Devletlerin devletler arası ve dış ticaretini veya haberleşmesini etkileyen konularda kullanılan bir bilgisayar dahil" konulmasıyla;

(2) paragraf (7) nin sonundaki "ve" nin çıkarılmasıyla;

(3) paragraf (8) in çıkartılması ve aşağıdakinin konulmasıyla:

"zarar" ın anlamı, bir program, bir sistem, bir data veya bir bilginin bütünlüğünde veya elde edilebilmesine herhangi bir zarardır.

(4) paragraf (9) un sonundan "dönemde" nin çıkarılıp bir noktalı virgül konulması; ve

(5) sonuna aşağıdakilerin eklenmesi:

"mahkumiyet" in anlamı bir bilgisayara izinli erişimle tecavüz veya izinsiz erişim esasıyla herhangi bir devletin yasasına tabi 1 seneden çok hapis ile cezalandırılabilir bir suç için bir mahkumiyeti içerecek.

"(11) "kayıp" ın anlamı,bir suçu telafi edecek bedel,bir zararın telafi edilmesi ve data, program, sistem

veya bir bilginin suç işlenmeden önceki şartlarına getirilmesi ve herhangi bir gelir kaybı, zorunlu

yapılan masraf veya hizmetin kesilmesinden dolayı sonuçta maruz kalınan zararlar dahil bir kurbana orta derecede maliyetidir.

"(12) "şahıs" ın anlamı, herhangi bir münferit şahıs, firma, korporasyon (dernek, şirket, zümre), eğitim

kurumu, finansal kurum, devletin müstakil dairesi veya diğer yasal müstakil işletmelerdir.

HUKUK DAVALARINDA HASAR.

başlık 18, bölüm 1030(g) Birleşik Devletler Yasası değiştirilmiştir

(1) ikinci kararın çıkarılması ve aşağıdakinin konulmasıyla:

"Bu bölümdeki bir ihlal için bir hukuk davası eğer davranış sadece altbölüm (a)(5)(B) nin

(i), (ii), (iii), (iv) ve (v) maddelerini ifade eden faktörlerden birisini kapsıyorsa getirilebilir.

Sadece alt bölüm (a)(5)(B)(i) de tanımlanan davranışı kapsayan bir ihlalin zararları ekonomik zararlar ile sınırlıdır." ve

(2) sonuna aşağıdakinin eklenmesiyle:

"Kusurlu tasarım veya bilgisayar donanımı, bilgisayar yazılımı veya aygıt yazılımı için bu başlığa tabi dava getirilemez.

(e) BELİRLİ BİLGİSAYAR HİLESİ VE SUİSTİMALİYLE ALAKASI OLAN KARAR TASHİHLERİNİN ANAHATLARI.

Birleşik Devletler yasası başlık 28 bölüm 994(p) gereğince, US Karar Düzeltme Komisyonu,

(iv) korumalı bir bilgisayara isteyerek izinsiz erişip ve sonucunda dikkatsizlikle zarara sebep olma; veya

(v) korumalı bir bilgisayara isteyerek izinsiz erişip sonucunda zarara sebep olma ; ve

(C) (A) alt paragrafının (i),(ii) veya (iii) şartlarında tarif edilen icraatların yol açtığı (veya bir suç durumunda, eğer tamamlandığında olacak idiyse, sebep olunduysa) –

(vi) 1 veya birden fazla kişiye 1 senelik dönem içinde toplam en az 5000 dolar değerinde zarar (ve bir araştırma, kovuşturma veya yalnızca Birleşik Devletler tarafından getirilmiş diğer bir tatbikat maksatları için, ilgili iletinin gidisinden doğan zarar diğer 1 veya birden fazla bilgisayarı etkiliyorsa);

(vii) 1 veya daha fazla kişinin tıbbi incelemesi, teşhisi, tedavisi veya bakımının değişmesi veya eksilmesi veya potansiyel değişiklik veya eksiklik;

(viii) herhangi birine fiziksel zarar vermek;

(ix) halk sağlığına veya emniyetine bir tehdit; veya

(x) milli güvenlik, milli savunma, adalet yönetimi tarafından veya hükümetin bundan ayrı bir bölümü için kullanılan bir bilgisayar sisteminin etkilenmesi;

(vi) bilerek ve dolandırıcılık kastıyla, herhangi bir parola veya izinsiz erişile bilinen bir bilgisayardan alınan benzer bilginin ticareti yapılması (bölüm1029 da tarif edildiği gibi); eğer

(A) söz konusu işlemler dış veya devletler arası ticareti etkilerse; veya

(B) söz konusu bilgisayar Birleşik Devletler Hükümeti tarafından veya için kullanılıyorsa;

(7) korumalı bir bilgisayara zarar verecek herhangi bir tehdit içeren, birinden para veya herhangi başka kıymetli bir şey sızdırmak kastiyle devletler arası veya dış ticarette yapılan herhangi bir haberleşme, bu bölümün altbölümünde tarif edildiği gibi cezalandırılır. **(a)** herkim bu bölümün (a) altbölümüne tabi bir suç işleme teşebbüsünde bulunursa, bu bölümün

(b) altbölümlerindeki şartlarla cezalandırılır.

(c) bu bölümün (a) veya (b) altbölümlerine tabi bir suç için ceza ---

Ek 4: BÖLÜM 2332B. – ULUSAL SINIRLARDA GERÇEKLEŞEN TERÖR EYLEMLERİ

(a) Yasaklanmış eylemler.-

(1) Suçlar.-

Ulusal sınırlarda gerçekleşen harekete bulaşan kimse ve alt bölüm (b) de tanımlanan şarttaki gibi –

(A) öldürmeler, kaçırmalar, sakatlamalar, ciddi bedensel hasar ile sonuçlanan bir saldırıda bulunmak,veya Birleşik Devletler içinde birine tehlikeli bir silahla saldırı; veya

(B) Birleşik Devletler içinde bir yapıyı, nakil aracını, veya diğer kişisel bir menkul eşyayı veya gayrimenkulu tahrip etmek

veya zarar verme teşebbüsü veya girişimi yoluyla veya Birleşik Devletlerin içinde bir yapıyı, nakil aracını veya diğer kişisel

bir menkul eşyayı veya gayrimenkulu tahrip etmek veya zarar vermek yoluyla bir başka kişide gerçek bir ciddi bedensel hasar riski meydana getiren; Birleşik Devletler veya herhangi bir Eyaletin yasalarının ihlali durumunda alt bölüm (c) de düzenlendiği gibi cezalandırılacak.

(2) Tehdit girişimleri ve teşebbüslerinin işlemi.

Paragraf (1) e tabi bir suça göre tehdit eden veya böyle davranmaya teşebbüs eden veya (girişen) bu gaye ile gizli ittifak kuran kimse alt bölüm (c) ye tabi olarak cezalandırılır.

(b) yargılama hakkına ait esaslar

(1) Şartlar.

(a) altbölümüne atfedilmiş şartlar

(A) suçun ilerlemesini sağlamakta dış ticaret veya posta veya devletler arası herhangi bir kolaylık kullanılmışsa,

(B) suç, dış veya devletler arası ticareti etkiler, geciktirir veya engeller veya eğer suç tamamlandığından dolayı devletler arası veya dış ticaret etkilenmiş, geciktirilmiş veya engellenmişse;

(B) kurban veya kastedilen kurban, Birleşik Devletler Hükümeti, resmi giysili servislerin bir üyesi veya yasamanın bir resmi memuru, çalışanı, veya

temsilcisi,Birleşik Devletlerin icra veya yargı ile ilgili şubeleri veya bir departmanının veya temsilciliğinin;

(D) Birleşik Devletler ye veya Birleşik Devletlerin herhangi bir departman veya temsilciliğine bütünüyle veya kısmen ait, zilyet olmuş, veya kiralanmış yapı, nakil aracı veya diğer gayrimenkul veya şahsi menkul eşyalar;

(E) suç Birleşik Devletlerin sınırları içindeki denizlerde işlenmişse (üstündeki hava sahası, altındaki deniz dibi ve toprakaltı ve yapay adalar ve orada kurulup yerleştirilmiş yapılar dahil); veya

(F) suç Birleşik Devletlerin denize veya deniz işlerine mahsus mülki yargılama hakkı içinde işlenmişse.

(2) Eğer paragraf (1) de, alt paragraflar (A) dan (F) ye kadar tanımlanan durum şartlarından en az birisi en az bir suçluya uygulanabiliyorsa bu bölümdeki bir suçun ittifakını birlikte kuranları ve bütün patronları ve bu bölümdeki bir suç işlendikten sonra suç ortağı olan şahısları yargılama hakkı olacak.

(c) Cezalar.-

(1) Cezalar.-

Bu bölümü ihlal eden kimse cezalandırılacak.-

(A) bir adam öldürme için veya bu bölümde yasaklanan, herhangi bir şahıs tarafından yapılıp herhangi başka bir şahsın ölümüyle neticelenen icraat, ölümle veya yıllar süreli veya hayat boyu hapisle;

(B) adam kaçırma için uzun süreli hürriyeti bağlayıcı cezalar veya hayat boyu hapisle;

(C) adam sakatlama için 35 yıla kadar hapisle;

(D) tehlikeli bir silah ile veya ciddi bedensel hasar ile sonuçlanan bir saldırı için 30 yıla kadar hapisle;

(E) herhangi bir yapı, nakil aracı veya başka bir gayrimenkul veya şahsi menkul eşyanın yıkılması ve zarar verilmesi için 25 yıla kadar hapis ile;

(F) bir suçu işlemeye teşebbüs etmek veya suçu işlemek amacıyla gizli ittifak kurmak için, işlenmiş suça uygulanabilecek maksimum süreli ceza

(G)bu bölüme tabi bir tehdit etme suçu işlemek için, 10 yıla kadar hapisle hapis ile.

(2) Müteakip karar.-

Herhangi başka bir kanun hükmüne rağmen, mahkeme bu bölümün ihlalinden mahkum olmuş bir şahısa tecil vermeyecek, bu bölüm altında konmuş hapis cezası süresini herhangi bir hapis cezası süresi ile aynı zamanda işletecek..

(d) Kanıt İhtiyacı.

Bu bölümdeki kovuşturmalara aşağıdakiler uygulanır.

(1) Bilgi.-

Bir yargı yetkisinin esasına uygun iddianamede suçlanan bir sanık hakkındaki bilgiyi kanıtlamak için kovuşturma istenmez .

(2) Devlet yasası.

Bu bölüm altında Devlet yasasının tanıması üzerine dayanan bir kovuşturmada, sadece Devlet yasası altındaki suçların unsurları kabul edilir ve ceza mahkeme usulü veya kanıtla ilgisi olan hükümler kabul edilmez

(e) Kendi sınırları dışında sahip olunan haklara yargı yetkisi

Kendi sınırları dışında sahip olunan haklara Federal yargı yetkisi vardır.

(1) bir tehdit , teşebbüs, bu suçu işlemek için gizli örgüt kurmak da dahil alt bölüm

(a) altında bir suçtan; ve

(2) bölüm 3' e tabi bir eylem, alt bölüm (a) ya tabi bir suç işlendikten sonra bir kişiyi fer'i faile çevirir.

(f) Soruşturma yetkisi.

Bu bölümün ihlallerine gelince, başka bir soruşturma yetkisine ek olarak, Baş Savcı bütün Federal

terörizm suçlarının ve bu başlığın 351(e), 844(e), 844(f)(1), 956(b), 1361,1366(b), 1366(c), 1751

(e), 2152 veya 2156 bölümlerinin bir ihlali için birincil soruşturma sorumluluğuna sahip olacak ve

Maliye Vekili, Baş Savcının isteği üzerine kendisine asiste edecek. Bu bölümdeki hiçbir şey,

Bölüm 3056 ya tabi Birleşik Devletlerin Gizli Servisinin yetkisiyle çatışmak için yorumlanmış olmayacak..

g)Tanımlamalar.

Bu bölümde kullanıldığı gibi.

(1) "ulusal sınırları geçen eylem"Birleşik Devletlerin içinde olan eylemlere ek olarak, US dışında olan eylemler

demektir;

(2) "devletler arası veya dış ticaret", bölüm 1985(b)(2) de verilen anlamdadır;

(3) "ciddi bedensel zarar", bölüm 1365(g)(3) de verilen anlamdadır;

(4) Birleşik Devletlerin mülki denizi" uluslararası yasalara uygun olarak, Birleşik Devletlerin ana çizgilerinden 12 deniz mili uzaklığa kadar olan deniz bölgesi demektir; ve

(5)"Federal terörizm suçu"

(A) tehdit veya, zorlama yoluyla devletin hareketini etkilemeyi veya nüfuz etmeyi, veya devletin icrasına karşı misilleme yapmayı hesaplayan bir suç; ve

(B) bir ihlalinde

(i) bölüm 32 (uçak ve uçak tesislerini harap etmekle ilgili), 37 (uluslararası havalimanlarında şiddetle ilgili),

81 (özel denize ait ve mülki yetki dairesini teşkil eden bölge içinde kundakçılık ile ilgili), 175 veya 175b (biyolojik silahlarla ilgili), 229 (kimyasal silahlarla ilgili), bölüm 351 in (a), (b), (c) veya (d) alt bölümlerinde

(ABD Kongresine, hükümete ve Yüksek Mahkemeye üyelerine suikast ve adam kaçırma ile ilgili), 831 (nükleer malzeme ile ilgili), 842(m) veya

(n) (plastik patlayıcılarla ilgili), 844(f) (2) veya

(3) (Devlet mülkünü ölüme riske edecek veya sebebiyet verecek şekilde bombalamak veya kundaklamakla ilgili)

844(i) (devletler arası ticarette kullanılan bir mülkü bombalamak veya kundaklamakla ilgili), 930(c)

(Federal bir servise tehlikeli bir silahla bir saldırı esnasında öldürmek veya öldürmeye teşebbüsle ilgili), 956(a)(1) (ülke dışında insanları öldürmek, kaçırmak veya sakatlamak için komplo ile ilgili), 1030(a)(1)

(bilgisayarların korunmasıyla ilgili), 1030(a)(5)(A)(i), 1030(a)(5)(B)(ii) de tanımlanan hasarla sonuçlanan

(v) (bilgisayarların korunmasıyla ilgili), 1114 (US nin memurlarını ve çalışanlarını öldürmek veya öldürmeye teşebbüs etmekle ilgili), 1116 (yabancı memurları, resmi konukları veya uluslararası korunan kişileri öldürmek

veya kasıtsız öldürmekle ilgili), 1203 (rehin almakla ilgili), 1362 (haberleşme hatları, istasyonları veya sistemlerini harap etmekle ilgili), 1363 (US nin özel denize ait binalarına veya mülki yetki dairesini teşkil eden bölge içindeki mülküne zarar vermekle ilgili), 1366(a) (bir enerji tesisini harap etmekle ilgili),

1751(a), (b), (c), veya (d) bu bölümün 2332a (yıkma özelliği olan silahlarla alakalı), 2332b (ulusal sınırlar içerisinde gerçekleşen terör hareketleriyle ilgili), 2332f (kamu yerlerini ve tesislerini bombalamakla alakalı),2339 (teröristlere yataklık etmekle ilgili), 2339A (teröristlere malzeme yardımı temin etmekle ilgili), 2339B (terörist organizasyonlara malzeme yardımı temin etmekle ilgili), 2339C (terörizmi finans etmekle ilgili), veya 2340A (işkence ile ilgili)

(ii) 1954 Atom Enerjisi Yasasının 236 ıncı bölümü (42 USC2284) (nükleer tesisler ve yakıt tesislerine sabotaj ile alakalı); veya

(iii) başlık 49, bölüm 46502 (uçak korsanlığı), bölüm 46504 ün ikinci kararı (uçak personelini tehlikeli bir silahla saldırmak ile ilgili), bölüm 46505(b)(3) veya (c) (uçakta insan hayatını tehlikeye sokmayı amaçlayan veya patlayıcı veya yangın çıkaran aletler ile alakalı), bölüm 46506 eğer cinayet veya cinayet teşebbüsü varsa (uçaktaki davranışlar için belli cezai yasaların uygulamasıyla ilgili), veya bölüm 60123(b) (devletler arası benzin veya rizikolu likit boru hattı tesisinin harap edilmesiyle ilgili)

(Başkanlık ve başkanlık personeline suikast veya kaçırılma ile ilgili), 1992 (trenlere kaza yaptırtmakla ilgili), 1993 (kitle taşıma araçlarına terörist saldırılar ve diğer şiddet içeren davranışlarla ilgili), 2155 (ulusal savunma materyallerini, binalarını, kuruluşlarını harap etmekle ilgili), 2280 (deniz işlerine ait gemi seferine karşı şiddet ile ilgili), 2281 denizcilikle ilgili yerleştirilmiş platformlara karşı şiddet ile ilgili), 2332 (Birleşik Devlerin vatandaşlarına karşı Birleşik Devlerin sınırların dışında meydana gelen tayini mümkün cinayetler ve diğer şiddet ile ilgili)

Ek 5: BÖLÜM 2332 – CEZAİ MÜEYYİDELER

(a) Cinayet –

Herkim bir Birleşik Devletler vatandaşını bu kişi Birleşik Devletlerin sınırlarının dışındayken öldürürse

(1) eğer öldürme cinayetse (bölüm 111 (a) da tarif edildiği gibi) bu bölüme tabi cezalandırılacak, ölüm veya hayat boyu veya belirli bir süre için hapis cezası veya her ikisi de;

(2) eğer bu başlığın 1112(a) bölümünde tarif edildiği gibi tahrikle öfkeye kapılarak öldürme ise, bu baslık altında para cezası veya 10 yıla kadar hapisle cezalandırılacak veya her ikisi de;

(3) eğer bu başlığın 1112(a) bölümünde tarif edildiği gibi ihmal ve tedbirsizlikle ölüme sebebiyet ise bu başlığa altında para cezası veya 3 yıldan çok olmayan hapis veya her ikisi de;

(b) cinayet teşebbüsü veya cinayet için iştirak

herkim, Birleşik Devletlerin dışında bir Birleşik Devletlerin vatandaşını öldürmeye teşebbüs eder veya öldürmek için bir ittifaka girerse-

(1) bu parçada tarif edildiği gibi bir cinayet olan bir öldürme teşebbüsünde, bu bölüme tabi bir para cezası veya 20 yıla kadar hapis veya her ikisi de; ve

(2) 2 veya daha fazla kişinin, bu başlığın 1111(a) bölümünde tarif edildiği gibi bir cinayet olan bir öldürmeyi
gerçekleştirmek için gizli bir ittifak kurması durumunda, eğer bu kişilerden birisi veya birden fazlası
ittifakın amacını yerine getirmek için herhangi bir bariz fiilde bulunursa, bu başlık altında bir para cezası veya belirli bir yıl sayısı veya hayat boyu hapis veya o kadar para cezası, o kadar hapsin her ikisiyle de
cezalandırılır.

(c) Diğer İcra hareketi.-

Herkim, Birleşik Devletlerin dışında fiziksel şiddet uygulamakla meşgul olursa,-

(1) bir Birleşik Devletleri vatandaşına ciddi bedensel hasar vermek kastıyla; veya

(2) neticesinde, bir Birleşik Devletler vatandaşında ciddi bedensel hasara sebebiyet verdiyse;

bu başlık altında para cezası veya 10 yıla kadar hapis veya her ikisiyle cezalandırılacak.

(d) Kovuşturma limiti.

Resmi onaylama kararında, bu suç bir devlete veya sivil halka karşı baskı yapmak, yıldırmak veya misilleme yapmak kastı taşıyorsa, cezai kovuşturmaların sorumluluğu için savcının veya savcının emrindeki en yüksek dereceli memurun yazılı onayı haricine bu başlıkta izah edilen bir suç için Birleşik Devletler tarafından taahhüt edilen bir kovuşturma olmayacaktır.