İNTERAKTİF DOLANDIRICILIK

Ufuk GÜRÇAM

YÜKSEK LİSANS TEZİ
İletişim Anabilim Dalı
Danışman: Prof.Dr.A.Haluk YÜKSEL

Eskişehir
Anadolu Üniversitesi Sosyal Bilimler Enstitüsü
Kasım 2008

JÜRİ VE ENSTİTÜ ONAYI

Ufuk GÜRÇAM'ın "İnteraktif Dolandırıcılık" başlıklı tezi **28 Ekim 2008** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca, **İletişim** Anabilim Dalında, **yüksek lisans tezi** olarak değerlendirilerek kabul edilmiştir.

			İmza
Üye (Tez Danışmanı)	:	**Prof.Dr.A.Haluk YÜKSEL**	.....
Üye	:	**Doç.Dr.R.Ayhan YILMAZ**	.....
Üye	:	**Doç.Dr.Erhan EROĞLU**	.....

Prof.Dr.Ramazan GEYLAN
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

ÖZGEÇMİŞ

Ufuk GÜRÇAM

İletişim Anabilim Dalı
Yüksek Lisans

Eğitim

Ls. 1998 Ankara Polis Akademisi

Lise 1994 Ankara Polis Koleji

İş

2002-Komiser-Eskişehir Emniyet Müdürlüğü

2006-Komiser-Ankara Emniyet Müdürlüğü

Alınan Burs ve Ödüller

2004- Üçüncülük Ödülü. Hürriyet Gazetesi Türkiye'nin en başarılı gençleri yarışması

Kişisel Bilgiler

Doğum yeri ve yılı: 22 Nisan 1980 Cinsiyet: Erkek Yabancı dil: İngilizce

ŞEKİLLER LİSTESİ

Şekil 1. Bir Keylogger olan "Proagent" programının arayüzü..... 70
Şekil 2. Phishing işleyiş şeması..... 74
Şekil 3. Sızdırma dolandırıcılığı amaçlı e-posta iletisinin nasıl görünebileceğini gösteren örnek..... 74
Şekil 4. Türkiye Cumhuriyeti Merkez Bankası logolu e-posta ile PHISHING (OLTA) Dolandırıcılığı..... 75
Şekil 5. Bir bankaya ait düzenlenen tuzak web sayfası..... 76
Şekil 6. Alışveriş sitesiyle ilgili örnek..... 77
Şekil 7. Kullanıcıya gönderilen phishing içerikli e-postadan kesit..... 78
Şekil 8. Sahte Google(Internet Arama Motoru) Sayfası..... 80
Şekil 9. "SQL Injection Attacks " işleyişi..... 93
Şekil 10. Alışveriş Kayıt Örneği..... 95
Şekil 11. Kredi Kartı Banka Doğrulama Programı..... 96
Şekil 12. Ortadaki Adam Saldırısı..... 99
Şekil 13. Dns Saldırısı(Pharming) Çalışma Sistemi.....101
Şekil 14. Dns Saldırısı(Pharming) Saldırı Örneği.....101
Şekil 15. 2006 yılı Türkiye İnteraktif Dolandırıcılık verileri.....144
Şekil 16. 2007 yılı Türkiye İnteraktif Dolandırıcılık verileri.....145
Şekil 17. 2008 yılı Türkiye İnteraktif Dolandırıcılık verileri.....146

İÇİNDEKİLER

ÖZ.....ii
ABSTRACT.....iii
JÜRİ VE ENSTİTÜ ONAYI.....iv
ÖZGEÇMİŞ.....v
ŞEKİLLER LİSTESİ.....vi
İÇİNDEKİLER.....vii

GİRİŞ.....1

BİRİNCİ BÖLÜM

YENİ BİR KİTLE İLETİŞİM ARACI OLARAK İNTERNET

1.INTERNET NEDİR?.....3
2.İNTERNETİN TARİHÇESİ.....5
3.İNTERNETİN GÜNÜMÜZDEKİ YERİ VE ÖNEMİ.....7
4.TÜRKİYE'DE INTERNET.....9

İKİNCİ BÖLÜM

SUÇ KAVRAMI

1.SUÇ KAVRAM VE TANIMI.....11
2.SUÇ KAVRAMININ MENŞEİ VE GELİŞMESİ.....11
3.SUÇUN NİTELİĞİ.....13
4.SUÇ VE SEBEPLERİ.....14

ÜÇÜNCÜ BÖLÜM.

GÜNÜMÜZDE 'YENİ' SUÇ KAVRAMI VE SANAL DÜNYA

1. "BİLİŞİM" VE "BİLİŞİM SUÇLARI" KAVRAMLARI.....20
2. HACK VE HACKER.....24
    2.1. Tarihsel Süreç.....24
    2.2. Genel Olarak Hacking.....27
    2.3. Tanımlama.....28
    2.4. Çeşitleri.....28
    2.5. Kavram Çeşitliliği.....29
    2.6. Hacker.....28
3.BİLİŞİM SUÇLARININ KRİMİNOLOJİSİ.....31
    3.1. Bilişim Suçlarında Kriminolojik Bakımdan İlk Gelişmeler.....32
    3.2. Kriminolojinin Bilişim Suçlarından Uzak Kalışı.....33
    3.3. Mevcut Normatif Yapının Yetersizliği.....34
    3.4. Bilişim Suçlarının Beyaz Yaka Suçlarıyla İlgisi.....35
    3.5. Bilişim Suçlarını İşlemeye İten Nedenler.....36
4.BİLİŞİM SUÇLARININ TASNİFİ.....38
    4.1.Bilgisayar Sistemlerine ve Servislerine Yetkisi Erişim ve Dinleme.....40

4.2.Bilgisayar Sabotajı....42
4.3.Bilgisayar Yoluyla Dolandırıcılık....44
4.4. Bilgisayar Yoluyla Sahtecilik....44
4.5. Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı....45
4.6.Yasadışı Yayınlar....45
5.BİLİŞİM SUÇLARINDA FAİL....46
6.BİLİŞİM SUÇLARINDA MAĞDUR....47
6.1. Mağdur bilim (victimology)....48
6.2. Bilişim Suçlarında Durum....49
6.3.Mağdurlarda çekingenlik....50
6.4.Meşru Müdafaa Düşüncesi....51
7. KLÂSİK SUÇLARA GÖRE BİLİŞİM SUÇLARININ YAPISAL GÖRÜNÜMÜ....52
8. BİLİŞİM SUÇLARININ KENDİSİNE ÖZGÜ NİTELİKLERİ....54
9. BİLİŞİM SUÇLARININ TÜRLERİNİ BELİRLEME SORUNU....55

DÖRDÜNCÜ BÖLÜM

İNTERAKTİF BANKA VE KREDİ KARTI DOLANDIRICILIĞI

1.İNTERNET BANKACILIĞI....58
1.1.Tanımlama....58
1.2.İnternet Bankacılığının Yaygınlaşma Nedenleri ve Tüketici Açısından Getirdiği Kolaylıklar....61
1.3.Bankaların İnternet Sitelerinin Çeşitleri....64
1.4.İnternet bankacılığı ve müşteri bilgilerinin korunması....67
2.İNTERNETTE DOLANDIRICILIK TÜRLERİ....68
2.1.Keylogger....68
2.2. Phishing(Olta)....71
2.3. Casus Yazılımlar Ve Trojanlar....80
2.4.Rus Senaryoları....84
2.5.Nijerya Mektupları....89
2.6.Sql İnjections Attacks....91
2.7.Order Log(Alışveriş Kayıtları) Ele Geçirme....94
2.8.Sosyal Mühendislik....97
2.9.Ortadaki Adam Saldırısı (Man-İn-The-İn-Middle Attack)....98
2.10.Dns Saldırısı(Pharming)....99
2.11.Yeniden Yükleyici Yöntemi(Re-Shıppers)....102
2.12.Brute Force ve Dictionary Attack....103
3.İNTERNET BANKACILIĞINDA MEVCUT ÖNLEMLER....105
3.1.Güvenlik Kalkanı....105
3.2.(Ssl) Şifreleme Sistemi....105
3.3.Sanal Klavye....106
3.4.Akıllı Anahtar....106
3.5.Ip Kısıtlaması....107
3.6.Tarih-Saat Kısıtlama....107
3.7.Sms Doğrulama....107
2.3.8.SET (Secure Electronic Transaction) Şifreleme Sistemi....107

4.İNTERNET SUÇLARINA KARŞI HUKUKİ DURUM.....109
4.1.Bilgi Teknolojisi Ve Elektronik Uygulama Zorunluluğunun Etkisi.....110
4.2.İnternet Hukuku.....111
4.3.Uluslararası Durum.....112
4.4.Ülkemizdeki Durum.....114
4.5.Dijital Delil ve Dijital Delillendirme.....117
4.6.Bilişim Suçlarına Müdahale.....121
4.7.Bilişim Suçlarında Örgütlenme.....122
4.8.Adli Bilişim.....123
4.9.Bilişim Suçlarında Koğuşturma.....128
4.10.Bilişim Suçlarıyla Mücadelede işbirliği.....137
4.11.Avrupa Konsey Siber Suç Sözleşmesinde İnteraktif Dolandırıcılık141

SONUÇ VE DEĞERLENDİRME.....144
KAYNAKÇA.....149

GİRİŞ

Bilgisayar Sistemleri ve Bilişim Teknolojileri baş döndürücü bir hızla gelişmeye devam etmektedir. Önceleri sadece askeri kurumların kullanım amacı için geliştirilen bilgisayarlar gün geçtikçe hayatın her alanına girmiş, sadece girmekle kalmayıp Internet'in yaratılmasıyla birlikte dünyamızın da dijital sinir sisteminin var olmasına neden olmuştur. Bu öyle bir sistemdir ki; ordular, istihbarat servisleri, kamu kuruluşları, finans dünyası, haberleşme dünyası, eğitim kurumları, sağlık dünyası, özel sektörün her alanı ve daha sayılabilecek bir çok alan bu yeni dijital sinir sistemin ucunda bağlı bulunan organlara benzetilebilir. Tabiki en büyük faktör "İnsan"dır.

İnsan oğlu büyüğünden küçüğüne gerek sosyal hayatta gerekse iş hayatında bilgisayar kullansın ya da kullanmasın, farkında olsun ya da olmasın bu dijital sinir sisteminin bir parçasıdır. Günümüzde cep veya ev telefonu kullanmayan, bankalar ile işlem yapmayan, sağlık, eğitim, ulaşım ve devlet hizmetlerinden yararlanmayan insan hemen hemen yoktur. İşte bütün bu hizmetlerden kesintisiz bir şekilde yaralanmamızı sağlayan yine bilgisayar sistemleridir. Veriler bilgisayarlarda bizim ya da başkaları tarafından tutulmakta, işlenmekte ve hizmetimize sunulmaktadır. Hayatımıza kolaylıklar getirmektedir. Çağın buluşu, sanayi devrimini geride bıraktığı düşünülen; bilişim teknolojileri ve Internet; topluma genel hizmetlerin kolay işletilmesinin dışında yeni bir iletişim kültürü kazandırmış, insanların birçok alışkanlıklarını değiştirmiştir. Artık günümüzde çoğu insan iletişim kurmak için Internet'i sıklıkla kullanır olmuş, kişisel bilgisayarlarında çeşitli özel bilgilerini depolayıp bunları işler hale gelerek, kağıttan kalemden, hesap defterlerinden günlerce gelmeyen mektuplardan ve online hizmetler sayesinde kuyrukta sıra beklemek gibi sayılabilecek bir çok sıkıntıdan kurtulmuş kısacası zamandan tasarruf ederek teknolojinin verdiği bir çok nimetten yararlanır hale gelmiştir.

Bilgisayar sistemleri ve Internet'in getirdiği hizmetler elbette bu kadar kısa bir şekilde anlatılamaz. Ancak hayatın her alanına girdiği, insanlığa yeni bir hayat tarzı getirdiği büyük bir gerçektir.

Bilişim teknolojilerinin hayatın bir çok alanına girmesiyle birlikte sosyal bir çevrede yaşayan insanın bulunduğu her yerde olduğu gibi bu alanda yada bu alanı kullanarak çeşitli suiistimaller ve suç işleme fiilleri olabilmekte, bununla birlikte yeni yeni suç tipleri ortaya çıkmaktadır.

Günümüz suçluları da kendilerini bu yeni teknolojiye adapte etmekte, gerek bu teknolojinin getirdiği yenilikleri kullanarak menfaat temini yoluna gidebilmekte, gerekse bu teknolojiyi hedef alarak art niyetli faaliyetlerini gerçekleştirebilmektedirler. Hayatımızda önemli bir yer tutan ve farkında olsak da olmasak da kullandığımız ya da yararlandığımız bu teknoloji sağladığı avantajların yanında sakıncalı durumlara da sebebiyet verebilmektedir. Telefon santrallerini yöneten bilgisayar sistemleri 112 acil servisini yanlışlıkla birisinin ev telefonuna yönlendirmiş olsaydı yada tüm telefon numaraları santraldeki bilgisayarların hatası sebebiyle birbirine karışmış olsaydı, yada bankaların bilgisayar sistemlerindeki bir arıza sonucu hesaplarımız üzerindeki tasarruflarımızı kullanamasaydık ve maddi bakımdan zarara uğrasaydık, evimize giderken birden bire trafik ışıkları garip bir şekilde yanlış yanarak iki tarafa aynı anda bilgisayarlarındaki arızalar yüzünden yeşil ışık yaksaydı insan hayatında yaşanabilecek en büyük karışıklıklar denilebilir. . Bu örnekler bir çok alan için çoğaltılabilir.

BİRİNCİ BÖLÜM

YENİ BİR KİTLE İLETİŞİM ARACI OLARAK İNTERNET

1.INTERNET NEDİR?

Internet, birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır.Internet, insanların her geçen gün gittikçe artan "üretilen bilgiyi saklama/paylaşma ve ona kolayca ulaşma" istekleri sonrasında ortaya çıkmış bir teknolojidir. Bu teknoloji yardımıyla pek çok alandaki bilgilere insanlar kolay, ucuz, hızlı ve güvenli bir şekilde erişebilmektedir. İnternet'i bu haliyle bir bilgi denizine, ya da büyükçe bir kütüphaneye benzetebiliriz. Internet'e, bakış açımıza bağlı olarak farklı tanımlamalar da getirebiliriz : Internet,

- 1997 sonu itibarıyla 100,000,000'u aşkın insanın kendi arasında etkileştiği, bilgi değiş-tokuşu yapabildiği ve kendi yazısız kuralları olan büyük bir topluluktur. Bu, internetin sosyal yönüdür.
- Pek çok yararlı bilginin bir tuşa basmak kadar yakın olduğu dev bir kütüphanedir.
- 1997 sonu itibarıyla, 20,000,000'u aşkın bilgisayarın bağlı olduğu çok büyük bir bilgisayar ve iletişim ağıdır.
- Kişilerin değişik konularda fikirlerini serbestçe söyleyebilecekleri ortamlar barındıran bir demokrasi platformudur.
- Evden alış-veriş, bankacılık hizmetleri, radyo-televizyon yayınları, günlük gazete servisleri vb gibi uygulamaları ile aslında internet aynı zamanda bir hayat kolaylaştırıcıdır.

Tüm bu tanımların arakesitinde yer alan ise "Bilgiye Ulaşım ve Onu Paylaşım, sonrasında da elde edilen bilgiyi kullanım" dır. Sonuç olarak, Internet, önümüzdeki yıllarda üretilecek bilgilerin dolaşım sistemidir. Ticari boyutunun da ortaya çıkmasıyla yaşamla daha çok iç içe geçmeye başlamıştır. Internet farklı bir ortam, farklı bir uzaydır. Kendi, yazılı olmayan, kuralları olan; kendi toplumu olan

bambaşka bir uzay. Klasik yaşama biçimlerini, değer yargılarını değiştiren; hayatımıza yeni kavramlar, yeni uğraşlar getiren bir şey denilebilir. Internet hayatı çok fazla bir şekilde etkilemektedir.

Internet'in etkilerini görmek ve onu hissetmek günümüzde çok daha kolaydır. Hayatımızda normal şartlarda yaptıklarımızı göz önüne getirelim ve Internet'in bunları nasıl değiştirdiğini; bunlara nasıl yeni anlamlar yüklediğini gözlemleyelim. Belki bazılarımız için daha az (ya da hiç), bazılarımız için daha çok (ya da aşırı çok) etkilenmeler olacaktır. Ancak gerçek olan, önümüzdeki yıllarda Internet olgusu her yönüyle bizimle olacak ve hayatımızda onunla ilintili pek çok sey yapıyor olacağız (Ağ üzerinden alışverişler, uçak/tren rezervasyonları, günlük gazetelere erişim, bilimsel dergileri okumak gibi.)

İnternet, 20. yüzyılın en büyük değişikliklerinden birisidir ve dünya çapında eşsiz bir iletişim ağıdır.[1] Internet dünyada geçerli olana TCP/IP protokolü ile bilgisayar sistemlerinin dünya çapında birbirine bağlayan ağdır.[2] TCP/IP, internet vasıtasıyla bilgi iletimi ve paylaşımının dayandığı, uyulması gerekli internet protokollerine denir. TCP/IP protokolleri, internet ağındaki veri iletişiminin kurallarını belirler.[3]

Net veya internet, merkezi olmayan, geniş seviyede planlanmış, hiyerarşik bir yapısı bulunmayan global bir (bilişim) ağ yapısıdır. Network olarak da ifade edilen internetin ilk adımlan, 1960'lann sonuna doğru, Pentagon'un sabit bilgisayar sistemlerinin nükleer saldırılara karşı hassasiyetiyle korunmasıyla ilgilenmeye başlamasından sonra, akademisyenler, ABD Hükümeti ve haberleşme uzmanlarının, uzun mesafelerden bilgisayarları, birbirlerine nasıl bağlayabileceklerini araştırmaya başlamaları ile atılmıştır.[4] Daha sonra ise

---

[1] Volkan Sırabaşı, **Internet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (internet Rejimi)**, (Adalet Yayınevi, Ankara, 2003) s. 50.

[2] Murat Önemli, **İnternet Suçlarıyla Mücadele Yöntemleri**, (yayımlanmamış yüksek lisans tezi) (TODAİE, Ankara, Nisan 2004) s.4

[3] Volkan Sırabaşı ,a.g.e., S.55

[4] Liz Duff –Simon Gardiner,**Computer Crime in Global Village: Strategies for Control adn Regulation –in Defence of the Hacker**, (International Journal of the Sociaology of Law ,24,1996) s.211-212

internet, 1990'lı yıllardan itibaren dünya çapında bir bilişim ağına dönüşmüş ve hızla kullanımı yaygınlaşmıştır.[5]

2005 yılı itibarıyla Dünya nüfusunun % 15'nin veya bir milyar kişinin internetle ilgilendiği ve bu rakamın 2009 yılında 6 milyar internete erişim aygıtına çıkabileceği ifade edilmektedir. Geleceğin internet cihazlarının ise, yalnızca bilgisayarlar olmayacağı, bu bağlamda trafik ışıklarının, asansörlerin, pek çok aletin (cihazın) ve hatta kalp pilinin bile bilgisayar yapısında olacağı tahmin edilmektedir.[6]

Amerikan Yüksek Mahkemesi kararlarına göre, "internet, birbirleri ile bağlı bulunan bilgisayarlardan oluşan uluslararası ağdır. İnternet, bireylerin dünya çapında haberleşmesi için tamamen yeni ve benzeri olmayan bir ortamdır".[7]

2.İNTERNETİN TARİHÇESİ

İnternet, bilgisayarları birbirine bağlayan, onları konuşturan, bu yolla insanların zahmetsizce elektronik nesne değişimine olanak veren bir teknolojidir; donanım ve yazılım teknolojisidir. İlk fikirleri 1960 başlarında ABD'de Licklider, Kleinrock ve arkadaşları tarafından ortaya atılan internet, 1965-70 yılları arası laboratuar testleri, 1970-83 saha testlerinden sonra, 1983-1993 yılları arası üniversite, hükümet ve araştırma kurumları arasında kullanılmaya başlanmıştır. 1993'te, Netscape'in dedesi sayabileceğimiz Mosaic programının parasız dağıtılması, internetin tüm iş dünyası ve evdeki insanlara erişerek patlamasına yol açmıştır. Artık bilgisayarlar; metin, ses, resim, videonun içiçe geçtiği, bağlantılarla, zaman, yerden ve bilgisayardan bağımsız olarak aynı sayfa ya da metin içinde bir araya gelebildiği, canlı, parçalara kıtalara dağılmış dev bir kütüphaneye erişim sağlayan bir araç; bir iletişim aracı haline geldi.

---

[5] Gerald R. Ferrara, - Stephen D.Lichtenstein, - Margo E. K.Reder, - Ray August, - William T.Schiano, **Cyber LAW Text and Cases**, (South-Westem Colege Publishing, United States, 2001), s.3.

[6] E.Messmer, 2002, **President's Advisor Predicts Cyber-Catastrophes Unless Security Improves, Network World Fusion**,(www.nwfusion.com/news/2002/0709schmidthtml 1.10.2004)

[7] Volkan Sırabaşı,a.g.e., s.52.

İnternet, her kullanıcıya kendi radyo, gazete ve televizyonun olabileceği bir elektronik yayın ortamı, kullanıcıyla etkileşime geçebilen, veritabanlarını sorgulayan bir ticaret ve çalışma ortamına dönüşmüştür.İnternet, nükleer bir savaş sırasında, pek çok bilgisayarın zarar gördüğü bir ortamda haberleşmeyi mümkün kılmak için tasarlanmış bir sistemdir. Mesajlar küçük paketlere bölünmekte ve başına adres ve parça bilgisi eklenerek, hedefe, bilgisayar ağındaki değişmeleri gözönüne alarak dinamik bir yol izleyerek ulaşmaktadır. Bu araştırmanın sonuçları ARPANET (Advanced Research Project Agency Network) adı verilen ileri/geliştirilmiş araştırma projeler ağında denenmiş ve Kaliforniya Üniversitesi'nce geliştirilen Unix işletim sistemi ile herkesin kullanımına açılmıştır. Bu ağ bir süre sonra, donanımı büyük ölçüde bağış usulü ile sağlanmış olan üniversiteleri birbirine bağlamada kullanıldı. 1989 yılında ABD hükümeti ARPANET'i finanse etmeyi bırakma kararı alınca ağa bağlı kullanıcılar, internet adı verilecek sistem için tasarılar hazırladılar. Sözcük o zamandan beri çifte anlamda, hem ağın kendisi hem de ağ üzerindeki iletişimi yöneten protokoller için kullanılmaya başlandı. Ticari bir hizmet olduğunda bile, internetin ilk müşterileri çoğunlukla araştırma kurumları, bilgisayar şirketleri, üniversite bilim adamları ve e-posta alış-verişi için ağı kullanan öğrencilerdi.[8] Anlaşılacağı üzere internet tek bir şebeke olmayıp, birbirlerine bağlı ağların adıdır. İnternet, bir çok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır.

İnternet, insanların her geçen gün gittikçe artan, üretilen bilgiyi saklama-paylaşma ve ona kolayca ulaşma istekleri sonrasında ortaya çıkmış bir teknolojidir. Bu teknoloji yardımıyla pek çok alandaki bilgilere insanlar kolay, ucuz, hızlı ve güvenli bir şekilde erişebilmektedir. İnternet bu haliyle bir bilgi denizine ya da büyükçe bir kütüphaneye benzetilebilmektedir.

İnternete, bakış açısına bağlı olarak farklı tanımlamalar da getirebilir. İnternet, sanayi toplumundan bilişim toplumuna geçişin habercisi, taşıyıcısı, bir ön modelidir. İnternet bilimsel ve teknolojik gelişmenin önemli bir etmeni, taşıyıcısı,

---

[8] Bill Gates, **Dijital Sinir Sistemiyle Düşünce Hızında Çalışmak,**(Çeviren:Ali Cevat Akkoyunlu, Doğan Kitapçılık, 4.Baskı, İstanbul, Nisan.1999).s:109

kendisi sürekli değişen, bilgi teknolojilerini değiştiren, giderek toplumu ve yaşamın tüm boyutlarını değişime zorlayan bir teknolojiler kümesidir.[9]

İnternet'te geç kalmak, telafisi mümkün olmayan sonuçlar doğurabilir; İnternet en basitinden çağdaş matbaadır.[10] İnternet sayesinde bölgesel farklılıklar ya da bilgi eksikliği nedeni ile fiyat farklılığı yaratmak da tarihe karışmak üzeredir. İnternet ile herkesin bir dokunuşla herhangi bir malın fiyatını farklı alternatiflerden öğrenebilmesi dünyanın en kolay işi haline gelmektedir. Artık çok ciddi ölçek ekonomileri oluşmakta ve bu ekonomiler fiyat rekabeti olasılığını giderek arttırmaktadır. İnternet göz ardı edilerek hiçbir strateji düşünülemez. Hayatın nasıl etkileneceğini düşünmeye başlamak ve çok ciddi olarak bir yerlerden başlamak gerekmektedir .

İnsanlar kalacakları oteli veya yemek yiyecekleri lokantaları internet bağlantıları yoksa tercih etmeyecekler, internetsiz bir otelin telefon ve faksı olmayan bir otelden farkı kalmayacaktır.

3.İNTERNETİN GÜNÜMÜZDEKİ YERİ VE ÖNEMİ

İnternet'i bir "iletişim ağı" olarak tanımladıktan ve bu ağ üzerinde bilgi dolaştığını belirttikten sonra, internet'in bu altyapı üzerinde neler sunduğunu tahmin etmek aslında o kadar da güç değildir. Bu "iletişim ağı"nın içinde bulunan her hangi iki bilgisayar arasındaki en temel işlem çift yönlü bilgi aktarımıdır. Burada bilgiden kasıt, bilgisayarlardan birinde bulunan bir dosya, bir bilgisayar programı ya da bir mesajdır.

Internet, teknik olarak, TCP/IP protokolü ile desteklenen pek çok servis sunar. Örnek olarak, Internet erişimi olan bir kullanıcı, eğer kendisine yetki verilmişse, Internete bağlı diğer herhangi bir bilgisayardaki bilgilere erişebilir, onları kendi bilgisayarına alabilir, kendi bilgisayarından da Internet erişimi olan başka bir bilgisayara dosya/bilgi gönderebilir. Bu özellik, dosya transfer protokolü

[9] Esra Öztop,**İnternet'in Bireye ve Sosyal Hayata Etkileri,Türkiye'deki Durum**,(2002),s.6

[10] http://inet-tr.org.tr/inetconf4/inet98-akgul.html

olarak bilinir. Benzer şekilde, internet uzerindeki kullanıcılar birbirlerine elektronik posta gönderebilirler. Bu da, posta iletim protokolü olarak bilinir.

İnternet, değişik protokoller aracılığı ile, insanlara "bilgiye erişim" olanakları sunar. Yani, internet yardımıyla "her çeşit" bilgiye erişebilirsiniz.

İçerik bakımından, Internetin sundukları bazen insan hayal gücünü zorlayacak boyutlara varmaktadır. Vizyondaki filmlerin kısa tanıtımlarını kolayca evimizdeki ekrana taşıyabilir ya da Amerikan Kongre Kütüphanesi'nde tarama yapabiliriz.

Tübitak arşivine bağlanıp Bilim ve Teknik dergilerinin yeni ve eski sayılarını tarayabilir, yazıları okuyabiliriz. Ya da, Hacettepe Üniversitesine uzanıp o anki Beytepe Kampüsü sıcaklıklarını grafiksel olarak görebiliriz. Başka bir örnek olarak, katılmak istediğimiz bir bilimsel toplantıya bildirimizi Internet üzerinden gönderebiliriz. Örnekleri arttırmak mümkün; Nasa servislerine bağlanıp, son uydu fotoğraflarını tarayabiliriz; ya da Şiir arşivlerine bağlanıp şiirler okuyabiliriz. Son yıllarda geliştirilen World Wide Web (WWW, Web) temelli internet araçları ile bilgiye ulaşım daha da kolaylaşmış ve ulaşılabilecek bilgiler ve sunulan servisler miktar ve çeşit olarak artmışlardır. İnternet'in sundukları; onu kullananların istekleri, hayal güçleri ve gelişen İnternet teknolojisi ile hep çoğalmaktadır.

İnternet, bilgiye ulaşmayı kolaylaştırmak için değişik 'bilgi arama/tarama' yöntemleri de sunar. Internet'in sundukları çok geniştir ve bu kadar bilgi arasında, bilinçsiz bir kullanımla, insan yolunu çok kolay kaybedebilir.

Bütün dünya üzerinde Internet'e; üniversiteler, araştırma enstitüleri, kamu kuruluşları, pek çok ticari kuruluş vb gibi değişik yerler bağlıdır ve İnternet'e bağlı bilgisayar sayısı 400,000,000 civarında tahmin edilmektedir. Bu sayı her gün süratle artmaktadır. Ortalama Internet kullanıcısı sayısının ise, 100,000,000 'un üzerinde olduğu tahmin edilmektedir.[11] Internet iletişim ağına bağlı bir bilgisayarın bir tek kullanıcısı olabildiği gibi, birden çok (bazen yüzlerce, binlerce) kullanıcısı

[11] http://www.webhocam.net/konuizle.asp?t=1769

da olabilir. Kişisel bilgisayarlar ve evden bağlantılar tek kullanıcılı internet bağlantılarına örnek olarak verilebilirler. Öte yandan, aynı anda birden çok kullanıcının erişebildiği ve kullandığı daha çok "unix" işletim sistemi ile çalışan orta ve büyük boy sistemler de çok kullanıcılı internet bağlantı örnekleridir.

Internet'in 1990'ların başlarından itibaren bu kadar yaygınlaşmasının en temel nedenlerinden birisi ve belki de en önemlisi "para kazandırabilecek potansiyele sahip" bir imkan olmasıdır. Bu iletişim ağına bağlı bilgisayarlar yolu ile alışverişler yapılabilmekte, borsa/bankacılık işlemleri yerine getirilebilmektedir. Bu haliyle internet'in "ağ teknolojisi" kimliğinin yanında bir de "medya" özelliğinden söz edebiliriz. Internet artık ciddi reklam paralarının dönmeye başladığı ve şirketlerin ürünlerini pazarladığı bir ortam haline gelmeye başlamıştır.[12]

4.TÜRKİYE'DE INTERNET

Türkiye Internet'e Nisan 1993'ten beri bağlıdır. İlk bağlantı ODTÜ'den gerçekleştirilmiştir. 64kbit/san hızında olan bu hat, çok uzun bir süre, tüm ülkenin tek çıkışı olmuş ve ilgili arkadaşlar büyük bir özveriyle İnternet'i tüm Türkiye'de (öncelikle akademik ortamlarda) yaygınlaştırmaya çalışmışlardır. Ege Üniversitesi'nden olan bağlantı ise, 1994 başlarında, 64kbit/san. hızı ile gerçekleştirilmiştir. Ardından sırayla, Bilkent Ün.(1995 Eylül), Boğaziçi Üniv. (1995 Kasım) ve İTÜ (1996 Şubat) bağlantıları gerçekleşmiştir. 1996 yılı Ağustos ayında da Turnet çalışmaya başlamıştır.[13]

1998'de de Ulaştırma Bakanlığı bünyesinde İnternet Üst Kurulu oluşturulmuştur. Daha sonra bu kurul, İnternet Kurulu olarak faaliyetlerini sürdürmeye devam etmiştir. 8-21 Nisan tarihleri arasını "İnternet Haftası" ilan edilmesi üst Kurulun faaliyetleri arasındadır. Her yıl kutlanan hafta her ne kadar son yıllarda sönük geçiyorsa da, Türkiye'de internetin kamuoyuna ulaşmasında büyük bir işlev yüklenmiştir.

---

[12] http://www.gencbilim.com/odev/odevgoster.php?il=eskisehir&id=18202

[13] http://www.sayfa.com/forum/showthread.php?t=4086

2000 yılında kullanıcı sayısı 1.785.000 olan internetin, 1 yıl İçinde % 100'den fazla hızlı yükselişini, 2003'ten 2004'e geçişte de sürdürdü.2007 yılına geldiğimizde kullanıcı sayısı 17 milyon civarındadır.

Dünya İnternet İstatistikleri Sitesi verilerine göre, toplam nüfusu 809 milyon 624 bin 686 olan Avrupa ülkelerinde, 314 milyon 792 bin 225 kişi internet kullanmaktadır. 50 milyon 471 bin 212 internet kullanıcısı ile Avrupa'da internetin en fazla kullanıldığı ülke Almanya'yı, 37 milyon 600 bin kişi ile İngiltere, 30 milyon 837 bin 595 kişi ile Fransa izlemektedir. İtalya'da 30 milyon 763 bin 940 kişi, Rusya'da 28 milyon kişi, İspanya'da 19 milyon 765 bin 32 kişi internet kullanırken, Türkiye ise 16 milyon internet kullanıcısı ile 7'nci sırada bulunmaktadır. Hollanda'da 12 milyon 60 bin kişi, Polonya'da 11 milyon 400 bin kişi internet kullanmaktadır. Almanya'da nüfusun yüzde 61.2'si, İngiltere'de yüzde 62.3'ü, Fransa'da yüzde 50.3'ü internet kullanırken, İtalya'da nüfusun yüzde 51.7'si, Rusya'da yüzde 19.5'i, İspanya'da yüzde 43.9'u, Türkiye'de ise nüfusun yüzde 21.1'i internet kullanmaktadır.[14]

Yurt içi ve yurt dışındaki alan adı sayısı 600 bin civarında. ADSL kullanıcısı 3.5 milyon, Kablo Net kullanıcısı 50 bin civarındadır. İnternete 700 bin bilgisayar kayıtlı durumdadır.[15]

---

[14] http://www.haberdefteri.com/haberbak.php?id=9049

[15] http://forum.iyinet.com/guncel-konular-haberler/54386-turkiyede-internet-14-yasinda.html

İKİNCİ BÖLÜM

SUÇ KAVRAMI

1.SUÇ KAVRAM VE TANIMI

Suç, insanın sosyal bir varlık olması ve bireyin toplumla çatışması nedeniyle eskiden beri varolan ve gelecekte de sürecek bir olgudur.

İnsan, toplum içinde yaşayarak, kendini denetleyerek ve sınırlayarak toplumun bir üyesi olurken bir taraftan kültürün, uygarlıkların gelişmesine katkıda bulunurken öte yandan toplumca kabul edilmeyen davranışların da ortaya çıkmasına yol açar.[16]

2.SUÇ KAVRAMININ MENŞEİ VE GELİŞMESİ

Suç denilen olaya, yani belirli hareketlerin yasak fiillerden sayılmaları ile, bunları işleyenlerin çeşitli tepkilere konu olmalarına, devlet müessesesi şeklinde gelişmiş insan toplumlarının meydana çıkışından çok önce bile rastlanmıştır. Tarihte hiçbir toplum yoktur ki, orada belirli fiiller yasaklanmamış ve bunun karşılığı olarak ceza müeyyidesi var bulunmamış olsun. Suçlar toplumların sosyal, ekonomik ve manevi şartlarına göre şekillenmiştir.

Toplumbilim (sosyoloji) kişinin, iştirakçisi olduğu toplumun bilinçli bir üyesi olabilmesi, toplumsal kültürün gereklerine göre hareket edebilen bir kişilik kazanabilmesi için, sosyalleşmenin gerekli olduğunu belirtmektedir. Sosyalleşmenin gereğine uygun olarak gerçekleşmesi zorunludur. Sosyalleşmede ise başta gelen araç cezalandırma ve ödüllendirmedir.[17]

---

[16] http://www.muttrafik.8m.com/sucpsik.html

[17] Ord.Prof.Dr. Sulhi Dönmezer'in bu yazısı kendisine ait "**Kriminoloji**" kitabından alınmıştır. (8.bası, Beta, İstanbul, 1994) s.55,56

İnsanlar ilkel devirlerde her şeyde bir ruh ve canlılık görmüş ve belirli fiil ve hareketlerin icra edilmemesine ilişkin emirleri, tabuların emri saymışlardır. Kötülük yapanları veya yapanları cezalandırmayanları sözü geçen kuvvetlerin, tabuların şiddetle cezalandıracaklarına, felâkete uğrayacaklarına inanılmıştır. Fakat bazı hallerde ilâhların, tabuları ihlâl edenleri hemen cezalandırmadıkları görüldüğünden toplumun müdahale ile kuralı ihlâl edeni cezalandırması zorunlu sayılmış ve böylece toplumun felaketlerden, kıtlıktan korunabileceği kabul edilmiştir.

Sonradan suç, dini esaslarla tanımlanmış, topluma zarar veren fiil ve hareketlerin aynı zamanda birer günah teşkil ettiği ve Allah'ın iradesine karşı olduğu kabul edilmiştir. Zamanla ve yüzyıllar içinde suç fikri gittikçe lâikleşmiş ve suçun zarar veren kişi ile toplum arasındaki ilişkileri ilgilendirdiği görüşüne varılmıştır.

18. yüzyılın başlangıcından itibaren suç fikri lâikleşmeye başlar ve suçun zarar veren kişi ile toplum arasındaki ilişkilerde aranması gerektiği fikri ortaya çıkar; bu düşünce kısa bir süre içinde yaygınlaşır. Gelişme, bazı yazarlarca, rasyonel bir suç kavramına yönelinmesi olarak ifade edilmiştir.

Suç fikrinin rasyonelleşmesinin asıl anlamı başta devletin, tekel bir yetkinin sahibi olarak suçları belirlemek ve ceza vermek hakkını elinde tutması, daha doğrusu eline almasıdır. Bu gelişmenin yüzyıllar boyu devam eden insanlık dışı ve dehşet verici uygulamalar sonunda ortaya çıktığını ise tarih göstermektedir.

Uzun yüzyıllar sonra böylece rasyonel bir suç kavramına ulaşılırken, ilkel esaslar daima etkisini göstermeye, varlıklarını hissettirmeye devam etmişlerdir. Bugün ceza kanunlarındaki bazı suç tariflerinin kökenini ilkel devirlerde bulmak kabildir.[18] Sosyal şartlar bugünde ilkel dönemlerinkine benzer şekiller alınca eski devirlerin hukukî müessese ve kavramlarının meydana çıktığı görülmektedir.

---

[18] Reckless, **The Crime Problem**, (second edit, New York, 1955), s.20

Bu günün kanun koyucuları, hiç şüphesiz, ilkel devirlerden gelen ve kalan âdet ve geleneklerle yetinmemekte ve çeşitli alanlardaki ilişkilere dayalı suçları koymaktadırlar.

Kanun koyucular, bugün, genel olarak, kamu sağlığını, güvenliğini ve tabiî kaynakları korumak, iş ve ticaret alanında uygunsuz ve hileli uygulamaları önlemek, devlet gelirlerini korumak maksatları ile suç koymaktadır.[19] Günümüzde genel ahlâk ve âdabı korumak amacı ile suç koymak söyle dursun, hatta, bu konuda bazı fiilleri suç olmaktan çıkarmak yada bazı fiilleri sadece idarî tedbir ve müeyyidelerle yolu tutulmaktadır.[20]

Türk kanun koyucusu da suç koyma faaliyetinde aynı maksatları izlemektedir. Ancak Türkiye'nin geçirdiği devamlı değişiklik rejimleri, vatandaşların davranışlarına şekil ve yön vermek maksadını güden ve bu maksatla suç koyan devrim kanunlarının da konulmasını gerektirmiştir.

Ancak kanun koyucunun belirli suçları yaratmak için koyduğu kanunların başarılı olabilmesi ve uygulanabilmesi kamuoyunun bunları tutmasına bağlıdır. Yeni suç koyan kanunların, çok kuvvetli olarak, kamuoyunca desteklenmesi gerekir. Bu sebeple esasında öteden beri var olan bir örf ve âdete dayanan kanunlar çok daha başarılı olarak uygulanırlar.[21]

3.SUÇUN NİTELİĞİ

Suç, evrensel, genel bir olaydır. Suç tarihin en eski devirlerinden itibaren var olmuştur ve ileride de var olmaya devam edecektir. Suçsuz bir toplum hayalden başka bir şey değildir. İnsanların içinde ihtiraslarla birlikte toplum

---

[19] Edwin H. Sultherland-C.E. Gehlke, **Crime and Punishment (Recent Social Trends in the United States**, (New York, 1933) s.1116 ve son. Zikreden Reckless, 20)

[20] Sulhi Dönmezer, **Ceza Adalet Reformunun İlkeleri** (Ceza Adalet Reformu İlkeleri Sempozyumu, 24-26 Şubat 1972, İstanbul, 1972), s.1 ve son

[21] Sulhi Dönmezer, **Toplum bilim**, (11 bası, İstanbul, 1994)

halinde yaşamanın ortaya çıkardığı çeşitli sosyal çelişkiler, uyumsuzluklar bulundukça suçta var olacaktır. Suç bir bakıma, bazı kişilerin davranışları ve tutumları ile bunların içinde yaşadıkları grupta yerleşmiş davranış örnekleri ile arasında bir çelişkidir. Bu çelişki her zaman ve her yerde zorunlu olarak var olacağından, suç genel ve evrensel bir olay teşkil eder ve adam öldürme, hırsızlık gibi çeşitli suçların farklılığına rağmen bir çeşit bilimsel yönden gözlemin yapılması kabil ve bilimin konusunu oluşturan bir olay niteliği ile varlığını korur.

Suçun diğer esaslı bir vasfı da göreceli olmasıdır (nisbiliğidir). Suçu oluşturan fiiller zaman ve ortama göre değişiktir. Bugün ağır suç sayılan eylemler geçmişte bazen hatta vatanseverliğe âlamet idi. Bu gün suç sayılmayan bazı fiillerde geçmişte en ahlâk dışı hareketler olarak sayılmakta idi.

Bazı yazarlar bu niteliğine dayanarak bunların bir bilimin araştırma konusunu oluşturamayacağını açıklamıştır. Ancak nevî ve biçimi ne olursa olsun, insan toplumda suça karşı tepkiyi, müeyyideyi isteyen duygular aynıdır. "O halde görülüyor ki, suçun nisbîliği, cezalandırılan fiilin ayniyetine değil; fakat ceza tepkisini tahrik eden duyguların özdeşliğine dayanır".[22]

4.SUÇ VE SEBEPLERİ

Suç evrensel ve genel bir olgudur.Suç tarihin en eski devirlerinden itibaren var olmuştur ve ileride de devam edecektir.

Her devir ve zamanda bir hareketin topluma zarar vermekte olduğu veya tehlikeli bulunduğu fikir ve düşüncesinde olan kanun koyucular sözü geçen fiilleri kanunla yasaklar ve ceza usullerini gösterirler.Topluma zarar verdiği yada tehlikeli olduğu kanun koyucu tarafından kabul edilen ve belirtilen eyleme suç denir.Dolayısıyla bir eylemin suçu oluşturması için kanunla düzenlenmiş olması gerekir.

---

[22] Bouzat-Pinatel, I, ; Dönmezer-Erman, III, ; Üzülmez, **Türk Hukukunda Tekerrür**, s.42

Suçun nedeni bir veya birden çok olabilir.Bunları genel olarak suçlunun kişiliğini yapan unsurlar, içinde bulunduğu fiziki ve sosyal şartlar, genel kültür v.s. gibi düşünülebilir.

Suçlunun kişiliği konusu suç nedeni olarak 'Biyolojik Faktörler', 'Fizyolojik Faktörler' ve 'Psikolojik Faktörler' olarak düşünülebilir.

İnsanda çoğu ahlaki güçler doğuştandır. Karakterimizin, duygularımızın ve melekelerimizin kaynağı değişmez bir şekilde saptanmıştır. Bu insan psikolojisinin asıl ve esasını oluşturur.

Fizyolojik faktörler insanları iradeleri dışında suç işlemeye yöneltir.Bunlar 'Doğuştan Suçlular' olarak adlandırılır.Doğuştan suçluları belli eden asıl nitelik bunların ufak, küçük suçları işleyerek işe başlamaları yerine birdenbire en büyük suçları işlemeye girişmeleri ve ahlak hissinin doğuştan yokluğu nedeni ile ıslahlarının mümkün olmayışıdır.

Yapılan incelemeler genellikle insan öldürenlerin bakışlarının donuk, sabit ve gözlerinin kanlı olduğunu göstermektedir.Hırsızlarda ise bakışlar hileli, hareketli ve gözler eğridir.Ayrıca insanın genlerini aldığı anne ve babasının fiziki ve ahlaki karakterlerini taşıdığı bir gerçektir.

Suçların başka nedenleri de vardır.Bunları şöyle sıralayabiliriz:

1-)Zeka ve Suç
2-)Aile ve Suç
3-)Öğrenim ve Suç
4-)Ekonomik Durum ve Suç
5-)Kitle Haberleşmesi ve Suç
6-)Genel Kültür ve Suç
7-)Yaş ve Suç
8-)Fiziki Bozukluk ve Suç
9-)Irk ve Suç
10-)Cinsiyet ve Suç

1-)Zeka ve Suç

Zekası az olan kişi bulunduğu kültürün sosyal değerlerini kavrama ve ona uyma yeteneğine sahip değildir.Hareketlerinin sonuçlarını göremez.Böyle kişiler telkine yatkın bir tip olduğundan zekası parlak ama suç yolundaki insanların etkisinde kalarak suç işleyebilirler.

2-)Aile ve Suç

Çocuğun karakterinin şekillenmesi ve beslenmesi yönünden aile ve evin önemi büyüktür. Aile içindeki ilişkiler, uyum, ailenin ekonomik durumu, kültür seviyesi çocuğun üzerinde ileride nasıl bir insan olacağında büyük etkisi vardır.

3-)Öğrenim ve Suç

İnsanların özelliklede çocukların aileden sonra en yakın çevresini okul oluşturur.Okul çocuğun hayatında ilk sosyal tecrübeleri edindiği yerdir.Buradaki gerek arkadaşları gerekse öğretmenleri ile ilişkilerinde kusurlu usul ve prensipler uygulandığında çocuğun karakterinin oluşmasında zararlı sonuçlar ortaya çıkabilir.

4-)Ekonomik Durum ve Suç

Yoksulluk suç üzerinde ya doğrudan doğruya yada dolaylı yoldan etki eder.Karnı aç olan bir kişinin çalışma eğilimi oldukça yüksektir.Yoksulluk ve zaruret insanların kötü mesken şartlarını ve bu tür ikamet bölgelerine sığınmış olan suçlularla daimi temas etmelerine sebep olur.Ayrıca çocuklar suçluların yaptıkları kötü hareketleri taklit etme imkanını bulmalarına, anne ve babanın aynı zamanda çalışmaya mecbur olmaları dolayısıyla da çocuklar ile yakın ilgilenememeleri suça yönelmeye sebep olabilir.

5-)Kitle Haberleşmesi ve Suç

Gazete, dergi, TV gibi basın ve yayın organlarının suça teşvik edici yayınlar yapmaları ve bu tür yayınların suça yatkın insanlar tarafından izlenmesi suça teşvik bakımından zararlı görülmektedir

6-)Genel Kültür ve Suç

Öğrenim durumu ile suç arasında yakın ilişki bulunduğu bilinmektedir.Yapılan araştırmalar okuma ve yazma bilmeyenlerin suç işleme oranının çok fazla olduğunu göstermektedir.

7-)Yaş ve Suç

Genellikle aktif olan, hareket ve şiddet gerektiren suçlar gençler tarafından işlenir.Buna karşılık hile ile bir arada işlenen suçlar yaş bakımından olgunluğu gerektirir.Yapılan araştırmalara göre suçluluğun küçük yaşlardan itibaren yavaş yavaş artarak orta yaşlarda yoğunlaşıp yaş ilerledikçe azaldığını ve ileri yaşlarda hemen hemen ortadan kalktığını göstermektedir.

8-)Fiziki Bozukluk ve Suç

Fiziki bozukluklar ve çirkin oluş ile suç arasında da bir ilişki olabileceği düşünülebilir. Çirkin insanın hayatta bir takım zevklere ve sıkıntılara güzel insanlardan daha fazla alanda rastlayacağı ve çevresinden göreceği muamelelerin aşağılık kompleksi ile onu belki de aşırı tepkilere sürükleyerek, suçu sonuçlayan bir sebep niteliği görebilir.

9-)Irk ve Suç

Irk verasetin grup bakımından görünüşünü belirtir.Bazı ırklar gerek iklim şartları gerek genel kültürleri bakımından diğerlerine nazaran suça daha eğilimlidirler.Örneğin; Güney İtalya'da oturanların çabuk hırslanan ve kanı sıcak

bünyeye sahip oldukları söylenebilir. Kültür ve sosyal gelenekler insanların suç işlemelerine sebep olabilir

10-)Cinsiyet ve Suç

İstatistikler erkeklerin kadınlardan daha çok suça eğilimli olduklarını göstermiştir.Kadının bedensel gücünün azlığı, cesaret azlığı gibi sebepler suç eğilimini azaltmaktadır.

ÜÇÜNCÜ BÖLÜM

GÜNÜMÜZDE 'YENİ' SUÇ KAVRAMI VE SANAL DÜNYA

Teknolojinin her geçen gün; insanoğlunu daha rahat ve daha mutlu yaşaması için sürekli değişim içerisinde bulunması sevindirici olmakla birlikte; bu değişim veya bu ilerleme suç kavramının da gelecekte daha farklı olacağının sinyallerini vermekte,şimdiden gerek ülkelerin gerekse de kişilerin başını fena şekilde ağrıtmaktadır.

Bilgisayar ve internet teknolojisinin hızlı gelişimi sonucu oluşan e-dünya düzeninde normlar ve etik değerleri[23] azami süratte şekillenmektedir.Eğitimde ticarete,devlet sektöründen özel sektöre,eğlenceden alışverişe kadar birçok avantaja olanak sağlayan bu hızlı gelişim,sosyal ve teknolojik yönden dengesiz değişimler,tehlike ve tehditleri de ortaya çıkarmıştır. Her dönemde,o döneme ait değerlere göre şekil alan suç kavramı,günümüzde gelişen teknoloji ile bu yönde kendini çoktan biçimlendirmeye başlamıştır. Günümüzde bilginin önem kazanması ve (sosyal,ekonomik,siyasal) konular[24] üzerinde söz sahibi olmak isteyenler için bilişim teknolojileri fevkalade önemli bir araç konumunda olmaktadır.

Suç kavramları arasında kendisine yer açan "Bilişim Suçları" da gelişen teknolojinin içerisinde ifade edilmeye başlamıştır.Bilişim teknolojileri ile beraber artık ülkeler arasındaki sınırlar kalkmış,bilgisayar ağları,Internet vb. ile uluslar arası bir boyut kazanmıştır.Bu bağlamda bilişim suçları ile gereken mücadelenin verilebilmesi ancak,dünya çapında bir işbirliği ile mümkün olabilmekte ise,bunun tersine ulusal bağlamda başarılı olmak neredeyse mümkün değildir.

---

[23] Semih Dokurer, **a.g.e.**,s.2

[24] Mehmet Özdemir -**Bilişim Suçları Ve Mücadelede Karşılaşılan Problemler ve Çözüm Önerileri**

Bilgi güvenliği konusunda G.J.Simmons'ın[25] belirttiği gibi "Bilgi güvenliği,fiziksel bir değerliliği bulunmayan bilgi temelli sistemlerde bilgi dolandırıcılığını tespit etmek,buna karşı korunmak veya başarılı olmasını engellemekle ilgilenir."Bilgi güvenliğinin sağlanması hususunda,bilgi edinen ve paylaşımında bulunanlar hassas olmalıdır.Çünkü bilgi güvenliği yalnız bir kuruma ait olmamakla birlikte,bu ortam içerisindeki herkese lanse edilmiş bir kavramdır.

1. "BİLİŞİM" VE "BİLİŞİM SUÇLARI" KAVRAMLARI

"Bilişim" (Informatics,Information System)[26] kelime anlamıyla;insanların teknik,ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin,özellikle elektronik makineler aracılığıyla düzenli ve akılcı bir şekilde işlenmesine denir.Halk arasında bilişim kavramı ile bilgisayar birlikte anılmaktadır.Buna rağmen bilişim bir bilim olmasına rağmen,bilgisayar ise bilişimin bir ürünüdür.Bununla birlikte bilgisayarın sözlükteki manasını dikkate aldığımızda da bu ayrımı görebiliriz.

Tanıma göre bilgisayar[27];çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi,önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç,veya elektronik beyin olarak ifade edilir. Bilişim ve bilgisayar terimleri arasındaki bariz fark; bilişim bilginin kendisi olarak tabir edilirken,bilgisayar ise bu bilgiyi işleyen araçtır.

"Bilişim Suçları" halk deyimiyle "Bilgisayar Suçları" olarak tanımlayabildiğimiz gibi "İletişim Suçları" , "Internet Suçları" , "Dijital Suçlar" , "Teknolojik Suçlar" , gibi tanımlamalar da yapabiliriz. [Computer Crimes, Cyber Crimes,Internet Technology Crimes,Digital Crimes][28] .Genel manada bilişim suçları, her türlü teknoloji kullanılarak,kanuni olmayan yollarla kişisel ya da

---

[25] .http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/s/Simmons:G=_J=.html,Çankaya,Ayhan – Bilişim Suçları

[26] http://www.bilisimterimleri.com/?arananterim=bilişim&dil=tr

[27] Türk Dil Kurumunun Hazırlamış Olduğu Türkçe Sözlükte **Bilgisayar** Tanımı

[28] http://www.bilisimterimleri.com

kurumsal bilgisayarlarda,sistemler üzerinde zarar verici etki bırakmaktır.Bilişim teknolojilerinde suç meydana gelebilmesi için mutlaka teknoloji kullanılmalıdır.Bu teknoloji bilgisayar,kredi kartı,telefon,poss makinesi,elektronik bir cihaz olarak düşünülebilir. Bilişim suçları hakkında AET Uzmanlar Komisyonu'nun Mayıs 1983 yılında Paris Toplantısında yaptığı tanımlamaya göre; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanun,gayri ahlakî ve yetki dışı gerçekleştirilen her türlü davranıştır." denmektedir.

Son zamanlarda, "cybercrime" kavramına eş anlamlı olarak "hi-tech crime" yani "yüksek teknoloji suçu" ve Verime" kavramları da kullanılmaktadır. Bu konudaki en farklı nitelemelerden birisi ise, "multi-jurisdictional erime" "çok yargısal suçlar" kavramıdır.[29] Bilişim suçları, özellikle dünya çapındaki internet ağı nedeniyle bu şekilde ifade edilmiştir. Bu suçlara yönelik son nitelemenin diğer bir nedeni ise, bu suçlarla mücadele ederken, birden fazla yargı yerine gerektiğinde yetki vererek, bilişim suçlarıyla mücadelede başarıyı artırabilmektir.

Bilgisayar teknolojisinin ve internetin hızlı gelişimi, yeni suç tiplerini ortaya çıkarmakta ve suçla mücadelede yeni yasaları gerekli kılmaktadır. Başlangıçta, bilişim suçları, geleneksel suçların bilgisayar yoluyla işlenmesi olarak kabul edilirken, zamanla teknolojinin getirmiş olduğu önceki suç tanımlarına benzemeyen yeni suç tipleri ortaya çıkmaktadır. Bilişim suç tiplerindeki çeşitlilik ve sürekli artış, bu suçlarda tek bir tanımın yeterli olmamasına neden olmaktadır.[30]

Amerikan Adalet Bakanlığı'nda ve kimi görüşlere göre, çoğunlukla bilişim suçlan, bilgisayar teknoloji bilgisini kullanarak, ceza kanundaki herhangi bir fiilin, işlenmesi veya araştırılması veya sürdürülmesi olarak tanımlanmaktadır.[31] Çünkü, bilişimin pek çok suçta kullanılabilmesi, daha dar bir tanımı yetersiz kılmaktadır. "Bilişim suçu", bilgisayar kullanılarak işlenen klâsik suçları da kapsamaktadır.

---

[29] Barbara Etter, **Leadership in the Hi-Tech Crime Environment**, (Australasian Centre For Policing Research To 2/2002 Pelp At The Aipm Sydney, 14 August 2002), s.1

[30] Michael Hatcher, - Jay Mcdannel, - Stacy Ostfeld , **Computer Crimes**, (American Criminal Law Review, Vo.36, no.397, 2001), s.398-399

[31] Robert Dıtzıon, - Elizabeth Geddes, - Many Rhodes, , **Computer Crimes**, (American Criminal Law Review, 40 no2, September 2003), s.285; Michael Hatcher, - Jay Mcdannel, - Stacy Ostfeld , a.g.e. s.399

Bilgisayar teknolojilerinde ve bunun daha üstünde yer alan "internet"teki hızlı gelişmeler, bilişim suçlarının değişik kategorilerini oluşturan yeni teknolojik suç çeşitlerini üretmektedir.[32]

Yabancı hukukta da bilişim suçları konusunda değişik tanımlamalar yer almakta ise de, üzerinde geniş kabul gören bir tanım olduğunu söylemek zordur. Bazı yazarlara göre, bilişim suçu, büyük miktarda para çalmak için bilişimi kullanılmasıdır. Diğerlerine göre, biraz önceki tanımlama içerisine, özel hayata saldırı ile hizmet hırsızlığı da girmektedir, ikinci görüşe göre, esasında tanımlama sorununda, servet, hizmet ve para kaynaklarına herhangi bir aldatma ile ulaşılması için bilgisayarın kullanılması önem taşımaktadır. Diğer bir görüşe göre ise, ekonomik sektördeki ilerlemeler dikkate alınarak daha felsefi ve kapsamlı bir tanım geliştirilmelidir. Çünkü, bilgisayarlar; asılsız malvarlığı oluşturmak, borsada manipulasyon yapmak, şirket içerisindeki bilgi kaynaklarına ulaşarak yetkili birisiymiş gibi milyonlarca Dolar para elde etmek için kolaylıkla kullanılabilir. Bilgisayar, büyük askeri mühimmat depolarına, küçük bir grup teröristin sabotaj yapmasına imkân sağlayabilir. Bilgisayar yoluyla örneğin, 2 milyar Dolarlık malî boyuta ulaşılabilir. Bilgisayar, bir butona basarak geniş bilgi kaynaklana ulaşmayı kişisel olarak sağlayan dev bir hesap makinesidir. Bilgisayar, samanlıkta iğne aranıyormuş gibi suçluları gizleyebilir. Çünkü, suçlular, bir bilgisayar programını çökerterek, suçun iz ve eserlerini silebilirler.[33]

Bilişim suçlan, hem bilişim teknolojisi bilgisi ve hem de özel yetenek gerektiren, üst standartta bir suç türüdür ve her geçen gün yeni türleri ortaya çıkmaktadır. Bilişim suçlarının sürekli yenilenen yapısı, kriminologlar, yasa koyucular, uygulayıcılar arasındaki tanım tartışmalarının başlıca nedenidir.[34]

---

[32] Robert Dıtzıon, Elizabeth Geddes, Many Rhodes, , a.g.e. s.285

[33] August Bequaı , **Computer Crime**, (Lexington Books, Massachusetts Toronto, 1978) s.3-4.

[34] N .Orlovskaya, **Analytical Review on the Issues of Cyber-crime**, (http:www.inter.criminology. org.ua/jetspeed_eng/materials/orlovskaya/en/cyber-crime.htm+%22 cyber+crime+concept%22+&hl=tr (10.1.2005).)

Bilişim suçlarında yeterli bir tanımlama; dolandırıcılık, mal, para, hizmet, siyasi ve ticari avantajlar elde etmek için hile ve aldatmada, bilişimin kullanımını da kapsayan nitelikte olmalıdır. Hatta bilişim suçu, doğrudan kendi teknik yapısına yönelik tehdit veya güç kullanımım da içermelidir. Bu suçlarda genellikle, sabotaj veya fidye sağlama olayları görülür. Bilişim suçlarında en temel nokta ise, bilgisayarın, hem araç ve hem de bu suçlan işleyenlerin hedefi durumunda olmasıdır.[35]

Bilişim suçları, Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983'deki Paris Toplantısı'nda "bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlakî veya yetki dışı gerçekleştirilen her türlü davranış" olarak tanımlanmıştır.[36]

Avrupa Komisyonunun bir raporunda belirtildiği üzere, bilişim suçları, siber alanda işlenir ve geleneksel devlet sınırlarında durmazlar. Bu suçlar, dünyada herhangi bir bilgisayar kullanıcısına karşı herhangi bir yerden işlenebilirler.[37]

Daha kısa bir tanımda ise bilişim suçu, bir bilişim sisteminin kullanıldığı suç olarak ifade edilmektedir.[38]

Bilişim alanında işlenen suçların tam ve doğru istatistiklerini elde etmenin zorluğu da, yeterli bir tanım yapılmasını zorlaştırmaktadır. Mevcut istatistikler, mağdurların değişik nedenlerle maruz kaldıkları bilişim suçlarını resmî makamlara bildirmemeleri nedeniyle de güven vermemektedir. Yalnızca Amerika'da, hükümet

---

[35] August Bequai , **a.g.e,** s.4

[36] Cevat Özel, **Bilişim ve Internet Suçları Üzerine Bir inceleme Internet Hukuku**,(www.law. ankara.edu.tr/yazi, (18.8.2004).)

[37] Communication from the European Commission to the Council and the European Parliament Creating a Safer Information Society By Improving the Security of Information Infrastrutures and Combating Computer-Related Crime 9 (2000), available at http://europa.eu.int/ISPO/eif/ InternetPoliciesSite/ Crime/CrimeCommEN.html, [hereinafter Creating a Safer Information Society], (10.1.2004).

[38] Jo-Ann M.Adams , **Comment Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet**, (12 Santa Clara Computer-High Tech.L.J., 1996), s.403.

ve iş dünyasının bilişim suçları nedeniyle toplam yıllık kayıplarının, milyarlarca Dolar olabileceği tahmin edilmektedir.[39]

Aynı şekilde, bilişim suçlarının neden olduğu gerçek zararın hesaplanmasındaki zorluklar da, bilişim suçlarını yeterli bir şekilde tanımlayabilmeyi zorlaşmaktadır.[40]

Esasında bilişim suçlarına bir çerçeve çizmek oldukça zordur. Bu nedenle bilişim suçlarına, çizgisiz çerçeveli suçlar da denilmektedir. Bu düşünce, gelişen teknolojinin bu suçların çerçevesini sürekli genişletmesine ve bu suçların akıl almaz boyutlara ulaşmasına dayanmaktadır.[41]

Bilişim suçu tanımının belli bir süre kapsayıcı olabilmesi için, genel bir yapıda olmasında yarar vardır. Bu bağlamda, bilişim suçu, bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suç olarak tanımlanabilir. Doğal olarak, bilgisayar da bu tanıma dahildir.

2.HACK VE HACKER

2.1. Tarihsel Süreç

1969 öncesi:ABD'de bulunan MIT' de (Massachusetts Institute of Technology) isimli üniversitede bilgisayarlar kullanılmaya başlandığında, bazı öğrenci ve asistanlar, bu makinelerin nasıl çalıştığını merak ederler ve bu yeni teknoloji hakkında ne varsa öğrenmeye çalışmışlardır. Ancak o dönem bilgisayarlar ulaşılamaz ve paha biçilemez nitelik taşımaktadır. Bu üniversiteden bazı şahıslar hesaplama işlemlerini daha çabuk yapabilmek için "hack" dedikleri programlama kisayolları oluşturmuştur. Bazen bu kısa yollar orijinal programdan daha iyi tasarlanmıştır.

---

[39] Michael Hatcher, Jay Mcdannel, Stacy Ostfeld , **a.g.e.** s.399.

[40] Robert Dıtzıon, Elizabeth Geddes, Many Rhodes, , **a.g.e.**, s.285

[41] Mustafa Karabal, **Bilişim Suçları ve Turk Polis Teşkilatı**, (http://www.turkhukuksitesi.com/hukukforum/art_showarticle (2.2.2005))

Hack fikri 1969'da, Bell Telephone isimli telefon şirketi laboratuarlarındaki iki çalışanının, Dennis Ritchie ve Ken Thompson'un bilgisayarların artık açık kurallarla çalıştırılması gerektiğini düşünmesiyle yaratılmıştır. İkili, geliştirdikleri bu yeni standart işletim sistemine UNIX ismini vermiştir.

1970-1979. 1970'lerde siber cephe alabildiğine açılmıştır. Bu işle ilgilenen herkes, kablolarla bağlanmış bir dünyanın nasıl çalıştığını araştırmaya ve bulmaya çalışmıştır.

1971'de, John Draper isimli bir Vietnam gazisi, Cap'n'Crunch (mısır gevreği markası) kutusundan çıkan promosyon düdüklerin 2600 MHz tonda ses çıkardığını fark etmiştir. Bedava telefon görüşmesi yapmak için düdüğü telefonun alıcısına üflemek yeterli olmuştur. O zamanın hacker'lari, "phreaking" adi verilen bu tür yöntemlerin kimseyi incitmediğini, telefon hizmetinin sınırsız bir kaynak olduğunu ileri sürmüşlerdir.

1978 de, Chicago'lu iki genç, Randy Seuss ve Ward Christiansen, ilk kişisel BBS'i (Bulletin Board System - ilan Tahtası Sistemi) kurmuşlardır. BBS'ler günümüzde halen çalışmaktadır.

1980-1986. IBM firması, 1981'de bağımsız işlemcisi, yazılımı, belleği ve depolama birimleri olan yeni bir bilgisayarı duyurmuştur. Bu modele PC (Personel Computer-Kişisel bilgisayar) adini vermişlerdir.

1983 yılında çevrilen War Games (Savaş Oyunları) adli film, hacker'ları farklı bir cepheden ele almıştır: Bu film izleyicileri hacker'larin her bilgisayar sistemine girebileceği konusunda uyarmıştır.

Büyük Hacker Savası. 1984'e, kendine Lex Luthor adini veren bir kişi Legion Of Doom (LOD - Kyyamet Lejyonu) adli hacker grubunu kurmuştur. Adını bir çizgi filmden alan LOD, en iyi hackerlara sahip siber-çete olarak ün salmıştır. Phiber Optik isimli gencin, grubun bir diğer üyesi Erik Bloodaxe ile kavga edip kulüpten atılmasına kadar bu böyle sürmüştür. Phiber'in arkadaşları rakip bir grup

kurmuştur: Masters Of Deception (MOD). 1990'den itibaren, LOD ve MOD, iki yıl boyunca çevrimiçi savaşlar sürdürürler, telefon hatlarını kilitleme, telefon görüşmelerini dinleme, birbirlerinin özel bilgisayarlarına girme gibi faaliyetler ile (FBI)'ın olaya el koyması sonucu doğmuştur. Phiber ve arkadasları tutuklanmıştır. Bu olay ile bir dönem sona ermiştir.

Yasaklar Dönemi (1986-1994). Devlet çevrimiçi sitelerini kurmuştur. ABD Kongresi, ciddi 1986'da Federal Computer Fraud and Abuse Act (Federal Bilgisayar Sahtekarlığı ve Kötüye Kullanma) adi altında bir yasa çıkarmıştır. Hacker olmak ağır cezalar almak anlamına gelmiştir.

1988'de Robert Morris isimli şahıs Internet worm (Internet solucan'ı) adını verdiği bir hack yöntemi ile ortaya çıkmıştır. Net'e bağlı 6000 bilgisayarın çökmesine neden olarak, yeni yasayla yargılanan ilk kişi olmuştur. 10000 dolar para cezası ve kamu hizmetlerinde çalışma mecburiyeti cezası almıştır.

Aynı yıl Condor takma adıyla tanınan ünlü hacker Kevin Mitnick, Dijital Equipment Company şirketinin bilgisayar ağına girmiştir. Yakalanıp 1 yıl hapis cezasına mahkum olmuştur.

Sundevil Operasyonu, ABD hükümetinin ülkedeki tüm hacker'lari (LOD dahil) ele geçirmek için 1990'da başlattığı bir operasyondur. Ancak çok etkili olmamıştır.

1994'den Bugüne. Rus mafyasının eline düştüğü ileri sürülen Vladimir Levin adlı bir genç, Citibank'ın bilgisayarlarına girerek müşteri hesaplarından, 10 milyon dolardan fazla paraya (resmi açıklamaya göre 2.5 milyon dolar) İsrail'deki banka hesaplarına transfer etmiştir. Şahıs 1995 yılında Interpol tarafından Heatrow Havaalanında tutuklanmıştır; Hackerların art arda tutuklanması siber ortamda ani bir dolandırıcılık azalmasına neden olmuştur.

1995 Şubatında Kevin Mitnick isimli şahıs tekrar tutuklanmıştır. Bu sefer FBI şahsı 20 bin kredi kartı çalmakla suçlamıştır. Bu şahsın kelepçelerle medyaya yansıyan görüntüleri insanların bu alemdeki suça ve suçlulara karşı ilgisini

azaltmıştır. Net kullanıcıları "password sniffer" gibi araçlar kullanarak özel bilgilere sızan veya "spoofing" gibi bir makineyi kandırarak hacker'a giriş izni veren araçlar kullanan hacker'lardan dehşete kapılmıştır.

1997, AOHell adlı program ile birlikte bir çok ABD linin üyesi olduğu American Online isimli program hacklenmiştir.

1998, Ünlü hacker grubu The Cult of Death Cow, Back Orifice adlı Trojan (truva atı) programını çıkarmıştır. En etkili hack araçlarından biri olarak bilinen Back Orifice girdiği bilgisayarın kontrolünü kötü niyetli kişilerin erişimine açmıştır. Basra Körfezi'nde tansiyonun yükseldiği günlerde Pentagon'un bilgisayar sistemlerine art arda saldırılar gerçekleşmiştir.

1999: Yazılım güvenliği,Microsoft'un Windows 98 işletim sistemini çıkarmasıyla birlikte, 1999 hack ve güvenlik yılı olmuştur. Windows'taki açıklar için yüzlerce uyarı ve yama yayınlanmıştır. Bilgisayarlar için çok sayıda anti-hack ürünleri çıkarılmıştır

2000 den günümüze Dos saldırıları, Dns saldırıları, Sql Saldırıları,Sosyal mühendislik vb. derken pek çok Hacker ortaya çıkmıştır.Ve sayıları artmaya devam etmektedir.

2.2.Genel Olarak Hacking

Bilgisayarların gelişiyle, bilgisayar korsanları (hackers) ortaya çıkmıştır. Başlangıçtaki, kişisel bilgisayarlar bile, bilişim korsanlarından uzak değildiler. İlk kişisel bilgisayar şirketinin kurulmasıyla, "blue boxes" (mavi kutular) adıyla bunların üretilip pazarlanması başlamıştır. Bu cihazlar, telefona bağlanabilmekte, telefon sinyalleri aynı şekilde yayılabilmekteydi. Bu yüzden, başka bir telefonla bu bilgisayarlara ulaşılabilmekteydi. "Phreaking" olarak da adlandırılan bu aktivite belki de, bilişim korsanlığının ilk şekliydi. Burada, başka (uzaktaki) telefonla bilgisayar sistemine izinsiz, keyfi ve yasadışı girme söz konusuydu.[42]

---

[42] Amanda CHANDLER , **The Changing Definition and Image of Hackers in Popular Discourse**, (International Journal of the Sociology of Law, 24, 1996), s.229

Bilgisayar sistemleri, interaktif (etkileşime açık) faktörlere bağlı olarak, tehditlere maruz kalacak yapıdadırlar. Bir bilgisayar üzerindeki erişilebilen bilgi yoğunluğu, onun işletim dilinin karmaşıklığı ve çeşidi insan veya kullanıcı faktörleri, bir bilgisayar sisteminin kolaylıkla hack edilebilmesinin başlıca nedenlerini oluşturmaktadır.[43]

2.3.Tanımlama

Hack kelimesi ve bunu yapan kişi anlamına gelen hacker kelimesi için tam bir türkçe karşılık bulmak güçtür. Fakat kavramları yaşadığımız toplum içerisinde değerlendirdiğimiz taktirde, bu kavramların çıkışında veya oluşumunda herhangi bir "türkçe içerik oluşturabilecek" katkımız olmadığı için olayı tanıma yada başka bir anlamada popüler hale getiren internete bağlı bilgisayarlara yapılan saldırılar olmuştur. Bu sebepten dolayı hack veya hacker kelimeleri türkçe de bilgisayara saldırı veya saldırgan, bilgisayar korsanı olarak anlam bulmaktadır. Fakat kavramların doğuşu ve orijinal dilinde kullanılan anlamlarına bakılacak olursak türkçedeki kullanımının tam doğru olduğu söylenemez.

2.4.Çeşitleri

2.4.1.Engelleme: Sistemin bir kaynağı yok edilir veya kullanılamaz hale getirilir. Donanımın bir kısmının bozulması iletişim hattının kesilmesi veya dosya yönetim sisteminin kapatılması gibi. Tek başına bir hack sınıflandırması olmasına karşın büyük ve belirli bir sistem içerisinde gerçekleştirilecek olan hack olaylarında dinlemeden sonra gerçekleştirilen ikinci adım olduğu gözlenmektedir.

2.4.2.Dinleme: İzin verilmemiş bir taraf bir kaynağa erişim elde eder. Yetkisiz taraf, bir şahıs, bir program veya bir bilgisayar olabilir. Ağdaki veriyi veya dosyaların kopyasını alabilir. Bir çok kaynak tarafından hacking olaylarının artmasının en büyük nedeni olarak gösterilmektedir. Bunun temel nedeni ise hacker'ler kullandıkları dinleme yöntemleri sayesinde hack edeceği sistem

---

[43] Erhan Erdönmez, **Investigation of Computer Crimes ,Thesis Prepared for the Degree of Master of Science** ,(University of North Texas ,Ağustos 2002),s.6

hakkında hemen hemen tüm bilgiyi elde eder yada istediği bilgiyi direkt olarak ağ üzerinden alır. Dinleme yöntemi aslında temel olarak, ağdaki bileşenleri dinlemek veya ağı üzerindeki bilgiyi dinlemek olarak iki başlık altında toplanabilir. Bunlardan birincisiTarama, "Scan" ikincisi ise Dinleme'dir "Sniffer"

2.4.3.Değiştirme: İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklik yapar. Bir veri dosyasının değiştirilmesi, farklı işlem yapmak üzere bir programın değiştirilmesi ve ağ üzerinde iletilen bir mesajın içeriğinin değiştirilmesi gibi. İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklik yapar. Bir veri dosyasının değiştirilmesi, farklı işlem yapmak üzere bir programın değiştirilmesi ve ağ üzerinde iletilen bir mesajın içeriğinin değiştirilmesi bu yönteme verilecek örneklerden bir kaçıdır.

2.4.4.Oluşturma: İzin verilmemiş bir taraf, sisteme yeni nesneler ekler. Ağ üzerine sahte mesaj yollanması veya bir dosyaya ilave kayıtlar eklenmesi. Bu hacking türü aslında amacı olarak tanımlana bilinir. Bu aşamadan sonra hacker sisteme sızmış ve amacına ulaşmış olmaktadır. Virüsler,Trojanlar bu kapsamdadır.

2.5.Kavram Çeşitliliği

Bilgisayar korsanlığı konusunda (phreaking, hacking, cracking .... gibi) pek çok terim kullanılmaktadır. Bu sözcükler, bilişimin kaynağı olarak gösterilen ABD'deki adlandırmalardan yayılmıştır. Bu kelimelerin hepsini tam olarak Türkçe'ye çevirmek zordur.

Hacking, bilgi veya program elde etmek, zarar vermek için geniş oyun sahaları açmak için bir bilgisayar sistemine yetJrisiz erişim olarak tanımlanabilir. Korsanlık (hacktivism) ise, aktivizim ile yakınlığı bulunan bir kavramdır.[44] **Snooper** (başkalarının işlerine burnunu sokan kişi) ise, mağdurların kişisel bilgilerini okuyabilir ve hatta onların bilgisayarlarını dahi ele geçirebilir. **Vandal** ise, mağdurun web sayfasını değiştirebilir. **Saboteur** ise, araştırma-geliştirme

[44] Dorothy Denning, **Activism, Hactivism and Cyberterrorism** , (Santa Monica,2002), s.263

bilgilerini (R&D) silebilir veya bir bilişim ağını felce uğratabilir. **Endüstriyel casus** (endustrial spy) ise, gizli ticari bilgileri çalabilir. Şantajcı (blackmailer) ise, dijital süreler, mantık bombaları (logic bomb) planlayabilir ve bir sistemi, mağdur gerekli ödemede bulunmazsa, çöpe dönüştürmekle tehdit edebilir.[45]

Yukarıdaki nitelemeleri artırmak mümkündür. Ancak, bunlardan en yaygın olanı, "hacking", "hacker" sözcükleridir.

2.6.Hacker

Hacker, öncelikle bilişim sistemlerine yetkisiz erişim yapan kişidir. Kendisini, efsane zannedebilir ve üst düzey bir bilişim uzmanı olarak görür. Hacker, şeytanca hareketleri sever[46] ve bilişim korsanlığını, genellikle tek bir nedenle yapmaz. Ancak, belirgin olan bir nokta olarak, davranışlarının temelinde heyacan veya duygusal bir yapı çoğunlukla görülür.[47] 0 çoğu zaman eylemlerini, bilişim sanatı olarak görebilir. Genellikle, bilişim korsanlığı yaptığında imzasını atmaktan hoşlanır.

Hackerlar, gelişim sürecinde "bilgi güçtür" sloganıyla bilişim sistemlerine herhangi bir sınırlama olmaksızın girme haklan olduğunu ileri sürerek, her türlü hareketlerini, meşru göstermeye çalışmışlardır.[48]

Hackerlar değişik sınıflandırmalara tâbi tutulabilir. Onlar, diğer beyaz yaka suçlulanndan daha popüler bir görünüm içerisindedirler. Onların popüler olmalarında, yaptıkların eylemlerin yanında, medyanın da önemli rolü vardır. Hackerlar, orta sınıf sokak çetelerine eşdeğer bir sosyal yapıda nitelenebilir. Ağırlıklı olarak, erkeklerden oluşur ve her zaman yalnız yaşayan kişilerdir.

---

[45] Marc D. Goodman,- Susan W.Brenner, **The Emerging Consensus on Criminal Conduct in Cyberspace**, (UCLA Journal of Law and Technology, 3, 2002), s.12

[46] Liz Duff –Simon Gardiner, **a.g.e.**, s.215.

[47] Eric Metchık , **A typologyof crime on the internet**, (Security Journal 9, 1997), s.28-29.

[48] Carlo Sarzana Ippolıto, **Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması , İtalya'daki Durum , Çev. Vesile Sonay Daragenli-** (İHFM,Sayı 3,1997) S.398

Hackerlar birbirleriyle bağlantı kurabilir; ancak aralarında ustaca yapılan korsanlıklarına (yetkisiz erişimlerine) göre bir hiyerarşi söz konusudur. Bu yapı, ilk başta Amerika'da hâkim olmuş ve sonra dünyaya yayılmıştır.[49]

Bilgisayar Endüstrisinde 'Bilgisayar Korsanı' kavramı, birincisi, bilişim sistemlerinin çalışma prensiplerini ve diğer bilgilerini araştırarak öğrenmekten hoşlanan ve bunların kapasitelerini arttırmak için çalışan kişi için; ikincisi de, programcılık hakkında teoriler üretmek yerine doğrudan programlama yapmaktan hoşlanan kişi için kullanılmaktadır. Hacker kelimesinin kökünde, yeni bir programın hızla ortaya çıkarılması veya genellikle mevcut zeka ürünü program üzerinde değişiklik yapılması anlamında kullanılan 'hacking' fiili türetilmiştir.

Hacker, ilk bakışta kendi masasında bilgisayar ekranında çalışma yapan bir kişidir. Fakat, dünyada farklılıklar yapabilir. Bunun için, birisini öldürmek veya bir protesto yürüyüşüne katılmak zorunda değildir. O, modern dünyanın adeta Robin Hood'dur. Kimi zaman, zenginler hakkındaki bilgileri alıp, fakirlere vermektedir. O,.yalnızca kendi bilgisayarını kullanır. Kimi zaman, hackerlık konusundaki görüşlerini internette yayınlar veya e-postayla pek çok kişiye ulaştırır. Buysa, suçla mücadele edenlerin öfkesini çekmeye yetmektedir.[50]

Almanya, çok tehlikeli olan "coas computer club" adlı hackerlar birliğini oluşturmuştur. Ancak, ne ilginçtir ki, hackerlar tarafından bilişim sistemlerine virüs sokulmasıyla yapılan bilişim ağlarına en büyük sızmalar ve büyük tahriple de en başta Almanya'dan başlamıştır.[51]

3.BİLİŞİM SUÇLARININ KRİMİNOLOJİSİ

Bilişim suçlarının ortaya çıkmasından sonra kriminolojik açıdan ele alınmaya başlandığını belirtmek mümkün ise de, bu incelemelerin bilişim

---

[49] Liz Duff –Simon Gardıner ,**a.g.e**, s.215-216

[50] Barry Shell , **Ethical Hacking**, (Georgia Straight Weekly, Vancouver, BC, Sept 14, 2000,) (http://css.sfu.ca/update/ethical-hacking.html)

[51] Carlo Sarzana Ippolıto, **a.g.e.**, s.398

suçlarının tümünü yeterince kapsadığını söylemek güçtür. Çünkü, bu suçların tür ve sayıları her geçen gün öngörülemez boyutlarda artmaktadır.

Bir görüşe göre, günümüzde bilgisayar kavramı sadece teknolojik devrim olmaktan çıkmış, suç kavramı ile birlikte anılan bir araç haline gelmiştir.[52] İşte bu noktada, bilişim suçlarının kapsamlı şekilde kriminolojik açıdan ele alınması gereği kaçınılmaz hâle gelmektedir.

3.1. Bilişim Suçlarında Kriminolojik Bakımdan İlk Gelişmeler

Bilgisayarlarla insanlığın tanışması, yaklaşık 50 yıl önce başlamıştır. Bilgisayar suçu kavramı ise, bu makinelerle sahtekârlık suçlarının kolaylıkla işlenebildiğinin fark edilmesiyle ilk defa 1960'larda ortaya çıkmıştır. Günümüzdeki bilişim suçları kategorileri ise, yakın zamanlarda, sabit ana bilgisayarlardan ayrılabilen taşınabilir bilgisayarların[53] üretilmesiyle doğmuştur.[54]

Bilişim suçu türlerinin sürekli artması karşısında, üzerinde anlaşma sağlanabilen bir tasnifin bile yapılamaması, kriminolojik açıdan bu suçların ele alınmasındaki önemli bir zorluğu oluşturmaktadır.[55]

Bilişim suçlarındaki inanılmaz artışın başlıca nedenlerinden birisi, bilişim sisteminin suç doğuran yapıda olmasıdır. Bir başka anlatımla, bilişim sisteminin kendine özgü yapısı, bu suçları tetiklemektedir.[56]

---

[52] Semih Dokurer, **Ülkemizde Bilişim Suçlan ve Mücadele Yöntemleri**,(www.dikey8.com, (29.06.2004))

[53] Bunlar, dizüstü (laptop) bilgisayarlar değil, monitör, klavye ve kasa içerisindeki harddiskten oluşan, ev ve işyerlerinde kullanılan bilgisayarları anlatmaktadır.

[54] Liz Duff –Simon Gardıner , **a.g.e**, s.213

[55] N .Orlovskaya , **a.g.e**, (10.1.2005)

[56] Aynı görüş için bkz: Olgun Değirmenci, **Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi**, (LHD., Kasım 2003), s.2750.

Bilişim suçlarının kriminolojik açıdan en kapsamlı ele alındığı yer, bilişim sisteminin anavatanı konumundaki ABD'dir. Özellikle, yaşanan alışılmadık kimi olayların nedeninin bilişim olduğunun anlaşılması, bilişim suçlarının kriminolojik açıdan ele alınmasında etkili olmuştur.

1971 yılında ABD'deki Newyork — Pennsylvania merkez demiryolu hattında 200'den fazla yük vagonunun bir engel nedeniyle rotasından sapması ve bunun her defasında ortalama 60.000 Dolarlık maliyete (zarara) neden olması, federal yargı merciinde incelenmiştir. Bu inceleme sonuçlarına göre olaylar, Pennsylvania Demiryolu Merkez Şirketinin bilgisayarlarına yapılan yetkisiz müdahalelerden kaynaklanıyordu. Üstelik bu yetkisiz erişim, organize bir nitelik taşıyordu. 1972 yılında ise California yetkilileri, devletin en geniş yapıdaki telefon şirketinden 1 milyon Dolarlık elektronik ekipmanı gizlice çalan bir mühendislik fakültesi öğrencisini yakaladı. Hırsızlık fiili, yalnızca bir telefon ve bilgisayarın gizli giriş koduyla işlenmişti. Fail, firmanın bilgisayarına siparişler yerleştirmişti. Sonra bunun kendisini sonuca götürdüğünü görmüştü. Bir başka anlatımla, başlangıçta yetkisiz erişimi fark eden olmamıştı. Yargılama sonunda fail, hırsızlık suçundan 60 gün hapis ve 3 yıl gözetim süresine mahkûm oldu. Daha sonra cezasını çektikten sonra bu kişi, firmalara, bilgisayarlarına yapılabilecek saldırılardan korunmak konusunda ticari danışmanlık yapmaya başladı.[57]

3.2. Kriminolojinin Bilişim Suçlarından Uzak Kalışı

Kriminolojinin başlangıçtan itibaren gelişiminde, bu sahada çalışanlar, "geleneksel suçlar" ya da "klasik suçlar" olarak bilinen alanda yoğunlaşmışlardır. Bu suçlar ise, toplumda daha ciddi nitelikte görülen ve geleneksel nitelik taşıyan, tecavüz, gasp, hırsızlık, cinayet olarak belirtilebilir. Bu sonuca dayalı olarak da, yasal yapı, bu suç tipleri üzerine kurulmuştur. Bununla birlikte, modern teknolojinin gelişmesiyle, geleneksel olmayan suçlara ilgi artmaya başlamıştır. Elektronik devrimi, yeni suç araçlarını da sağlamıştır. Modern teknolojinin yardımıyla, milyonlarca Doları çalmak mümkün hâle gelmiştir. Bilişim suçları, bu yeni sahanın bir ürünüdür. Bu suçlar, yalnızca kriminologların yeni çalışma

[57] August Bequai , a.g.e , s.1.

alanlarını oluşturmakla kalmayıp, aynı zamanda değişen teknolojinin risklerine karşı toplumsal uyumumuzu da test etmektedir.[58]

Bilişim suçlarıyla kriminologların ilgilerinin azlığında, bilişim suçlarının ciddi anlamda 1970'li yıllardan itibaren görülmeye başlanılmasının etkisi de unutmamalıdır. Nitekim, 1970'li yıllardan önce dünyada kullanılan bilgisayar sayısı ve bilişim ağları da oldukça azdı.[59]

3.3. Mevcut Normatif Yapının Yetersizliği

Yukarıdaki, "Bilişim Suçlarında Kriminolojik Bakımdan İlk Gelişmeler" başlığındaki iki olay, en azından ABD'de gelişmeye başlayan bilişim suçlarının ne olduğunu örnek olarak ortaya koymuştur. Daha sonra, ABD Ticaret Odası, teknolojik suçların yeni şekillerinin (1970'li yıllardaki) yıllık maliyetinin 100 milyon Dolar olabileceğini tespit etmiştir. Üstelik, teknolojik suçların diğer çeşitlerinde bu rakamlar daha da yüksektir. Bu sonuçlar, bilişim suçu faillerinin, organize olarak, gerekli kaynak ve bilgi düzeyine sahip bulunduklarını, büyük dolandırıcılık eylemleriyle toplumu tehdit eden bir nitelik taşıdıklarını düşündürmeye başlamıştır. Bu tehdit, yalnızca kişilerin ekonomik ve özel (mahrem) alanlarını değil, aynı zamanda idareyle ilgili pek çok sisteme de yönelmektedir. Mevcut yasal yapı, bu sorunla mücadelede yeterli görünmüyordu. Bu nedenle, mevzuatın bu tehditlerle baş edebilecek hâle getirilmesi gerekmekteydi. Çünkü, tarihsel olarak yürürlükteki yasal yapı, yalnızca geleneksel toplumsal suçlan önleyebilecek durumdaydı.[60]

Esasında, ortaya çıkmaya başlayan bilişim suçlarının bu boyutu karşısında mevcut yasal düzenlemelerin yeterli olmamasını normal karşılamak gerekmektedir. Çünkü, klâsik suçları düzenleyen mevcut yasalar yapılırken ya da bu yasaların mehazı olan yasalar düzenlenirken, bilgisayar veya bilişim sistemi

---

[58] August Bequai , **a.g.e**, s.2.

[59] Erhan Erdönmez, **a.g.e,** s.1.

[60] August Bequai , **a.g.e**, s.1

gibi bir teknolojik olgu bulunmamaktaydı. Bu nedenle, mevcut yasaların, bilişim suçlarıyla mücadeleye imkânı vermesini beklemek de, makul bir yaklaşım olamazdı.

Diğer yandan, bilgisayar ve bilişim sistemlerine geçiş de, kendiliğinden ve sıradan olmamıştır. Bilişim sistemine ulaşmak, önemli teknolojik çalışmaları gerektirmiştir. Bu yapı içerinde oluşan bilişim suçlarıyla etkin mücadele için de, mevcut yasalarda, bilişim sistemine ait teknolojik yapı göz önüne alınarak değişiklik yapılması doğal bir sonuçtur.

3.4. Bilişim Suçlarının Beyaz Yaka Suçlarıyla İlgisi

Beyaz yaka suçları düşüncesi, ilk defa ABD'de Edvin H, SUTHERLAND tarafından, Amerikan Sosyoloji Derneğinin 1939 yılında yapılan toplantısında ortaya atılmıştır. SUTHERLAND, o güne kadarki kriminolojik çalışmalarda, toplumun daha düşük statüdeki kesimine ilişkin suçlar ile sokak suçlarına yönelme olduğunu, toplumun üst kesimindeki kişilerin işledikleri suçlara yeterli İlgi ve dikkatin gösterilmediğini belirtmiştir. Üstelik SUTHERLAND, toplumda ayrıcalıklı konumdaki bu kişilerce işlenen suçların, çok daha ciddi ve zararlı olduğunu vurgulamıştır.[61]

Beyaz yaka suçlarının ittifakla kabul edilen, tatmin edici bir tanımı olduğunu söylemek güçtür.[62] Bu suçlar SUTHERLAND tarafından, toplumda mesleki açıdan üst seviyede, saygın görünümdeki kişiler tarafından işlenen suçlar olarak tanımlanmaktadır.[63] Anılan kişiler tarafından işlenen suçun nitelikleri açısından ise

---

[61] Cynthia Barnett , **The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data**, (http://www.fbi.gov/ucr/whitecollarforweb.pdf (12.3.2005));Daniel MORIARTY, **'What is white collar crime?** (http://www2.als.edu/faculty/dmoriarty/wccdescription.html+%22white+collar+crime%22+description&hl=tr (3.3.2005))

[62] Daniel Moriarty, **a.g.e.**, (3.3.2005).

[63] Cynthia Barnett , **a.g.e.**, (12.3.2005)

beyaz yaka suçları, yasal olmayan ve doğrudan fizikî bir uygulamaya dayanmayan dolandırıcılık ve aldatma (gizleme) fiilleri olarak tanımlanmaktadır.[64]

Teknolojideki gelişmelere bağlı olarak bilişim suçları, beyaz yaka suçlarının kapsamında değişikliğe neden olmuştur.[65] Özellikle, büyük boyutlu bilişim suçlarının işlenebilmesinde, hem teknik yapıya, hem de teknolojik bilgiye ihtiyaç olması ve bunların da belirli bir malî külfeti gerektirmesi, bu suçların belli bir düzeyin üstünde malî güce sahip kimselerce işlenebilmesini olanaklı kılmaktadır.

ABD'de işlenen bilişim suçlan, beyaz yaka suçlarının en geniş kısmını oluşturmaktadır. ABD'de 1997 ilâ 1999 yıllarında FBI tarafından yapılan bir araştırmaya göre, bilgisayar kullanılarak gerçekleştirilen suçların % 42'sinin beyaz yaka suçları kapsamında olduğu belirlenmiştir. Bu kapsamdaki beyaz yaka suçlarının en yaygın olanı ise, değişik türdeki (yetkisiz veri elde edilmesi dahil) hırsızlık fiilleridir.[66]

ABD'de, beyaz yaka suçlularının, bilişim teknolojisini çok çabuk benimsedikleri ve bilgisayarı suçta en fazla kullananların da, beyaz yaka suçluları olduğu kabul edilmektedir.[67]

3.5. Bilişim Suçlarını İşlemeye İten Nedenler

Bilişimin fail davranışlarını nasıl etkilediği, bilişimin kendisine has yapısı karşısında oldukça anlamlıdır. Klâsik suçlarda, sanığı suça iten nedenlere göre, bilişim suçlarında çok daha farklı ve geniş bir alan bulunduğu rahatlıkla söylenebilir.

---

[64] August Bequai , **a.g.e**, s.1

[65] Erhan Erdönmez, **a.g.e.**, s.1.

[66] Cynthia Barnett , **a.g.e.** (12.3.2005).

[67] Hilary Conner , **Conducting Forensic Research: A Tutorial For Mystery Writers** (http:// \AMw.writing-world.c»m/mystery/forensics.shtml+vvhite+collar+crirninal%27s+related+ with+computer+crime&hl=tr (25.1.2005))

Bilişim suçlarının işlenme nedenlerinin belirlenmesinin pek çok açıdan önemli olduğu tartışmasızdır. Özellikle, bu suçlarla mücadelede yasal yaptırımlar tek başına yeterli değildir. Klâsik suçlardan farklı olarak, bilişim suçlarının; sayıları, türleri ve işlenebilme olanakları inanılmaz ölçüde artmaktadır. Bu suçların belki de en dikkat çekici özellikleri, suçun etki alanının ve sonuçlarının hayal sınırlarını zorlayacak ölçülerde olabilmesidir.

Bilgisayar teknolojisi ve internetteki hızlı gelişmeler, teknolojiye bağlı suçlu davranışlarını doğurmaktadır. Bu nedenle, yeni suçlarla ilgili suçlu davranışlarıyla başa çıkmak için uzmanlaşmayı içeren yasalara ihtiyaç doğmaktadır.[68]

Bilişim suçluları, kendileri hakkında nadiren dava açılabildiğini ve böyle bir dava açılsa bile, davada mahkûmiyete yeterli delil elde edilemeyeceğini ve mahkûmiyet olasılığının azlığını (bir başka deyişle güncelleştirilmeyen yasalarda fazla ceza alınmayacağını) bilmektedirler. Üstelik bilişim suçluları, mağdur şirket yetkililerinin bilgi vermekte isteksiz davranacaklarının farkındadırlar. Çünkü, mağdur şirket yetkilileri, bilgi verip, bilişim suçuna maruz kaldıklarını söyledikleri zaman, hissedarlarının ve kredi kaynaklarının (kredi verenlerin) güvenlerini kaybedeceklerini düşünürler. Ayrıca, bu suçlular, keşif, araştırma ve dava sürecinin bilişim suçlarına karşı, etkili olmadığını da bilirler. Çünkü, kriminologlar, çabalarını ve çalışma sahalarını diğer klâsik suçlara yöneltmişlerdir ve yeterince çalışılmamış olan bilişim suçlan alanından uzaktırlar. Bilişim suçlan alanındaki bilgisizlik, bilişim suçu faillerinin ilk savunma hatlarını oluşturmaktadır.[69]

Bilişim suçu faillerinden bazıları, belli bir yerde çalışmakla birlikte, isimsiz olarak interneti kullanarak, çalıştıkları iş dışında bilgi elde eden ve bunları kişisel kazanç için kullanan kimselerdir. Bu kimseler, çalıştıkları işten kovulma aşamasındadırlar ve işlerinde mutsuzdurlar. Bu failler, çalıştıkları işyerlerinin bilgisayarlarıyla suç işlemektedirler ve işverenleriyle de ilişkileri bozuk durum-

---

[68] Robert Dıtzıon, - Elizabeth Geddes, - Many Rhodes, **a.g.e.** , s.285.

[69] August Bequaı , **a.g.e.**, s.1-2 ; Diğer yandan, bilişim sistemindeki suça yatkın bu yönün giderilmesi yönünde yeterince çaba sarfedildiğini söylemek de güçtür; Olgun Değirmenci, **a.g.e.**, s.2750.

dadır. Bu failler, bilişim sistemindeki hassas bilgileri çalmak ve bunları satarak kazanç elde etmeyi isterler.[70]

Bazı failler, kişisel kazanç içiş, diğer bir kısmı meydan okumak için, kimileri ise, geniş bir alanda tehlike oluşturmak için bilişim suçunu işlemektedir. Bilişim suçu failleriyle ilgili olarak yapılan çalışmalarda bu son gruptakilere, önceki fail tiplerine odaklanıldığı için, gerektiği şekilde dikkat edilmemektedir. Bir çalışmada, bir düzineden fazla bilişim failinin, kendilerini bilgisayarlara çukurlar açan (tuzak kuran) yapıda gördüklerini ortaya çıkarmıştır. Diğer bir çalışmada, birkaç yüz bilişim failinin ortalama her birinin yaklaşık 400.000 Dolar çaldığı anlaşılmıştır. Diğer çalışmalarda ise, bilişim suçu faillerinin, teknisyenler, yöneticiler ve programcılar olduğu görülmüştür. Bilişim suçu failleri, genellikle bu suçu makinelere meydan okuyarak neşeyle (coşkuyla) işlerler ve korunmasız olan bilgisayarları keşfederler; büyük firmalara saldırarak milyonlarca dolar almayı amaçlarlar. Bir araştırmaya göre failler, örneğin, Almanya, Norveç, Danimarka, İngiltere, Güney Kore, Japonya'daki firmalara karşı dolandırıcılık suçlarını işlemişlerdir. Bilişim hırsızlığı, genellikle para, hizmet ve gizli ticari bilgileri içerir. Bununla birlikte, bu failler yakalandığında verilen mahkûmiyet karan, klâsik hırsızlık suçundan verilen mahkûmiyet kararlarına benzemektedir. Bu sahadaki çalışmalar, bilişim suçlarının tehdit boyutunu ve gerçek etkisini asgariye indirme eğilimindedir.[71]

4.BİLİŞİM SUÇLARININ TASNİFİ

Bilişim suçlarını, başka bir açıdan üç boyutta ifade etmek de mümkündür[72]:

1. Fiilin hedefi olarak bilgisayar : Bu halde, suç konusu fiil, bilgisayara (bilişim sistemine) odaklanmaktadır. Bunun değişik amaçları olabilir. Örneğin, hedef bilgisayarın çalışmasının engellenmesi, yetkisiz erişim gibi.

---

[70] Diane Sears Campbell, **Focus on Cyber-Fraud**, (The Internal Auditor, 59, No 1, Şubat 2002), s.30.

[71] August Bequai , **a.g.e**, s.4..

[72] Scott L Ksander , **INFORENSICS**, (Purdue Univesity, Calvin College Seminar, power point sunumu, 2003), s.8; David L.CARTER, David, L .CARTER ,**Computer Crime Categories How Techno-criminals Operate**, (FBI Law Enforcement Bulletin, v.64, July 1995), S.21-24.

2. Fiilin aracı olarak bilgisayar : Burada, değişik sonuçların elde edilmesi için bilgisayarın (bilişim sisteminin) vasıta olarak kullanılması söz konusudur. Örneğin, başkasının eserini kendisininmiş gibi göstermek, tehdit veya taciz etmek için elektronik posta göndermek veya taklit edilmiş bir belge için bilgisayarı kullanmak gibi.

3. Fiilde tesadüfen bağlantı kurulan bilgisayar : Bu halde ise, fiilde bilgisayar (bilişim sistemi) hedef ya da araç değildir; ancak tesadüfen bilgisayarla bağlantı kurulmuş olmaktadır. Bu tesadüfi yetkisiz bağlantı (erişim) ise, erişilen bilgisayarın tarih ve zaman çizelgesinden anlaşılmaktadır.

Bir başka tasnife göre ise, suçta bilgisayarın dört rolü olabilir. Bunlar; 1) Fiziksel olarak, 2) Konu (hedef) olarak, 3) Araç olarak ve 4) Sembol olaraktır. Uygulamada bu dört hâl de sıklıkla görülmesine rağmen, bilişim eğitiminde ve doktrinde yalnızca bilgisayarı araç ve konu (hedef) edinen suçlara odaklanılmaktadır. Adeta, bilgisayarın fiziksel ve sembol olarak hedef alındığı suçlar ihmal edilmektedir.[73]

Diğer bir tasnife göre ise, bilişim suçları iki grupta toplanabilir. Birincisi bilişim yazılımlarına (programlarına) zorla girmek, ikincisi ise herhangi bir suçu işlemek için bilişimi araç olarak kullanmaktır.[74]

Başka bir tasnifte ise, bilişim suçları, sanıklara odaklanılarak yapılmaktadır. Bilgisayarın kötüye kullanılması, üç belirgin seviyede toplanabilir. Birincisi, şirket suçlarıdır. Suçun işlendiği yerde, şirket politikalarını değiştirmek için şirketin yapısal bir pozisyonundaki kişiler tarafından bilişim suçunun işlenmesidir, ikinci seviye ise, mesleki suçlardır. Buradaki sanıklar, işverenlerine karşı kimi nedenlerle kişisel olarak suç işlemektedirler. Üçüncü seviyede ise, yetkisiz erişimler yoluyla dışarıdan sisteme yapılan saldırılar söz konusudur. Burada, bilgisayarlardaki bilgi veya programlara zarar verilmekte veya bilişim sahtekârlığı

---

[73] Erhan Erdönmez, **a.g.e.**, s. 13

[74] I.Blıznyuk, **Legal Aspect Of Cyber-Crime**,(Bulletin of the National Academy of the Ministry of Internal Affairs No 2, 1999), s.285-286.

yapılmaktadır. Bunları gerçekleştirmenin ilk adımı ise, yetkisiz erişimdir. Yetkisiz erişimden önce ise, hedef bilgisayara göz gezdirilmektedir.[75]

Suçun işlenmesindeki esas konuyu suçlar arasındaki farklar oluşturur. Bir hedefe ulaşabilmek için türlü yollar kullanılabilir,bunun ötesinde asıl amaç hedeftir.Suç çeşitleri ayrımında[76] 11.06.1999 tarihinde Birleşmiş Milletler ve Avrupa Birliği tarafından hazırlanan "Bilişim Suçları" raporuna göre ; suç çeşitleri altıya ayrılmaktadır

4.1.Bilgisayar Sistemlerine ve Servislerine Yetkisi Erişim ve Dinleme

"Erişim" sistemin bir kısmına, bütününe, bilgisayar ağı veya içerdiği verilere,programlara; yine programlar,casus yazılımlar,virüsler,trojanlar,wormlar vb. ile ulaşma anlamındadır.Günümüzde özel hayatın gizliliğinin korunması için kanunlarda gerekli müeyyideler konulması ile birlikte dinlemeler, erişimler, izinsiz kişi ya da kurum bilgisayarlarına, sistemlerine girmek suç olarak kabul edilmiştir.

Günlük yaşantımızda gelişen teknoloji ile birlikte daha rahat ve modern bir ortam sağlayan iletişim kavramı ile birlikte gelişen bilgisayar teknolojisi sayesinde işlemler kolaylaşmakta ve kişiler,bankalar,resmi kuruluşlar,ticari kuruluşlar,hastaneler,bilgi depolayan sistemler,istihbarat birimleri,hızlı iletişim gerektiren işlemler çoğu zaman bilgisayar teknolojileri kullanarak yapılmaktadır. Türkiye'de işlemekte olan kamu kurumları,şirketler,özel ve tüzel eğitim kurumları,bankalar,ticari kurumlar ve birçok organizasyon; teknolojinin getirmiş olduğu gelişmelerden faydalanmakta ve bu sayede daha rahat ve kolay işlemlerini tamamlamakta,bir yandan kahvaltısını yaparken diğer yandan Internet üzerinden alışveriş yapabilmekte,büyük miktarda paraları rahatça bir yerden başka bir yere aktarabilmekte, kamu hizmeti olarak online pasaport, hastane muayene fişi, iş başvurusu gerçekleştirebilmekte, bir çok işlemi zahmetsiz bir şekilde yürütebilmektedir.Fakat bu işlemler sırasında belirli bir politikanın

---

[75] Liz Duff –Simon Gardıner, **a.g.e**, s.213-214.

[76] Mehmet Özdemir, **Bilişim Suçları Ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler Ve Çözüm Önerileri,** (http://www.caginpolisi.com.tr/24/43-44-45-46.htm-2006),

yapılmaması,gerekli düzenlemelerin uygulamaya konulamaması sonucunda kişi ya da kurumlar küçümsenmeyecek şekilde tehlikelere maruz kalmakta ve sonuç olarak bilişim suçu ortaya çıkmaktadır.

Bilgilerin toplandığı bu tür sistemlere, bilgisayarlara girmek,bilgilere erişmek suç olarak kabul edilmektedir.Günümüzde telefon dinlemeleri veya kişilerin özel mülklerine girmek nasıl savcı izni olmadan mümkün olmamakta ise yine kişiler veya kurumlar arası haberleşmenin bilgisayar üzerinden dinlenmesi veya izinsiz bilgilerin alınması da kişi özel mülkü ya da kişilerin şahsiyetlerine taciz olarak kabul edilmektedir ve suç oluşturmaktadır.

Casus Yazılımlar Ve Etkileri[77]

Casus yazılımlar bir bilgisayara kurulduktan sonra bilgisayara girdikten sonra bilgisayarda farklı etkiler bırakarak, ya da bilgisayar içerisinde deyim yerindeyse casusluk yaparak rahatsız eden yazılımlar olarak ifade edilir.

Casus yazılımların belli başlı amaçları; eriştiği ya da kurulduğu bilgisayarlardaki verileri, gezilen siteleri, bilgisayar içeriğindeki bilgilerin işe yarayan kısımlarını belli bir hedefe(doğrudan merkeze) göndermesine ya da bilgisayardan istenmeyen reklamların çıkmasına, internetten reklam indirmesine yol açmaktadır.

Casus yazılımların bu şekilde çalışmasının başlıca sebepleri arasında;bu tür yazılımların milyonlarca bilgisayarda olması ve herhangi bir reklamın yukarıda bahsettiğimiz şekilde yayınlanması demek, milyon dolarlarla hesap edilebilecek bir getiri demektir.Yani bu sayede büyük kitlelere ulaşılmakta ve casus yazılımlar esas amaçlarına ulaşmaktadır.

Casus yazılımların kişiye ve bilgisayarına yönelik zararların başında; kişisel bilgileri ele geçirmek diyebiliriz.Bu tür programlar interneti yavaşlatırken, dışarı veri gönderip bilgisayara reklam yükler. Bilgisayarda açıklar oluşturur ve

[77] Ferruh Mavituna , **Casus yazılımlar nedir ne değildir ?** (http://ferruh.mavituna.com/article/?218)

bilgisayarı yavaşlatır. Bazıları (dialer) dediğimiz programlar ile yurtdışı internet bağlantısı yaparak yüksek miktarda telefon faturası ödemeye sebep olur. Dialer dediğimiz programlar genellikle pornografik sitelerden bilgisayara bulaşır.

4.2.Bilgisayar Sabotajı

Bu suç türü iki şekilde karşımıza çıkmaktadır.

1. Bilgisayar teknolojisi kullanarak sistemine sızılan bilgisayardaki bilgilerin silinmesi, yok edilmesi ve değiştirilmesi.

2. Hedef alınan sisteme uzaktan erişerek değil de bilakis fiziksel zarar vererek yada sistem başında bulunarak bilgisayardaki bilgileri silmek,yok etmek veya değiştirerek zarar verilmesidir. 2.sinde önemli olan mala verilen zarar değil de içindeki bilgilerdir.

Yetkisiz erişimin aktif sahası olarak da nitelendirilen "Bilgisayar Sabotajı",yalnız sisteme erişimle kalmamakla birlikte,eriştiği sistem (bilgisayar)'ın içerdiği bilgileri silme veya değiştirme olarak ifade edilir.Fiziksel olarak bilgilerin yok edilmesi veya silinmesi yani bilgilere sanal ortam haricinde yapılan dış etkiler de bilgisayar sabotajına girmektedir.

Günümüzde tüm dünya ülkelerinin baş belası olarak kabul edilen ve son zamanlarda etkili olan "Bilgisayar Sabotajı" suçu ile ilgili olarak birçok örnek vermek mümkündür.Çünkü bu tür olaylarda mali zarar yüklü miktarda olmakta ve derhal önlem alınması gerekmektedir.Örnek vermek gerekirse: Bilgisayarın içerdiği bilgileri kısmen ya da tamamen alıp tehdit yoluyla para sızdırması olmakta,girdiği bilgisayara zarar vererek verilerin kaybolmasına ya da kendi menfaatleri doğrultusunda kullanmak şeklinde olmaktadır.

Genellikle Rusya,Doğu Avrupa ve Uzakdoğu'da odaklanan hacker,cracker grupları belirli bir örgütsel hiyerarşi ve çalışma sistemi çerçevesinde para karşılığı dijital bilgi çalma,bozma gibi faaliyetler yürütmektedirler.(E-Mafya)[78]

Virüsler,Wormlar,Zombiler[79]

Virüsler ve wormlar kötü amaçlı olarak yazılmış kodlardır. Virüsler, bilgisayarda çalıştırıldığında herhangi bir şekilde zarar veren küçük programcıklardır ve bu programcıklar sanılanın aksine bilgisayarda cok yer kaplamazlar.Wormlar ise virüsler gibi kodlardan üretilmiştir,fakat virüslerden farkı virüs ile etkileşim halinde olunca aktif olur,fakat wormlar bilgisayar girdiği andan itibaren çalışmaya başlar ve kendisini farklı bilgisayarlar aramaya devam ederler.

Bir diğer farkı da Bilgisayar kurtlarının(wormların), bilgisayarınızın hafızasında boş yer kalmayana kadar kendini kopyalan programlardır. Bilgisayar kurtları bilgisayarın hafızasını kaplar ve böylece bilgisayarın yavaşlamasını ve hatta çökmesini amaçlar. Virüsler, disket, cd, internet, e-posta gibi yolları kullanarak bilgisayara bulaşırlar. Bilgisayar kurtları(wormlar) ilk önce bilg kendinsayar belleği(Ram)de bir yer bulur ve kendini oraya kopyalar daha sonra ise yeni kopyayı çalıştırır. Bu programın çalıştırılmasıyla bir döngü oluşur ve devamlı olarak ilk başlatılan programın kopyası üretilmekte sonra da bu kopyalar çalıştırılmaktadır. Bu kopyalama hafızada yer kalmayıncaya kadar devam eder ve hafıza dolduktan sonra bilgisayar yavaş çalışmaya başlayacak veya çökecektir. Zombiler (Ddos saldırıları)'nın hedefi sistemi işlemez hale getirmektir.Bazı Ddos atakları hedef sistemi iflas ettirmek için tasarlanmışken diğer bazıları da hedef sistemi meşgul edip normal işleyişini yavaşlatmak için tasarlanmıştır.Ddos atağı düzenleyen kişi kimliğini ele vermemek için atakları "zombi" adı verilen bilgisayarlar üzerinden yapmaktadır.

---

[78] http://www.baskent.edu.tr/~cigir/emafya.htm

[79] http://www.tbmpd.org.tr/modules.php?name=Sections&op= viewarticle&artid=10&page=1

Bu tür kötü amaçlı yazılmış kodlar,başkalarına zarar vermediği sürece suç sayılmamaktadır.Fakat bu tür kodlar; kişi ya da kurumlara intikal eder ve zarar verirse suç teşkil etmeye başlar.

4.3.Bilgisayar Yoluyla Dolandırıcılık

Dolandırıcılık genel bağlamda; Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamaya" denmektedir.Bilişim kavramı olarak "Dolandırıcılık" bilgisayar veya iletişim araçlarıyla kişileri şaşırtma,aldatma,kandırma olarak tarif edilebilir.[80]

Bilgisayar Yoluyla Dolandırıcılık; kredi kartlarının bir benzerinin yardımcı programlarla (Card Generator vb.)[81] oluşturulması ile,yetkisiz ve izinsiz erişilen bilgilerin kopyasını olmak şeklinde, finans bilgilerinin tutulduğu programlarla yapılan değişiklik ile istenilen kişinin hesabına istenildiği kadar para aktarmak suretiyle ve kişiler arasında mali alışverişi olan kişilerin adına mail vs. şeklinde iletişim kurarak; kişileri kandırarak dolandırıcılık suçu işlenmektedir.

4.4. Bilgisayar Yoluyla Sahtecilik

Kendisine ve başkasına yasa dışı ekonomik menfaat temin etmek ve mağdura zarar vermek maksadıyla; bilgisayar sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır.

Günümüzde başkalarının adına e-mail göndererek,ticari ve özel ilişkileri zedelenmesini sağlamak,başkalarının adına web sitesi hazırlamak ve bu web sitesinin tanıtım amacıyla başkalarına e-mail ve mesaj göndererek (iletişim kurarak) ve bu mesajlarda da mağdur olan şahsın telefonlarını vererek, sahte para, sahte evrak,sahte bilet vb. basma yönetimiyle bu suç işlenmektedir.

---

[80] Tck Madde/157,**Dolandırıcılık Tanımı**

[81] http://www.olympos.org/article/articleview/261/1/10-Yılmaz,Murat

4.5. Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

"Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" yazılımların; yasadışı yöntemlerle kopyalanmasını,çoğaltılmasını,satılmasını,dağıtılmasının ve kullanılmasını ifade eder.

Günümüzde korsan CD basımı ve dağıtılması korkunç büyüklükte boyutlara ulaşmakta,yapılan operasyonlar sonucu ele geçirilen lisanssız ürünlerin mali değerinin yüksekliği bu gerçeği ortaya koymaktadır.Tüketici (Yazılımı Satın Alan) da lisanssız çoğaltılan ürünleri ucuz olmasından dolayı tercih etmektedir.Unutmamak gerekir ki korsan yazılımları alan ve satan kişiler kanun önünde suçlu sayılmaktadır.Bu korsan yazılımlar; güvenlikli olmamakla birlikte;kullanımından doğan sorunlar karşısında herhangi bir müracaatta bulunulamamaktadır.Zira bu tür korsan yazılımlar genellikle bilgisayar ve kullanıldığı teknolojik araca zarar vermekte,tamir edilmesi imkansız sorunlara yol açmakta,bazı durumlarda boş çıkmakta, bazen de virüs barındırmaktadır.

4.6.Yasadışı Yayınlar

Yasadışı olarak kabul edilen unsurların bilgisayar sistemleri, ağları, internet aracılığıyla yayınlanması ve dağıtılması olarak ifade edilir.Kanunun yasaklamış olduğu bu materyaller; web siteleri(sayfaları), elektronik postalar, haber grupları, forumlar,iletişim sağlayan her türlü araç,optik araçlar tarafından kayıt yapan tüm sistemler olarak kabul edilir.

Yasadışı yayınları üç gruba ayırmak mümkündür.

Bunlardan birincisi,vatanın bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli internet siteleridir(sayfalarıdır).Bu tür siteleri hazırlayanların asıl amacı sansür konulmuş anonim olan interneti kullanarak kendilerine taraf toplamayı hedeflerler ve bilinen klasik yollardan ulaştıramadıkları ideolojilerini,vatanın bütünlüğünü bozacak düşüncelerini bu sayede ifade

etmektedirler.[82]

Yasadışı yayınların bir diğeri ise toplumun genel ahlakına, ar ve haya duygularına aykırı düşen yayınlardır.Bunlar pornografik görüntü veya yazılar şeklinde olmaktadır.Belki de her gün binlerce pornografik yayın internet üzerinden faaliyete geçmekte,bunların çoğu da çocuk pornografisi üzerine olmaktadır. İnternet aracılığıyla fiilen işlenen suçlardan üçüncüsü ise; bir kişiye,kuruma vb. karşı yapılan hakaret ve sövme suçudur.Bu suç türü internet üzerinden başkalarının adına uygun olmayan e-mailler göndererek kişi ya da kurumların itibarını zedelemek suretiyle olabilmektedir. Bir başka yol ise yine kişi ya da kurumların sahip oldukları adın,lakabın web üzerinden satın alınarak,kişi aleyhine yayında bulunmak suretiyle medyana gelebilmektedir.

5.BİLİŞİM SUÇLARINDA FAİL

Bilişim suçu faili bilişimle ilgili yeni teknolojinin ürünüdür. Bilişim suçu faili, organize bir suçla veya beyaz yaka suçlan veya yabancı istihbarat servisleriyle bile birleşebilir. Gelişmiş ülkelerdeki bilgisayar ve bunu kullanan bay ve bayanların sayıları dikkate alındığında, dünya çapında bilişim suçları için çok geniş ve devamlı büyüyen hem ticari ve hem de kamusal alan söz konusudur. Bugün bilgisayar kullanmayan büyük şirket kalmamıştır. Hatta bilgisayardan etkilenmeyen birey kalmamış gibidir. Üstelik, "elektronik para (kaynak) aktarım sistemi" olarak da bilinen nakit para kullanmayan bir toplum için teknolojinin gelişimi çok daha önemlidir. Bu yeni teknoloji, tedavüldeki nakit para yerine kullanılacak elektronik yapıyı araştırmaktadır. Bu elektronik yapı ise, hiç kuşkusuz bilgisayardır .[83]

Genel olarak belli bir düzeyin üzerindeki bilgisayar kullanıcılarında değişik özelliklerin görülebildiği ortaya konulmaktadır. Bu özelliklerin başlıcaları; meraklı olmak, detaylarla ilgilenmek, kendi meslek veya tutkularıyla ilgili problem veya

---

[82] http://www.hp.uab.edu/image_archive/ug/ | http://f27.parsimony.net/forum66647

[83] August Bequai , **a.g.e.**, s.4; Gordon Stevenson, **Computer Fraud: Detection and Prevention**, (Computer Fraud & Security, Volume 2000, Issue 11,1 November 2000) s.13.

sıkıntılı konulan çözmek, sezgiye dayalı düşünmeye yönelmek, zor konularda orijinal çözümler üretmektir.[84]

Bilgisayarlar, daha önce hiçbir suçta görülmemiş bir biçimde suç işleyenlere, kimliklerini gizleme olanağı sunmaktadır ve bilişim sistemlerindeki bireylerin ve şirketlerin özel ve gizli alanlarına kolaylıkla izinsiz girme ve orada kalma imkânı vermektedir.[85]

Bilişim suçunun konusu, bilişim teknolojisidir ve bu suçu işleyenler de, bilişim teknolojisinden yararlanmaktadırlar. Bilişim teknolojisindeki katlanarak artan ilerlemeler, hem bilişim suçlarına konu alanı ve olanakları artırmakta ve hem de bu teknoloji bilişim suçu faillerine yeni suç işleme kolaylıkları sağlamaktadır.

Bilişim suçu faillerinin teknolojideki yenilikleri suç işlerken kullanmaları ise, suçla mücadele eden görevlileri bilişim suçlarıyla mücadelede yeterli olmaktan uzak tutmaktadır. Bu bakımdan, bu suçlarla mücadele eden birimlerin, faillerin suç işleme tekniklerini, kullandıkları teknolojiyi ve faillerin niteliklerini bilmeleri ve buna göre stratejiler üretmeleri zorunludur.[86]

Bilişim suçlarıyla ilgili çalışmalar, çoğunlukla bilişim faillerini; genç, eğitimli, teknik yeteneğe sahip ve genellikle de agresif olarak nitelendirmektedir.[87]

6.BİLİŞİM SUÇLARINDA MAĞDUR

Bilişim suçları, hem bilişimi ve hem de kullanıcıları etkilemektedir. Esasında bu suçlardan, bilgisayarlar, bilgi sistemleri ve kullanıcılar zarar görmektedir. Daha da ötesi, bilişim suçlan, bireyleri ve organizasyonları mağdur etmektedir. Böylece bilişim suçları mağdur bilim (victimology)'de yeni bir alan

---

[84] Scott L KsandER , **a.g.e.**, s.28.

[85] D.Loren-M.F.S. Mercer, **Computer Forensic Charasteristics and Presevatyion of Digital Evidence** , (Vol 73 ,Number 3, Mart 2004), S.29.

[86] David, L .Carter ,**a.g.e.**,s.26

[87] August Bequai , **a.g.e.**, s.4.

açmaktadır. İlâve olarak, bilişim suçları, mağdur bilimin doğası içerisinde, bilgi ve onu kullanan ya da sahibi arasında ve insanların siber alana bakış tarzında yeni boyutlar açmaktadır.[88]

6.1. Mağdur bilim (victimology)

Genel olarak bir suça bakış açısında, mağdur yeterince önemsenmemektedir. Çünkü, suç soruşturmalarının temel amacı sanığı (suçluyu) bulmaktır ve soruşturma görevlileri sanıkla ilgili delillere yoğunlaşırlar. Bu yaklaşıma rağmen mağdur, her suçun merkezi durumundadır. Mağdur, suçun son tanığıdır. Mağdura ulaşılabiliyorsa, suçla ilgili en büyük bilgiler elde edilebilir. Mağdur ölmüş ise, soruşturma görevlilerince suç yeri gözlemlenerek daha detaylı anlatılmalıdır. Daha da ötesi, sanıklar genellikle suç işlemeden önce biraz düşündükten sonra mağdurları seçerler; hatta bu düşünme çok ani bile olsa durumun çoğunlukla böyle olduğu söylenebilir. Sanığın mağduru seçme ölçülerini anlamak, sanık hakkında pek çok şeyi açıklayabilir; soruşturma görevlilerini uyarır ve diğer potansiyel mağdurların korunmasını sağlayabilir.[89]

Viktimoloji (victimology), bir suçun mağdur veya mağdurlarını öğrenme sürecidir. Bu süreçte, sanığın neden bir suçta özel bir mağduru seçtiği anlaşılmaya çalışılır. Eğer, sanığın nasıl ve niçin özel bir mağduru seçtiği anlaşılabilirse, sanık ile mağdur arasında bir takım bağlar kurulabilir. Bu bağlar, coğrafi nitelikte, okulla ilgili, kişinin tutkularıyla ilgili veya daha yakın ya da kişisel olabilir.[90]

---

[88] Soumyo D. Moitra, **Analysis And Modelling of Cybercirme : Prospects And Potential**, (Max Planck Enstitute, 2004), s.23-24.

[89] Eoghan Casey, **Digital Evidence and Computer Crime : Forensic Science and Internet** , (Academic Pres, London 2000), s. 163-164.

[90] Soumyo D. Moitra, **a.g.e.** s.24.

6.2. Bilişim Suçlarında Durum

Bilişim suçlarında suçtan zarar görenlerin (mağdurların) davranışları, bu suçlarla mücadelede başarılı olunabilmesinde ciddi bir etkiye sahiptir. Başka bir anlatımla suçtan zarar görenler bu suçlarla mücadelede ana unsurlardandır.

Bilişim suçlarının süreçlerini anlamada ve bu suçlara karşı uygun politikalar geliştirebilmede mağdurların doğrudan ya da dolaylı şekilde yaşadıkları tecrübelerin önemli katkısı olacaktır.[91]

Bilişim suçları konusunda, kimi nitelemeler ve tasnifler yapılmakta ise de, bu suçların değişken yapıda olması, bu suçların belli başlıklar altında toplanabilmesini ve etkilerinin boyutlarını anlayabilmeyi zorlaştırmaktadır. Bu zorluk ise, zaten sınırlı sayıdaki suç istatistiklerine sahip olan suçla mücadele edenlerin problemde başarılı olabilmelerini ve yeni çözümler üretebilmelerini engellemektedir. Maalesef dünya ülkelerinde, bilişim suçlarının etki ve boyudan hakkında kesin bilgilere ulaşılamamaktadır. Bu suçların önemli bir miktarı, henüz rapor bile edilememiştir.[92]

Bu suçlar hakkında yapılan çalışmalar, ortaya konulan bilgiler, bir bakıma tam olarak bilinemeyen ve sürekli zarar verme boyutu artan bir hastalığın (aysberkin), yalnızca suyun üzerinde görünebilen resmine ilişkindir. Nasıl ki bir hastalığın tedavi edilebilmesi; öncelikle onun, ne olduğunun, boyutlarının, etkilerinin, neden olabileceği sonuçların ve nasıl oluştuğunun tam olarak bilinmesine bağlı ise, bilişim suçları için de, öncelikle bu bilgilerin tam olarak elde edilmesi gerekmektedir. Bu bakımdan da, bilişim suçlarının mağdurları en önemli kaynaklardandır.

---

[91] Soumyo D. Moitra, **a.g.e.**, s.24.

[92] Barbara Etter, a.g.e., S.4

6.3.Mağdurlarda çekingenlik

Bilişim suçlarıyla mücadelede, bu suçların resmî makamlara bildirilmemesi, adeta suç işleyenleri teşvik etmekte, bilişim, deyim yerindeyse suç işleme serbest bölgesi haline gelmektedir. Başta malî sektörde olmak üzere, pek çok şirket, maruz kaldıkları bilişim suçlarını gizlemekte, resmî makamlara bildirmemektedirler.

Bu çekingenliğin değişik nedenleri bulunmaktadır. Bunların başlıcaları şöyledir:[93]

1. Potansiyel olarak kötü bir etkiye maruz kalmamak,
2. Müşterilerin olumsuz bir tavrına neden olmaktan veya müşterilerin güvenini kaybetmekten korkmak,
3. Şöhretlerine bir zarar gelmemesini sağlamak,
4. Algılama eksikliğine sahip olmak,
5. Hisse fiyatları üzerinde olumsuz bir etkiye neden olmamak
6. Kanunları yeterince bilmemek veya kanunlara güvenmemek,
7. Kanunu uygulayan görevlilere yeterince güvenmemek,
8. Diğer nedenler.

Bilişim mağdurlarındaki farklı kaygıların temel nedeni, bilişim alanına devletin hâkim olamamasıdır. Nasıl ki, terör veya iç savaş olan bir alanda, yasalar yeterince uygulanamaz ve bölgede zarar görenler, şikayetin sonuçsuz kalacağını ve üstelik daha çok şey kaybedeceklerini düşünürlerse, bir bakıma bilişim alanındaki başıboş ve sağlıklı şekilde denetlenemeyen yapı, mağdurları çekingen kılmaktadır.

Esasında, bilişim suçu sanıklarının, klâsik suçlardaki sanıklar gibi yakalanıp, gerekli cezaya çarptırılacaklarına dair güven duygusu topluma verilebilse, mağdurların, resmî makamlara suçu bildirme konusundaki, kâr-zarar hesabı

---

[93] Hatcher-Mcdannel-Ostfeld, **a.g.e,,** s.399; ETTER, **a.g.e.**, s.4; Conley, John M.-Bryan, Robert M,, **A Survey of Computer Crime Legislation in the United States**, (Information & Communications Technology Law, March 1999, Vol.8, Issue 1), s.25-26.

yapmaları belki azaltılabilir ya da en azından sonuçta, suçu işleyenin yakalanıp gerekli cezayı göreceği düşüncesi, diğer kaygıların önüne geçebilir.

Mağdurlardaki resmî makamlara bildirim konusundaki çekingenlik, esasında tüm toplum için söz konusudur. Bilişim suçlarıyla ilgili bilgi eksikliği ise, sorunu daha da artırmaktadır.

Bilişim alanının kendisine özgü yapısı ve henüz keşfedilemeyen geniş bir deryayı oluşturması, yasaların ve uygulayıcıların başarılı olabileceklerini kuşkulu hâle getirmektedir. Üstelik, bu kuşkular giderilmeye çalışılsa bile, bilişim teknolojisinin sürekli akıl almaz biçimde gelişmesi, sorunu daha da derinleştirmektedir.

Bilişim suçu mağdurlarının kanun uygulayıcılarıyla işbirliğine yanaşmamaları, bilişim suçlarında yargılama yapılmasını da engellemektedir.[94]

6.4.Meşru Müdafaa Düşüncesi

Bilişim suçu mağdurları, kimi zaman ihkak-ı hak yoluna gitmeyi tercih etmektedirler. Başka bir söyleyişle, kendilerini meşru müdafa ettiklerini düşünmektedirler. Oysa, ceza kanunlarındaki meşru müdafa, cana veya ırza yönelik, defedilmesi için başka olanak bulunmayan zorunlu bir tehlike karşısında, sanığa karşı koyabilme hakkıdır. Bu açıdan bakıldığında, örneğin, banka hesabından bilişim yoluyla para çalınmasına maruz kalan mağdurun, bu kez sanığın banka hesabından aynı şekilde para hırsızlamasında, cana veya ırza yönelik bir tehlikeden söz etmek mümkün değildir. Başka bir anlatımla, burada meşru müdafa hakkından söz edilemez.

Bir an için bilişim suçlarında meşru müdafaa hakkı olabilir denildiğinde, bunun koşullarını ve ölçüsünü koyabilmek olanaklı değildir ve zaten böyle bir hakka, meşru müdafa da denilemez. Bu varsayımdaki yaklaşım, bilişim suçlarını çok daha fazlalaştırır. Bir bakıma bilişim suçlarının işlenmesini teşvik eder. Çünkü,

---

[94] John M Conley, Robert M Bryan, **a.g.e.**, s.25-26.

bilişim suçunu işleyen hemen herkes, uğramış olduğum saldırıya karşılık veriyordum savunmasına yönelebilecektir.

7. KLÂSİK SUÇLARA GÖRE BİLİŞİM SUÇLARININ YAPISAL GÖRÜNÜMÜ

Kamu ve özel sektörün işlemlerinde neredeyse tümüyle bilgisayarlara yönelmeleri, bilgisayar kullanımının hızla artması, suç işleme şeklinde değişikliklere neden olmuştur. Klâsik suçlar, suç konusuna fiziken odaklanarak işlenirken, bilişim alanında işlenen suçlarda bu yapıya gerek kalmamıştır. Aksine, bilişim suçlarında, klâsik suçlardaki fizik yapı yerine, soyut veya sanal bir alan söz konusudur. Üstelik, bu soyut alan, toplum üzerinde, ekonomik ve sosyal bakımdan sarsıcı bir etkiye neden olabilir.[95]

Bilişim suçlarındaki gelişmeler pek çok tartışmaya neden olmaktadır. 20. yüzyılın sonlarındaki en çok tartışılan konulardan birisi, bilişim (siber) alanı, onunla ilişkiler, bilişim suçlarının boyutları olmuştur. Özellikle, bu suçların ulusal ve uluslararası boyutları bu tartışmaları sürekli artırmaktadır. Bilişim suçlarının boyutlarının ortaya konulabilmesi, bir taraftan yapılacak kanun çalışmalarında, diğer taraftan ise suçla mücadeledeki yeni yaklaşımlarda önem taşımaktadır. Bu bakımdan, suçun yapısal ve yasal özellikleri, stratejik analizlerde ve suçların önlenebilmesinde başlıca etkenlerdendir.[96]

Bir zamanlar suçlar, aslında yerel ve bölgesel bir karakterdeydi. Bugün ise, telekomünikasyon ve bilgisayar teknolojisi sayesinde, suçlar ve bozulma (yozlaşma), coğrafi sınırlar içerisinde kalmamaktadır. Üstelik, teknoloji, suçların doğal yapışım da değiştirmektedir. Suç kavramındaki önemli değişim ise, suçlu davranışlarındaki ve suç şekillerindeki farklılıklardan kaynaklanmaktadır. Dünyadaki globalleşmeye bağlı olarak, ekonomi ve uluslararası yapıdaki suçlarda ve bozulmalarda, klâsik suçlara göre çok daha fazla artış görülmektedir ve suç

---

[95] Gerald R.Ferrera, - Stephan D .Lıchtenstein,.- Margo E. Reder, K.- Ray August, - William T . Schıano, **CyberLaw Text and Cases**, (West Thomson Learning, South-Western College, 2001.) S.297.

[96] S. David Wall, **Cathing Cybercriminals : Policing the Internet**, (International Review of Law Computers, Volume 12, Number 2,1998), s.201; Carter, **a.g.e.** s.21; Ditzion-Geddes-Rhodes, **a.g.e.**, s.285.

istatistiklerinde, klâsik suçlar karşısında bilişim suçlarında anormal farklar yer almaktadır.[97]

Bilişim suçlarının, klâsik suçlara göre daha yaygın olarak işlenmesi, teknolojik uzmanlığı olmayan kolluk görevlilerini, bu suçlarla mücadele etmede ve bu suç türleri anlamakta başarısız kılmaktadır. Bilişim suç türlerini anlayıp, iyi tahlil edebilmek, kolluk görevlilerinin yeni stratejiler geliştirmelerine yardım edecektir.[98]

Klasik suçlarda, suçun etki alanı sınırlıdır. Genellikle, temadi eden bazı suçlar hariç, suçun işlenmesiyle sonuçları genellikle dar bir alanda görülür ve sona erer. Oysa, bilişim suçlarında, işlenen suçun, kimi zaman sonuçlarını tahmin edebilmek mümkün değildir. Üstelik bilişim suçu işlenip tamamlandıktan sonra, suçun sonuçlan tamamlanmayabilir. Örneğin, bir virüs saldırısında, saldırgan eylemini tamamladıktan sonra, bunun doğurduğu sonuçlar bitmez. Saldırıya konu virüsün, kaç bilgisayara yayıldığı ve ne kadar zarara neden olduğunu tahmin etmek, neredeyse imkânsız gibidir. Çünkü, virüsler çok çabuk yayılır ve bir yerde durmayabilir. Virüsün bulaştığı yerler veya bilgisayarlar, başka yerler veya bilgisayarlarla bağlantıya geçtiklerinde, farkında olmadan virüsü yayarlar. Buysa, bilişim suçlarını, klâsik suçlardan ayıran, önemli bir özelliktir ve ciddi bir sorundur.

Diğer yandan, virüslerin fark edilmesi de zordur. Fark edildiklerinde ise, bunların tümüyle temizlenmeleri her zaman mümkün olamamaktadır. Üstelik her gün yeni ve farklı özellikleri taşıyan virüsler üretilmekte ve yeni bilişim suçları işlenmektedir. Açıkçası, bu alandaki mevcut sorunlara çözüm bulunamadan, daha karmaşık sorunlar üremektedir.

Konuyla ilgili (ABD'de) yapılan bir araştırmada, bilişim fakültesi mezunu Morris, internet güvenliğinin yetersizliğini ve bunun nasıl suç işlemede kullanıldığını ispatlayan bir program üretmiştir. Bu amaçla tasarlamış olduğu internet solucanını (worm), internette serbest bırakmış; takip için küçük işaretler

---

[97] I. Louise Shelley , **Crime and Corruption in the Digital Age**, (Journal of International Affairs 51 Vol.2, no.605, September 1998), s.20.

[98] David, L .Carter , **a.g.e.**, s.21.

kullanmıştır. O, solucanın, tahmin ettiğinden çok daha fazla makinelere zarar verdiğini ve üredığini (çoğaldığını) keşfetmiştir. Sonuçta, pek çok bilgisayar zarar görmüştür. Morris, solucanın nasıl yok edileceğini ve yeniden zarar vermesinin nasıl engelleneceğini programcılara e-postayla mesaj göndererek bildirmiştir.

Fakat bu mesaj, internetteki engeller nedeniyle ulaştırılamamıştır.. Bunun sonucunda, üniversitelerdeki 6.200 bilgisayar, askeri siteler, tıbbi araştırma araçları zarar görmüştür. Oluşan zararın giderilme maliyeti 98 milyon Dolan geçmiştir. Morris, daha sonra yakalanmış ve suçlu bulunarak mahkûm edilmiştir.[99] Üstelik, olayın meydana geldiği 1988 yılındaki rakamlara göre, günümüzdeki bilgisayar kullanıcılarının ve bilgisayarların sayılarının, bir hayli artmış olması, işin vehametini artırmaktadır. 21. yüzyılda, bilişim kullanımındaki artış, internetin sürekli büyümesi ve teknolojideki sürekli gelişmeler, bilişim suçlarının ve çeşitlerinin katlanarak artmasına neden olmaktadır.[100]

8. BİLİŞİM SUÇLARININ KENDİSİNE ÖZGÜ NİTELİKLERİ

Bilişim suçları, toprak sınırına dayanmadan, pek çok imkânlar içerisinde, herhangi bir sansüre maruz kalmadan ve yargısal yetkileri yetersiz kılarak işlenebilmektedir.[101] Siber alanda, adeta "ulusal vatandaşlıktan "internet vatandaşlığına geçilmektedir.[102]

Esasında, bilişim suçlarının bünyesindeki global yapı, bir başka anlatımla ülkeler üstü işlenebilme ve sonuç doğurabilme özelliği, bu suçları işleyenlere,

---

[99] ABD'de Morris hakkında açılan dava, 1984 tarihli The Computer Fraud and Abuse Act (CFAA)'da, 1986 yılında yapılan değişiklik sonrasındaki açılan ilk davadır. Morris, temyiz başvurusunda, olayda suç işlemek kastının olmadığını, 1986 tarihinde yapılan değişiklikle The Computer Fraud and Abuse Act adlı Kanuna göre, birinci olarak yetkisiz şekilde federal bir bilişim sistemine erişmek kastının, ikinci olarak da bilişim sisteminin kullanılmasını engelleme niyetinin olduğunun ispat edilmesi gerektiğini savunmuş ise de, yalnızca yasaklanmış bilişim sistemine erişim niyetinin olması yeterli görülerek başvurusu reddedilmiştir. Frank, P.Andreano, , **The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem**, (AM. J. CRIM. L, Vol.27:81), s.89-90.

[100] Gerald R. Ferrara, - Stephen D.Lichtenstein, - Margo E. K.Reder, - Ray August, - William T.Schiano, **a.g.e**, s.89-90.

[101] I. Louise Shelley , **a.g.e.**, s.20.

[102] S.David.Wall, **a.g.e.**, s.201,

ikinci bir vatandaşlık konumu sağlamaktadır. Bilişim suçlarının bünyesinden kaynaklanan bu nitelik, yani "internet vatandaşlığı kavramı", bu suçlarla mücadelede bir çıkış noktası olarak kullanılabilir. Bir devletin tek başına bilişim suçlarıyla mücadelede başarılı olabilmesi mümkün değildir. Bu bakımdan, bilişim suçlarını dünya çapında işleyen faillere, internet vatandaşlığı niteliği vermek, uluslararası işbirliğinde çıkış noktası olarak düşünülebilir. Bilişim suçlarını böylesi bir kimlikle gerçekleştiren kişilerin, internet bağlantısı olan her ülkede yakalanıp, hakkında soruşturma başlatılabilmesi yolu açılabilir.

Bilişim suçu faillerinin, bilişim ve telekomünikasyon ağlarına kolayca erişebilmeleri, dünya finans sisteminin bütünlüğünü tehdit etmekte, gitgide daha fazla zarar ortaya çıkmakta, buysa, devletlerin vatandaşlarını korumalarını zorlaştırmaktadır. Bilişim suçları, insan hakları için büyük bir tehlike oluşturmaktadır. Açıkçası, bilişim ve telekomünikasyon teknolojisindeki baş döndürücü gelişim ve bu alandaki risk algılamasındaki (anlayışındaki) azalma, suçluların bu alanda ciddi şekilde suç işleme kapasitelerini artırmaktadır. Bilişim ve telekomünikasyon alanında ileri teknoloji karşısında devlet, (sanal yapıda) sınırlarını savunabilme gücünü kaybetmektedir. Yargı yetkisi, internet ortamında yalnızca bir adres olarak beliren sanığa karşı uygulanamamaktadır. 21. yüzyıl, daha büyük teknolojik buluşlara sahne olmaktadır; fakat mevzuat ve bunu uygulayanlar bilişim suçları için hazır değildirler.[103]

9. BİLİŞİM SUÇLARININ TÜRLERİNİ BELİRLEME SORUNU

Bir görüşe göre bilişim suçlarını başlangıçta iki türde (kategoride) ele almak mümkündür. Bunlar; bilişim sahtekârlığı ve bilişimin kötüye kullanılmasıdır. Bilişim sahtekârlığı, bilişim ortamında para veya bir değeri elde etmek için bilgilerin değiştirilmesi veya bilerek yanlış bilgi kullanımıdır. Örneğin, bir bilişim sistemine, mal veya hizmet elde etmek için, kasıtlı olarak aldatıcı bilgilerin girilmesi gibi. Bilişimin kötüye kullanılması ise, hedef alınan bir bilişim sisteminin güvenliğinin

[103] I. Louise Shelley , **a.g.e.**, s.20

ihlâl edilmesi, saldırıya uğratılmasıdır. Bilişim kötüye kullanılması, bilişim dolandırıcılığına göre, daha az nitelikli fiiller olarak görülmektedir.[104]

Bilişim sahtekârlığı, periyodik denetimlerle fark edilemeyebilir. Özellikle bilgi veya dosya sahtekârlığını anlamak, gereken iz ve esere ulaşılamadığı için oldukça zor olabilir. Bilişim sahtekârlığını işlemenin çeşitli biçimleri vardır. En yaygın biçimi, yoğun olarak teknolojinin kullanılmasıdır.[105]

Bilişimle ilgili suç türlerini, çok değişik şekillerde ortaya koymak mümkündür. Ancak, konuyu makul bir seviyede ele alarak, en çok görülen ve en ağır nitelikli olanlarından başlamak üzere, suç türlerinin ele alınmasında yarar vardır. Özellikle bilişim suçlarıyla mücadelede, başta yasal yapıda olmak üzere, gerekli alanlardaki örneğin, kolluk görevlilerinin bilgi ve teknik donanımla ilgili eksikliklerinin giderilebilmesi bakımından, işlenen bilişim suç türlerinin bilinmesi önemlidir. Bu arada, öncelikle bilişim suçlarının artış (patlama) nedenleri de dikkate alınmalıdır.

---

[104] Comsec, **Computer Forencics and Cyber Investigations,** power point sunumu, (International and Technical Resourc Center 2004), s.6-8.

[105] Erhan Erdönmez, **a.g.e.**.s.13

DÖRDÜNCÜ BÖLÜM

İNTERAKTİF BANKA VE KREDİ KARTI DOLANDIRICILIĞI

Son dönemde, internet vasıtasıyla yapılan dolandırıcılık eylemleri ile elde edilen paraların yurtdışına transferinde banka müşterilerinin de aracı olarak kullanıldığı olaylarla karşılaşılmaktadır.

İnternet üzerinden sohbet (chat), elektronik posta veya "dolandırıcılık amacıyla kurulan bazı siteler" aracılığıyla banka müşterilerine ulaşıldığı ve çeşitli gerekçeler sunularak müşterilerin banka hesap bilgilerinin (şube adı, hesap numarası, vs.) talep edildiği ve yurtdışındaki hesaplara para transferinde aracılık teklif edildiği tespit edilmiştir. Bu yöntemlerle elde edilen müşteri hesaplarına, internet üzerinden yapılan dolandırıcılık eylemleriyle başka hesaplardan para transferi gerçekleştirilmektedir. Daha sonra müşterilerden, hesaplarına gelen paraları; belirtilen hesaplara veya kişilere transfer etmeleri talep edilmektedir. Bu durumda, banka müşterileri farkında olmadan dolandırıcılık eylemine iştirak etmiş olmaktadırlar.[106]

Bankacılık işlemlerinin internet üzerinden yapılmasıyla zamandan ve emekten tasarruf sağlanmış ve müşterilere kendi hesaplarını yönetme imkânı tanınmıştır. Fakat bilişim sektörünün hızla gelişiyor olması, sorunların ve çözümlerin dakikalar içinde değişmesi son kullanıcın bunu takibini zorlaştırmaktadır. Sağlanan bu faydaların yanı sıra gerek kullanıcıların yeterli özeni göstermemesi, gerekse güvenlik önlemleri hakkındaki bilgi eksiklikleri banka müşterilerinin mağdur olmalarına sebep vermektedir. [107]

İnternet bireylere ve şirketlere fazla çaba,para ve zaman harcamaksızın büyük bir izleyici-dinleyici kitlesine ulaşmasını sağlar.Herhangi biri bir internet sitesi hazırlayarak veya e-mail göndererek veya sohbetlere katılarak milyonlarca insana ulaşabilir.İnternet dolandırıcıları için kendi mesajlarını gerçekçi ve

[106] http://www.fuartakip.com/haberler/index.asp?ID=51

[107] http://www.kom.gov.tr/turkce/gundem.aspx?idd=32

uygulanabilir yapmak oldukça kolaydır.Fakat yatırımcılar için gerçek ve kurguyu ayırt etmek hemen hemen olanaksızdır.[108]

Internet dolandırıcıları yanlış bilgileri yaymak için chat,online gazete veya e-bülten içeren çeşitli internet araçlarını kullanırlar.Dolandırıcıların parmaklarının ucunda bulunan bu araçların hepsi oldukça düşük maliyetlere malolur. [109]

1.İNTERNET BANKACILIĞI

1.1.Tanımlama

Dijital çağ ve internet günümüzün en popüler kavramlarından biri olmuştur. İnternet ve BT teknolojileri Sanayi Devrimi'nden bu yana insanlığın yaşadığı en önemli aşama olarak kabul edilmektedir. 21. yüzyıl şirketler ve diğer organizasyonların interneti stratejik planlarının merkezine yerleştirecekleri bir yüzyıl olacaktır.

Bu gelişme, diğer mallardan farklı olarak elektronik ortamda transfer edilebilen ve dağıtımı yapılabilen finansal ürünler için daha fazla geçerlilik kazanmaktadır. Finansal kurumlar, sanal nitelikte kabul edilebilecek olan para ile iş yapmaktadırlar. Dolayısıyla internet ortamına en kolay taşınabilecek ve kullanıma en uygun olan ürünlerin finansal hizmetler sektörüne ait olduğunu ifade edebiliriz. İnternet bankacılığı konusundaki hızlı gelişim süreci de bu trendi kanıtlar mahiyettedir.

E-bankacılığın geleneksel bankacılık sektörü üzerinde çok önemli etkileri mevcuttur. İşlemlerin büyük ölçüde fiziksel olmaması ve on-line ortamda yapılması, işlem maliyetlerinin düşürülmesine ve hizmetlerin iyileştirilmesine olanak sağlamaktadır. Sunulan hizmetin iyileştirilmesi ve hizmet sunuş hızı daha

---

[108] http://www.crime-research.org/articles/Internet_fraud_0405

[109] http://www.crime-research.org/articles/Internet_fraud_0405

fazla müşteriye ulaşmayı ve neticede daha fazla fon toplayarak bunun piyasaya arzını sağlayacaktır. İnsan kullanılmadan gerçekleştirilen bu işlemler; maliyetleri, harcanan zamanı, gecikmeleri ve hataları azaltacaktır.

Dolayısıyla e-banking, bankacılığın daha etkin bir yapıya kavuşmasına katkıda bulunacaktır. Gerçekten de geleneksel bankacılıkta ortaya çıkan maliyetleri, internette gerçekleştirilen bir işlemin maliyetiyle karşılaştırdığımızda, internet ortamında gerçekleşen maliyetlerin şubelerde gerçekleşen maliyetlerin %1'i olduğu görülmektedir.

İnternet coğrafi sınırların ötesinde tüm dünyaya açılan bir penceredir. Böyle olunca internet kendi doğal ortamında bankalara coğrafi bir genişleme imkanı sunmaktadır. İnternetin sınırı yoktur ve web siteleri tüm dünyadaki müşterilerine hizmet sunabilmektedirler. Bu hem fon toplamayı ve hem de fon kullandırmayı evrensel bir boyuta taşıyarak bankacığın global bir yapı kazanmasına sebebiyet verecektir. Ayrıca bankaların yeni bir pazara, yeni bir coğrafyaya girerken birleşme, satın alma gibi zorluklarını azaltmaktadır.

Diğer taraftan finansal piyasalar giderek çok daha açık hale gelmektedir. Hiç kuşku yok ki bu trend hızla devam edecektir. Böylece internet sayesinde çok sayıda uluslararası banka diğer piyasalara girebilecek ve oradakilerin ekmeğini elinden alabilecektir. Rekabetin çok şiddetleneceği böyle ortamlarda yerel bankalar var olma mücadelesi verecektir. Yerel bankalar için bir çözüm yolu olarak güçlü uluslararası bankalarla işbirliği yolunu seçmek mümkün görünmektedir. Bu durumda bile yerel bankalar bir katma değere sahip olabileceklerdir.

İnternetten yararlanan bankalar için bir diğer olumlu sonuç, ürün ve hizmetlerini genişletme imkanı bulabilmeleri, yeni ve mevcut müşterilere bankacılık hizmetlerinden çok daha fazlasını verebilmeleri, çapraz satış yapabilmeleridir. İnternet yoluyla finansal süpermarket oluşturmak ve farklı ürünleri eş zamanlı olarak sunmak farklı fiyatlama yoluyla daha cazip ve kolay hale getirilebilmektedir. Böylece daha fazla ve kaliteli ürünle daha hızlı hizmet sunabilmektedirler. Zamanla birçok bankacılık ürününün web'e uyarlanmasıyla

bankalar, mevduat toplamada ve değişik alanlarda krediler kullandırarak fon kullandırmada önemli adımlar atmakta ve bu süreç devam etmektedir. Ancak burada altı çizilmesi gereken önemli bir nokta, sözü edilen bu fırsatların yanı sıra internet yoluyla yapılacak finansal hizmetlerin maliyetlerinin düşük olması piyasaya girmeyi de kolaylaştırdığından, rekabeti arttırarak bu da piyasada kar marjlarının düşmesine neden olabilecektir. Müşteriler, online bağlantı sağladıklarında tüm finansal siteleri ziyaret etme olanağı bulacak ve çok kısa bir sürede ürünlerle ilgili fiyat araştırması yapabilecek, dolayısıyla tam rekabetin önemli şartlarından biri olan enformasyon maliyetlerinin sıfıra yakın olma şartı gerçekleşecektir. Bu durum ise kar marjlarının baskı altına alınmasının diğer bir nedeni olacaktır.

Teknolojideki gelişmeler ve rekabetin hızla artmasıyla banka müşterileri de davranış ve tercihlerini değiştirmeye başlamıştır. Öncelikle daha fazlasını istemeye başlayan müşteriler, çok fazla seçenek olması nedeniyle daha az sadık olmaya başlamışlardır. Müşterilerin birkaç tedarikçiyi dolaşıp ürün ve hizmetlerini karşılaştırması her zamankinden daha kolaydır. Böylece ihtiyacına en uygun cevabı verecek bankaya kolayca ulaşan müşteri saldırgan bir strateji izleyerek yüksek mevduat faizi ve düşük faizli kredi dağıtan bankalara yönelecektir. Bu durum 150 yıllık geçmişi olan geleneksel bankacılık sektörü için ciddi bir tehdittir. Bu tehdidi bertaraf etmek için birçok geleneksel banka, internet bankacılığı konusunda girişimler yapmaktadırlar. Ancak izlenen strateji savunmacı bir stratejidir ve mevcut konumu ve müşterileri elde tutmak için başvurulan bir yoldur.

Tüm bu değerlendirmeler dikkate alındığında, internet kanalıyla sunulan hizmetlerin her geçen gün çeşitlenip artması, bankaları ister istemez bu konuda yatırım yapmaya itmektedir. Çok büyük çaplı e-banking projelerini finanse eden bankalar yeni oluşan bu rekabetçi dünyada yerlerini almak, müşterileri tutmak ve karlarını sürekli hale getirmek çabasındadırlar. Bankaların internet bankacılığına yatırım yapmalarının en az dört gerekçesi bulunmaktadır. İlki, kimsenin internet bankacılığının gelişeceğinden kuşku duymaması, ancak tek bilinmezliğin gelişmenin hızında olmasıdır. İkincisi, bankaların internet bankacılığı alanında en kârlı faaliyetlerinin ellerinden alınacağı korkusunu taşımaları. Üçüncüsü, bankaların kendi aralarında rekabet etme zorunlulukları, son olarak ise banka

sermayedarlarının, teknoloji hisselerinin yükselmesi buna karşın diğer hisselerin gerilemesi karşılığında dot.com firmasına sahip olarak hisselerinin yükseldiğini görmek istemeleridir.

İnternetin elektronik doğası, alternatif ödeme sistemlerine izin vermektedir. Bankaların e-ticaret ödeme akışlarını kontrol etmeleri mümkün görünmektedir. Bireyler ve firmalar sahip olmuş oldukları kredi kartları vasıtasıyla internet üzerinden alışveriş yapabilmektedirler. Böylece bankalar, firma ve kişilerin sahip olmuş oldukları kredi kartları vasıtasıyla internet üzerinden işlem hacimlerini arttırabileceklerdir. Öte yandan internetin yapısı gereği tüm dünyaya açık bir network olması, internet üzerinden gerçekleştirilecek bankacılık işlemlerinin riskli olabileceği korkusunu gündeme getirmiştir. Günümüzde bu riskleri ortadan kaldırmak ya da kontrol altına almak için birçok teknik ve standart geliştirilmiştir.

Ülkemiz açısından internet bankacılığının geldiği son noktayı irdeleyecek olursak, Türkiye'de bankacılık sektöründe internet kullanımının iki şekilde gerçekleştirildiğini görürüz. Bankaların büyük bir bölümü internette bir site oluşturarak, kurumları, ürünleri ve hizmetleri hakkında bilgi vermekte, şube ve ATM adresleri ile çeşitli faiz oranlarını müşteriye sunmaktadırlar. Daha çok bankaların kendini tanıtma ve sunduğu hizmetlerini müşterilerine internet yoluyla pazarlama amacıyla kullanılan bu siteler interaktif bir yapıya da sahip değillerdir. Bir çeşit elektronik broşür görevi gören bu siteler reklam amaçlı kullanılmaktadır.

1.2.İnternet Bankacılığının Yaygınlaşma Nedenleri ve Tüketici Açısından Getirdiği Kolaylıklar

Başlarda güvenlik, maliyet gibi nedenlerle yaygınlaşması sınırlı kalan İnternet bankacılığı bu konularda sağlanan gelişmelerle daha geniş kesimler tarafından benimsenmeye başlanmıştır.

Aşağıda İnternet bankacılığının yaygınlaşma nedenleri ve müşteriye sunduğu kolaylıklar verilmektedir.

Önceleri bankaların online bankacılık yapabilmeleri için kendi sistemlerini geliştirmelerini gerektirmiştir. Bu, özellikle küçük bankalar açısından bu dağıtım kanalını kullanmayı maliyetlerin yüksekliği nedeniyle imkansız hale getirmekteydi. Daha sonraları özellikle İnternetin gelişmesi, yaygınlaşması ve İnternet bankacılığı destek hizmetlerinin bankalar tarafından üçüncü firmalardan satın alınabilmesi daha çok bankanın bu hizmetleri vermesini mümkün kılmıştır.

Şahsi bilgisayarların fiyatlarının düşmesi ve yaygınlaşması potansiyel İnternet kullanıcı sayısını artırmış, bankaların İnternet bankacılığına ilgisinin artması ve İnternet bankacılığının daha yaygın müşteri kitlesi tarafından kullanılması ile birlikte müşteri başına maliyetler düşüş göstermiştir.

Evler dışında işyerleri, kafeler, oteller gibi birçok yerden İnternete ulaşmak da mümkün hale gelmiştir. İnternete ulaşmada kullanılan programların aynısının online bankacılık için de kullanılabiliyor olması, getirdiği kolaylık nedeniyle İnternet bankacılığının yaygınlaşmasına neden olan başka bir faktördür.

Diğer bir neden de insanların İnternet bankacılığını kullanmalarında en büyük engel olan güvenlik endişelerinin azalmasıdır. Bu hem İnternet ulaşımının sağlandığı programlarda meydana gelen gelişmeler hem de gittikçe daha fazla insanın internet bankacılığını kullanması sonucunda olmuştur. Bugün İnternet erişim programları tarafından kullanılan SSL (Secure Socket Layer) ve 128 bit şifreleme programları sayesinde bilgisayar ile banka arasındaki bilgi transferi sırasında gerekli olan yeterli güvenlik düzeyinin sağlanması mümkündür.

İnternet bankacılığı tüketici açısından birçok kolaylık getirmektedir. Bu kolaylıklardan bir kısmı İnternet bankacılığının avantajlarını ortaya koyması açısından aşağıda verilmiştir.

•İnternet bankası kullanıcıları şubede sırada beklemek zorunda değillerdir, hatta para çekme dışında her türlü işlemi evlerinin rahat ortamlarından gerçekleştirebilmektedirler.

•İnternet bankacılığını kullanarak 24 saat bankacılık yapabilmektedir. EFT gibi

bazı işlemler için hala belli saatler arasında işlemi gerçekleştirme zorunluluğu varsa da günün herhangi bir saatinde bir sonraki gün için EFT talimatı verebilmektedir. Bu talimatlar daha sonra herhangi bir müdahaleye gerek kalmadan banka tarafından gerçekleştirilebilmektedir.

•İnternet bankacılığı ile hesaplara doğrudan girip istenilen araştırmalar yapılabilmektedir.Bu araştırmalar hesaplara yapılan kayıtlardan günü gününe haberdar olunmasını ve yanlışlık yapılması halinde gerekli düzeltmelerin zamanında gerçekleştirilmesini sağlamaktadır. Örneğin kredi kartlarının müşterinin bilgisi dışında kullanılması halinde bundan çok daha çabuk haberdar olunması ve gerekli müdahalelerin yapılması mümkün hale gelebilmektedir. Tüketici açısından İnternet bankacılığının bütün işlemlerinin bu aşamada herhangi bir ücret alınmadan gerçekleştirilmesi önemli bir avantajdır.

•İnternete ulaşımının olduğu dünyanın her yerinden hesaplara ulaşabilmektedir. Diğer bir perakende bankacılık yöntemi olan telefon bankacılığında yurt dışında olduğunuz sürelerde bankanıza ulaşmak için uluslar arası telefon görüşmesi yapılması gerekirken,İnternet bankacılığında böyle bir maliyete katlanmaya gerek kalmamaktadır.

•Fatura ödeme fonksiyonu İnternet bankası kullanıcılarına çok büyük kolaylıklar sağlamaktadır. Bankalara verilecek talimatlarla faturaların postada kaybolmasından veya bu faturaları fiziki olarak gidip ödemekten kurtulmak mümkündür. Evden uzakta iken bile faturaların ödenmesinde herhangi bir sorunla karşılaşılmamaktadır. Bankayla şirketler arasında kurulan bağlantılar ile ödenmesi gereken faturaların tarihini ve tutarlarını kontrol etmek ve ona göre vadesiz hesaba para aktarmak mümkün olabilmektedir. Türkiye'de özellikle telefon, su, elektrik vb. faturalarda fatura tutarlarının İnternet'ten görülebilmesi imkanı Amerika'da çok yaygınlaşmış değildir.

•Yaşlılık, hastalık veya herhangi başka bir nedenden dolayı şubeye gitme imkanı olmayanlar için İnternet bankacılığı büyük kolaylık sağlamaktadır.

•Tüketiciler açısından özetlenmek istenirse daha önce ancak şubeye giderek ve önemli zaman harcanarak yapılabilen birçok işlemin büyük kolaylıkla ve uygunlukla İnternet bankacılığı aracılığı ile yapılabildiği görülecektir.

Yukarıda anlatılanlar dışında İnternet bankacılığı sayesinde hesaplar hakkında zamanında ve daha fazla bilgiye sahip olarak daha iyi finansal kararlar alınabilir. Hesaplar hakkında daha fazla bilgiye sahip olmak aynı zamanda vadesiz hesaplarda gereksiz miktarlar tutmayarak daha fazla faiz geliri elde etme imkanı veya yazılan çekler karşılığında yeterli tutarlar bulundurmayı kolaylaştırma imkanı sağlar. Yukarıda anlatılan kolaylıklar genellikle kişiler açısından ele alınmıştır. Şirketler açısından da yukarıdaki kolaylıkların bir kısmı geçerli olup, bazı ek kolaylıkların da İnternet bankacılığı ile birlikte geldiği görülmektedir

1.3.Bankaların İnternet Sitelerinin Çeşitleri

---Yalnızca Bilgi Verme Amacıyla Yapılanlar

Önceleri birçok İnternet sitesinde olduğu gibi bankaların İnternet sitelerinde de herhangi bir işlem yapmak mümkün değildi. Bankalar İnternet siteleri sunulan ürünler hakkında bilgi alınabilen, faiz oranları, şube, ATM adresleri ve telefonları gibi, bankanın diğer hizmet kanallarına ulaşma konusunda müşterilere yardımcı olan bir araç konumunda kalmıştır.

---Bankacılık İşlemleri Yapılabilen Siteler

İnternet teknolojisinde meydana gelen gelişmelerin İnterneti online bankacılık için yeterince güvenli hale getirmesinden sonra, Wells Fargo adındaki Amerikan bankası Mayıs 1995'te dünyadaki ilk İnternet üzerinden bankacılık hizmetini sunan banka haline gelmiştir (Online Banking Report). Ancak bu ilk sistem müşterilere işlem yapma imkanı vermemekte, yalnızca hesap hareketleri ve bakiyeleri görüntüleme imkanı vermiştir. Wells Fargo'yu takiben Ekim 1995'de bütün bankacılık işlemlerinin gerçekleştirilebildiği ilk banka olan Security First Network Bank, İnternet üzerinden işlemlere başlamıştır. Adı geçen banka şube ağı olmaksızın yalnızca İnternet üzerinden hizmet veren bankalardan, FDIC

tarafından sigortalanan ilk banka olma özelliğini de taşımaktadır. Bu bankalar vadesiz ve vadeli mevduata yüksek faiz vererek müşteri çekmeye çalışmaktadırlar. Ayrı bir İnternet bankası olan Net.Bank, 1999 yılında ilk kâra geçen İnternet bankası olmuştur.

Bankacılık işlemlerinin yapılmasının mümkün olduğu İnternet sitelerinde genellikle bütün geleneksel bankacılık işlemlerinin sunulduğunu görülmektedir. Bunlar hesap bakiyesi görüntüleme, transferler, hisse senedi işlemleri, sigortacılık işlemleri gibi işlemlerdir.

Amerika'da bankaların İnternet siteleri incelendiğinde, hesaplar arasında yapılan transferlerden kastedilenin kişinin kendi hesapları arasında yaptığı transferler olduğu görülmektedir.

Türkiye'de kullanılan anlamda EFT işlemleri kişiler için İnternet üzerinden yapılamamaktadır. Amerika'da hesabınızdan üçüncü kişilere para göndermenin tek yolu, fatura ödeme fonksiyonunu kullanmaktır. Fatura ödeme fonksiyonu ise iki şekilde çalışmaktadır. Birincisinde, bankanın daha önce elektronik ödeme anlaşması yaptığı şirketlere,elektronik olarak kendi hesabınızdan ne tutarda ve hangi tarihte ödeme yapmak istediğinizi tanımlayarak transferi elektronik olarak gerçekleştirmek mümkün olmaktadır. Yalnız bu fonksiyon genellikle büyük şirketler için kullanılabilmektedir. Diğer seçenekte ise fatura ödemesi yapılmak istenen şirketin adresi ve diğer bilgileri girilmekte ve ödeme yapılmak istenen tutar ve tarih belirtilmektedir. Banka daha sonra bu şirkete belirtilen tarihte bir çek göndermekte ve ödeme bu şekilde gerçekleştirilmektedir. Görüldüğü gibi burada kişilerin hesabından üçüncü kişilerin hesabına elektronik olarak bir tutarın transfer edilmesine imkan verilmemektedir. Bu husus Amerika'daki İnternet bankacılığına güvenlik açısından şüpheyle bakan insanları bir ölçüde rahatlatmaktadır. Çünkü birisinin sizin hesabınızdan EFT yolu ile başka bir hesaba para aktarması yerine sizin adınıza bir adrese çek göndererek bu çeki bozdurmaya çalışması, daha uzun ve başarısızlığa uğrama ihtimali daha yüksek olan bir yöntemdir.

Amerika'da Türkiye'den farklı olarak İnternet üzerinden yeni hesap açılması dahi mümkündür. Bu herhangi bir şubesi olmayan yalnızca İnternet üzerinden

faaliyet gösteren bankalar için önemli bir konudur. Örneğin Citibank İnternet sitesinde müşteriler için açılabilecek hesap türlerini vermektedir. Müşteri bu hesap türleri arasından açmak istediği türü seçtikten sonra isim, adres,telefon numarası, annesinin kızlık soyadı, sosyal güvenlik numarası, pasaport numarası gibi bilgileri girerek bir form doldurmaktadır. Form doldurulduktan birkaç gün sonra kişilere posta ile imza kartonları gönderilmektedir. Kişiler imza kartonunu yatırdıkları mevduatla birlikte gönderdikten sonra, iki ile yedi gün içinde hesapları açılmakta ve kendilerine bir banka kartı gönderilmektedir. Citibank'da İnternet şubesini kullanmak için bu banka kartı ve kartın şifresi yeterlidir. Bazı bankalar şifreyi posta ile gönderirken bazı bankalar da İnternet üzerinden daha çabuk ulaşım imkanı vermektedirler.

Amerika'da İnternet'in her alandaki uygulamalarının yaygınlaşmasıyla ortaya çıkan bir başka eğilim ise e-finans ile e-ticaretin birbiriyle çok yakınlaşmasıdır. Bu iki şekilde olabilmektedir.

Bunlardan birincisi banka dışı şirketlerin bankaların geleneksel fonksiyonları olarak görülen bazı fonksiyonları yerine getirmesidir. e-Ticaretin gelişmesi ile İnternet üzerinden yapılan ticaret sonrasında alınan malların bedellerinin malları satana nasıl ödeneceği ile ilgili bazı ihtiyaçlar gündeme gelmiştir. Örneğin İnternetteki en büyük açık artırma şirketlerinden birisi olan eBay'de herhangi bir kişi mallarını satmak için başvurabileceği gibi yine herhangi bir kişi de açık artırmalara katılarak bu malları alabilmektedir. Bu işlem sonucunda malın bedelinin ödenmesi gündeme gelmektedir.

İkinci olarak bankaların İnternet sitelerine gelen müşterilerine klasik bankacılık işlemlerini sunmalarının yanında, bazı mallar satın almaya yönlendirmek şeklindeki eğilimi gösterebiliriz.

Buradaki amaç müşteri tabanından mümkün olan en yüksek kazancı sağlamaktır. Burada yapılması gereken uygulama müşterilerin bankanın İnternet sitesinden ayrıldığı anda banka sitesinden ayrıldığına ve banka ürünleri ile ilgili garantilerin -mevduat sigortası vs- artık mevcut olmadığına ilişkin uyarıların siteye konulmasıdır.

1.4.İnternet bankacılığı ve müşteri bilgilerinin korunması

Elektronik ticaretin getirdiği en önemli avantajlardan birisi kişilerin tercihleri hakkında bilgi toplanmasını çok kolaylaştırmasıdır. Bankalar ve diğer şirketler toplanan bu bilgiler sayesinde kişilerin tercihleri doğrultusunda hedeflenmiş pazarlama yöntemleri uygulayabileceklerdir.

Ürünlerin geliştirilmesi aşamasından, reklam ve satış aşamasına kadar her aşamada müşteri istekleri göz önünde bulundurulduğundan, ürünün başarılı olma ihtimali artmış olacaktır Bütün bunların hem müşterinin, hem de satışları artırıcı etkisi nedeniyle şirketin yararına olduğu düşünülebilir. Ancak müşteri bilgilerinin toplanmasının bu kadar kolay hale gelmesi ve kişiler hakkında her türlü bilginin toplanarak bunun bilgisayar ortamında saklanması, kişilerde toplanan bu bilgilerin kendi bilgileri dışında ve aleyhlerine sonuçlar doğurabilecek şekilde kullanılabileceği endişesini doğurmaktadır. Kişiler hakkında toplanan bilgiler; kişilerin gelir düzeylerinden nerelerde çalıştıklarına, kredi kartları ile yaptıkları alışveriş çeşit ve eğilimlerinden sağlık bilgilerine kadar çeşitlilik göstermektedir. Bu aşamada örneğin bir bankanın kişilerin sağlık harcamaları ile ilgili öğrendiği bilgileri aynı gruba ait sigorta şirketi ile paylaşması sonucunda, bu kişinin satın almak istediği sigorta reddedilebilmektedir. Amerika'da yasa koyucu da benzer kaygılarla 1999 yılında Gramm-Leach-Bliley Kanunu'nu yürürlüğe koymuş ve müşterilerin kişisel kayıt ve bilgilerinin korunması yönünde bankalara idari, teknik ve fiziksel tedbirlerin alınması yükümlülüğünü yüklemiştir. Bu kaygılara cevap vermek amacıyla bankalar müşteri bilgilerini ne şekilde kullanacakları ve bunları kendi grup şirketleri veya üçüncü şirketlerin pazarlama çalışmalarında kullanılmak üzere nasıl paylaşacakları konularını belirten bir bildiriyi İnternet sitelerine koymaktadırlar. Bu konu ile ilgili örnek bildiriler bankaların İnternet sitelerinde görülebilmektedir.

Bankaların kişisel bilgilerin korunması bildirileri, müşterilerin bilgilerini kullanmadan önce müşterilerden onay alınması esasına dayanılarak düzenlenen bildiriler veya müşterilerin bilgilerin kullanılmasını reddetmedikçe bu onayın var olduğunu varsayan bildiriler olmak üzere iki şekilde düzenlenebilmektedir. Birinci

tarzda düzenlenen bildiriler kişilerin özel bilgilerinin korunması konusunda daha hassas davranan kurumlar tarafından düzenlenmektedir

2.İNTERNETTE DOLANDIRICILIK TÜRLERİ

2.1Keylogger

2.1.1.Tanımı: İnternet kullanan banka müşterilerinin veya internet üzerinden ticaret yapan kullanıcıların online işlem şifrelerinin çalınması keylogger, yani klavye tuş girdilerini kayıt eden yazılımlar veya donanımlar vasıtasıyla da yapılmaktadır. Kullanıcıların bilgisayarlarına yerleştirilen keylogger adlı yazılım-donanım bilgisayarda yapılan her türlü işlemlerin bir kaydını tutar, bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntüleri de olabilir. Bu kayıtlar ya sistemde bir txt (metin) dosyası olarak tutulur ya da klavye girdileri e-posta ile saldırgana (hacker) gönderilir.

Bir çok bilgisayar güvenliği kitabında keyloggerdan bahsedilir ancak bu konunun tamamına değinilmez. Yakın zamanda keylogger dan yayılan tehdit neredeyse iki katına çıkmıştır. [110]

2.1.2.Çeşitleri

---Donanım Keylogger:Birkaç biçim ve formda oluşturulmaktadır. Mesela klavye ile bağlantı noktasında harici bir ek olabilirler.klavye kablosunu eşleştirmek için kullanılan silindir şeklinde parçalardır.Kurulumu bir dakikadan daha az zamanda gerçekleşir ve bilgisayarın arkasında bulunduğundan dolayı tespiti oldukça güçtür.Yine donanım keyloggerları klavye içine de yerleştirilebilmektedir.Özellikle batılı ülkelerde keyloggerlı bir çok donanın satılmaktadır.Yapılan bir testte Klavye ile bağlantı noktası arasına yerleştirilen KeyGhost isimli donanım keyloggeri, Windows aygıt listesinde bulunamamıştır.[111] Tespiti oldukça güçtür.

---

[110] S.Garfinkel, G.Spafford, And A.Schwartz, , **Practical Unix & Internet Security**, (O'Reilly & Associates, 3rd edition, 2003.) .s.21

[111] Keyghost, http://www.keyghost.com

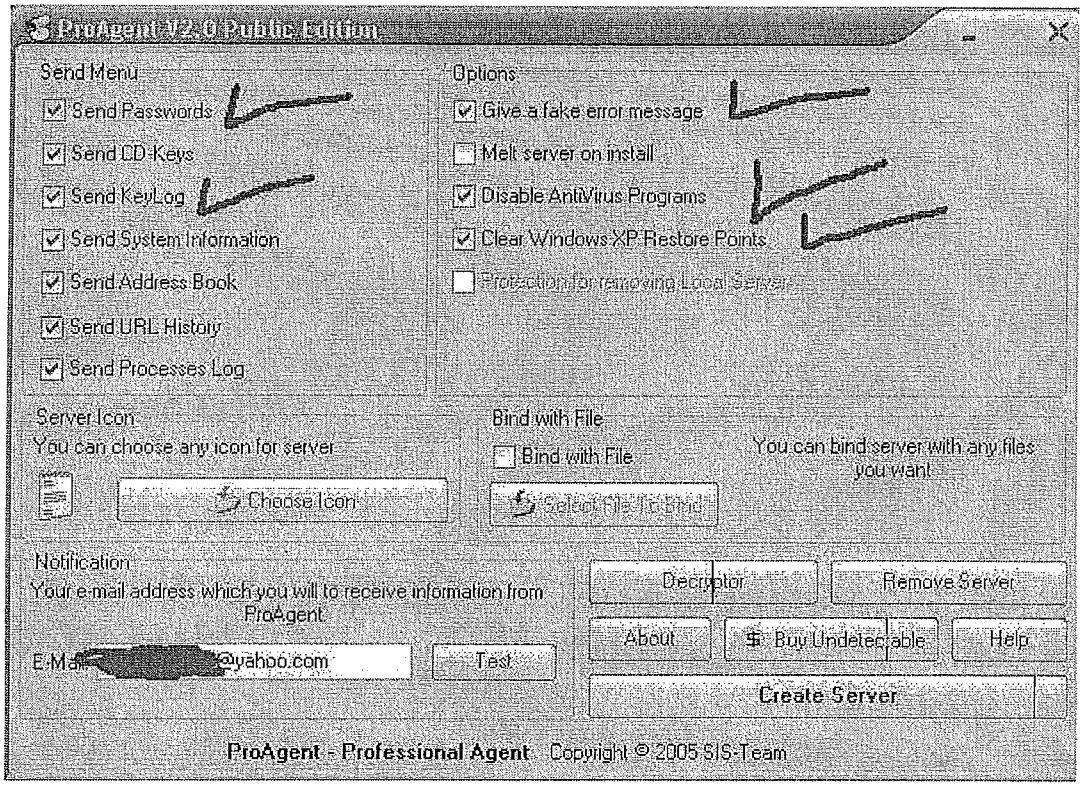
---Yazılım Keylogger : Internet arama motorları kullanılarak Keylogger yazılımına ulaşılabilir veya internette pek çok keylogger forumu bulunmaktadır.

1) Kötü niyetli kişiler tarafından yazılan ve işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın kısmen veya tamamen yönetici haklarını saldırgana teslim eden truva atı (trojan) adlı yazılımlar aracılığıyla keylogger yazılımları sisteme yüklenirler.

2) Keylogger yazılımı bilgisayara kullanıcı tarafından yüklenebilir

Örneğin; güvenilmeyen bir bilgisayarda bilgisayar sahibi tarafından sisteme başkaları tarafından giriş yapılması halinde (login olunması) ne gibi işlemler yapıldığı bilgisayar sahibi tarafından bilinmek istenebilir. Bu durumda sisteme yüklenecek bir keylogger yazılımı ile bilgisayarda başka kullanıcıların yaptıkları bütün işlemler kaydedilmiş olur. Eğer bilgisayar pek çok kişiye açık bir ağda ise bilgisayarda yapılan bütün işlemler keyloggerı yükleyen kişi tarafından öğrenilebilir.

Ayrıca işletim sistemlerinde tespit edilen açıklarla sisteme rahatlıkla uzaktan müdahale edilebilmekte ve bu müdahalelerin başında sisteme dosya aktarma, aktarılan dosyayı çalıştırma gibi işlemlerle sonrasında kullanıcılar takip edilebilmektedir. Bu tür açıklar, yamalarla kapanmış olmakla birlikte sistemlerini güncellemeyen kullanıcılar halen büyük bir tehlike altında bulunmaktadırlar.



Şekil 1: Bir keylogger olan Proagent programının arayüzü,[112]

2.1.3.Keylogger Önleyici Ölçüler [113]:Pratik olarak keylogger bilgisayara yüklendikten sonra izlenmesi imkansızdır. Fakat birkaç önleyici ölçü mevcuttur.

a-Kullanıcı özelliği güvenlik nedeniyle sınırlandırılmış Windows işletim sistemini kullanmak gerekmektedir.

b-Bilgisayar yöneticisi kuvvetli ve özelliği zor tespit edilen şifrelerle bilgisayarı donatmalıdır.

c-Bilgisayar yöneticisi şifresiyle internete bağlanılmadığı sürece keylogger sızması oldukça zor olmaktadır.

---

[112] www.zabforum.com/showthread.php?t=290

[113] Kishore Subramanyam, Charles E. Frank, Donald H. Galli , **Keyloggers: The Overlooked Threat to Computer Security,** s.4

d-Donanım keyloggerlarına karşı ise biligisayar klavye bağlantı noktaları ve klavyenin içi bir uzman tarafından incelenmelidir.

2.2. Phishing(Olta)

- **Tanımı**

İnternet suçları arasında en yaygın ve tehlikeli olanlarından biridir. Bu saldırıların amacı bireylerin veya kurumların finansal işlem yapmak için kullanılan bilgilerini ele geçirmektir.

Dolandırıcılığı gerçekleştirecek kişi/kişiler; bir banka, kart şirketi veya finansal işlemler gerçekleştiren bir finans şirketinden geliyormuş gibi hazırladığı sahte e-postayı, elde edebildiği tüm e-posta adreslerine gönderir. E-postanın konusu; müşterilerin bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacı içeren ifadelerden ve ilgili kurumların sayfalarının birebir kopyası şeklinde görünen internet sayfalarına giden linklerden oluşmaktadır.

Bazı müşteriler, tehlikenin farkında olmadan, istenilen bilgileri doldurarak e-postalara cevap verirler. Bunun sonucunda, müşterinin kişisel bilgileri ve şifreleri dolandırıcılar tarafından çalınmış olur.

Phishing metodu ile yapılan online dolandırıcılıkta :

- Kredi, debit/atm kart numaraları/CVV2
- Şifreler ve parolalar
- Hesap numaraları
- İnternet Bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri, bilgileri ele geçirilebilmektedir.

Yapılan araştırmalarda phishing saldırısına maruz kalan kullanıcıların %19'u e-mail aracılığı ile gelen bağlantılara giriş yapmakta , bunların ise %3'ü finansal

ve şahsi bilgilerini bu bağlantılara veri girişi yaparak yollamışlardır.[114] Ancak yinede bireysel phishing saldırıları için başarılı oranları belirleyici bir çalışma mevcut değildir.

Bir çok phishing , eşsesli saldırıları veya alan aldatmacalarını kullanır.[115]

Phishing saldırıları teknik ve sosyal korunmasızlıklardan faydalanır. Saldırıların birçok çeşidi mevcuttur. Ancak önemli olan saldırılara karşı mutlaka tedbir vardır.[116]

Phishing saldırılarında;saldırıların gücünü arttırmak için kullanılan sosyal temasların fikri "I LOVE YOU" virüsü gibi adresleri e-postayla gönderme temeli üzerine kuruludur.[117]

Yapılan bir çalışmada 400 öğrenciden %80 i hayali bir albaydan gelen gömülü bir bağlantıyı kabul ederek aldanmışlardır.[118]

- **Çalışması**

Phishing ile dolandırıcılar internet kullanıcılarını Fake (sahte) e-posta yöntemi ile ağlarına düşürmeyi denemektedirler ve kullanıcıların bilgilerini almaktadırlar.

E-posta yöntemini kullanan dolandırıcılar burada da kullanıcıları bir çok şekilde aldatma yoluna gidiyorlar. Genel anlamda;

---

[114] Gartner Inc. Gartner study finds significant increase in e-mail phishing attacks.http://www.gartner.com/5 about/press releases/asset 71087 11.jsp, April 2004.

[115] E. Gabrilovich And A.Gontmakher, **The Homograph Attack**,(Communications of the ACM, 45(2):128, February 2002)

[116] Aaron Emigh. Online identity theft: **Phishing technology, chokepoints and counter- measures**. ITTC Report on Online Identity Theft Technology and Countermeaures; (http://www.anti-phishing.org/Phishing-dhs-report.pdf, October 2005)

[117] http://securityresponse.symantec.com/avcenter/venc/data/vbs.loveletter.a.html, (May 2001).

[118] Aaron J. Ferguson. **Fostering e-mail security awareness: The West Point carronade. Educause Quarterly**, (28(1), 2005.)

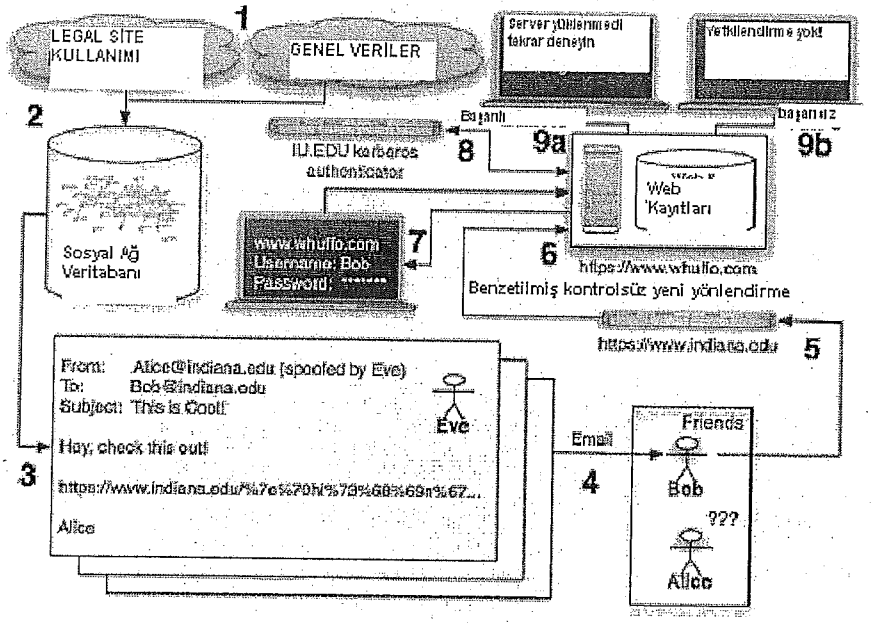
a) E-postalara devamlı temas halinde olunan kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir posta gönderilir. Bu e-postalarda kullanıcıya kurumun web sitesine giderek şifresinin süresinin dolduğu söylenir ve altta o sayfaya yönlendirileceği bir link(bağlantı yolu) verilir. Korsan daha önceden hazırladığı ve kuruluşun sitenin aynısı olan bu siteye kurbanına getirdikten sonra, ondan şifreyi girmesini ister, sonra da kullanıcı kendi şifresini yeni şifresiyle değiştirir (normal de değiştirmez. Esasen eski şifre hala geçerli olduğu için korsan bu şifre ile internet aracılığı ile para transferi, e-ticaret vb. işler yapabilir)

b) Bazı e-postalarda ise; örneğin bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara ödül olarak BMW marka bir araç kazandıkları ancak gerekli kişisel bilgileri vermeleri gerektiği söylenir. Bu gibi durumlarda bilgilerini veren kullanıcının tüm bilgileri dolandırıcının yani korsanın eline geçmektedir.

c) Bir başka kullanılan teknikte ise; gelen e-posta da müşteriye kişisel bilgilerini güncellemesi gerektiği tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verebilmeleri için gerekli olduğu söylenir.

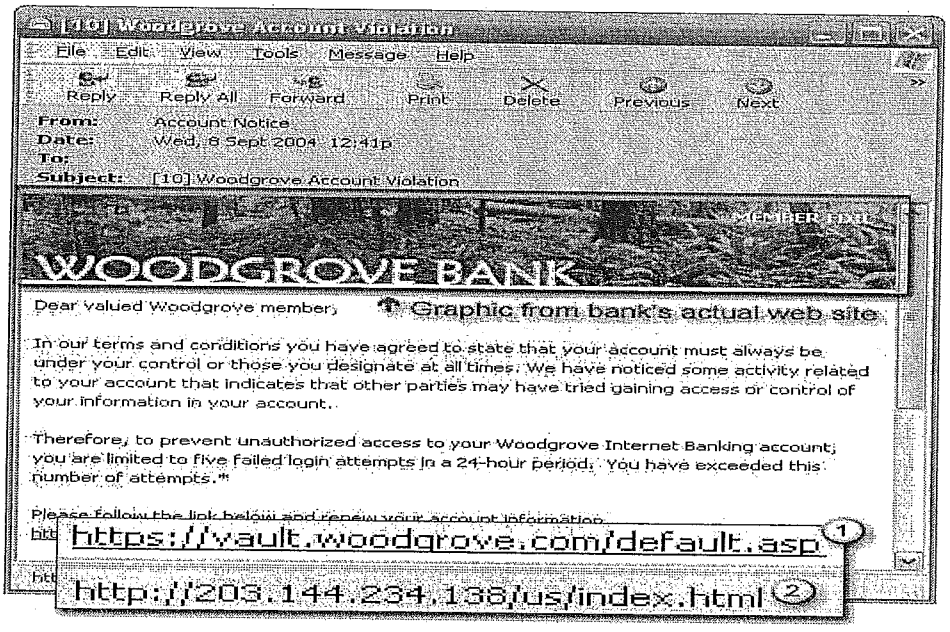
d) Son zamanlarda bazı bankaların başlatmış oldukları ve cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi linki (bağlantı yolu) verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istendiği belirtilmektedir.[119]

[119] http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=38&Itemid=28



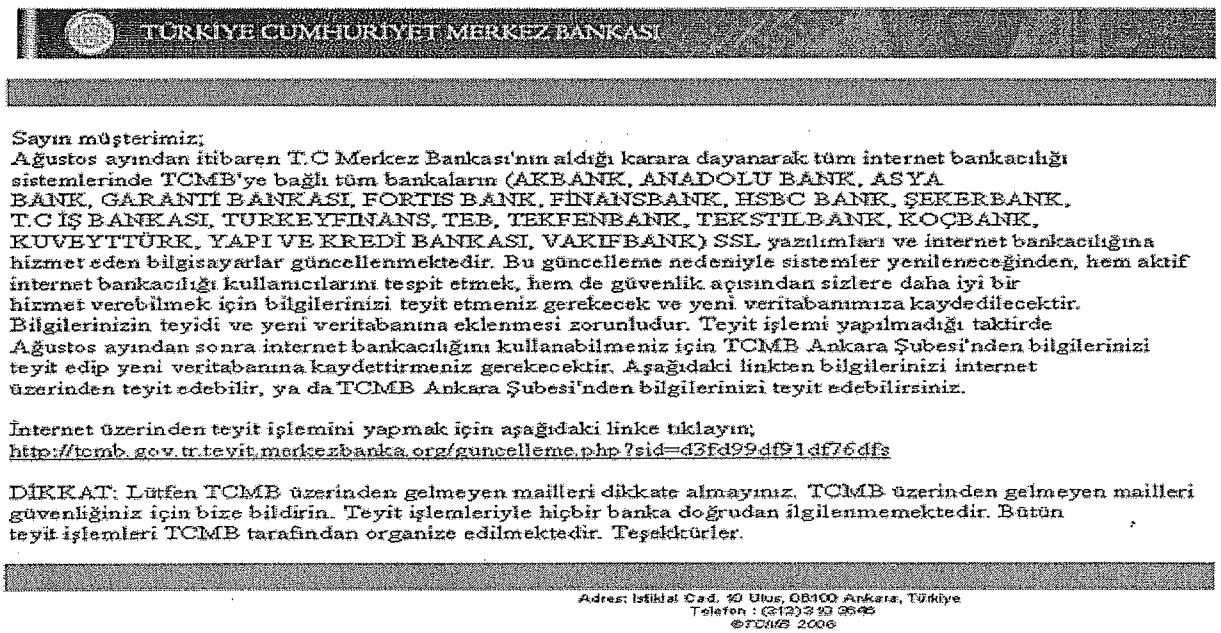
Şekil 2: Phishing işleyiş şeması

- **Örnekler**



Şekil 3: Sızdırma dolandırıcılığı amaçlı e-posta iletisinin nasıl görünebileceğini gösteren örnek

Sızdırma amaçlı e-posta iletisinin daha da meşru görünmesi için, dolandırıcılar bu iletiye yasal bir Web sitesineymiş (1) gibi görünen, ama gerçekte sahtekar bir dolandırıcılık sitesine (2) ya da resmi sitenin birebir aynısı gibi görünen bir açılır pencereye götüren bir bağlantı ekleyebilir. Bu düzmece siteler, "sahte" Web sitesi olarak da bilinir. Bu sahte sitelerden birine gidildiğinde farkına varılmadan kişisel bilgiler dolandırıcılara gönderilir. Bu durumda, kişisel bilgiler kullanılarak alışveriş yapılabilir, yeni kredi kartı için başvurulabilir veya kimlik bilgileri ele geçirilebilir.[120]



TÜRKİYE CUMHURİYET MERKEZ BANKASI

Sayın müşterimiz;
Ağustos ayından itibaren T.C Merkez Bankası'nın aldığı karara dayanarak tüm internet bankacılığı sistemlerinde TCMB'ye bağlı tüm bankaların (AKBANK, ANADOLU BANK, ASYA BANK, GARANTİ BANKASI, FORTIS BANK, FİNANSBANK, HSBC BANK, ŞEKERBANK, T.C İŞ BANKASI, TURKEYFINANS, TEB, TEKFENBANK, TEKSTILBANK, KOÇBANK, KUVEYTTÜRK, YAPI VE KREDİ BANKASI, VAKIFBANK) SSL yazılımları ve internet bankacılığına hizmet eden bilgisayarlar güncellenmektedir. Bu güncelleme nedeniyle sistemler yenileneceğinden, hem aktif internet bankacılığı kullanıcılarını tespit etmek, hem de güvenlik açısından sizlere daha iyi bir hizmet verebilmek için bilgilerinizi teyit etmeniz gerekecek ve yeni veritabanımıza kaydedilecektir. Bilgilerinizin teyidi ve yeni veritabanına eklenmesi zorunludur. Teyit işlemi yapılmadığı taktirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilir, ya da TCMB Ankara Şubesi'nden bilgilerinizi teyit edebilirsiniz.

İnternet üzerinden teyit işlemini yapmak için aşağıdaki linke tıklayın;
http://tcmb.gov.tr.teyit.merkezbanka.org/guncelleme.php?sid=d3fd99df91df76dfs

DİKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB üzerinden gelmeyen mailleri güvenliğiniz için bize bildirin. Teyit işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Bütün teyit işlemleri TCMB tarafından organize edilmektedir. Teşekkürler.

Adres: İstiklal Cad. 10 Ulus, 06100 Ankara, Türkiye
Telefon : (312) 3 9 9646
©TCMB 2006

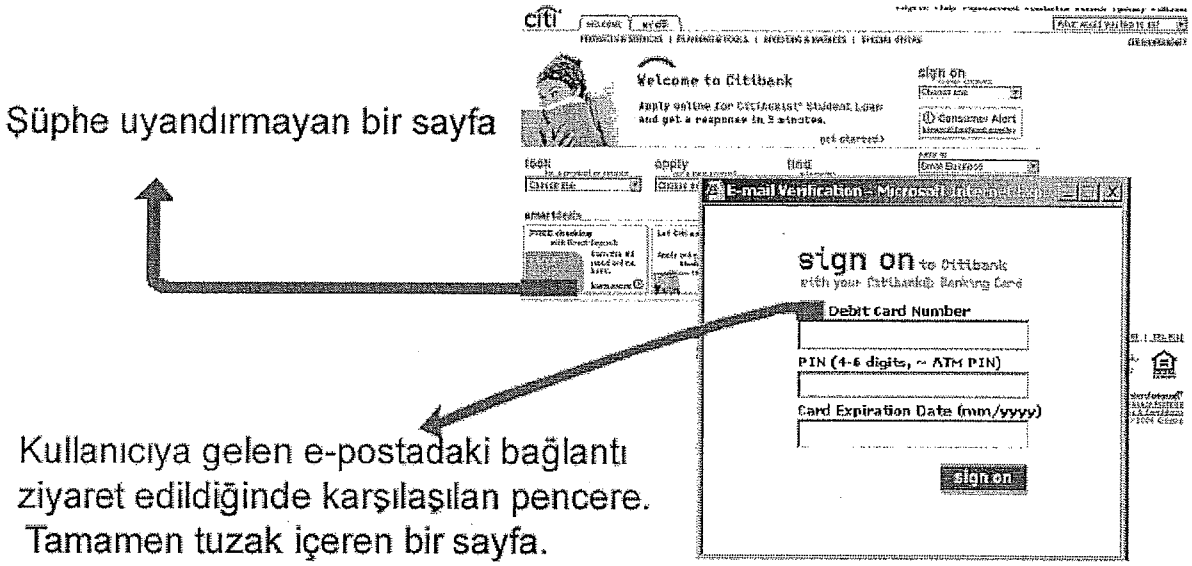
Şekil 4 :Türkiye Cumhuriyeti Merkez Bankası logolu e-posta ile PHISHING (OLTA) Dolandırıcılığı

İnternet kullanıcılarının e-posta adreslerine gönderilen ve Merkez Bankası logosu kullanılarak hazırlanan sahte e-posta'da "mevduat bankaları nezdinde bulunan müşteri hesaplarının TCMB nezdinde teyit işlemlerinin yapılması" istenmekte ve MB ile hiçbir ilgisi olmayan bir internet adresine yönlendirme yapılmaktadır.

Yönlendirilen sitede"TCMB'nin teyit işlemleri için aşağıdaki formdan hizmet aldığını bankayı seçin ve karşınıza gelecek olan formdan bilgilerinizi yeniden

[120] http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=114&Itemid=34

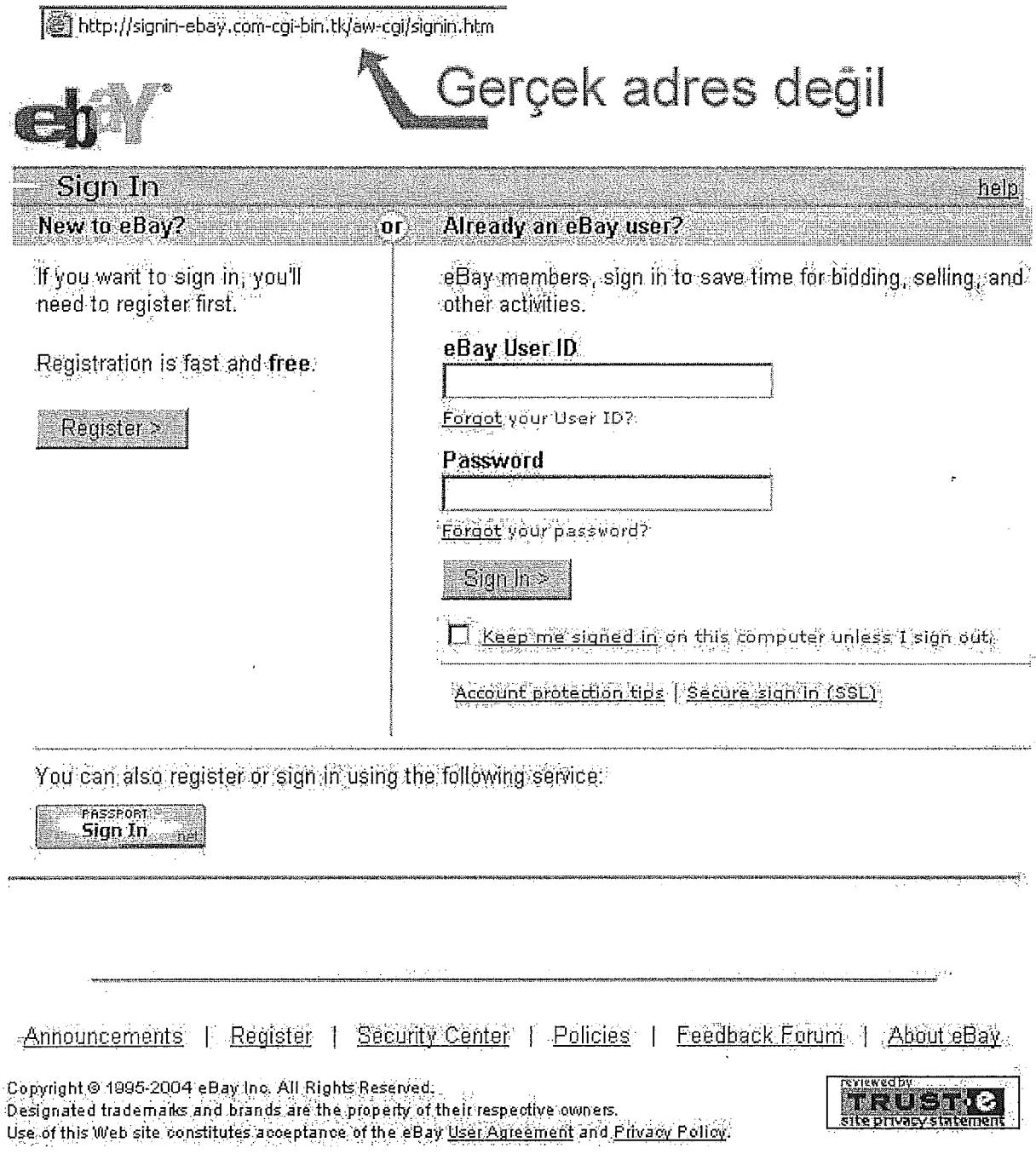
girerek teyit edin. Böylece bilgileriniz yeni veritabanımıza aktarılacaktır."sahte uyarısı ile hesap sahiplerinin hesap ve kimlik bilgileri istenmektedir. Bu şekilde hesap bilgilerini ele geçirebilecek olan dolandırıcılar hesap üzerinde para hareketleri yapabilmektedirler.



Şekil 5: Bir bankaya ait düzenlenen tuzak web sayfası.

Açılan penceredeki bilgileri dolduran kullanıcı, özel bilgilerinin başka şahısların eline geçeceğinden habersizdir.[121]

[121] http://ileriseviye.org/arasayfa.php?inode=phishing.html



Şekil 6: Alışveriş sitesiyle ilgili örnek:

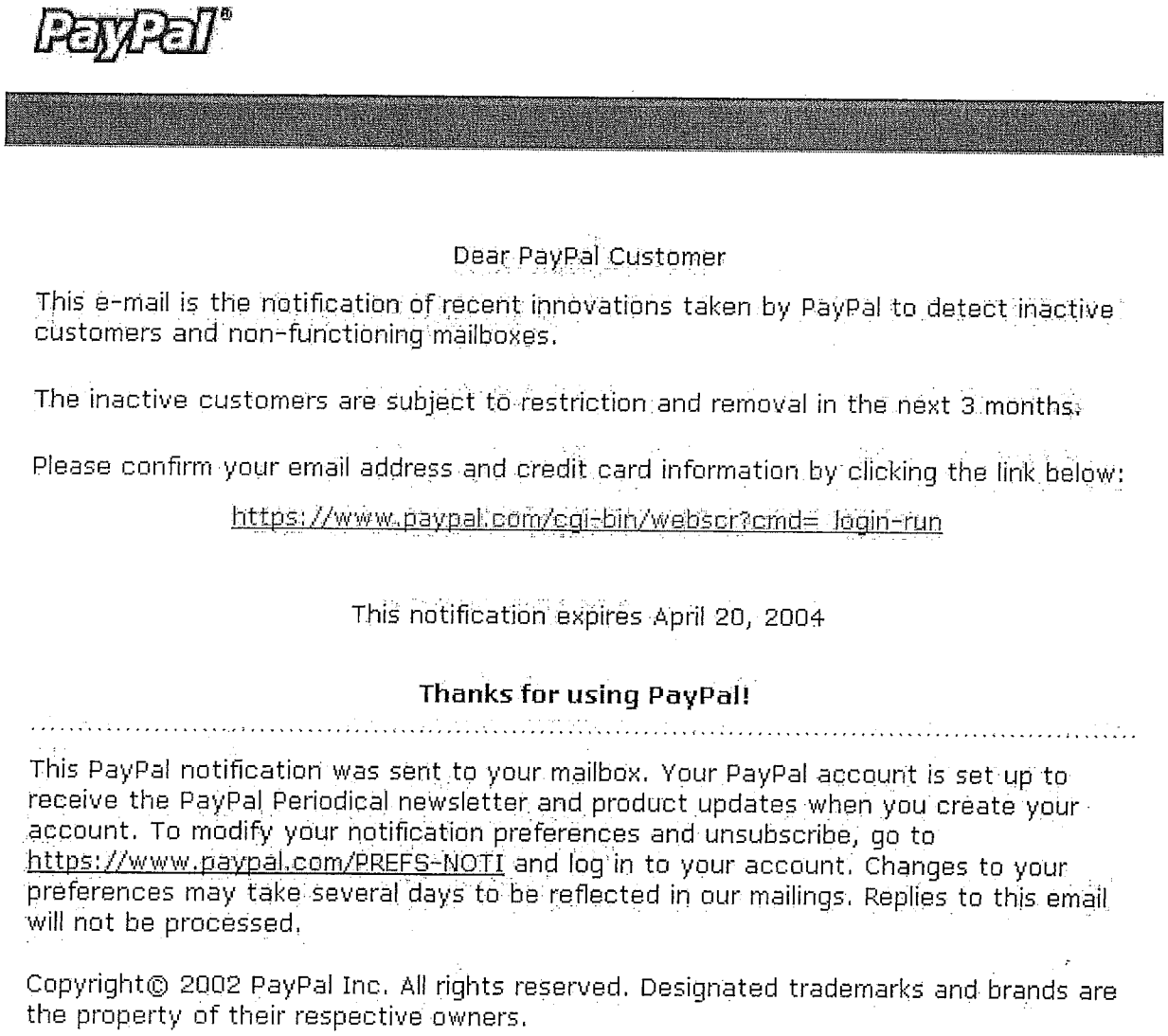
Kullanıcı yönlendirildiği adrese dikkat ederse gerçek alışveriş sitesi adresi olmadığı görülür. Fakat ilk görünüşte olağan dışı bir durum sezinlenmez. Alışveriş sitesiyle birebir aynısı olan bu sahte site görünüş olarak kullanıcıda şüphe uyandırmaz.

Gönderici olarak görülen e-posta adresi : services@paypal.com

E-Posta başlığı : Please, update your Paypal account

Hedef kitle : Paypal kullanıcıları

Ele geçirilmek istenen bilgiler: Kullanıcıların Paypal bilgileri(Kullanıcı adı ve şifresi)



PayPal®

Dear PayPal Customer

This e-mail is the notification of recent innovations taken by PayPal to detect inactive customers and non-functioning mailboxes.

The inactive customers are subject to restriction and removal in the next 3 months.

Please confirm your email address and credit card information by clicking the link below:

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

This notification expires April 20, 2004

Thanks for using PayPal!

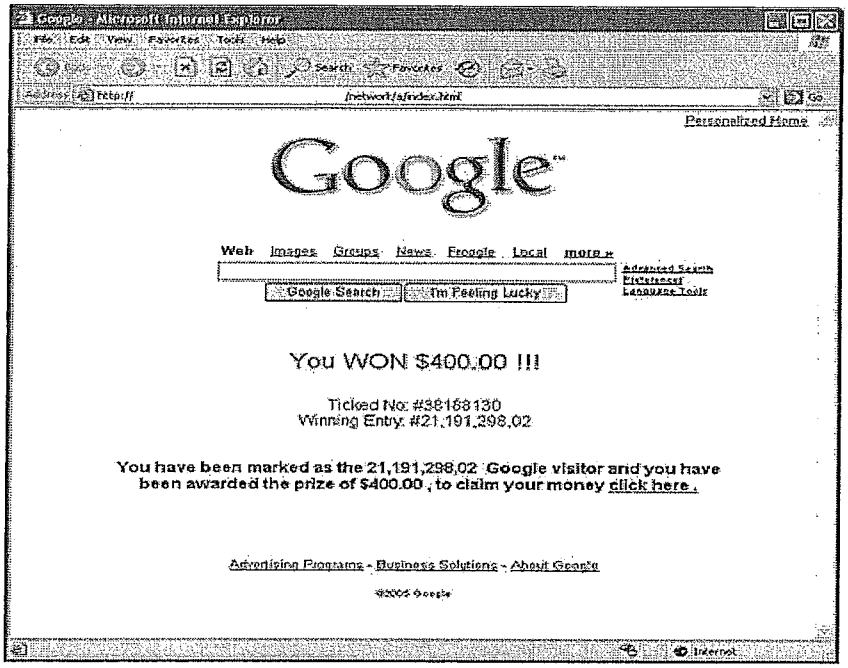
This PayPal notification was sent to your mailbox. Your PayPal account is set up to receive the PayPal Periodical newsletter and product updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account. Changes to your preferences may take several days to be reflected in our mailings. Replies to this email will not be processed.

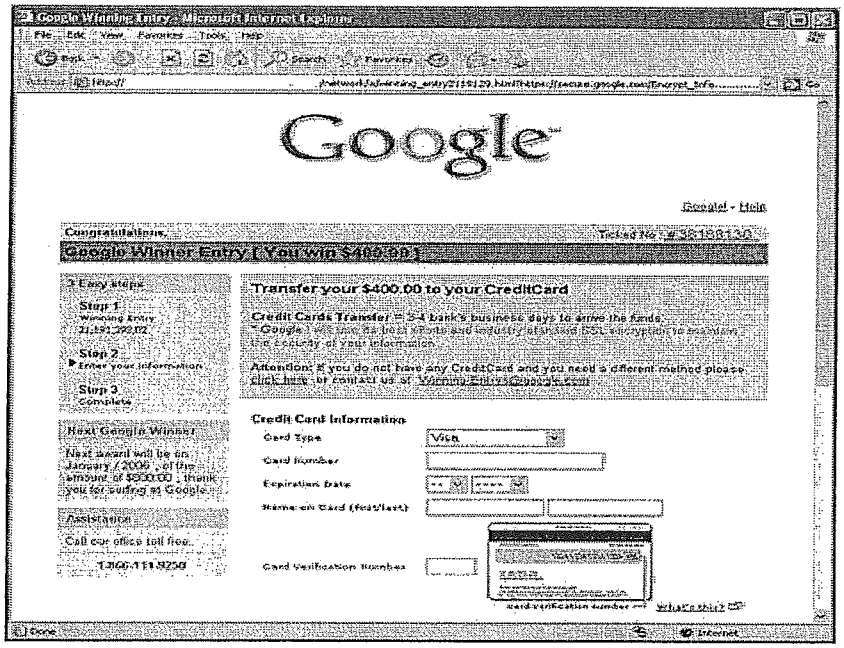
Copyright© 2002 PayPal Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

Şekil 7: Kullanıcıya gönderilen phishing içerikli e-postadan kesit

Paypal (Web üzerinden kredi kartı kullanımı sağlayan bir sistem) üyesi bir internet kullanıcısı bu tür bir e-posta ile karşılaştığında bu e-postadaki yönergeyi

gerçekleştirmeme olasılığını düşünmek gerekir. Mesajda belirtilen bağlantıya gidildiğinde aşağıdaki sayfaya da belirtilen adrese yönlendirilir. Adrese dikkat edildiğinde bu adresin gerçek paypal adresi olmadığı görülmektedir





Şekil 8: Sahte Google(Internet Arama Motoru) Sayfası

Sahte google ana sayfası ziyaretçinin $400 ödül kazandığını söylemekte ve ödülü almak için bir link içermektedir. Parayı alabilmeleri için "kazananların" kredi kartı ve adres bilgilerini girmeleri istenir.[122]

2.3. Casus Yazılımlar Ve Trojanlar

2.3.1.Casus Yazılımlar

- Tanımı

Casus Yazılımlar bilgisayara girdikten sonra bilgisayarda farklı etkiler ile casusluk yapan veya rahatsız eden yazılımlardır.

Bu rahatsızlık yöntemlerden en popülerleri;

-Bilgisayardaki verileri, gezilen siteleri belli bir merkeze gönderme

[122] http://www.olympos.org/article/articleview/1518/1/9/sahte_google_sayfalarina_dikkat(2007)

-Reklam gösterme, İnternet'ten reklam indirme

- Çalışması

I. İstatistik : İstatistik konusu hafife alınmaması gereken bir konudur. Çünkü bu bahsettiğimiz programlar 1000 veya 5000 kişi tarafından değil, milyonlarca kişi tarafından kullanılmaktadır. Dolayısıyla bu bilgiler ciddi bir getiri kaynağıdır. Örnek olarak en çok girilen siteler firmaya hem istatistiksel açıdan bir satış bilgisi verdiği gibi hem de kendi işini pazarlama açısından firmaya da ciddi bir veri sağlar.

II. Reklam : İstatistik' te de belirtildiği gibi kişi sayısının hafife alınmaması gerekmektedir. Bu sebepten dolayı bu tip programların kullanıcılarına gösterdikleri ve tıklattıkları reklamdan ne kadar getiri kazanacağı tahmin edilebilir. Casus yazılımlar genellikle kanunidir o yüzden karşıdaki firmanın çok büyük olması pek bir anlam ifade etmez.

Bir de bu noktada şunu ifade etmek lazım, programcılar için bazı casus yazılım firmaları reklam tabanlı sistemler hazırlamışlardır. Bu sayede programı yazan kişi getiri elde etmek için bunlara üye olur ve programına bu sistemi dahil eder. Bu durumun sonucunda da casus yazılım hızla büyümektedir.

Yüklenen oyunlarda, yükleme programlarında, yardımcı araçlarda ve daha bir çok şeyde ayrıntı gibi gelir ve sisteme yerleşirler. Kısaca bulaşma yöntemleri programlardır. Yüklediğiniz programlar ile birlikte gelirler.

Bu programlar

1. Kişisel Bilgileri Ele Geçirir.
2. İnternet'i Yavaşlatır .
3. Dışarıya veri gönderir ve İnternet'ten reklam yükler .
4. Bilgisayarda açık oluşturma imkanı vardır .
5. Arka planda çalıştıklarından dolayı Bilgisayarı Yavaşlatır .
6. Yüksek Telefon Faturalarına sebep olabilir .

Aslında bu tip uygulamalar arayıcı (dialer) olarak bilinir ancak casus yazılım kavramına dahildir. Bu tip uygulamalar modem aracılığı ile başka bir bilgisayara bağlanır ve normal telefon faturası üzerinden ücret ödemenize sebep olur. Genelde pornografik yayın yapan sitelerde bulunur.

Bilinen ve bilgisayarda çoğunlukla olan bazı kullanımı yaygın casus yazılımlar;

1. Gator 2. Kazaa 3. Imesh 4. Alexa 5. Google Toolbar (Ayarları doğru düzenlenmediği takdirde girdiğiniz siteleri merkezine gönderir) 6. Cute FTP 7. Getright [123]

2.3.2.Trojanlar

- Tanımı

Trojan (Truva Atı) kısaca ;bir bilgisayarın,başka bir bilgisayara girmesinde ,onu ele geçirmesinde kullanılan bir proğramdır.

Trojan (Truva Atı) denilen bu program türünü bilmek çok önemlidir.Çünkü bu programlar virüslerden daha tehlikelidirler. Bir virüsün yapabileceği en kötü şey bilgisayara format atmaktır. Ancak size trojan bulaştırmış bir kişi, şifreleri,kişisel dosyaları hatta kredi kartı numaralarını bile alma ihtimali vardır.

Trojanların ilk çıkışı sanıldığı gibi kötü niyetli olmamıştır. 90 lı yılların başlarında, şirketler de çalışan bazı kişiler, akşama kadar işlerini bitiremedikleri için evde de bilgisayar başında çalışmaları gerekmiştir. Ancak tüm muhasebe kayıtları, şirket bilgileri şirketlerdeki bilgisayarlarda kaldığından dolayı o bilgilere devamlı ulaşmak istemişlerdir.Yani her gün işte ki bilgisayarını eve taşıması yerine , evdeki bilgisayarından iş yerindeki bilgisayarına bağlanıp işlerini evden de devam etmek istemiştir. Bundan dolayı iş deki bilgisayarını açık bırakıp trojanın

[123] http://bilisim.istanbul.edu.tr/makaleler/casusyazilim.htm(2007)

serverini çalıştırıp, eve gidince de client ini çalıştırıp bağlanmışlardır. Fakat sonraları, bu bilgisayarlara kaçak olarak başka kişilerin girmesiyle trojanlar bu günkü hallerini almışlardır. Geçmişte basit yapıda olan trojanlar,günümüzde bilgisayarlarda ki hızlı gelişmeye paralel olarak gelişmiş ve bir çok kişi tarafından kullanılır hale gelmiştir.

- Çalışması

Bir bilgisayara trojanın bulaşması için server dosyasının çalıştırılması zorunludur. Ancak bu server dosyası salt bir server.exe olmayabilir. İsmi değiştirilebilir. En çok kullanılan bir yöntemde serveri başka bir dosya ile birleştirmektir. Geçmiş yıllardaki basit trojanlarla bu yapılamamıştır fakat günümüzdeki trojanların bir çoğuyla bu yapılabilmektedir. Birleştirilen dosyanın resim dosyası(jpg,gif,bmp),video dosyası(mpeg,avi) veya program dosyası(exe) olması da hiç önemli değildir,tüm uzantılı dosyalarla serveri birleştirilebilir, ancak hangi dosya ile birleştirilirse birleştirilsin, birleştirilmiş bir serverın uzantısı exe olması zorunludur. Yani bir trojanın gif,avi,jpg vb. formatlarda olması imkansızdır. Bir jpg ile birleştirilmiş bir serveri girilmek istenen bilgisayar çalıştırırsa, o sadece resmi görecektir ama arka planda trojanda çoktan bulaşmış olacaktır. Trojan bulaşırken iki işlem gerçekleştirir.

1.işlem ; Windows un her açılışında otomatik olarak çalışacak şekilde trojan kendini açılışa koyacaktır. Bir dosyanın Windows un her açıldığında otomatik olarak çalışması için win.ini,system.ini,autoexec.bat,config.sys veya regedit dosyalarından birinin belirli yerine, kendini her açılışta çalışacak şekilde kayıt ettirmesi gereklidir.Trojan da bunu yapar ve bu dosyalardan birine kendini kayıt ettirir. Böylece Windows her açıldığında trojan otomatik olarak arka planda çalışacaktır. Trojanın bu özelliği sayesinde, karşı bilgisayara bir kere değilde, o PC her online olduğunda bağlanılabilir.

2.işlem ; Trojanın bulaşırken gerçekleştirdiği 2. işlemse kurban bilgisayarın bir portunu açmaktır. İnternete girmek için kullanılan Modemlerin 65536 tane portu vardır, bunlar sanaldır, yani modemin içinde sadece tek bir çıkış ve tek bir giriş vardır ancak internetteyken yapılan işlemleri karıştırmamak için bu portlar

kullanılır, çünkü internete girildiğinde aynı anda hem explorer kullanılır,sohbete bağlanılır,hemde mp3 indirilebilir, bu işlemlerin karışmaması içinde modem gelen-giden verilerin yerini karıştırmamak için bu portları kullanır, mesela explorer 80. portu kullanır,Sohbet 1029,FTP(Dosya transferi) 21. portu kulanırlar, böylece internet trafiği karışmamış olur. Yani modemlerin sanal olarak 65536 tane portu vardır. Trojan kullanarak karşı bilgisayara girerken bir porttan girilmesi gereklidir. Bu portun hangi port olacağı trojana göre değişir (örn:netbus 1234. portu kullanır,Blade runner trojanı ise 5401. portu kullanır). Şimdiki trojanların çoğunda istenilen port seçilebilmektedir.

Trojan bu iki işlemi arka planda yapar ve bu yazılan uzun işlemler saniye bile sürmez. Bu iki işlem her trojanın yaptığı işlemlerdir, bunların yanında trojanların kendilerine has bulaşınca yaptığı işlemler vardır, örneğin bazı trojanlar bulaşınca kurbanın ISS (internet bağlantı) şifrelerini trojanı kullanan şahsın e-mail adresine gönderir.

- Kullanım Amaçları

  Trojanların kullanım amaçları çok fazladır.

  Katagorilere ayırırsak:

  ---Şifreyi Ele Geçirme Amaçlı

  a.Net Account,Icq Password,e-mail şifresi.

  b.Çeşitli Dosyalar (Kurbanın dosyalarını download ve upload etme, silme, değiştirme)

  ---Eğlence Amaçlı

- Fiziksel Eğlenceler (CD-ROM, Monitor, Mouse)
- Programsal Eğlenceler (Kurbanla chat, Matrix)
- Görüntüsel Eğlenceler (Desktop Capture,)
- Casusluk
- Keylogging
- ICQ spy

Sayısı tam olarak bilinmemekle birlikte yüzlerce trojan vardır ve her geçen gün bunların sayısı artmaktadır.Sayıları arttıkça özellikleri de artmaktadır. En çok raslanan trojanlar ; BO(back Orifice), Subseven, Sokets des troie ftp , Blade runner,Netbus Trojanları'dır.Türkler tarafından yapılmış trojanlarda vardır:Truva atı, Schoolbus, Thief ve CAsus da Türkler tarafında yapılan bazı trojanlardır.[124]

2.4.Rus Senaryoları

Son günlerde karşılaşılan interaktif dolandırıcılık suçları incelendiğinde, suçların sistemli olarak işlendiği ve genellikle Rusya'dan internete bağlanan kişiler tarafından gerçekleştirildiği görülmüştür. Karşılaşılan bu suçlarda temel senaryo şöyledir:

Dolandırıcı internet üzerinden bağlantı olarak kullanacağı şahısla temasa geçer ve kendisinin Türkiye'de bulunan kişi ve/veya kuruluşlarla ticari ilişki içerisinde olduğunu bu kişilerden belirli meblağlarda para alacağını fakat Rusya'da ticari verginin yüksek olması nedeniyle %15 - %30 oranında kesinti yapıldığını söyler.

Ayrıca gerçek kişiler arasında yapılan para transferlerinde verginin çok düşük olduğunu söyleyerek internette tanıştığı ve Türkiye'de olan şahıstan kendisine yardım etmesini ister. Dolandırıcı internetten tanıştığı şâhsa kendi banka hesabını vermesini müşterisinin onun hesabına parayı aktaracağını, Türkiye'de bulunan vatandaşımızın da emeği karşılığında %5-10 parayı aldıktan sonra kalan meblağı Western-Union ile kendisine göndermesini ister.

Aslında Rusya'daki dolandırıcı, internet bankacılığı şifrelerini ele geçirdiği kişinin hesabında bulunan parayı, doğrudan Rusya'ya havale edemediği için, aracı kullanarak kendisine göndermenin yolunu bu şekilde bulmuştur.[125]

---

[124] http://www.akdenizforum.com/showthread.php/trojanlar-trojanlar-hakkinda-hersey-545.html(2007)

[125] http://www.kom.gov.tr/turkce/gundem.aspx?idd=32(2007)

Örnek Olay 1:

Rusya'dan 3 "hacker" Türkiye'de internet hesabı bulunan kişilerin adreslerine virüslü mail göndererek hesap bilgilerini elde etmiş, bu bilgileri şebeke liderleri M.M. ve C.U'ya iletip, M.M. ve C.U'nun bu bilgilerle girdikleri hesaplarda bulunan yüklü miktardaki paraları şebekenin diğer elemanları adına sahte kimlik ve belgelerle açılan hesaplara aktarmışlardır.

Şebeke, hesaplardan aktarılan paraların yüzde 10'unu komisyon olarak Rus "hacker"lara gönderip, son 2 haftada bu kişilere 33 bin dolarlık havale yapıp, böylece 2 haftada vatandaşların hesaplarından internet aracılığıyla 330 bin dolar çekmişlerdir.

Türkiye'den Rusya'ya komisyon olarak aktarılan paraların Leonid K, Vitaly V. ile Dimitriy V. adlı kişilerin hesaplarına havale yapıldığı, bu kişilerle ilgili İnterpol kanalıyla araştırma yapılmıştır.

Şebeke elemanlarının gösterdikleri yerlere yapılan aramalarda 3 bilgisayar, 3 diz üstü bilgisayar, 2 flash bellek, CD'ler, değişik kişiler adına düzenlenmiş sahte kimlikler, kredi kartları, hesap cüzdanları, 45 bin YTL, 14 bin 550 dolar, çok miktarda altın bilezik ve takılar, 350 gram esrar ve 1 ruhsatsız tabanca ele geçirilmiştir.

Bilgisayarlar ve CD'lerdeki bilgileri inceleyen uzman polisler, bugüne kadar yaklaşık bin kişinin hesabından yüz binlerce dolar para havalesi yapıldığını ve yaklaşık 1 milyon kişinin internet hesap bilgilerinin kayıtlı olduğunu belirtmişlerdir.[126]

Örnek Olay 2:

Türkiye'de yapılan bir çok internet dolandırıcılığında adı geçen ancak bir türlü yakalanamayan efsane Rus hacker Sergei Andrusyak Mali Suçlarla

[126] http://www.8sutun.com/node/27841/print(2006)

Mücadele Şube Müdürlüğü'nün düzenlediği Hortum Operasyonu'nda yakalanmıştır. Rus hackeri 4 ayda hesabına yatırılan 500 bin YTL ele vermiştir.

Bankanın para çekmek için riskli olduğunu düşünen çete üyeleri anlaştıkları mobilyacı, kuyumcu ve benzin istasyonlarına yüzde 30 komisyon veren üyeler buradan paramatiklerine yükledikleri paralarla alış veriş yapmış gibi görünerek para çekmişlerdir. 4 aylık inceleme sonucunda rus hackerın hesabına komisyon olarak 500 bin YTL yatırıldığı öğrenilmiştir.

Olayları organize eden Rus Hacker Sergei Andrusyak kullandığı özel bir programla IP numaralarını gizlemiş ve bu nedenle de tespiti mümkün olamamıştır. Ukrayna'da Fizik eğitimi alan ve Rusya'da bir şirkette bilgisayar programcılığı yapan Andrusyak'ın Türkiye'de bu yöntemle yapılan dolandırıcılıklarda sürekli adı geçmektedir.[127]

Örnek Olay 3:

Ankara'da, internetteki mesajlaşma programlarında tanıştığı kişileri dolandırdığı belirlenen, Rus uyruklu Nataşa S. isimli kadın yakalanmış hakkında adli işlem gerçekleştirilmiştir.

"Boris Nickini" takma adını kullanan Nataşa S'nin, Türkiye'de, internetteki bir mesajlaşma programında tanıştığı şahısları kullanarak, internet hesabı açık olan bazı şahısların internet şifrelerini kırdırarak, bilgileri dışında hesaplarından bu şahıslara komisyon karşılığında havale aktardığı, komisyon dışında kalan paraları ise kendi adına Rusya'ya havale ettirdiği öğrenilmiştir. Nataşa S'nin, bu şahıslardan biri adına bir bankanın Ankara Şubesi'ne havale yaptığının belirlenmesi üzerine adına yapılan havaleyi çekmek isterken görevliler tarafından yakalanmıştır.[128]

---

[127] http://www.tuncaykarakas.com/print_version.php?id=476(2007)

[128] http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=3513306&p=2(2008)

Örnek Olay 4

İnternet bankacılığı üzerinden şifreleri toplayan Rus mafyası ve hacker'ları, Türklerle işbirliği halinde banka hesaplarını boşaltmaktadırlar. Antalya'da avukat bir şahıs bu konuya maruz kalmıştır.

Şahsın hesabından yaklaşık 7000 YTL, EFT yapılıp, internet üzerinden başka bir hesaba aktarılması üzerine şahıs banka ile irtibata geçip, savcılığa başvurmuştur. Parayı başka bir hesaba aktaran şahıs ,çekemeden polise yakalanmıştır.Ancak bu konunun korkunç tarafını şahısn Rus mafyasından aldığı talimatla bu işe girdiğini itiraf etmesi oluşturmuştur. Internet bankacılığı artık bu konunun gündeme gelmesiyle beraber uluslar arası bir boyut kazanmıştır.

Rus mafyası internet dolandırıcılığında uluslararası organize bir şebekedir. Rus mafyası ve Rus hacker'ları, Türkiye'de kendilerine polisin deyimiyle 'maşalar' bulmaktadırlar. Türklerin, Rus mafyasıyla buluştuğu adres yine internetdir. Özel şifreli ve bir o kadar güvenlik mekanizması olan chat odalarında alışveriş şöyle işlemektedir:

Rus mafyası dünyanın her tarafından toplamış olduğu kart bilgilerini, şifrelerini tanesi 10 dolardan satışa çıkarır. Kredi kartlarının içinin boşaltıldığı bu sistemde, chat odasında Türklerle gerçekleştirilen pazarlıkta, binlerce kredi kartı bilgisi, tanesi 10 dolardan satın alınır. Rusların verdiği hesaba, para yatırılır ve Türk dolandırıcılar elde ettikleri bilgililerle kredi kartlarını boşaltır. Bir de internet bankacılığının yaygınlaşmasıyla, Rus mafyası internet hesaplarını bizzat kendileri takip etmektedirler. Türkiye'de belki 3 - 4 aracı kullanırlar. Hesaptan EFT yoluyla çekilen paralar, gerçek bir ismin hesabına havale edilir. O kişi paranın yüzde 5'ini alır, ve başka bir hesaba transfer eder. Transfer edilen kişi yüzde 10'unu alır, o yine başka bir hesaba transfer eder. Ruslara para, nihai olarak nakit şeklinde, sınırdan, hiçbir banka transferi olmadan elden teslim edilir. Çünkü Ruslar dolandırıcılığın kendileriyle irtibatlandırılmasını istememektedirler.[129]

[129] http://www.suc.gen.tr/modules.php?name=News&file=article&sid=289(2007)

2.5.Nijerya Mektupları

Kendisinin yurt dışında herhangi bir ülkede genellikle de Nijerya'da ikamet ettiğini beyan eden kişi, üst düzey bir bürokrat ya da siyasi olduğunu bazı sebeplerden istifasının istendiği ve banka hesaplarına el konulacağını elektronik posta yoluyla beyan eder. Bu kişi banka hesaplarında parayı üzerinde çıkartamayacağı için mağdurdan bir hesap açtırmasını, kendisine % 30 komisyon vereceğini söyler ve çok yüklü meblağlardaki paranın bu hesaba gönderileceğini belirtir. Hesabı açtıran mağdur parayı yatırabileceğini söylemesi üzerine yurt dışındaki bu dolandırıcı şahıs bankasının parayı gönderebilmesi için EFT masrafı olan tutarın mağdur tarafından önce yatırılmasını akabinde yüklü meblağdaki paranın mağdurun hesabına geçeceğini beyan ederek mağdurdan bu parayı kendisine göndermesi sağlamaktadır.[130]

Örnek Mektup

"Kimden : webemaildelivery006@....
Tarih : 29 Ağustos 2006
Konu : Sayın Bay/Bayan

Sayın Bay/Bayan

Bunu çok (kişiye) yazdım ama hiç cevap alamadım. Anlatmaya çalıştım ama aldığım cevapların çoğu şaka yapıyor olduğum şeklindeydi. Umarım size de şaka gibi gelmez Bay/Bayan. Emailinizi bir internet dergisinde gördüm şu sıralarda internet kullanımını geliştirmek üzere ofislere dağıtılan ve tüm personelin paylaştığı dergide.

Umarım kötü ingilizcemi maruz görürsünüz. İngilizcem iyi değil, zaten pek eğitimli birisi de değilim.

---

[130] http://www.eosb.org.tr/tr/duyurular.asp?id=680(2008)

Ben Bay Kola Fashonu. First Bank of Nigeria'nın Portharcourt'taki Doğu Şubesi'nde temizlikçiyim. Bankama, işime bağlı birisiyim. Bu nedenle şube müdürü bana çok güvenirdi.

Eşimin cenazesini kaldırdığımızdan dolayı bir hafta boyunca ofise gidemediğimden dolayı işlerin çok biriktiği bir Pazartesi günüydü ki şube müdürümüz beni ofisine çağırdı. Ortaya bir kutu çıkardı ve onu saklamamı istedi. Kutunun içinde para olduğunu biliyordum ama kaç para olduğunu bilmiyordum. Kutunun içinde 20 milyon 10 bin dolar olduğunu ve bu parayı banka hesaplarından çaldığını söyledi. Kutuyu geri isteyene kadar evimde saklamamı, bunun karşılığında bana paranın yüzde 10'unu vereceğini söyledi. Neden beni seçtiğini sordum. ben sadece sıradan bir temizlikçiydim; zengin olmak istiyordum. Eve dönerken bir video kamera ödünç aldım; 15 yaşındaki oğlum, paraları sayarken filmimi çekti. Parayı söz verdiğim gibi sakladım. Size bu epostayı gönderme nedenim, müdürün evine silahlı soyguncuların baskın yaptığını ve bunun sonucunda öldürüldüğünü öğrenmiş olmam. Artık parayı kullanabilmemin hiç bir yolu yoktu çünkü sıradan bir temizlikçi olarak bu kadar parayı nereden bulduğumu açıklayacak bir yalan bulamazdım. Size bu epostayı bu nedenle gönderiyorum – parayı yabancı birisine göndermek istiyorum. Bu şekilde paranın bulunması imkansız olacaktır. Sizden para ya da banka hesap bilgilerinizi istemiyorum. Tek istediğim isminizi ve adresinizi göndermeniz. Kutuyu UPS'in doğu şubesinin müdürü olan ablama vereceğim. O da kutuyu şahsen sizin ev adresinize ulaştıracak. Bu yolla paket kontrolden geçirilmeyecek çünkü ablam UPS'teki tüm kontrolörlerin başıdır. Bir ev veya ofis adresine ihtiyacım var çünkü ablam kimseyle otel, restaurant, park, havaalanı gibi yerlerde buluşmaz, para değiş tokuşu yapmaz. Onunla ancak bir ev veya ofiste buluşabilirsiniz. Eğer sizin için uygun değilse, size yanıt vermeyeceğim çünkü parayı kaybetmek istemem. Harcamalar bu şekilde halledilecek, sizin ödemeniz gereken bir şey olmayacak. Parayı aldığınızda lütfen bana bilgi verin, kutudan temin ettiğim biraz para ile alacağım biletlerle oğlumla Nijerya'dan sizin ülkenize geleceğiz. Ben geldiğimde paranın yüzde 30'u sizin olacak, yüzde 70'ini bana verirsiniz.

Lütfen bundan kimseye bahsetmeyin, avukatınıza bile. Ancak bu şekilde bu işi yapabiliriz. Ben de sadece ablama söyledim çünkü kutuyu taşımada bize yardım etmesi gerekiyor.

Sizden cesaretlendirici bir cevap almayı umuyorum.

Size bu mesajı gönderdiğim eposta adresi bir arkadaşıma ait olduğundan lütfen cevabınızı (kolafashonu0@...) email adresime gönderin. Aksi durumda bir arkadaşın epostasından yazışmaya başlamak uygun olmaz.

İyi günler

Kola Fashonu"

2.6.Sql İnjections Attacks

İnternet üzerinden veri paylaşımı arttıkça veri güvenliğinin sağlanması önemli bir olgu haline gelmiştir. Bilişim sistemlerini çökertmek, yavaşlatmak üzerine yapılan saldırılarla birlikte değerli olan bilgilerin çalınmasına yönelik saldırılar daha tehlikeli hale gelmiştir. Değerli olan bilgilere günümüzde örnek olarak kredi kartı bilgileri ve banka hesapları verilebilir.[131]

SQL (*Structured Query Language*) veritabanlarında data çekme, silme ve değiştirme gibi işlemler için kullanılan basit yapılı bir dildir. Bugün hemen hemen tüm web uygulamalarının altyapısında veritabanı desteği vardır ve bu web uygulamaları veritabanı ile SQL aracılığıyla anlaşırlar.

Bir siteye mesaj bırakıldığında bu mesaj veritabanına kaydedilir. O mesaj onaylandığında veritabanındaki bir alan güncellenmiş olur. Yönetici veritabanındaki kaydı silerek o mesajın siteden silinmesini sağlar.[132]

---

[131] Ed.Gavın, **Protecting Your "Crown Jewels": New Approaches to Securing Critical Data**, Erişim: [http://www.bitpipe.com/detail/RES/1129646348_201.html] (2005)

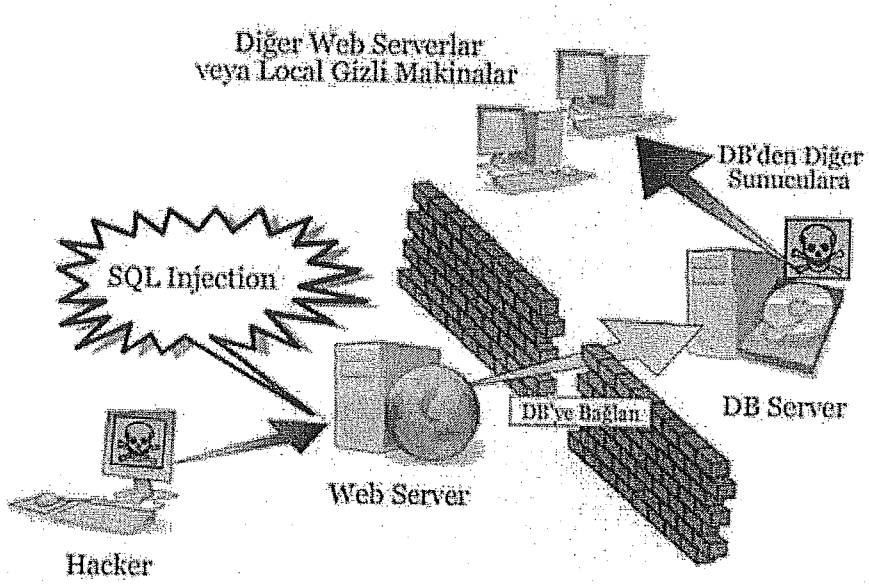
[132] http://ferruh.mavituna.com/makale/sql-injection-a-giris-ve-sql-injection-nedir/(2006)

SQL Injection kelime manasıyla da anlaşılabileceği gibi SQL sorgularının arasına dışarıdan zararlı veri ekleme işlemine verilen isimdir. Dinamik web uygulamalarında bir veritabanı ve o veritabanı üzerinde çalışan SQL sorguları vardır. Bu sorgular masum amaçlı bir veya birden fazla tablodan veriler çekerek etkileşimi sağlamayı amaçlamaktadır. Ama dışarıdaki kullanıcının uygulamaya gelen girdilere zararlı veri karıştırması sonucu masum sorgular korkunç bir faciaya sebep olurlar.

Web uygulamaları genelde kullanıcıyla etkileşime geçerek dinamik bir arayüz sunarlar. Bu sırada kullanıcıdan bir takım girdiler (Formdan, URL Sorgularından, çerezlerden vs.) alırlar ve bunu uygulama içinde işleme sokarlar ve belli bir çıktı verirler. Bu sırada uygulamada bir takım veritabanına erişecek kodlar, veritabanı üzerinde bir takım sorgular çalışırlar ve belli bir veri elde ederler. Sonra da bu veriyi düzenleyip kullanıcıya gönderirler. İşte SQL Injection bu işlemler sırasında devreye girer. Çünkü veritabanı üzerinde bir takım sorgular çalıştırılmak istenmiştir. Böylece zararlı sorgularımız veritabanı üzerinde çalıştırılmış olur.

SQL Injection'ın uygulamaya verebileceği zarar sadece sorgu çalıştırmaktan ibaret değildir. Sistem, veritabanı ve uygulama yetkilerine göre sistemi tamamen devre dışı bırakabileceği gibi aynı ağdaki internete açık olmayan kurumsal makinelerdeki bilgileri erişimden, o ağ kaynaklarını kullanarak başka yerlere saldırı yapmaya kadar uzanabilen bir yolu açmış demektir.[133]

[133] http://www.forumklas.org/archives.php/Sql-injection-Anlatimi-/5154 (2007)



Şekil 9: "SQL Injection Attacks " işleyişi

Dış saldırlara karşı çeşitli güvenlik duvarı (firewall), antivirus ve antispyware gibi çeşitli programlar, SSL (secure socket layer) benzeri şifreleme yöntemleri ve kullanıcı hakların kısıtlanması gibi yaptırımlar mevcuttur.[134] Veri tabanından bilgi çalınmasına karşı yapılabilecek hazır yazılım tarzında çok fazla ürün bulunmaktadır. Tasarımlarına bağlı olarak güvenlik duvarları genelde iç bilgisayarlara her türlü hakkı verirken, SSL tarzında uygulamalar verinin şifrelenmesi ve başka kişiler tarafından okunmasını engellenmesi amacına yönelik olduğundan veri tabanlarına karşı yapılan saldırılara yaptırımları çok fazla değildir.

Veri sorgulamasına ve girişine izin verilen her hangi bir kullanıcı sistemin içinde kabul edilir. Veritabanı uygulamalarında veritabanı genelde sunucu bilgisayar (server) üzerinde bulunmakta ve istemci bilgisayarlardan (client) veri girişi veya sorgulaması yapılmaktadır.

İnternete servis vermek üzere sunucu tabanlı uygulamalardan ASP (Advanced Server Page) ve PhP (Hypertext Preprocessor) en fazla bilinenleridir.

---

[134] R. C.Burgess, M. P. Small, **Computer Security In The Workplace**, (North Charleston, North Carolina: SEO Pres-2005)s.3

ASP ve PhP tabanlı web programları, derlenmiş kendi başına çalışabilen (executable binary) dosya yaratmadan web üzerinde kullanım sağlarlar. ASP ve PHP sunucu tabanlı uygulamalarla beraber çalışan SQL (Structured Query Language) veri tabanları veri girişini ve sorgulamasını kolaylaştırır. SQL veri tabanlarına MySQL, PostgreSQL, MS SQL ve Oracle örnek gösterilebilir. Microsoft Internet Explorer veya Netscape gibi herhangi bir tarayıcı (browser) aracılığıyla bu veri tabanlarına veri girilebilir veya veri tabanlarından veri sorgulanabilir.[135]

Veri girişinin ve sorgusunun hızlandırılması amacıyla sunucu tabanlı bilgisayarlarda PHP ve ASP gibi kolay hayata geçirilen uygulamalar bazı temel kurallara dikkat edilmezse veri tabanına karşı saldırılara açık vermektedir.

Sunucu temelli SQL veri tabanları ile beraber kullanılan PhP ve ASP uygulamaları programcılık hatalarından (bug) başka güvenlik sorunları vardır.[136] ASP ve PhP temelli uygulamalarda veri tabanlarındaki değerli bilgilere izinsiz ulaşmaya olanak veren tasarım boşlukları bulunabilmektedir. Veri girişi ve sorgulaması için geliştirilen uygulamanın bir an evvel uygulamaya konulma isteği güvenlik açıklarını ortaya çıkarmaktadır. Veri tabanlarında ihtiyaç duyulan güvenliğinin sağlanması, kullanılacak uygulamanın tamamlanma süresini uzatmaktadır. Tasarım aşamasında uygulamada yapılan güvenlik açıklıkları, uygulamanın kullanılması sırasında sorunlara yok açabilmektedir. Veri tabanlarındaki açıklar kredi katı bilgileri gibi değerli bilgilerin veya adli sicil gibi kişisel bilgilerin çalınmasına neden olmaktadır.

2.7.Order Log(Alışveriş Kayıtları) Ele Geçirme

İnternet üzerinde bulunan bir çok online alış veriş sitesi kredi kartı ile online para transferi yapmak suretiyle müşterilerine hizmet vermektedir. Bu hizmetleri sırasında ister istemez müşterilerine ait bazı bilgileride veritabanlarında tutmakta,

---

[135] M.Achour, F.Betz, A.Dovgal, G.Hojtsy, **PhP Manual**, (Erişim [http://www.php.net/manual/en/]-2005)

[136] S.Castano, Mg.Fugını, **Database Security**, (Milan, Addison-Wesley & ACM Pres-1995)

bunları online olarak kaydetmektedirler. Bu bilgiler arasında müşterinin satın aldığı ürün, teslimat adresi, müşterinin telefonu, e-posta adresi, ürünü aldığı tarih ve bazı sitelerin veritabanlarında ise müşterinin kredi kartı numarası ile kartın son kullanma tarihi tutulmaktadır. Normal şartlar altında müşterinin sadece kredi kartı numarasının ve kredi kartının son kullanma tarihinin internet alış veriş sitesinin veritabanında tutulmasında her hangibir sakınca olmamakla birlikte bazı durumlarda suç soruşurmaları içinde oldukça işe yaramaktadır.

Örneğin internet üzerinden cep telefonuna kontör yüklenebilmesi durumunda hangi telefon numarasına hangi kart ile ödeme yapılarak kontör yüklendiği bilgisi bazı durumlarda başkasının kart bilgisini kullanarak kontör yükleyen suçluları kolayca ele verebilmektedir ancak ülkemizde bu işlemi sadece bir GSM servsi sağlayıcısı yapmaktadır. Yada sahte alış veriş yapan şahsın sitenin veritabanındaki kart bilgisi ile adresinin karşılaştırılması sonucu teslimat adresinden yola çıkarak suçlular yakalanabilmektedir. Aşağıda örnek olarak internet üzerindeki bir online alış veriş sitesinin veritabanından ufak bir parça yer almaktadır. Buna bilişim dilinde Order Log (Alış veriş kaydı) denmektedir.

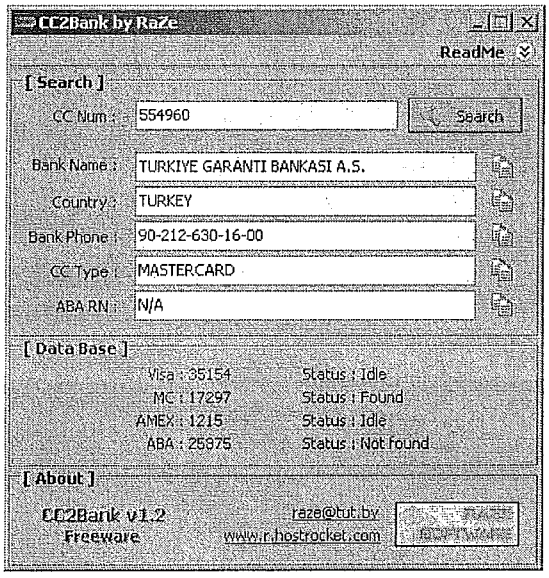
```
Bill-Address1 = 521 Blackhawk Club Drive
Bill-City = Danville
Bill-Country = US United States
Bill-Email = a94506@yahoo.com
Bill-Firstname = Michael
Bill-Lastname = Deffina
Bill-Phone = 925-736-8433
Bill-State = CA
Bill-Zip = 94506
Card-Expiry = 3/2006
Card-Number = 4337369000000914
CardAuth-Amount = 9.94
Date = Mon Dec 29 04:55:46 2003 GMT
Item-Code-1 = HF-ADNOK7210
Item-Count = 1
Item-Description-1 = Hands-free Audio Adaptor 7250i
Item-Id-1 = adaptor7210
Item-Quantity-1 = 1
Item-Taxable-1 = YES
```

Şekil 10: Alışveriş Kayıt Örneği

Burada da görüldüğü gibi alış veriş yapan kişiye ait bir çok bilgi online alış veriş sitesinin veritabanında yer almaktadır. İşte bu aşamada uzman bilgisayar

korsanları yani hacker'lar devreye girmekte ve suçun işlenmesi için kredi kartı bilgilerini temin etmek üzere online alış veriş sitelerinin güvenlik önlemlerini kırarak bu sitelerin order log'larının (alışveriş kayıtları) tutulduğu veritabanlarını ele geçirmektedirler. Yukarıda da belirtildiği gibi aslında bu veri tabanlarında tutulan bilgiler tek başına hiç bir işe yaramamaktadır. Özellikle sadece kredi kartının numarası ve son kullanma tarihi hiç bir işe yaramamaktadır. Gerek online alışveriş gerekse bankaların algoritmasına göre boş pvc manyetik kartlarına yazmak için gerekli olan kredi kartının arkasında bulunan Cvv2 güvenlik kodu bu veri tabanı kayıtlarında bulunmadığı için suçlular bu aşamadan itibaren başka bir yöntem ile gerekli bilgileri kart sahibinden almaya çalışmaktadırlar.

Bu aşamada suçlular, veritabanındaki kayıtlardan yola çıkarak online alışveriş sitesinden alış veriş yapan kişilerin bir çok bilgisini elde ettikleri için (özellikle şahsın mail adresi), hedef olarak bu kişileri seçmekte ve elde ettikleri 16 haneli kredi kartı numarasın ilk 6 hanesinden (BIN ID) şahsın sahip olduğu kredi kartının bankasını öğrenmektedirler. Kartın hangi bankaya ait olduğunu öğrenmek için örnekteki gibi programlar kullanmaktadırlar.



Şekil 11: Kredi Kartı Banka Doğrulama Programı

Suçlular böyle programlar vasıtası ile hedef şahısların kartlarının ait olduğu bankayı öğrendikten sonra elde ettikleri veritabanı kayıtlarına göre kart sahibinin

mail adresine sanki bankaymış gibi e-posta (spam mail) atmakta ve yapılan alış verişin teyyidi için güvenlik amacıyla gönderilmiş bir teyyid maili hissi uyandırmaktadırlar. Bu mail ile şahıslardan mail ekindeki forma veya verilen internet adresindeki siteye girip buradaki forma kart bilgilerini tekrar girmesi ve alışverişi onaylaması istenmektedir. Mali alan kurban kişiler mailde kart bilgilerinin ve yaptıkları alışverişin detayını gördükleri için şüphelenmemekte ve formu doldurma işlemini gerçekleştirmektedirler. Ancak bu tarz mailler vasıtası ile fazladan şahsın kredi kartının Cvv2 güvenlik kodu ve ATM cihazlarında kullanılabilecek pin kodu da istenmektedir. Kurban kişiler formu doldurduktan sonra suçlular için tamamlanmış bilgiler artık hazır demektir. Bu aşamadan sonra suçlular ellerindeki bilgileri bankaların algoritmalarına göre boş pvc kartlara yazarak kullanabilmektedirler. Bu bilgiler ile gerek boş pvc kartlara yazma işlemi gerçekleştirerek para çekebilmekte gerek sonradan nakite çevirebilecek alışverişler gerçekleştirebilmekte gerekse de online alışveriş yapabilmektedirler.

2.8.Sosyal Mühendislik

Temel amacı; sistemlere izinsiz girmek yada dolandırma yolu ile bağlantı kurmak, izinsiz ağa (network) girmek, endistüriyel casusluk, kimlik hırsızlığı, sistem yada ağın (network) bozulmasına yol açmaktır.

Sosyal mühendislik iki ana kategoride tarif edilebilir; hem insan kaynaklı, hem de bilgisayar kaynaklı saldırı metodudur. Sosyal mühendislik kişileri aldatarak değerli bilgi ve parolalarını ellerinden almayı amaçlamaktadır. Bu amaçla örneğin e- posta (e-mail) atarak şifre elde etmeye çalışırlar, "shoulder surfing" sörf metodu ile basitçe kişisel bilgileri toplanan kişiye uygun parola tahminleri yapılır. Bu noktada sosyal mühendislerin çalışma etodolojisini anlayabilmek için bir örnek çalışmaya bakmak gerekir:

Klasik bir saldırı metodolojisi: görev - bilgi erişimi: Eldeki bilgilerle bir şey yapın diye söylense, elbette temel olarak dijital yada yazılı materyalin kopya tarihi değerli olacaktır. Rakipler açısından şirket adına ne kadar çok bilgi toplanabilirse o kadar çok şirketin durumuna yönelik şirket hedefleri, planları, hareketleri,

stratejileri hakkında değerlendirme yapılabilir. Rakip ile ilgili alınabilecek birkaç bilgi aşağıda belirtilmiştir.

Pazar ve yeni ürün planları Kaynak kodları Şirket stratejileri Üretim, teknolojik çalışmalar Olağan ticaret metotları Ürün tasarımı, araştırma ve maliyetler Anlaşmalar ve akit tedbirleri; teslim, fiyatlandırma, bilimsel terimler. Şirket internet sitesi Müşteri ve destekleyici bilgileri Birleşme ve elde etme planları Mali bütçeler, gelirler, vergiler. Pazar, reklam giderleri. Kaynakların fiyatları, stratejiler, listeler. Sorumlular, operasyonlar, organizasyon şeması, isim/aylık cetvelleri.

Ayrıca tescilli bir şirket çalışması için sıcak hedefe yönelik, personel kayıtları olabilir. Aşağıdaki bilgilerden herhangi biri de değerli olabilir. Ev adresleri Ev telefon numarası Karı koca ve çocuk adları Sosyal Güvenlik numarası Hasta kayıtları Kredi kartı kayıtları Performans değerlendirmeleri Tüm bu veriler toplanarak elde bulunan veya internetten kolaylıkla bulunabilecek yardımcı program veya metotlar ile hedefe kolaylıkla varılabilecektir.[137]

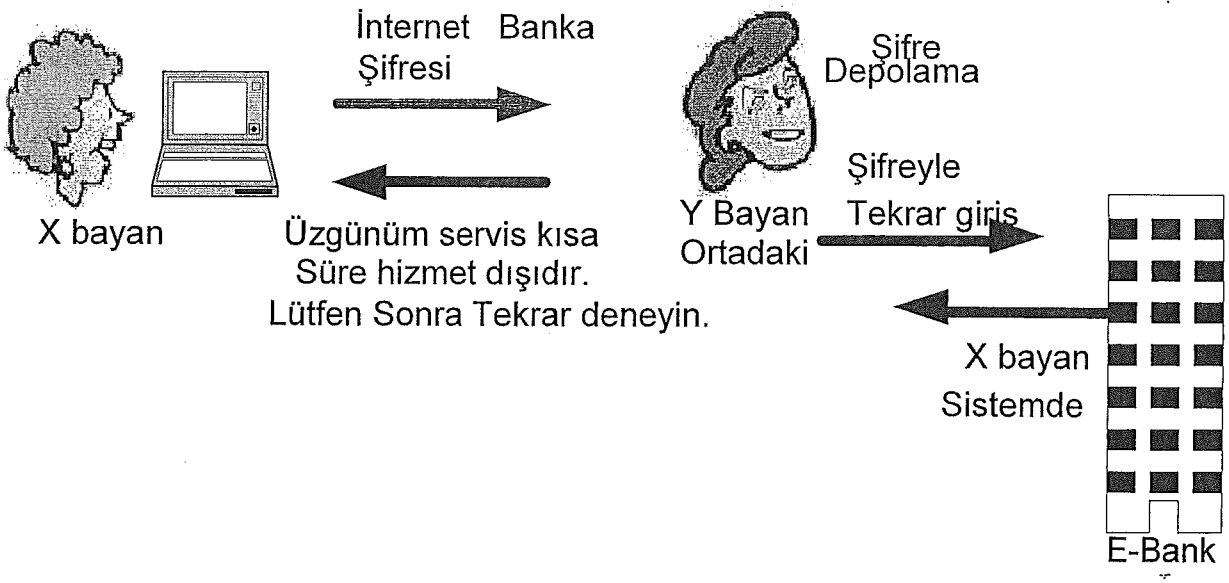
2.9.Ortadaki Adam Saldırısı (Man-İn-The-İn-Middle Attack)

Bu atak türü yapılan bağlantıların arasına girip iki tarafa da sanki karşıdaki kişi gibi davranmakla yada bir tarafı devre dışı bırakarak yapılır. Bu sayede mesela kendi şifresiyle şirketine evinden girmiş birinin bağlantısında araya girerek şirkete sanki o kişiymiş gibi davranarak şirket bilgilerine ulaşmak mümkündür. Şifreli bilgi transferi yapılmaması bu tür olaylara sebebiyet verebilir.[138]

---

[137] http://www.bilgiportal.com/v1/idx/50/717/Hukuk/makale/Internette-Biliim-Sularnda-Kullanlan-Metotlar-.html(2007)

[138] http://www.haylazturk.com/mail-yardim/37167-phishingden-sonra-simdi-de-vhishing-moda.html(2007)



Şekil 12: Ortadaki Adam Saldırısı

Bu kategorideki birçok saldırı ARP(Adres çözme protokolü) zehirlemesine veya önbellek zehirlenmesine dayanmaktadır. Temel olarak, ARP aldatması, IP ve Ethernet protokollerinin kesintiye uğratılması metodudur. Bundan dolayı bu kısım ARP protokolleri veya ARP saldırıları ile alakalı değildir.

Saldırgan, hedef ağdaki AP ile aynı tipteki bir özel sanal ağ sunucusunu birleştirir. Kullanıcı gerçek sunucuya ulaşmak istediğinde, aldatılmış olan sunucu cevap verir, böylece kullanıcı sahte sunucuya bağlanır.Bu tipteki saldırılar bu yazıda anlatılamayacak kadar karmaşıktır.[139]

2.10.Dns Saldırısı(Pharming)

İnternet tarayıcısında bir adres yazıp gönderdiğimizde, arka planda ilk çalışan makineler olan DNS (isim sunucuları) bu yazılan adresin neresi olduğunu, ve buna karşılık gelen makinelerin nerede olduğunu bulur.

Basit bir benzetme ile DNS'leri telefon defterleri olarak görebiliriz. Bu denli önemli olan DNS'lerin çalışmamasının, ya da DNS zehirlenmesi olarak

[139] http://www.sabote.com/archives.php/kablosuz-aglarda-saldiri-ve-guvenlik/6857(2007)

adlandırılan, DNS'lerin yanlış adrese yönlendirmesinin, internet ile alakalı her türlü işlemi ne denli kaotik bir hale sokacağı tahmin edilebilir. [140]

Değişken DNS sayesinde kullanıcılar, aslında ulaşmak istedikleri siteler için yazım hatalarından dolayı yanlış adres girmiş olsalar bile tekrar yönlendirilmektedirler.

Değişken DNS, İngiltere'de Barclays Banks şirketine karşı kullanılmıştır. Bu olayda e-postada kullanılan bazı ek karakterler kullanıcıyı sonunda e-posta dolandırıcılarının sitesine ulaştırmıştır.

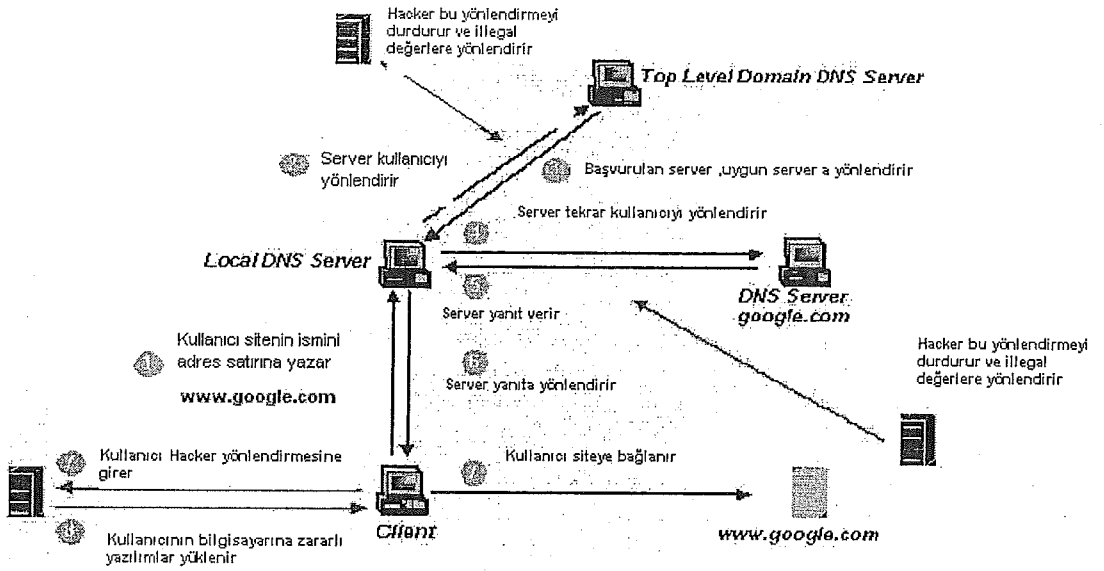
DNS sisteminin kendisine, DNSsec gibi güvenlik arttırıcı geliştirmeler yapılması planlanmaktadır. DNSsec, DNS Güvenlik Uzantıları anlamına gelmektedir. Bu şekilde DNS verilerine doğruluk ve yetki sorgulamaları yapılabileceği öngörülmektedir.

Yapılan çoğu dolandırıcılık saldırısı kişisel bilgisayar seviyesinde DNS zehirlemesi yapılarak gerçekleştirilmektedir. (Örn: yerel sunucu dosyalarına eklemeler yapılıyor) DNS sunucularını onarmak bunu önleyememektedir. Fakat çift taraflı yetkilendirmenin büyük yardımı olabilecektir.[141]

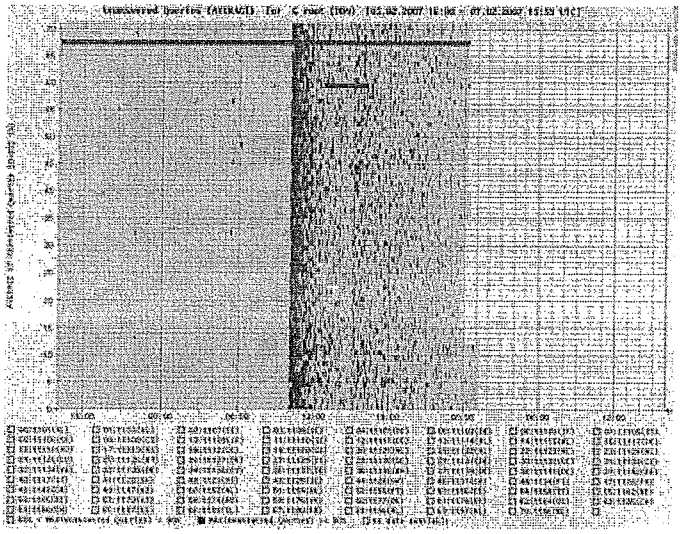
---

[140] http://teknokeyif.wordpress.com/2007/02/08/dns-saldirisi/(2008)

[141] http://www.geyikmerkezi.com/coskunoglundan-ulastirma-bakanina-tt-sorularifo-bilisim_haberi_son_haberler4932.html(2007)



Şekil 13: Dns Saldırısı(Pharming) Çalışma Sistemi



Şekil 14: Dns Saldırısı(Pharming) Saldırı Örneği

Yukarıdaki grafikteki sarı bölgeler, zaman eksenindeki aralık için cevapsız kalınan sürenin %60'ın üzerinde olduğu, kırmızılar ise bu sürenin %90'ın üzerinde olduğunu göstermektedir. Bu grafik G tipi sunucular için olup, dünyadaki en fazla

koruma altına olan sınıftır ve yaklaşık 2 saatlik bir sürede çoğunlukla %90'lık bölgeden, %60 a düşebilmiş, ve 12 saat içinde de tamamen normal hale dönebilmiştir

2.11.Yeniden Yükleyici Yöntemi(Re-Shıppers)

Yeniden yükleme dolandırıcılığı,zayıf legal sistemlerle küçük işletme veya bireyler aracılığıyla ülkelere hile ile eşya taşımayı içerir.Eşyalar genellikle çalıntı veya aldatmaca içeren kredi kartlarıyla temin edilir.[142]

- Nijerya Versiyonu

Dolandırıcılar chat veya çöpçatan siteleriyle özellikle batı ülkelerindeki yalnız bayanları hedef alan insan ordusundan oluşur.Dolandırıcılar ,yalnız bayanlara onların bulunduğu ülkelere gelerek evlenme sözü verirler.

Suçlu gelecekteki eşinden , yanına gelmeden önce çeşitli özürlerle alacak olduğu bazı eşyalar için izin ister. Kadın kabul ettiği zaman suçlu eşyaları satın almak için çeşitli internet sitelerinden eşzamanlı şekilde kredi kartını kullanır.

Bir çok defasında teslimat adresi olarak kendi adresini kullanır ancak fatura adresi muhtemel eşinin adresidir.Paketler suçluya ulaştığında , batılı yalnız bayana gelmemek için çeşitli mazeretler söylemeye başlar. Bayan para harcamadığı için,yanlışlıları ve hileyi göremez ve paketlerin teslim edildiğine dair şirketlerden yazılar adresine ulaşır.

Ertesi gün bütün paketler suçlunun gerçek adresine yani Nijerya'ya gönderilir.Ve suçlu artık muhtemel eşiyle işi bittiği için tamamen iletişimini keser.Bayan ödemeyi kabul ettiği varsayılan alışveriş şirketinden muazzam bir

---

[142] http://en.wikipedia.org/wiki/Internet_fraud(2008)

fatura alır.İstemeyerekte olsa bayan artık suça iştirak eden yeniden yükleyici konumuna gelmiş olmaktadır.

- Doğu Avrupa Versiyonu

Sınıflandırılmış reklamcılık ile insanları toplamayı hedefleyen dolandırıcılık türüdür.Suçlular kendilerini ABD de varlığını sürdürmeye çalışan ve büyüyen bir Avrupa şirketi olarak takdim ederler ve insanlardan bu anlamda pay verme vaadiyle para toplarlar ve daha birçok şekilde mağdur ederler.Genellikle e-mail adreslerine gelen reklam mailleri iletişim aracı olarak kullanılır.Dolandırıcılar masum kurbana ABD'den mal temin edeceklerini,bunun için Avrupa'ya ulaşması için bir yeniden yükleyiciye ihtiyaç duyduklarını açıklar ve bu yeniden yükleyicinin kendisi olmasını teklif ederler.Yine Nijerya metodunda olduğu gibi eşyalar dolandırıcılara faturada mağdurun evine gider.Bazen suçlular yeniden yükleyicinin hizmetleri karşılığında sahte çekler gönderirler. Mağdur çeklerin zaman içinde sahte olduğunu anlar, kutular suçlulara ulaşmıştır ve suçlu-mağdur iletişimi kesilmiştir.

- Çin Versiyonu

Suçlular, büyüyen Çinli bir şirket denemesi olarak ABD veya Avrupa'da bir varlığı korumaya çalıştığını anlatan yine reklam mailleriyle hedef kitleye ulaşmaya çalışır.Ve aynı Doğu Avrupa versiyonunda olduğu gibi, mağdurları suçun iştirakçisi haline getirmeyi hedefler.

2.12.Brute Force ve Dictionary Attack

"Brute force attack" programlar kullanılarak olasılık ve deneme yanılma ile şifre kırma yöntemidir. Herhangi bir brute attack programı sırayla bütün olasılıkları dener. Dictionary Attack ise bir dosya içerisine yazılmış şifrelerin bir program yardımıyla denenmesidir. Örneğin 4 haneli bir şifreyi denerken aaaa,aaab,aaac sırasıyla denemeye başlar, bu yöntemler iyi sonuç vermesine rağmen oldukça zaman isterler.

Brute Force ve Dictionary Attack gibi şifre deneme saldırıları bazen çok ciddi süreçler boyunca sürebilir ve saldırganın bu saldırılar sonucunda istediğini ele geçirme ihtimali yüksektir.

Brute Force Attack ile işlemcinin gücüne bağlı olarak saniyede 2 milyon şifre denenebilir.[143]

Dictionary Attack'te ise saldırganın kullanıcı veritabanını ele geçirdiğinde şifreleri elde edebilmek için yapacağı ilk iş belli olasılıkları deneyerek şifreleri bulmaya çalışmaktır. Örneğin olması muhtemel şifreleri karıştırıp şifreler üretir.

Sözlükteki kelimeler sayılarla değişik kombinasyonlarla denenip karıştırılmış halleri kullanıcı veritabanıyla karşılaştırılabilir. Günümüz teknolojisiyle kolay şifreleri (kullanıcıların genelin yaptığı basit anlamlı kelimelerden oluşan şifreler) bu yöntemle çözmek düşünüldüğü kadar uzun zaman almayabilir. Uzun şifreler yada karışık şifreler için bu geçerli değildir ama bütün kullanıcıları bu hassasiyet ve yeterlilikte olmadıkları gerçeği göz ardı edilmemelidir. Ayrıca birden fazla hesabın aynı şifreye sahip olması da saldırganın işin kolaylaştırır.[144]

İnteraktif banka dolandırıcılığında kullanılan şifrelerin ele geçirilmesi amacıyla bilgisayar korsanları olasılık ihtimalini de göz ardı etmezler. Kullanıcı hakkında bilinen temel özellikler(yaş, doğum tarihi,anne baba ismi vb) bu 2 yöntemle programlar vasıtasıyla kullanılır.Sonuçta üretilen şifreler banka dolandırıcılığının önünü açar.Özellikle şifre seçimindeki basitlikler bu yöntemlerin işlevini kolaylaştırır.

---

[143] http://www.indirsek.com/program.php?progID=1427/Advanced-ZIP-Password-Recovery-4.0(2007)

[144] http://www.vbmaster.org/sorular-cevaplar/424-veritabanenda-saklanan-uifrelerin-gvenliri.html(2007)

3.İNTERNET BANKACILIĞINDA MEVCUT ÖNLEMLER

3.1.Güvenlik Kalkanı

Bilgisayara bilgi dışında yüklenebilecek 'keylogger' ve benzeri programlarının, internet şubesine girerken kullanılan şifre/parolayı hafızalarında tutmasını engelleyen bir uygulamadır.

Güvenlik kalkanı ufak boyutta yazılımlardır. İnternet Şubesi'nin genelinde değil, sadece şifre ve parola giriş alanlarında aktifleşerek, gereken yerde ve gereken zamanda bilgisayarı koruyan bu yazılım, işlem hızınızı azaltmaz.[145]

3.2.(Ssl) Şifreleme Sistemi

SSL network üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla Netscape tarafından geliştirilmiş bir güvenlik protokolüdür.[146]

Ssl internet explorer ve nerscape navigator browserler ve üst versiyonlarında çalışabilir. Günümüzde, internet tarayıcılarının büyük çoğunluğu tarafından kullanılmaktadır. Ssl güvenliğinin varlığını iki şekilde anlarız. Birincisi http:// nin https:// olmasından anlıyoruz. İkincisinde ise, browserların altında çıkan kilit simgesinden anlarız. İnterner explorerda ssl varlığında sağ alt köşesinde bir kilit simgesi çıkar. Ssl olmadığı zaman ise bu kilit simgesi görünmez.

SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği ve bütünlüğü korunur.

---

[145] http://www.isbank.com.tr/sss/foSikcaSorulanSorular.asp?iKodSikcaSorulanSoru=306(2007)

[146] http://www.turkeyhack.org/ssl-security-hakkinda-her-8364-y-t1249.html?s=2b56506afc3aba1ae932525d4677e6d1&(2007)

Bankalar SSL-40 bit şifreleme yerine, artık güvenlik açısından 128 bit şifrelemeli güvenlik programını kullanmaktadırlar. Bu anahtar bilgi ne kadar uzun olursa şifrelenen bilgilerin çözülmesi de o kadar zor olur.

3.3.Sanal Klavye

Sanal Klavye, bilgisayarın klavyesindeki tuşları kullanmadan, fare kullanarak ekrandan şifre girişi yapmaya olanak sağlayan bir sistemdir.[147]

Şifreleri 'Keylogger' programlarına karşı güvenlik altına almak amacıyla kullanılmaktadır. Hemen hemen bütün internet bankalarında sanal klavye uygulaması mevcuttur.

3.4.Akıllı Anahtar

İnternet bankacılığına her giriş için farklı bir şifre üreten küçük boyutlu cihazlardır.

Akıllı Anahtarın Özellikleri:

- Akıllı Anahtar iki kademeli güvenlik sağlar.
- Ekstra güvenlikle birlikte para çıkışı ve ödeme işlemlerini yapmaya devam etmeyi sağlar.
- Akıllı Anahtar ile ek bir şifre hatırlamaya gerek yoktur.
- Akıllı Anahtar ile internet bankacılığına her girişte yeni ve tek kullanımlık şifre olur.
- Akıllı Anahtarın kullanımı kolaydır.
- Akıllı Anahtar cihazı her yere taşınabilir.
- Herhangi bir yazılım yüklemesi gerektirmez; işletim sisteminden bağımsız çalışır.
- Akıllı Anahtar bankaların ücretsiz hizmetleri arasındadır.

---

[147] http://www.bilgi-yarismasi.com/sanalklavye.html(2008)

3.5.Ip Kısıtlaması

IP adresi, internete bağlanırken servis sağlayıcınız tarafından bilgisayara özel olarak verilen numaralar bütünüdür. IP adresi a.b.c.d formatında noktalarla ayrılmış 4 bölümden oluşmaktadır. Her bir bölümdeki değerler 0 - 255 arasında değişmektedir (Örneğin 199.111.80.8 gibi).

IP sınırlaması yaparak İnternet Şubesine herhangi bir IP adresinden girilmesini engelleyerek sadece müşterinin belirlediği IP adreslerinden girilmesi sağlanmaktadır.[148]

3.6.Tarih-Saat Kısıtlama

İnternet Şubesi'ni kullanırken yalnızca müşterinin belirlediği tarih ve saat aralığında (örneğin, yalnızca hafta sonu, hafta içi 09:00-18:00 saatleri arası gibi) giriş yapılmasına olanak sağlayarak, belirlenen tarih ve saatler dışında kalan zamanda İnternet Şubesi'ne erişimin kısıtlanmasını sağlamaktadır.[149]

3.7.Sms Doğrulama

SMS ile Doğrulama", İnternet Şubesi üzerinden yapılan para transferleri, bilgi güncellemeleri ve bazı ödeme işlemlerinin gerçekleştirilmesi öncesinde müşteriden SMS yoluyla onay alma işlemidir.

3.8.SET (Secure Electronic Transaction) Şifreleme Sistemi

SET (Secure Electronic Transaction-Güvenli Elektronik İşlem) banka kartları ve ödemeler ile ilgili bilgilerin güvenliğini sağlamak amacıyla Visa,

---

[148] http://www.akbank.com/1125.aspx(2008)

[149] http://www.akbank.com/1125.aspx(2008)

Mastercard, Microsoft, Netscape, GTE, IBM, SAIC, Terisa Systems ve Verisign'ın katılımıyla oluşan bir konsorsiyum tarafından geliştirilmiştir.[150]

SET iletiminin yapılabilmesi için uygulamaya katılan tüm tarafların gerekli SET yazılımını sağlayıp sistemlerine yüklenmesi gerekmektedir. Müşteri her hangi bir bankada bir hesap açtığında bir sertifika alır ve kendisine iki anahtar sağlanır. Dijital imza sipariş için kullanılırken anahtarlardan biri şifreleme, diğeri kimlik belirleme ve ödeme bilgileri için kullanılır.[151]

Bir SET uygulamasında öncelikle banka veya kredi kartı şirketi, müşteri ve satıcı için elektronik ortamda sertifikalar üretir. Sertifikaların kopyaları her siparişte alıcı ve satıcı arasında karşılıklı olarak birbirlerine iletilir. Bu bilgiler şifreli olup ancak yetkililer tarafından okunabilmektedir. Bu aşamadan sonra internet üzerinden alışveriş yapmak isteyen kullanıcı istediği ürünü seçer ve sipariş eder, satıcı daha önce edindiği sertifikayı müşteriye iletir ve müşteri böylece satıcıyı belirler. Müşteri siparişini birinci adımda gizli anahtar ile şifreler ve daha sonra açık anahtarını kullanarak ikinci şifrelemeyi gerçekleştirir. Bu durumda satıcı sadece müşteri siparişinin şifre çözümünü yapabilir. Bu esnada siparişin parasal kısmı ve kredi kart numarası şifrelenmiş olarak aktarılır. Satıcı kendi özel anahtarını kullanarak gizli anahtarının ve daha sonra da siparişin şifresini çözer. Bu esnada satıcı siparişin kopyası ile birlikte ödeme bilgilerini bankaya iletir. Banka önce müşteriye ait bilgileri kontrol eder ve daha sonra bilgileri açar. Sonra müşterinin ödeme bilgilerini kontrol eder ve satıcıya gerekli garantiyi verir. Satıcı bunun üzerine müşterisinin siparişini yerine getirir.

SET protokolü hakkında performansının yavaş olması, kullanımının tecrübe gerektirmesi ya da kullanıcıların deneyim kazanabilmeleri için gereken yatırım miktarı açısından olumsuz yaklaşımlar söz konusudur. Ancak SET'in sağladığı yüksek güvenliğin getirdiği avantajlar bu olumsuzlukların etkisini en aza

---

[150] http://www.eticaretgaranti.com.tr(2008)

[151] http://www.adambilgisayar.com.tr/ticaret.html(2008)

indirmekte ve SET protokolü firmalar için vazgeçilmez bir standart halini almaktadır.[152]

4.İNTERNET SUÇLARINA KARŞI HUKUKİ DURUM

Bilgi teknolojisinin hızlı ilerleyişi hukuk dalında çalışma yapanları ilerleyen yıllarda nasıl etkileyecektir? Sistemimiz ve onu işletenler bu duruma uyum sağlama için neler yapabilir, sorunsalına uygun yaklaşımların geliştirilmesinin gerekliliği ortadadır.

İnternet elektronik bir dünya olarak, fiziksel dünya ile paralel gitmektedir. İnternet yapısı önceden tasarlanmış bir network (ağ) yapısından çok, hızlı ilerleyen birçok bilgisayarın dahil olduğu network (ağ) yapılarının büyük bir network (ağ) havuzunda birleşiminden oluşmaktadır. Bugün artık entegre bir yapıya sahip olan internet, bilgilerin sunulduğu, tartışıldığı, yenilerinin yaratıldığı, depolandığı, işlem gördüğü ve iletişim için kullanıldığı dünya çapında bir çevreyi oluşturmuştur.

İnternet ile bilgi, fiziksel dünyadan elektronik dünyaya doğru bir göç yaşamaktadır (Buna bilişim dünyası, Siber Dünya da denilmektedir). Bu durum ilk olarak 2. Dünya Savaşı sonrası süreçte gelişmiştir. Her ne kadar da kişisel bilgisayarlar 1970' li yıllarda kullanılmaya başladı ise de, bu geçiş çok yavaş ve birbirinden kopuk olmuştur. 1980 ve 90' lı yıllarda artık bir çok bilgi elektronik formatta yada kağıttan, elektronik ortama aktarım süreci yaşamıştır. İnternetin ilk olarak orta ölçekte iletişimde kullanımı ile, bu süreç hızlanmış ve "kağıtsız büro" kavramını ortaya çıkmıştır.

---

[152] C.DOLANBAY, **e-ticaret Strateji ve Yöntemler**, (Meteksan Sistem Yayınları Ankara, 2000) s.21

4.1.Bilgi Teknolojisi Ve Elektronik Uygulama Zorunluluğunun Etkisi

Yüzyılımızdaki üç süreç bize hukuk uygulamaların elektronik değişimi ile ilgili zorunluluğu açıklamaktadır. Bunlar; maddi yapıdan çıkarım, her yerde her zaman hazır sunum ve her düzenlemeye uygunluktur.

Çalışma alanındaki bilgilerin içeriğinin fiziksel formattan, elektronik formata dönüşümü yani bunların maddi yapıdan çıkarım sürecinde olması konusuna eğilmek gerekmektedir. Bu süreç tabi ki her yerde bankalarda, okullarda, alışveriş merkezlerinde, kütüphanelerde, mahkemelerde, devlet kurumlarında, kontrollü veya kontrolsüz olarak oluşmaktadır. Çok sağlam bürokratik yapıya giren yeni kavram eskinin yerine kesinlikle olmaz, böyle bir şey mümkün değil, sistemi engeller, gibi bir yaklaşım her zaman var olacaktır. Ayrıca yüz yüze iletişim üzerine kurulu fiziksel ortam yerine, elektronik etkileşim ile ilgili giderek daha çok artan kullanım baskısı bizim bu konudaki girişimlerimizin daha hızlı olmasını gerektirmektedir.

Her yerde her zaman hazır sunum kavramı; maddi yapıdan çıkarım , bilgi yaklaşımının bir sonucu olarak ortaya çıkan bir kavramdır. Dokümanlar ile insan ve mekanın durumları arasında bulunan fiziksel mesafe engel oluşturabilecektir. Elektronik mesafe kavramı ise, coğrafik durumunuza bakılmaksızın sanki aynı odadaymışsınız gibi, bilgi ve kurumların içine girilebilir gibi erişilebilir duruma getirmektedir. Ayrıca bilgi ve kurumlar sadece bir yerde olmaz böylelikle her yerde bulunabilirler. Ve sadece her yerde olmak ile kalınmayacak ve her yerde varlığını hissettirecektir. Her yerde her zaman hazır sunum kavramı elektronik dünyanın dikkate değer özelliklerinden biri olan aynı zamanda birçok yerde mevcut olma durumunu ifade etmektedir.[153] Nitekim bu kavram Bilişim Şurasında "e- Devlet yapısına özgü düzenlemelerin gerçekleştirilmesi" gerekliliği ortaya konarak ulusal yapıdaki vatandaşın her yerden her zaman hazır olarak kurumlara elektronik ulaşımı hedeflenmektedir.[154]

---

[153] Robin WIDDISON, , **Electronic Law Practice: An Exercise in Legal Futurology,(** Modern Law Review, N: 60,1997), s 143

[154] Türkiye Bilişim Şurası , **Türkiye Bilişim Şurası Raporu 10-12 Mayıs 2002-Ankara**, (http://www.bilisimsurasi.org.tr/home.php?golink=rapor, 18.08.2002), s.293-300

Her düzenlemeye uygunluk ; yukarıdaki iki kavramı birleştiren bir kavramdır. İlk olarak uygunluğa intibak kabiliyetini gösterir. Bilgisayarlar diğer şeylere oranla insan yapısına uyum sağlayabilen dünyadaki çok az şeyden biridir. Daktilo devamlı daktilodur, fotokopi makinesi fotokopi makinesidir, telefon bir telefondur. Bir bilgisayar, her ne kadar da yazı yazsa, fotokopi çekse, telefon, faks aleti olarak kullanılabilse de günlük olarak, dosyalama aracı olarak, grafik çizme aracı olarak, kütüphane olarak, kütüphaneci olarak ve sayılamayacak kadar çok şeyi yapabilmektedir. Böylelikle bilgi teknolojisini her nerede kullanmak istiyor isek orada kullanabiliriz. Var olan formları yenilikçi uygulamalar adına istediğimiz şekilde bilgi teknolojisi ile sınıflandırıp sunabiliriz. Elektronik formdaki bilgi her bir bireysel kullanıcı tarafından düzenlemeye, sınıflamaya, seçilmeye ve sunulmaya hazır bilgi anlamına gelmektedir.

Her düzenlemeye uygunluk, bilgi teknolojisi tabanlı çalışma araçlarının karakteristik anahtar özelliği olmamakla birlikte, sosyal alanı ilgilendiren özellikle işin nasıl, ne zaman ve nerede yapıldığı ile ilgilidir. 1970' lerde kişisel bilgisayar kullanıcılarının ilk öncüleri devletlerin ve diğer tabu haline getirilmiş değerlerin önünde bilgi teknolojisini özgür bırakmıştır. Bu bireyler arasında bilgisayarın demokratik ortamda, dünyaya yayılan gücünün artık politik bir anahtar ve sosyal bir nesne olması ile ilgilidir. Dünyadaki yapılan iş yeniden şekillenmiştir. Çalışanların iş merkezli çalışmalarından esnek ev temelli ve kişi temelli çalışmaya dönük bir yol ortaya çıkmıştır.[155] Maddi yapıdan çıkarım, her yerde her zaman hazır sunum ve her düzenlemeye uygunluk kavramları alışkanlıkları ve çalışma yapılarını derinden etkileyebilecek kavramlar olarak sistemleri zorlamaktadır. Bu etki ile yeniden yapılanan bilgi sistemi beraberinde belli sıkıntıları da meydana getirmiştir. Tabi ki bu süreçte bu bilgi ile ilgili art niyetli ve bilginin suç aracı kullanımı gibi bir durum ortaya çıkmıştır.

4.2.İnternet Hukuku

Kitle iletişim aracı olarak internet bir dizi sorunu da beraberinde getirmiştir. Bu sorunlar sadece teknik, ekonomik ve yönetsel sorunlar olmayıp, doğrudan

[155] Robin WIDDISON, **a.g.e.**, s 163

doğruya kullanıcıyla ilgili etik ve hukuki sorunlar olarak da karşımıza çıkmaktadır. Mevcut kitle iletişim hukukunun bu yeni teknoloji karşısında yetersiz kalışı, yeni düzenleme ve yaklaşımları zorunlu kılmıştır. Tüm bu düzenlemelere İnternet Hukuku başlığı altında yer vermek mümkündür.

İnternet kullanımında yaşanan hukuki sorunlar çoğunlukla ticari uzlaşmazlıkların çözümü aşamasında karşımıza çıksa da, kişilik haklarının ihlali, yasadışı örgüt ve oluşumların propagandası da son zamanlarda sıkça karşılaştığımız olaylar arasında yer almaktadır. İnternet üzerinden işlenen, kredi kartlarında dolandırıcılık, gönderilmeyen ürünler, sahte e-yatırımlar gibi suçların her sene katlanarak arttığı belirtilmektedir.[156]

İnternet üzerinden işlenen suçların gerçekten bir suç olarak değerlendirilebilmesi ve sorumluların cezalandırılabilmesi için yapılan eylemin kanunlarda tanımlı bir suç olması gerekmektedir. Bu tanımlamaların yapılması ve tanımlanan suçların ispat edilebilmesi için gerekli düzenlemelerin bir an önce hayata geçirilmesi gerekmektedir. İnternet kullanımında yaşanan hukuki sorunların çözümünde karşılaşılan güçlüklerin temelinde de bunlar yatmaktadır. Yasalardaki açıklar ve delil toplamada henüz kesin bir yolun belirlenememesi hukuk çevrelerinin yaşadığı en büyük sıkıntılar arasında yer almaktadır.

4.3.Uluslararası Durum

Uluslararası hukuk bakımından internetteki hukuk düzenlemelerini incelersek, tam bir yeknesaklık sağlandığı söylemek çok güçtür. Her ülke şimdilik kendi politikası ve dünya görüşüne göre düzenleme yapmaktadır. Mesela, bazı ülkelerde internete giriş izinle olabildiği gibi, bazılarında devletin kontrolünde olan tek bir servis sağlayıcı bulunabilmektedir. Bazı ülkelerde de devletin politikasına ve dünya görüşüne uymayan sitelerin o ülkede görüntülenmesi kısmen de olsa engellenebilmektedir. Bu ülkelere örnek olarak: Beyaz Rusya, Burma, Çin, Irak,

[156] http://www.madran.net/?p=15(2007)

İran, Kuzey Kore, Küba, Libya, Sudan, Suriye, Suudi Arabistan, Tunus ve Vietnam'ı sayabiliriz.

Düzenlemeler bakımından en çok sistemini oturtmuş gözüken ülke ABD'dir. Başkan'a bağlı özel birimlerin yanı sıra, Adalet Bakanlığı, FBI ve CIA'nin suça karşı çalışan birimleri oluşturulmuş, internet yoluyla işlenen suçlarla mücadelede önemli mesafeler kaydedilmiştir. En önemli gelişme ise internet üzerindeki hak ve yükümlülüklerin, temel özgürlüklerin özel kanunlarla düzenlenmiş olmasıdır.

Ancak, ifade edilmelidir ki, 11 Eylül terör saldırısından sonra ABD özgürlük politikalarını tekrar gözden geçirmiş, internetin terör örgütlerinin haberleşmesi açısından büyük bir tehlike arzettiğini düşünerek sansür ve izleme yöntemlerine başvurmaya başlamıştır.

Avrupa ülkelerine baktığımızda, ülkelerin birbirinden bağımsız düzenlemeye gittikleri görülse de, düzenlemelerde ve uygulamalarda yeknesaklik için çalışmalar başlamıştır.

Almanya'nın düzenlemelerinden Teleservisler Kanunu, önemi bakımından dikkat çekmektedir. Türkiye'de ortak tanımları bile henüz yapılamayan internet sujeleri, (erişim sağlayıcı, içerik sağlayıcı, servis sağlayıcı) bu kanunda hak ve sorumluluk bakımından oldukça iyi düzenlenmiştir.

G8 ve OECD bünyesinde de bir takım çalışmalar yapılmakta, genelde ortak mevzuat, ortak usul hükümleri ve etkin işbirliği amaçlanmaktadır.

İnternet ve Ceza Hukuku alanında şu ana kadar yapılan en kapsamlı çalışma Avrupa Konseyi'nin oluşturduğu "siber suçlar konvansiyonu"dur. Bu sözleşmede amaç, ceza kanunları ile düzenlenmesi gerekli olan eylemlerin ne olduğunu açık bir şekilde tespit etmek, sivil özgürlük ve güvenlik kavramları arasındaki uyuşmazlıkların nasıl aşılacağı konusunda üye ülkelere yol göstermektir. Bu sözleşmeye Avrupa Konseyi üye ülkeler dışında ABD, Kanada ve Japonya da destek vermektedir. İnternette işlenen yasadışı eylemler hakkında ulusal mevzuatların uyumlaştırılması ve elektronik ortamdaki delillerin

derlenmesini ayrıntılı düzenlemiştir. Ayrıca, usul hukuku açısından, soruşturma usulü, suçluların iadesi, iletişimin engellenmesi ve üye ülkelerin işbirliği düzenlenmiştir. Etkin işbirliği için karşılıklı yardım, bilgi verme ve "log" dediğimiz trafik verilerinin tutulması konuları da düzenlenmiştir.

4.4.Ülkemizdeki Durum

Bilişim sistemine girme, sistemi engelleme,bozma, verileri yok etme veya değiştirme, tüzel kişiler hakkında güvenlik tedbiri uygulanması, banka ve kredi kartlarının kötüye kullanılması kapsamındaki suçları tanımlayan kanun maddeleri TCK'nın 243 -246.maddelerinde yer almaktadır.

Avrupa birliği uyum yasaları çerçevesinde hazırlanan, suçlara ve cezalara yeni düzenlemeler getiren 5237 sayılı yeni TCK, 1 Haziran 2005 tarihi itibari ile yürürlüğe girmiştir. 79 yıldır yürürlükte bulunan ve 06.Haziran.1991 yılında ilk olarak bilişim suçları olgusunun metine girdiği 765 sayılı (eski TCK) Türk Ceza Kanunu'na ek olarak bir çok düzenlenme yapılmış bilişim alanında işlenen suçlarda oldukça genişletilmeye çalışılmıştır.

Yeni TCK ile birlikte; Bilişim Suçları, onuncu bölüm altında "Bilişim Alanında Suçlar" başlığı altına alınmış ve eski TCK ya ek olarak Banka ve Kredi Kartlarına karşı işlenen suçlara ve Tüzel Kişilerin bilişim suçları işlemesine yönelik maddeler eklenmiştir.

Yeni Türk Ceza Kanunundaki bu düzenlemelerin yanında, bilişim sistemleri ile işlenebilecek ancak tek başlarına tamamen bilişim suçu olarak adlandırılamayacak suç tipleriyle ilgilide düzenlemeler yapılmıştır.

Eski TCK da bilişim suçları madde 525/a/b/c/d altında çok kısa ve yetersiz olarak bahsedilirken, 5237 sayılı yeni TCK da 243–244–245–246 'ıncı maddeler ile bir çok farklı başlık altındaki maddelerde bilişim suçlarına da yönelik düzenlemelerde bulunulmuştur. Örneğin; yeni TCK'nın ikinci kısmı olan kişilere karşı suçların, dokuzuncu bölümünde, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında; madde 135 ile "kişisel verilerin kaydedilmesi" suçu,

madde 136 ile "kişisel verileri hukuka aykırı olarak verme ve ele geçirme" suçu, madde 138 ile "verileri yok etme" suçu konularında düzenlemeler ve eklemeler yapılmıştır.

Yeni TCK 243. madde 1. Fıkrasında *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir"* hükmü yer almaktadır.

Maddenin bu fıkrası ile birlikte hukukumuz bilişim sisteminin her alanına yetkisiz olarak her ne suretle olursa olsun girmeyi ve girdikten sonra orada kalmayı suç olarak saymakla birlikte, bilişim sisteminde her hangi bir zarar verilmese bile yahut bilişim sistemi üzerindeki veriler silinip, değiştirilmese veya yetkisiz olarak girişi yapılan bilişim sisteminin çalışması engellenip, bozulmasa bile suç saymıştır.

Böylelikle hukukumuz Avrupa Siber Suç Sözleşmesinin ikinci maddesinde belirtilmiş olan "hukuka aykırı erişimi" hususunu bünyesine katmış, eski TCK' da ki bir eksikliği gidermiş olmuştur. Eski TCK da bilişim sistemine salt olarak giriş ve orda kalınması suç olarak tamamen sayılmamakla birlikte verilerin ele geçirilmesi yok edilmesi veya değiştirilmesi durumu da suç gerçekleşmiş olmaktaydı. Bu fıkra ile birlikte hukukumuz isabetle sadece bilişim sistemlerinin güvenliğinin ihlalini bile suç saymakla diğer ülkelerdeki gibi bir olgu içerisine girmiş ve büyük bir isabette bulunmuştur.

Yeni TCK 244. madde 1. Fıkrasında *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."* hükmü yer almaktadır.

2 . Fıkrasında ise *"Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır."* hükmü yer almaktadır.

Bu maddenin 1'nci fıkrası ile birlikte; yukarıdaki madde 243'ün 1'nci fıkrasındaki bilişim sistemine girme eylemi gerçekleştikten sonra bilişim sisteminin işleyişinin engellenmesi veya bozulması durumunda kanun koyucu cezalandırmada bulunmuştur. 2'nci fıkrası ile birlikte ise; bilişim sistemindeki verilerin bozulmasını, silinmesini, değiştirilmesini, kullanılamaz hale gelmesini, yeni ve farklı verilerin yerleştirilmesini yahut mevcut verilerin başka bir yere aktarılması eylemini de cezalandırmaktadır.

Yeni TCK ile birlikte Avrupa Siber Suç Sözleşmesinin de yer alan 4'üncü ve 5'inci maddeler ile uyumluluk sağlanmıştır. ASS' de 4 madde ile bilişim sistemi üzerindeki verilere etki etme, 5'inci madde ile de sistem etki etme hususları düzenlenmiştir.

Yeni TCK ile birlikte yasa koyucu sadece bilişim suçunda suça konu yazılım ve verileri koruma altına almamış, bilişim sisteminin donanımına karşı yapılabilecek ızrar eylemini de bozmak, yok etmek, erişilmez kılmak ibareleriyle suç saymıştır. Bu suç tanımlaması ile yasa koyucu salt olarak bilişim sisteminin tümünü ve bilişim sisteminin içerdiği yazılımları verileri korumayı hedeflememiş, aynı zamanda bu bilişim sistemini eğitimden ticarete, devlet işlerinden bilimsel çalışmalara kadar sayılabilecek daha birçok alandaki kullanıcılarını da korumayı hedeflemiştir. Burada herkes suçun mağduru olabilir. Bura dikkat edilmesi gereken şey mağdur olarak illaki zarar gören bilişim sisteminin sahibi olunması gerekmemektedir. Örneğin bir internet sunucusu yurt içi yahut yurt dışı kaynaklı bir firmaya ait olabilir ancak o web sunucusu üzerinde yayın yapmakta olan web sayfası hukukumuzca korunması gereken tüzel kişi, özel kişi veya kamu kurumu olabilir. Burada fail internet ortamının verdiği bağlantılılık sebebiyle yine yurt dışındaki bir şahıs veya tüzel kişi olabilir, fail ve mağdur bakımından yerellik esas değildir. Böyle bir durumda adli istinabe yoluyla diğer ülkelerle temasa geçilmesi gerekmektedir.

Yeni TCK 245. madde 1. Fıkrasında "*Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan*

altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır." hükmü yer almaktadır.

Yeni Tck'da ki önemli bir gelişme olan Banka ve Kredi kartlarına yönelik işlenebilecek bilişim suçlarının cezalandırılması söz konusudur. Ancak burada dikkat edilmesi gereken kredi kartları suçlarının sadece bilişim sistemi yoluyla işlenmemesidir. Çalıntı bir kredi kartının başka bir pos cihazında kullanılmasında her hangi bir bilişim suçu söz konusu olmamaktadır. Bu bağlamda bilişim suçu olarak kredi kartı suçlarını değerlendirirken bakılması gereken suçun ne tür bir aktivite ve araç ile işlendiğidir. Suç bilişim sistemleri kullanılarak kartın oluşturulması, kart bilgilerinin bilişim sistemleri kullanılarak ele geçirilmesi veya elde edilmiş kartın bilişim sistemleri aracılığı ile menfaat temini amacıyla kullanılması durumunda bilişim suçları başlığı altında yer almalıdır görüşleri daha şimdiden yukarıda ki fıkraya muhalefet eder biçimde ortaya çıkmaktadır.

Bu bağlamda uygulamada birçok hata ile karşılaşılmaktadır. Banka ve kredi kartlarının kötüye kullanılması bazı durumlarda hırsızlık, dolandırıcılık, emniyeti suistimal suçlarını da oluşturabilmektedir. Sahte kimlik bilgileri ile kredi kartı başvuruları ya da yan kesicilik sonucu elde edilmiş kredi kartı ile menfaat temini çoğu zaman nitelikli dolandırıcılık suçu ile karıştırılarak bilişim suçları olarak daha şimdiden değerlendirmelerde bulunulmaktadır. Yasa koyucunun bu madde üzerinde daha açıklayıcı ve bilgilendirici şekilde düzenlemelerde bulunmasının elzem olduğu görüşü oldukça yaygındır.

4.5.Dijital Delil ve Dijital Delillendirme

Bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere kısaca dijital delil ve bunların ilgili birimlere unulmasına da dijital delillendirme diyebiliriz. Dijital deliller bir çok tipte karşımıza çıkmaktadır.

Bunlardan bazıları şu şekildedir:

- Veri dosyaları

- Kurtarılmış silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Chat Kayıtları
- İnternet Geçmişi
- Web Sayfaları
- Kayıt Logları
- Abone Kayıtları

Dijital deliller, normal delillere göre yapı itibariyle bazı sıkıntıları barındırmaktadır:[157]

- Dijital Delillerin Bütünlüğü: Dijital veriler üzerinde çok kolay bir şekilde değiştirme, silme ve yenisini oluşturma gibi işlemlerin yapılabilmesi bu delillerin bütünlüğünü sağlamayı çok zorlaştırmaktadır.

- Dijital Delillerin Doğrulanması: Bir kişiyi dijital delillerle birlikte yakaladıktan sonra mahkeme sürecinde o verilerin gerçekten o kişiye ait olduğunun ispatı gerekmektedir. Fakat delil olarak ele geçirilen verilerin aynısı her hangi bir kişi tarafından da oluşturulabilir. Hatta sanık bu verilerin daha sonra, polis tarafından bile oluşturulduğunu iddia edebilir.

- Dijital Delillerin İnkar Edilememesi: Dijital delillendirme işlemindeki dijital delilin sahibi, onu ele geçiren şahıslar (Ör: Polis), delilin alındığı medya, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların daha sonradan inkar edilememesi gerekmektedir.

- Dijital Delillerin Doğruluğu: Dijital delillerin ele geçirilmesi esnasında kullanılan teknikler ve kullanılan bilgilerin (Örneğin delilin ele geçirilme zamanı)

---

[157] Chet Hosmer, **Proving the Integrity of Digital Evidence with Time**,(International Journal of Digital Evidence, Spring 2002 Volume 1) s.3

doğruluğunun ispatı gerekir.

- Dijital Delillerin Daha Sonradan Ele Alınabilirliği: Dijital deliller oluşturulduktan sonra, bu delilleri üçüncü bir şahıs inceleyebilmelidir.

Dijital Delillerin Teknik Olarak Doğrulanması ise;Verilerin güvenliğinde bahsedilebilecek 3 önemli husus vardır [158]

Bunlar:

- Verilerin gizliliğinin sağlanması : İletilen verilerin üçüncü kişiler tarafından öğrenilememesi
- Verilerin bütünlüğünün sağlanması: Alıcıya ulaşan verilerin, göndericiden ilk çıktığı hali ile aynı olduğunun ispatı
- Verilerin inkar edilememesinin sağlanması: Göndericinin gönderdiği verilerin gerçekte kendisi tarafından gönderilmediğini iddia edememesi

Doğrulama, yine dijital güvenlik alanında çok sık bahsedilen kavramlardan biri olmakla birlikte, yukarıdaki maddelerin her biri içinde genellikle yer aldığı için ayrı bir başlıkta ele alınmamıştır.

Bahsedilen güvenlik tekniklerinin, dijital delillerin olay yerinden toplandığı andan itibaren mahkeme esnasına kadar bütünlüğünün bozulmadığının ispatı ve inkar edilememesinde oldukça büyük önemi bulunmaktadır. Bugüne kadar bu teknikleri kapsayan bir çok güvenlik metodu geliştirilmiştir. Genel olarak veriler üzerindeki bütünlük sağlama, doğrulama, şifreleme, inkar edememe gibi konular Kriptoloji bilimi altında incelenmiştir. Kriptoloji alıcı ve gönderici arasında iletilen veriler üzerinde belirli matematiksel işlemler gerçekleştirip, güvenlik için çeşitli mekanizmaları sağlar.

---

[158] James. F. Kurose, Keith W. Ross, **Computer Networking**, (2003 Pearson Education, 2. Edition) s.6

Dijital Delil Elde Etmede Asgari Standartlar şöyle belirtilebilir:[159]

1. Elde edilecek delil zarar verilmeden koruma altına alınmalıdır.
2. Varsayıma dayanılmamalı, delil elde etme sırasında her şey kontrol edilerek işlemler yürütülmelidir.
3. Delilin her bir kısmı için, birbirinden farklı takip numarası veya tanımlama bilgisi verilmelidir.
4. Bilişim araçlarının yazım koruması (MAC) yapılmalı ve daha sonra işlemlerin kontrol onayı yapılacağından, araştırılan alanın aslına uygun bir kopyası alınmalıdır.
5. Daima (kağıtta bile) aslına uygun kopya üzerinde çalışılmalıdır.
6. Yapılan tüm işlemler boyunca, atılan tüm adımlar ve her şey tutanağa bağlanmalıdır.
7. Bilişim araçları, önCeden olabilecek (delil elde edilmesine engel olmak amacıyla yapılan) tuzaklar için kontrol edilmelidir.
8. İlgili görülen verilerin yazıcıdan çıktısı alınmalıdır.
9. Mahkemede tekrar görülebileceği farz edilerek, delil elde etmeyle ilgili (analiz) rapor hazırlanmalıdır.

Dijital delil araştırmasındaki genel uygulamalar ise şöyledir:[160]

1. Araştırma sırasında muhafaza altına alınma işlemleri sırasıyla tutanağa geçirilmelidir.
2. Delil araştırmasında gerekli olan lisanslı ve yetkili bütün yazılımlar hazır bulundurulmalıdır.
3. Erişilebilen kaynaklarla ilgili kullanılabilecek bütün araçlar mevcut olmalıdır.
4. Mümkün olduğu ölçüde araştırma sırasında, uzmanlar, bilişim sistemindeki donanım (hardware) ve yazılımlara (software) erişmiş olmalıdır.
5. Araştırma sırasında kullanılan usuller, daima belgelerle ortaya konulmalı, yani denetime olanak tanınmalıdır.

---

[159] Scott L Ksander , **a.g.e.**, S. 14

[160] Scott L Ksander , **a.g.e.,** s. 15

6. Bir suçun araştırması bile yapılsa, hiç kimseye yasaların ihlal edilmesi yetkisi verilemez.

4.6.Bilişim Suçlarına Müdahale

Bilişim suçlarına müdahale oldukça kritik ve çok hassas bir konudur. Çünkü toplanacak deliller dijital delillerdir ve bu deliller yapı itibariyle bozulmaya ve değiştirilmeye müsait verilerdir. Bilişim suçuna müdahale aslında suçun ilk tespit edildiği anda başlar. En kritik nokta da bu aşamadır. Eğer suçu ilk fark eden kişinin bu alanda yeterli bilgisi yoksa, çok önemli bilgi ve delilleri sistem dışı yok edebilir. Bu yüzden ilgili kişilere mutlaka konu ile ilgili bilgi ve eğitimler verilmeli, olağan dışı herhangi bir olay fark ettiklerinde bilişim suçları konusunda eğitilmiş bir güvenlik görevlisine ulaşmaları sağlanmalıdır.

Olay yerine gelen güvenlik görevlisinin, eğer saldırı hala devam ediyorsa ilk yapacağı şey saldırıyı herhangi bir dijital delile zarar vermeyecek şekilde kesip(Örneğin ağ üzerinden gelen bir saldırıysa, bilgisayarı kapatmak yerine, ağ kablosunun çekilmesi daha mantıklıdır), bütün her şeyi olduğu gibi dondurup, bilişim suçları araştırma ekibine haber vermektir. Bilişim suçları ekibi gelene kadar olay yerine herhangi bir müdahale gerçekleşmemelidir

Bilişim suçları araştırma ekibi en az şu kişilerden oluşmalıdır:[161]

- **Üst düzey operasyon yöneticisi** : Bilişim suçlarında olay yerine müdahale konusunda uzman, olay yerinin nasıl çevrilip, korunacağını, nerede ve nasıl bir araştırma yöntemi izleyeceklerini planlayan, araştırmadan sorumlu en üst düzey kişidir.
- **Polis** : Olay yerine giriş, olay yerini koruma, ilgili delillerin ve şüphelilerin alınıp gerekli adli işlemlerin yapılmasını sağlar.
- **Müdahaleci** : Olay yerine ilk ulaşan personel, güvenlik görevlisi v.b
- **Bilişim suçu olay yeri inceleme uzmanları**: İlgili delillerin standartlara uygun şekilde bozulmadan toplanıp, aktarılmasını sağlar.

---

[161] Debra Littlejohn Shınder, **Scene of Cybercrime – Computer Forensics Handbook**, (Syngress Publishing, USA, 2002) s.26

Bilişim suçları araştırma ekibi, olay yerinde gerekli bütün işlemleri yaptıktan sonra, elde edilen delilleri bilgisayar adli tıbbı uzmanlarına iletir. Bilgisayar Adli Tıbbı, potansiyel delilleri tespit etmek üzere bilgisayar araştırma ve analiz tekniklerinin uygulanması şeklinde tanımlanmaktadır.[162]

4.7.Bilişim Suçlarında Örgütlenme

Uluslararası boyutta kredi kartı dolandırıcılığında örgütlü suçluluk yaygınlaşmış durumdadır. Kredi kartı dolandırıcılığında, değişik türde örgütlü suçlar görülmektedir. Kredi kartı dolandırıcıları bir seferde zengin olmaktansa, sistematik şekilde geniş bir zaman dilimi içinde hareket etmeyi tercih etmektedirler. Internet yoluyla yapılan satışlarda kullanılan kredi kartı bilgilerini, satıcı firmaların kayıtlarından elde eden korsanlar, kredi kartı sahiplerinin hesap hareketlerini takip ederek, ele geçirdikleri kredi kartı bilgileriyle aylık miktarlara yakın alışveriş yapmaktadırlar. Bu alışverişlerde, alınan mallar ve satıcı firmalar hayalidir (sahtedir). Bu suç yapısında, firma yetkilileri de bu suçun içerisindedirler ve örgütlü hareket söz konusudur.[163]

Esasında, bilgisayarların örgütlü olarak pek çok suç türünde kullanımı yaygınlaşmıştır. Örneğin, fikri haklarla ilgili suçlar, ekonomik suçlar, uyuşturucu ticareti, karaborsayla ilgili suçlar, ihaleye fesat karıştırma ve hatta adam öldürmede bile örgütlerin bilgisayar kullandıkları görülmekte dir.[164]

Tüm bu nedenlerle, 5237 sayılı TCK'nında, Hükümet Tasarısındaki "Suç işlemek için örgütlenme" kenar başlıklı 351. maddesindeki gibi bir hükme yer verilmemesi yerinde olmamıştır.

---

[162] Judd Robins, **Computer forensic definition**, (available at:http://rr.sns.org/incident/legal-standarts.php 2004)

[163] Fred Cohen, **Computer Fraud Scenarios**, (Computer & Security, Volume 2003, Issue 1, January 2003), s.16-17

[164] Rosa Codina, **Information Age Crime** ,(June 2003) s.2

4.8.Adli Bilişim

Klasik suçlardaki soruşturma evresinde delil elde etme, fizik ve kimya gibi geleneksel bilimlere dayanır ve fiziksel nitelikteki suçlar araştırılır. Bir cinayetin aydınlatılmasında, bir taraftan kimyasal analizler (örneğin, DNA testi gibi) yapılırken, diğer taraftan da cinayet mahallinin (örneğin, maktulün bulunduğu yer, ateş etme mesafesi, kaç el ateş edildiği gibi) fiziksel olarak detaylı incelemesi yapılır.

"Yeni suç alanı" (the new crime scene) olarak da adlandırılan bilişim suçlarında ise, soruşturma evresindeki araştırmalar, bilgi teknolojisine ve bu teknolojiyi kullanan bilişim sistemlerine dayanır.[165] Bilgi teknolojisi, pek çok alanda dünyanın çehresinde olumlu değişikliklere ve baş döndürücü gelişmelere neden olurken, diğer taraftan da, bu alanda suç işlemeye teşvik edici ve işlenen suçları gizleyici özelliği vardır. Bilgi teknolojisinin, suç araştırmalarında da rolü giderek yoğunlaşmaktadır.

Soruşturma ve kovuşturma evrelerinde bilgisayarların ve elektronik delilin rolü her geçen gün artarken, bu tür delillere yüzde yüz ispat gücünü-kazandırma çabaları ve arayışları sürmektedir.[166] Bu alandaki çalışmalarda, başta ABD olmak üzere bilişim teknolojisini fazlaca kullanan ülkelerde, (computer forensics) kavramı öne çıkmaktadır. "Computer forensics" kavramı, "bilgisayar adlî bilimi" olarak da ifade edilebilir[167] ise de, "adli bilişim" kavramını kullanmayı tercih ediyoruz.[168]

---

[165] Ed Busch, **Forensics - What To Do After The Break-In** (DSA (Data SystemsAnalysts), Information Technology Solutions for a Global Market, 2001), s.3

[166] Ajoy Ghosh, **Guidelines for the Management of IT Evidence**, (APEC Telecommunications and Information Working Group 29th Meeting 21-26 March 2004 | Hong Kong, China, This paper is a presentation of the recently published Standards Australia handbook), s.1

[167] Mehmet Yayla , **Uluslararası Platformda ve Türkiye'de Bilişim Suçları: Ankara İl Jandarma Komutanlığında Alan Çalışması**, (Kara Harp Okulu Savunma Bilimleri Enstitüsü, yayımlanmamış yüksek lisans tezi,Ankara, 2004), s.78.

[168] Aynı yaklaşım için bkz.: Leyla Berber Keser , **Adlî Bilişim**, (Yetkin Yayınevi, Ankara, 2004), s.37 vd

Bir de, "digital forensic science" şeklinde ifade edilen "elektronik adlî bilim" kavramı söz konusudur. Elektronik adlî bilim ise; suçların, yetkisiz erişimlerin veya yıkıcı hareketlerin ortaya çıkarılması amacıyla elektronik kaynaklardan elde edilen elektronik delili, toplama, geçerli kılma, tanımlama, analiz etme, yorumlama, belgeleme, sunma ve muhafaza etmeyle ilgili bilimsel delil elde etme ve ispatlama metotlarının kullanımıdır. Bu tanım, ABD'de Ağustos 2001'de elliden fazla üniversite araştırmacısı, adlî bilişim görevlisi ve analistin katılımıyla New York'taki uygulamalı seminerde (Digital Forensic Research Workshop) (DFRWS) yapılmıştır.[169] Bu tanım, adlî bilişimin yasal yolla veri (bilgi) edinmesinde geniş bir bakış açısı vermektedir.

Adli bilişim, bilişim alanındaki olayların yeniden inşası için veya ortaya çıkarılmasını kolaylaştırmak için bilimsel yöntemler kullanılarak delil elde etme ve ispatlama metotlarının kullanılması çalışmalarıdır.[170]

Adli bilişimin başlangıcı, ilk kez bir bilişim sistem yöneticisinin, bilişim sistemini keşfetmek üzere yetkisiz erişimde bulunan bir korsanın ne yaptığını ve nasıl yaptığını anlamaya başlamasına dayandırılmaktadır. Burada, bilişim sistemine yapılan saldırının keşfi birinci sorundur. Eğer saldırı devam ediyor ise, ikinci sorun ise, bunun durdurulmasıdır. Üçüncü aşama ise, bay ya da bayan korsanı cezalandırıncaya kadar takip etmektir. Dördüncü sorun ise, her şeyden önce yetkisiz erişime izin veren bilişim sistem açığını tamir etmektir. Başlangıçta bilgisayar korsanları kötü niyetli fiillere yönelmektense, bu işi nasıl başardıklarının sevinciyle, ağırlıklı olarak yetkisiz erişim fiiliyle ilgilenmekteydiler. Bu nedenle, bu tür korsanlarla ilgili delil elde etmek kaygılanılacak bir iş değildi.[171]

---

[169] Peter Stephenson, **Structured Investigation of Digital Incidents in Complex Computing Environments**,(Information Systems Security, July/August 2003), s.29; Brian CARRIER, , **Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers**,(International Journal of Digital Evidence, Volume 1, Issue 4, Winter 2003), s.2.

[170] Brian Carrier , **a.g.e.**, s.2

[171] Michael Potaczala , **Computer Forensics**, (CHS5937 Topics in Forensic Science, 12.6.2001), s.1; Henry B.Wolfe, , **An Introduction to Computer Forensics: Gathering Evidence in a Computing Environment**,(Informing Science Challenges to Informing Clients: A Transdisciplinary Approach, June 2001), s.569

Zamanla, bilgisayarlar teknolojisinin ilerlemesi, bilişim kullanımının artması, bilişim ağlarının genişlemesi gibi nedenlerle, bilişim suçları ve failleri gittikçe karmaşık hâle gelmiş ve başlangıçtaki basit yapı bir anda kaybolmuştur. Artık bilişim suçlarıyla ilgili delil elde etme işi, yani adlî bilişim, uzmanlık gerektiren, sıradışı ve zor bir uğraş haline gelmiştir.

Adli bilişimin doğmasının önemli bir nedeni de internettir. İnternet, bir taraftan suçlu hareketlerinde çok sayıda seçenek sağlarken, diğer taraftan da hem klâsik suçların örneğin beyaz yaka suçlarında olduğu gibi yeni versiyonlarına ve hem de internete özgü ortamda tamamen yeni suçların ortaya çıkmasına neden olmuştur. Suçlular için bu yeni suçları keşfetmek, katlanarak devam ederken, bu gelişmeler adlî bilişimin doğumuna da neden olmuştur.[172]

Adli bilişimin Türk Hukukunda yeni bir kavram olduğu söylenebilir. Bu kavram, bilişim suçlarının soruşturma evresinde, mahkemelere sunulacak delillerin toplanmasının çerçevesini belirlemeyi, nelerin delil olabilmesi için ne tür işlemlerin yapılması gerektiğini anlatır.[173]

Ülkemizde adlî bilişim alanındaki çalışmaların temelinin, 1982 yılında Emniyet Genel Müdürlüğünde Bilgi İşlem Daire Başkanlığının kurulmasından çok daha sonra, EGM bünyesinde, Bilişim Suçlan Bürosunun kurulmasıyla atıldığı söylenebilir. 2001 yılında bu büro, İnternet ve Bilişim Suçları Şube Müdürlüğü olarak değiştirilmiştir.[174]

Adli bilişim, bir bilgisayarda veya iletişim aygıtındaki silinmiş veya var.olan bir elektronik delille ilgili yapılan araştırmadır. Adlî bilişim, sonunda yasal veya idarî bir süreçte sunulmak üzere, bilişim sistemi üzerine yapılan zorunlu bir[175] süreçtir .

---

[172] Gordon Stevenson, **a.g.e.,** s.13

[173] Mehmet Yayla , **a.g.e.**, s. 78

[174] Mustafa Karabal, **Bilişim Suçları ve Turk Polis Teşkilatı**,(http://www.turkhukuksitesi.com/hukukforum/art_showarticle -2.2.2005)

[175] Linda Volonino, **Electronnic Evidence And Computer Forensics** (2003), s.460

Adli bilişim, bilişim alanındaki depolanmış bilgileri elektronik olarak işleme tabi tutmayı gerektirir ve bilişim suçlarının ortaya konulmasında, elde edilecek delillerin; a) tanımlanması, b) korunması, c) analizi ve d) mahkemede kabul edilecek şekilde yasal çerçevede dijital delil olarak ortaya konulması (sunum) safhalarından meydana gelen yapıyı anlatmaktadır.[176] Bir başka deyişle adlî bilişim, bilişim suçlarında delil elde edilebilmesi amacıyla, çeşitli teknikler kullanılarak delil elde etme, inceleme ve analiz işlemleri olarak tanımlanabilir.[177]

Adli bilişim, bilgisayar delillerini muhafaza etme, tanımlama, sonuç çıkarma ve belgeleme görevleriyle uğraşmaktadır. Adlî bilişim, bilgisayarın sabit disk sürücüsünün (hard disk drive) otopsi işlemini yapmaktadır. Çünkü, bilişim suçu sonrasında, bilişim sisteminde (özellikle sabit disk sürücüsünde) çeşitli seviyelerde depolanan bilgiler, uzman ekiplerce, özel yazılım araçları ve tekniklerle bulunup gömülü) bilgi keşfedilmeye çalışılmaktadır.[178]

Adli bilişim, işlenmiş bir suçun delillerini, tamamen bilişim sistemlerinin kullandığı yazılımlar ve araçlardan önceden tanımlanmış usulde ortaya çıkarıp bunları muhafaza etmeye ilişkin bir takım işidir.[179]

Adli bilişim, geleneksel bir yaklaşımla ele alındığında, sahasında ölümden sonra yapılan, verimli bir sonuç alınıp alınamayacağı belli olmayan pahalı bir araştırma yapısıdır.[180]

Adli bilişim, klâsik suçlardaki araştırmalara göre, çok daha gelişmiş bir araştırmayı ve ileri derecede bilgisayar uzmanlığını gerektirmektedir. Bir başka

---

[176] Steve Romig , **Forensic Computing**, (November 4, 1999, romig@acm.org/(2.4.2004); Linda Volonino, **a.g.e.**, s.460.

[177] Judd Robins, , **"Cumputer Forensic Defination"**, (http://rr.sns.org/incident/legalstandarts .php(1.3.2005); MOHAY, (9.12.2003)

[178] Michael Barba, , **Computer Forensic Investigations** (www.computer-forensic.com/(1.3.2005); PALMER, **a.g.e.**, s.6

[179] Ed Busch, **a.g.e.**, s. 15

[180] Ajoy Ghosh, **a.g.e**, s.1

anlatımla adlî bilişim klâsik suçlardaki araştırmalardan farklıdır ve adlî bilişimdeki araştırmada, araştırma konularına kolaylıkla ulaşabilmeyi sağlayacak teknik ve araçlar gerekmektedir.[181]

Suç ve bununla mücadele her ülkenin önemli sıkıntılarındandır. Genel olarak suçla mücadelede problemi tanımlamak ise, suçla mücadele edenlerin ve hatta devletin başarılı olmasında önemli bir etkendir.

1930 yılında ABD Kongresinde başsavcının Amerika'da işlenen suçlarla ilgili bir bilgi arşivi oluşturulmasını istemesiyle, bu konuda Tekdüze Suç Raporlama (Uniform Crime Reporting) (UCR) programıyla; ülkedeki işlenen suçların yıllık istatistikleri ve başlıca işlenen suç türleri tespit edilmeye (rapor edilmeye) başlanılmıştır. Bu programla, geleneksel suçların başlıca türleri örneğin; adam öldürme, hırsızlık, zorla ırza geçme, soygun, kundaklama gibi suçlar hakkında detaylı bilgiler toplanmıştır. Yeni (new) UCR programında[182] ise, mevcut suçların 22 kategorisinin bilgisayarlar kullanılarak gerçekleştirildiği rapor edilmiştir. Burada, program görevlilerinin rapor edecekleri suçlarda bilgisayar kullanılıp kullanılmadığını belirlemeleri ve bu soruyu cevaplamaları gerekmektedir. Özellikle (ırk veya dini kaynaklı) nefrete dayalı suçlarda, bilişim suçlarının olup olmadığı mutlaka detaylı şekilde incelenmelidir. Nefret suçları, çoğunlukla, saldırı, vandalizm ve hatta cinayet gibi suçları beraberinde getirmektedir.[183]

Dünyada özellikle 1990'lı yıllardan itibaren internetin yaygınlaşmasıyla bilişim suçlarındaki patlama, problemin tanımlanması çabalarını artırmıştır. İnternete bağlı olan büyük kuruluşlar, hükümetler ve hatta çok küçük ortaklıklar bile risk altındadırlar. Problemin tanımında, ülkelerin her yıl suç istatistikleri çıkarmaları ve suç trendini gözlemleri önem taşımaktadır. ABD'de, 2000 yılında yapılan anketlerde, suça maruz kalma oranı % 59 iken, 2001 yılında bu rakam %

---

[181] Leyla Berber Keser , **a.g.e.**, s.40

[182] Bu programın adı: **National Incident Based Reporting System (FN20XNIBSR)**

[183] Marc Goodman, ***Making Computer Crime Count***, (http://newfirstsearchoclc.org/images/ WSPL/wsppdf1/ HTML/03, (4.12.2004)

70'e çıkmıştır. Hatta, bilişim suçlarından dolayı uğranılan zararlar katlanarak artmakta bilişim suçlarına hedef olan sistem açıkları (çatlakları) çoğalmaktadır .

FBI ve Ulusal Beyaz Yaka Suç Merkezi'nin (National White Collar Crime Center) 2000 yılındaki çalışmalarında, bilişim suçlarının mevcut kapsamı anlaşılmaya başlanılmıştır. Bu kuruluşlar, internetteki dolandırıcılığın boyutlarını takip etmek için İnternet Dolandırıcılığı Şikayet Merkezi "Internet Fraud Complaint Center" (IFCC) (FN22) kurmuşlardır. Bu Merkez, şikayet sayılarını, türlerini, içeriklerini detaylı şekilde inceleyerek, gerçekte işlenen internet suçlarının boyutlarını tahmin etmeye çalışmaktadır. Bununla birlikte IFCC, internetteki suçların genel görünümünü ortaya koymaya çalışmaktadır. IFCC'ye göre, bu çalışmaların dışında, bilişim suçlan üzerine federal yapıda, devletler bazında, yerel adlî kolluk görevlilerince mutlaka daha kapsamlı araştırma ve çalışmalar yapılmalıdır .[184]

4.9.Bilişim Suçlarında Koğuşturma

Türk Ceza Yasasının 243,244,245. maddelerinde düzenlenen Bilişim Suçları ile ilgili fiilleri işleyen kişi,kişiler ,kurum ve kuruluşlar hakkında koğuşturma Cumhuriyet Savcılıkları kanalı ile resen takibi yapılacak suçlardandır.Bu suçlar şahsi dava yada takibi şikayete bağlı olarak tanzim edilen suçlardan değildir.Keza Yeni Ceza Usul Yasası Şahsi Dava ayrımını kabul etmemiştir.

Dolayısı ile Cumhuriyet Savcısı Bilişim Suçlarından Her hangi birisinin ,Ceza Usul Yasasının 160.Maddesi delaleti ile ihbar veya bir başka surette fiilin işlendiği izlenimini veren bir hali öğrenir öğrenmez gerekli araştırma,koğuşturma ve delillendirme işleminin ardından yine aynı yasanın 170 maddesi gereğince Kamu Davasını açacaktır.

1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Yeni Türk Ceza Yasasında 243 -246. maddeleri arasında düzenlenen Bilişim Suçlarına bakmakla görevli mahkeme kanunun metninde tayin edilmemiştir. Dolayısı ile bu konuda

---

[184] Diane Sears Campbell, **a.g.e.,** s.30. GOODMAN, **a.g.e**, (4.12.2004)..

Ceza Hukukunun yargılamaya ilişkin genel görevle ilgili kuralları uygulama alanı bulacaktır.Buna göre;

Sulh Ceza ve Ağır Ceza Mahkemelerinin görevleri dışında kalan,özel yasasında Asliye Ceza Mahkemesince görülüp karara bağlanacağı açıklanan veya özel yasasında hangi mahkemede görülüp karara bağlanacağı açıklanmamış olmakla birlikte Sulh ve Ağır Ceza Mahkemesinin görevi içinde bulunmayan bütün ceza davalarına bakmakla görevli olan Asliye Ceza Mahkemeleri, BİLİŞİM SUÇLARINA bakmakla da görevli mahkemeler olacaktır.

Yeni Türk Ceza Yasasının Bilişim Suçları ile ilgili düzenlemeleri incelendiği zaman görev alanları kanunla belirtilmiş olan Sulh Ceza Mahkemeleri ile yine görev alanları yasa ile belirlenmiş olan Ağır Ceza Mahkemelerinin görev tanımı ile ilgili bir ilişkilendirme yapılmadığı, suçun hangi mahkeme tarafından bakılacağının belirtilmediği görülecektir.Dolayısı ile yukarıda da arz edildiği üzere görev alanları belirtilmemiş bu suçlara ait yargılamaya genel görevli mahkeme olan ASLİYE CEZA MAHKEMELERİ tarafından bakılacaktır. Nitekim uygulamada bu şekilde davalar görülmekle birlikte yargılamaya ilişkin görev yönünden uyuşmazlık çıkmamaktadır.

4.9.1.Ceza Sorumluluğu: Ceza sorumluluğu kişiseldir[185] ve bu kural, ceza hukukunun esaslı ilkelerinden birisidir. Bu kavram, "kusurluluk, nedensellik, hukuka aykırılık ve kısacası genel suç kavramının temelini oluşturur"[186]. Anayasa'nın 38. maddesinin yedinci fıkrasında da "ceza sorumluluğu şahsîdir" hükmüyle konu teminat altına alınmıştır.

Ceza hukukunda hâkim olan "fiilin sübjektifliği ilkesi"ne göre, suçtan söz edilebilmesi için, failin kanunî tipe uyan ve zararlı bir fiili işlemesi yeterli olmayıp,

---

[185] Ceza hukukunda sorumluluk, tarihi süreçte başkasının fiilinden sorumluluk, objektif sorumluluk, kusurlu sorumluluk ve kişilik yönünden sorumluluk şeklinde aşamalar katetmiştir. Bu konuda geniş bilgi için bkz.: Nevzat Toroslu , **Ceza Hukuku**, (Savaş Yayınevi, Ankara, 2001), s.83 vd; özellikle objektif sorumluluk için bkz.: Muharrem ÖZEN , **Ceza Hukukunda Objektif Sorumluluk**/(US-A Yayıncılık, Ankara, 1998), s.22 vd

[186] Faruk Erem - Ahmet Danışman - Mehmet Emin Artuk , **Ceza Hukuku Genel Hükümler**, (Seçkin Yayınevi, Ankara, 1997), s.416

bunun yanında fiilin psikolojik açıdan da faille bir (nedensellik) bağının kurulabilmesi gerekmektedir. Bu yaklaşım, cezaî sorumluluğun subjektifleştirilmesi sürecinin bir ürünü ve insanlığın bir zaferidir.[187]

Fiil ile fail arasındaki psikolojik bağlantı ise, failin iradesini anlatır ve ceza sorumluluğunun temelinde insan davranışının iradi olması yer almaktadır. Bunun sonucu olarak, fiil hukuka aykırı olsa bile iradi değilse, fail fiilinden sorumlu tutulmamaktadır. Fiil ile fail arasındaki psikolojik bağlantı, kusurluluğu ortaya koymaktadır. Kusurluluk ise, "failin psişik faaliyeti ile sonuç arasındaki ilişkiden ibarettir".[188]

Bilişim suçlarında ve özellikle de internet ortamında işlenen suçlarda ceza sorumluluğunun belirlenmesi, bu alanın kendisine özgü teknik yapısı, internet ortamındaki (bilişim ağındaki) sujeler karşısında tartışmalı ve önemli bir konudur.

4.9.2.Bilişim Suçlarında Mahkemenin yetkisi

Genel kural gereğince davaya bakmak yetkisi, suçun işlendiği yere mahkemesine aittir.[189] Bilişim suçlarıyla ilgili açılan davada yetkili mahkeme, bu suçların bünyesi ve işlenme şekillerine göre tartışmalı konular içermektedir. Bunları ele alırken suçun işlenme şekillerine göre sonuca gitmek yararlı olabilir. Bu bakımdan suçun işlenme şekillerini belli gruplarda toplayabiliriz

Suçun Ülke İçerisinden İşlenmesi;

Bilişim suçunun Türkiye içerisinde işlenmesi, tartışmaların en az olabildiği kısımdır. Bilişim suçu ülke içerisinde işlendiğinde, ceza muhakemesindeki genel

---

[187] Nevzat Toroslu , **Ceza Hukuku,** (Savaş Yayınevi, Ankara, 2001) s.82-83; Muharrem ÖZEN , **a.g.e.**,,s.15-16

[188] Kayıhan İçel-Füsun Sokullu/Akıncı-İzzet Özgenç-Adem Sözüer-Fatih S.Mahmutoğlu-Yener Ünver, ,**İçel Suç Teorisi**, s.198

[189] 1412 sayılı CMUK.m.8/1 ve 5271 sayılı CMK.m.12/1

yetki kuralları uygulanarak yetkili mahkeme belirlenir. CMK'nın 12. maddesine[190] göre suçun işlendiği yer mahkemesi belirlenir. Eğer suç teşebbüs aşamasında kalmışsa, son icra hareketinin yapıldığı, kesintisiz suçlarda kesintinin gerçekleştiği ve zincirleme suçlarda son suçun işlendiği yer mahkemesi yetkilidir.

CMK'nın 12. maddesinin (5) numaralı fıkrasındaki, *"Görsel veya işitsel yayınlarda da bu maddenin üçüncü fıkrası hükmü uygulanır. Görsel ve işitsel yayın, mağdurun yerleşim yerinde ve oturduğu yerde işitilmiş veya görülmüşse o yer mahkemesi de yetkilidir"* hükmüne, internet ortamında gerçekleştirilen suçlar da girmektedir. Çünkü, maddedeki "görsel veya işitsel yayın" kavramında, yayının çeşidi değil, niteliği ve sonucu önemlidir. İnternet de, görsel bir yayındır ve bu nedenle, internet yoluyla işlenen bir suçta, failin internete girerek suçu işlediği yer mahkemesinin yanında, mağdurun kullandığı bilgisayarının bulunduğu yer mahkemesi de yetkili olacaktır.

CMK'nın 12/5 maddesinde yollama yapılan (3) numaralı fıkrasındaki, *"Suç, ülkede yayımlanan bir basılı eserle işlenmişse yetki, eserin yayım merkezi olan yer mahkemesine aittir. Ancak, aynı eserin birden çok yerde basılması durumunda suç, eserin yayım merkezi dısındaki baskısında meydana gelmişse, bu suç için eserin basıldığı yer mahkemesi de yetkilidir"* hükmü, internet yoluyla işlenen suçlarda, "eserin yayım merkezi" ve "eserin yayım merkezi dışındaki baskısı" kavramları bakımından ele alınmalıdır.

Eserin yayım merkezi, internette her zaman kolaylıkla belirlenemeyebilir. İnternette bir web sitesi tarafından yapılan (haber, yorum, reklam vs gibi) yayınlarda, yayın merkezi web sitesinin kurulduğu yerdir denilebilir. Örneğin, internet ortamındaki bir şirkete ait web sitesinden suç işlenmişse, bu site için eserin yayım merkezi, web sitesinin şirket tarafından kullanıldığı yer olarak düşünülebilir.

Ancak, sanal alemdeki web sitesi merkezi, basılmış eserin merkezi kadar kolay bir yapı içermez. İnternet ortamında, internete bağlanan herhangi bir kişi (istisnai olarak bir engel yoksa) rahatlıkla bir web sitesi kurabilir. Kurulan bu site,

---

[190] 1412 sayılı CMUK'nın 8. maddesine göre

çoğunlukla bir ana web sitesi üzerinden kurulmaktadır ve bu sitenin kurulduğu adla faaliyette bulunmaktadır. Bu gibi hallerde, bir ana web sitesi ve bir de yeni kurulmuş web sitesi bulunmaktadır. Ana web sitesinin kurulduğu merkez belirlenebilir. İnternet kullanıcısının kurduğu web sitesinin merkezi, CMK'nın 12/3. maddesindeki gibi bir yapı taşımaz. 12/3 maddesindeki eserin yayım merkezi, normal şartlarda bir organizasyonu, bir işletmeyi ve alt yapısını anlatır. Oysa, internet kullanıcısının birey olarak kurduğu web sitesinde, kurum yapısı değil, bir kişi söz konusudur. Bu bakımdan, CMK'nın 12/5 yollamasıyla 12/3. maddesindeki, eserin yayım merkezi kavramı, içerik olarak internet ortamında birey tarafından kurulan web sitesine nitelik olarak uymamaktadır. Bu durum, bilişim suçlarının işlendiği alanın (internetin) kendine özgü ve benzersiz yapısından kaynaklanmaktadır.

Siber Suç Sözleşmesinin 22. maddesindeki yargı yetkisiyle ilgili hükümde, Sözleşmeyi onaylayan devletlerin, Sözleşmedeki ceza hukukuyla ilgili 2 ilâ 11. maddelerdeki yargı yetkilerini düzenlerken uymaları gereken ölçütler sunulmuştur. İlk başta ülke sınırlarındaki yetki üzerinde durulmuştur. Buna göre, ulusal devlet sınırları içerisinde işlenen suçlarda yargı yetkisini oluşturmalıdır. Türk hukukunda, tüm suçlar bakımından durum bu şekildedir.[191]

Sözleşmenin 22. maddesindeki diğer bir ölçüt ise, faile göre kişisellik ilkesidir. Buna göre, bir devlet vatandaşı, ülke dışında (başka ülkede) suç işlediğinde, fiil, suçun işlendiği yerde de suç ise, devlet, kendi vatandaşını yargılama yetkisine sahiptir.

Birey tarafından kurulan web sitesinin merkezinin, bireyin web sitesini kurarken kullandığı bilgisayarın bulunduğu yerdir ya da bireyin oturduğu yerdir diyelim. Acaba bu yaklaşım doğru mudur?

İnternet ortamında bir web sitesi kurmak için bireyin oturduğu yerdeki kendi bilgisayarını kullanması şart değildir; herhangi bir internet karedeki veya bir

---

[191] Serap Keskin , **Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi**,(HFM.,. Sayı 1-2, 2001), s.177

şekilde ulaşılan bilgisayar kullanılarak da web sitesi kurulabilir. Üstelik, birey web sitesini Ankara'da kullandığı bilgisayarla internete bağlanarak kurduktan sonra, ikamet ettiği İstanbul'a dönüp, web sitesini burada kullanmaya başlayıp ve bu sitede yaptığı yayınlarla internet ortamında suç işlemekte ise, bu durumda ne olacaktır?

CMK'nın 12/5 yollamasıyla, (3) numaralı fıkradaki eserin yayım merkezi kavramı, bünye itibarıyla her zaman bilişim suçlarına uymamaktadır. Esasında, bu şekilde internet ortamında birey tarafından oluşturulan web siteleriyle işlenen suçlarda, suçun birey tarafından işlendiği yerin, CMKm.12/3 maddesine göre değil, 12/1 maddesine göre belirlenmesi daha yerinde olacaktır.

CMK'nın 12/3 maddesindeki "eserin yayım merkezi dışındaki baskısı" kavramı da, internet ortamında işlenen suçlara uymamaktadır. 12/3. maddesindeki basılı eserlerde (örneğin gazete, dergi gibi) eserin birden çok yerde basılması halinde, farklı basım yerleri de yetkili kılınmaktadır. Oysa, internet ortamındaki yayınlarda, çoğunlukla, yayının farklı baskısı kavramına uygun bir alan düşünülmesi zordur. İnternette yapılan yayın, adı üstünde dünya çapındadır ve bir anda internet ağındaki her yerde aynı yayın görünmektedir. Bu bakımdan İstanbul merkezli internet ortamındaki bir yayında, bunun Ankara için ayrı yayını söz konusu değildir. Tüm bu nedenlerle, CMK'nın 12/5 yollamasıyla, 12/3 fıkrasındaki hüküm, bünye itibarıyla intternet ortamındaki suç teşkil eden yayınlara uymamaktadır.

Suçun Ülke Dışından İşlenmesi;

Bilişim suçlarının en sorunlu ve tartışmalı konularından birisi, ülke dışından işlenen bilişim suçlarında yargı yetkisinin ve dolayısıyla yetkili mahkemenin belirlenmesidir. Dünya çapındaki bilişim ağının ismi olan internet, bilişim suçlarında yargı yetkisini içinden çıkılmaz bir hâle getirmiştir, internette, fiziksel anlamdaki ülke sınırları ortadan kalmış, dünya çapında iletişim sanal ortamda anlık bir zaman diliminde yüz yüze hâle gelmiştir. İnternetle, geleneksel ceza yargılanmasındaki yargı yetkisi, bir bakıma nostalji olma yolundadır. Üstelik, bu konudaki her tespit ya da çözüm yaklaşımları, belki ifade edildiği (tartışıldığı) anda bile,

bilişim teknolojisindeki artarak devam eden ilerlemeler karşısında, yeni yaklaşım niteliğini taşımamaktadır. Bütün bu olumsuzluklara ve zorluklara rağmen, dünya çapında konu üzerindeki tartışmalar devam etmektedir.

İnternet ortamında işlenen suçların yaygın olanları, malî içerikli suçlar olarak belirtilebilir. Özellikle internet ortamındaki elektronik ticaret (e-ticaret) (e-business), bankacılık işlemlerinin online olarak internet üzerinden gerçekleştirilmesi, malî suçların öne çıkmasında etkili olmaktadır.

Yargı yetkisi, mahkemenin, bir davanın kovuşturma evresinde duruşmasını yapmak, davanın çözümünü tartışmak ve bir karar vermek otoritesidir. Internet ortamında işlenen suçlarda, dünyanın herhangi bir yerinden, mesafe ve fiziksel sınırlar olmaksızın suç işlenebilmektedir.[192]

Internet ortamında işlenen suçlardaki yargı yetkisi sorunu, geleneksel hukuk uygulayıcılarını ve yasama organlarını en önemli sorunlarından birisi durumundadır. Eğer uluslararası suçlara karşı etkili bir mücadele ile farklı devletlerden polis ve kanun uygulayıcıları arasında uluslararası işbirliği oluşturulabilire, egemenlik bir noktada toplanmış olacaktır ve bu suçlara karşı daha güçlü mücadele yapılabilecektir.[193]

Mahkemelerin karar verme yetkisini içeren yargı yetkisi, genel olarak coğrafi egemenliğe dayalıdır. İnternette işlenen suçlarda ise, coğrafi sınırlar farklıdır. Meksika'daki birisi tarafından yazılan suç içeren e-posta, Italya'daki internet sunucusu vasıtasıyla isviçre'de okunduğunda, Norveçlilerin itibarını zedeleyen nitelikte ise, burada yargı yetkisi nasıl belirlenecektir? Özellikle, internet ortamında, bundan çok daha karmaşık sıklıkla görülen suçlarda, yargı yetkisi sorununun içerisinden nasıl çıkılacaktır? Norveçli kişiler, hangi mahkemeye başvurabilir? italya'ya mı, isviçre'ye mi, Meksika'ya mı, yoksa Norveç'e mi? Mağdur için Norveç mahkemesine başvurabilmek en uygun gözde çözüm olabilir.

---

[192] Gerald R.Ferrera, - Stephan D .Lıchtenstein,.- Margo E. Reder, K.- Ray August, - William T . Schiano, **a.g.e.**, s.15

[193] Toby Graham, , **E-fraud and Jurisdiction**, (www.taylorwessing.com/topical/dispute_resolution/efraud_and3fisdiction_winter2001.html+computer+crirne+court+jurisdiction+dispute&hl=tr(5.9.2004)

Fakat, bu olayda, Meksika'da işlenen, İtalya'daki web sunucusunun aracı olduğu ve suç içeren e-postanın isviçre'de okunduğu bir yapıda, Norveç mahkemesi nasıl yargı yetkisine sahip olabilecektir? Örnekteki fiil, çocuk pornografisi ya da dolandırıcılık veya sahtecilik gibi farklı bir suç da olabilirdi. Bu durumda yargı yetkisi sorunu nasıl çözümlenecektir?[194]

Bir görüşe göre, yargı yetkisi, özellikle internet ortamında işlenen suçlarda, yalnızca bir adres olarak ulaşılabilen sanığa karşı uygulanamaz.[195]

Başka bir göre, internet yoluyla ülke dışından işlenen suçlarda, kural olarak ancak o yayının yapıldığı ülkede suç işlenmiş sayılır ve bu yayının sonucu başka ülkelerde ortaya çıkmış olsa bile, bu ülkeler suçun işlendiği yer olarak kabul edilemezler. Çünkü, bu tür suçlar "sonuçsuz suçlar" ya da "sonucu harekete bitişik suçlar" niteliğindedir ve hareketin yapılmasıyla birlikte suç tamamlanmış olduğu için, bu suçlarda bağlama noktası olacak sonucun gerçekleştiği yer kıstası uygulanamaz.[196]

Karşı görüşe göre ise, internetin global yapısı gözetildiğinde, internet yoluyla işlenen suçlarda, yalnızca suç teşkil eden yayının yapıldığı yeri yetkili saymak yerinde olmaz; bu suçlar "mesafe suçlan" niteliğindedir ve hareket ile netice çok farklı yerlerde gerçekleşebilir. Burada önemli olan failin kastıdır. Fail, hareketinin sonuçlarının farklı mesafelerde (ülkelerde) gerçekleşmesini istemişse, sonucun gerçekleştiği her ülke de yetkili sayılacaktır. Bu bağlamda, Türkiye dışından internet yoluyla işlenen bir suç, sonuçlarını ülkemizde de göstermişse, bu suçta Türkiye mahkemeleri de yetkili sayılacaktır.[197]

---

[194] Henry H.Perritt, , **Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction**,(www.kentlaw.edu/cyberlaw/resources/interjuris.html+computer +crime+jurisdiction&hl=tr (11.11.2004)

[195] I. Louise Shelley , **a.g.e.**, s.20

[196] Bu görüş için bkz.: Hasan Sinar, **internet ve Ceza Hukuku**, (Beta Basım, İstanbul, 200*r), s. 127

[197] Hasan Sinar, **a.g.e.**, s.127-127

Bir başka görüşe göre ise, bu konuda evrensel yargı yetkisi düşünülmelidir. Çünkü, internet ortamında işlenen suçlarda dünya, global bir köye dönüşmüştür. Dünyanın herhangi bir yerindeki (internete bağlanan) bilgisayardan pek çok ülkeyi etkileyen suçlar işlenmektedir. Böylesi bir durumda ülkesel yargı yetkisiyle sorunu çözebilmek mümkün değildir. Evrensel yargı yetkisinin kapsamlı şekilde değerlendirilmesi ve yetki konusu tartışılmalıdır. Evrensel yargı yetkisine tâbi (klasik) suçlar konusunda da tam bir görüş birliği sağlanamamıştır. Bununla birlikte, evrensel yargı yetkisinin dayanağı olan çeşitli anlaşmalarda, suçluların iadesi, dava açmak yükümlülüğü gibi dikkate değer farklı seçenekler yer almaktadır. Siber suçlarda devletler yalnızca evrensel yargı yetkisine izin vermekle kalmamalı, aynı zamanda farklı seçeneklere bağlı olarak uluslararası hukuk altında suçlarla ilgili yargı yetkisi uygulamalarını gerçekleştirmelidirler. Nuremberg Mahkemesi, işgal edilmiş topraklar altındaki yasama hakkının bir kısmı olarak, çeşitli ülkelerin yasama gücünün egemenlik uygulamalarını Nuremberg Karakteri olarak ortaya koymuştur. Tersine, eski Yugoslavya'yla ilgili komisyon uzmanları Nuremberg Mahkemesine bir örnek olarak dayanmışlar; ilgili devletler, ulusal yargı yetkilerini, ulusal ilkeler doğrultusunda, uluslararası mahkemeye devretmişlerdir .[198]

İnternet ortamında (yukarıdaki örnekte olduğu gibi) farklı ülkeleri içeren suçlarda, failin suçu işlediği fiziksel olarak bulunduğu ülkenin mahkemesi yalnızca yetkili olsun denebilir mi? Bu soruya evet denilirse, yargılamanın yapıldığı yerde, suçlunun iadesi, failin suçlanmasına ilişkin ekstra yasal fiziksel araçların temini, yargılama yerinde nasıl kullanılabilecektir? Davada hangi ülkenin ceza mevzuatı uygulanacaktır? Bu davada (yukarıdaki örnek olayda) Norveçliler büyük oranda failin cezalandırılmasını istemektedirler ve failin fiziksel olarak bulunduğu Meksika'nın davaya ilgisi oldukça zayıftır; fakat yasama organlan çoğunlukla suçların tanımına bağlı yargı yetkisine odaklanırlar ve ceza mahkemeleri de, diğer bir ülkenin yargı yetkisini ilgilendiren davada yargı yetkisini nadiren kullanırlar. Bu sorunlara tatminkar cevap verilememesi, internet ortamında işlenen suçlarda, aracıların sorumluluğunu artırma yaklaşımını yoğunlaştırmaktadır; çünkü, tatminsiz

---

[198] Hans Corell , **The Challenge of Borderless Cyber-Çrime**, (The Rule of Law in the Global Village, Issues of Sovereignty and Universality, Syposium on the Occasion of the Signing of the United Nations Convention Against Transnational Organized Crime, http://www.unodc.org/palermo/corein.doc (3.3.2005).

cevaplar, internet ortamında hizmet veren organizatörlere karşı yasal yapı hakkında belirsizliği artırmaktadır. Diğer yandan, internet ortamında faili (yazarı) bilinmeyen suçlarda, mağdur için, internet servis sağlayıcılarına yönelmeden başka çare kalmamaktadır. Eğer aracının kimliği de belirlenemiyorsa, kusuru olmayan mağdurun suçu sineye çekmekten başka çaresi kalmamaktadır. Bu sorunlar hakkında kesin ve tatminkar bir çözüm yolu bulmak mümkün görünmemektedir.

4.10.Bilişim Suçlarıyla Mücadelede işbirliği

Bilişim suçlarıyla mücadelede değişik boyutlarda işbirliği gerekmektedir. Bu işbirliğini iki ana grupta toplamak mümkündür. Birincisi, ulusal düzeyde, ikincisi ise, uluslararası alanda işbirliğidir.

4.10.1. Ulusal Düzeydeki İşbirliği

Bilişim suçlarıyla mücadelede ulusal düzeyde işbirliği, birinci ve önemli bir adımdır. Klâsik suçlardan farklı olarak bu suçlarla mücadelede, yalnızca adlî kolluk görevlilerinin çabası yeterli değildir. Ulusal düzeydeki işbirliğini şu ana başlıklarda toplamak mümkündür:

1. Suçla mücadele birimleri ile yargı kurumları arasında işbirliği,
2. Suçla mücadele birimleri ile özel sektör arasında işbirliği,
3. Suçla mücadele birimleri ile suçtan zarar gören veya risk altındaki gerçek kişiler ve organizasyonlar arasında işbirliği,
4. Bilişim suçu sanık ve mahkûmlarıyla işbirliği.

Esasında, bilişim suçlarıyla uğraşan güvenlik görevlileri, aşağıdaki faktörlerden dolayı yıldırıcı (ürkütücü) bir görevle karşı karşıyadırlar. Bu faktörler şunlardır:

a. Bilişim teknolojisindeki çok hızlı gelişmeler,
b. Her hafta 5-6 çeşit yeni bilişim suçu türünün ya da güvenlik açığının ortaya çıktığı göz önüne alındığında çok hızlı şekilde değişen bilişim suçu tehditleri,

c. Bilgisayar donanım ve yazılımlarındaki her geçen gün ortaya çıkan yeni tehditler ve saldırıya açık yapılar,

d. Bilgisayar ya da bilişim sistemleri kullanılarak sürekli artan dolandırıcılık, yetkisiz erişim ve diğer bilişim suçları.[199]

Bilişim suçlarıyla ilgili bu akıl almaz artış karşısında, suçla mücadelede görevli personelin düzenli periyodik eğitime alınması gerekli ise de, yeterli olamamaktadır. Çünkü, verilen eğitimler, eğitimin başladığı andan önceki boyutla ilgilidir ve bu eğitimin verilebilmesi de zaman almaktadır. Örneğin, 3 ya da 6 aylık eğitime tâbi tutulan personel, eğitimini tamamladığında, eğitim gördüğü (3 ya da 6 aylık) dönemdeki bilişim suçlarındaki yeni gelişmelere yabancı kalmaktadır. Buysa, her hafta 5-6 yeni bilişim suçunun ortaya çıktığı düşünüldüğünde, sürekli bir yabancı kalınan kısır döngüye neden olmaktadır.

Sonuç olarak, bilişim suçlarının kendisine özgü hızla üreyen kapsamı, bu suçla mücadelede suç işleyenlerle işbirliğini zorunlu kılmaktadır. Bir bakıma, adlî kolluk görevlilerinin bu işbirliği, en hızlı eğitim olanaklarından birisi olarak nitelendirilebilir.

4.10.2. Uluslar arası işbirliği

Internet, çocuk pornosundan, terörist faaliyetlere kadar pek çok türde sınırı olmayan bir suç işleme ortamı sağlamaktadır. Bu suçlarlar mücadelede ve bu suçlar hakkında yapılan soruşturmalarda, karşılıklı hukukî yardımlaşma ve işbirliği büyük önem taşımaktadır. Bu işbirliği federal yapıdaki (örneğin ABD gibi) devletlerde, önce eyaletler (federe devletler) arasında ve sonra da dünya çapında devletler arasında olmalıdır. Bu işbirliği, sadece bu suçların dünyanın herhangi bir yerinden işlenebilmesinden değil, belki de öncelikle bilgisayarın birkaç tuşuna basılarak hem sistemlere ve hem de insan hayatına yönelen tehditkar özelliğinden kaynaklanmaktadır.[200]

---

[199] Rosa Codına, a.g.e., s.2f

[200] Montes Javıer , **Confronting Cyber-Crime**, (Americas, September/October 2003, Vol.55, Issue 5), s.53

ABD'de, bilişim suçlarıyla mücadelede uluslararası işbirliği Adalet Bakanlığı öncülüğünde yapılmaktadır. İnternet dolandırıcılığı konusunda G-8'ler olarak bilinen ülkelerle toplantılar yapılmış ve bu ülkelerin adalet bakanlarının katıldığı toplantılar sonunda, elektronik ticaretin gelişme ve büyümesine, internet dolandırıcılığı önemli bir tehdit olarak tanımlanmış, bu tehdide karşı, önlemler alınması, kapsamlı araştırmalar yapılması ve soruşturmalar yürütülmesi kararlaştırılmıştır. G-8 ülkeleri arasındaki işbirliğinde, "Lyon Group" adıyla oluşturulan Grup tarafından kurulan yüksek teknoloji alt komisyonları ve projelerle bilişim suçları takip edilecektir .[201]

1971 yılında, ABD, İngiltere, Kanada, Avustralya ile Yeni Zelanda arasında, "Echelon" ismiyle uydu kaynaklı haberleşmeye dayanan karşılıklı bilgi paylaşımı başlatılmıştır. Projenin kapasitesi ve öncelikleri zamanla genişlemiş, global bir yapıda pek çok sahada iletişimi kapsar hâle gelmiştir. Günümüzde Echelon'un, her gün üç milyar civarında telefon, e-mail mesajları, internet üzerinden yükleme işlemleri, uydu üzerinden iletişimi vs.yi kapsadığı tahmin edilmektedir. Sistem, bütün bu rastlantısal iletimlerin tümünü bir araya getirmekte, bunları süzgeçten geçirmekte ve sanal alemdeki bilgi programlarını takip etmektedir. Bazı kaynaklar Echelon'un internet üzerindeki bilgi akışının yaklaşık % 90'nı taradığını belirtmektedirler.[202]

Bununla birlikte, Echelon'un mevcut hedeflerinin ve çalışmalarının yerel iletişimle sınırlı kalıp kalmadığı bilinmemekle birlikte, Echelon, çeşitli yollardan bilgi toplamayı sürdürmektedir. Echelon benzeri projeler hayata geçirilmeye çalışılmaktadır. Örneğin, Rusya, Fransa, İsrail, Hindistan, Pakistan ve bir kısım ülkelerin benzer bir proje üzerinde çalıştıkları iddia edilmektedir.[203]

---

[201] Bruce Swartz, **Internet fraud** , (FDCH Congressional Testimony,2001) s.3

[202] David J.Loundy , **Computer Crime, Information Warfare and Economic Espionage**, (Carolina Academic Press, USA., 2003,) s.664

[203] David J.Loundy , **a.g.e.**, s.664, 670.

Bu projeyle (ABD tarafından), dünyadaki tüm faks, telefon, telgraf, e-posta, mobil telefon ve internet ağı dinlenmekte (takip edilmekte) ve dünya çapındaki siber mafyanın boyutları tespit edilmeye çalışılmaktadır.[204]

Avrupa Konseyi Siber Suç Sözleşmesi, Avrupa Konseyine üye ülkeler ve bu belgeyi imza eden diğer ülkeler (Avrupa Konseyine üye olmayan; ABD, Japonya, Kanada ve Güney Afrika) arasında daha geniş bir birlik sağlamak olduğu düşüncesinden hareketle; bu Sözleşmeye taraf olan diğer ülkelerle işbirliğinin geliştirilmesini, ortak bir ceza politikasının kabul edilmesini amaçlamaktadır.[205]

Sözleşmenin "Uluslararası işbirliği" başlıklı III. Babının "Uluslararası işbirliği ile ilgili genel prensipler" şeklindeki (1. Başlığında) 23. maddede;

"Taraf devletler birbirleriyle, bu babda belirtilen koşullar çerçevesinde, tek tip olarak ya da karşılık şekilde kabul edilen anlaşmaları ve suça karşı uluslararası işbirliği kurumlarını kullanarak, bilgisayar sistem ve verileriyle ilişkili suçların soruşturulması ve hukukî işlemlerin gerçekleştirilmesi ya da bir suçla ilgili elektronik formdaki delillerin elde edilmesi amacıyla en üst seviyede işbirliğine gitmelidir" hükmü yer almaktadır.

Hedeflenen uluslararası işbirliğini istenilen düzeyde sağlamak kolay değildir. Öncelikle, işbirliğine gidecek devletlerin mevzuatlarının birbiriyle (özellikle fiili suç sayma konusunda) uyumlu olması gerekmektedir, işbirliği istenilen fiil, devletlerden birisinde suç değilse, işbirliği baştan imkânsız hâle gelmektedir.

İşbirliği isteyen devlete gerekli karşılığı verebilmek için, karşı tarafın bilişimle ilgili talepleri zamanında anlayıp, gerekli işlemleri yapması gerekmektedir.

---

[204] Mustafa Karabal, **Bilişim Suçları ve Turk Polis Teşkilatı**, (http://www.turkhukuksitesi.com/hukukforum/art_showarticle (2.2.2005).

[205] Sözleşmenin Önsözünden; ayrıca bu konuda bkz.: Durmuş Tezcan, **Internet Karşısında Özel Hayatın Korunması ve Adlî Yardımlaşma**, (Uluslararası Internet Hukuku Sempozyumu, 21-22 Mayıs 2001, DEÜ.yayını, İzmir, 2002), s.539

Bu nedenle, işbirliği içerisinde olacak devletlerin bilişimle ilgili teknik yapıları ve bu konudaki birimlerinin özellikleri de işbirliğinde önemli etkiye sahiptir.

Bilişim suçlarıyla dünya çapında mücadele edebilmek için, bilişim teknolojisini kullanan tüm devletlerle işbirliği gerekmektedir. Böyle bir işbirliği sağlanamadığı sürece bilişim suçu sanıkları, bu işbirliğinin olmadığı devletlere yönelerek, buralardan suç işlemeyi tercih edeceklerdir.

4.11.Avrupa Konseyi Siber Suç Sözleşmesinde İnteraktif Dolandırıcılık

Avrupa Konseyi Siber Suç Sözleşmesi, dışişleri bakanlarınca 8 Kasım 2001 tarihinde kabul edilmiş ve 23 Kasım 2001 tarihinde Macaristan'ın Budapeşte kentinde imzaya açılmıştır. 26 ülkenin temsilci bakanları ile birlikte Kanada, Japonya, Güney Afrika ve ABD tarafından Sözleşme imzalanmış,[206] 1 Temmuz 2004 tarihinde Sözleşme yürürlüğe girmiş bulunmaktadır.[207] Sözleşme, Türkiye tarafından imzalanmamıştır.

Sözleşmenin 7. maddesinde, "Her bir taraf devlet, bir hak olmaksızın kaşıdı olarak yapılan, açıkça okunabilir ve anlaşılabilir olup olmadığına bakmaksızın, yasal amaçlar için kullanılması ve ele alınması niyetiyle sahte veriler olarak sonuçlanan bilgisayar verilerinin girilmesi, değiştirilmesi, silinmesi veya yerlerinden kaldırmasına yönelik fiilleri gerekli yasal ve benzeri önlemlerle iç hukukunda birer suç eylemi olarak ortaya koymalıdır. Bir taraf devlet suç sorumluluğunun yüklenmesinden önce sahtekârlık veya benzeri bir kötü niyeti aramaya gerek duyabilir" denilmektedir.

Bu maddedeki suç sayılacak fiilde, "yasal amaçlar için kullanılması ve ele alınması" saiki ön koşul niteliğindedir ve belgelerdeki sahtecilik suçunun, bilgisayar ortamındaki yansıması söz konusudur. Burada, elektronik ortamdaki verilerin doğruluğu ve bütünlüğü korunmak istenmektedir. Bu noktada madde, elektronik delillerin başta yargı mercileri olmak üzere, yasal alanda

[206] Schjolberg, (8.8.2004); http://conventions.coe.int (20.10.2004)

[207] http://conventions.coe.int (20.10.2004)

kullanılabilmesine de katkı sağlamayı amaçlamaktadır. 7. maddede, isteyen taraf devletin, "sahtekârlık veya benzeri bir kötü niyeti" suçun işlenmesinde arayabilme olanağı da getirilmiştir.

Sözleşmenin 7. maddesinde,

"Her bir taraf devlet, bir hak olmaksızın kasıtlı olarak yapılan kendi veya başkasına ekonomik bir menfaat temin etmek kötü niyetiyle veya dolandırıcılık niyetiyle diğer bir kişinin mal kaybına sebep olan,

a. Her türlü bilgisayar veri girişi, değiştirilmesi, silinmesi ve yerinden kaldırılması,
b. Bir bilgisayar sisteminin çalışmasına yönelik her türlü müdahale fiillerini gerekli yasal ve benzeri önlemlerle iç hukukunda birer suç eylemi olarak ortaya koymalıdır" hükmü yer almaktadır.

Sözleşmenin 8. maddesi, önceki maddelerinden örneğin, Sözleşmenin 4. maddesindeki verilere müdahale, 5. maddesindeki sistemlere müdahaleden daha özel bir nitelik taşımaktadır. Örneğin, Sözleşmenin hem 4. ve hem de 8. maddesine uyan bir fiil söz konusu olduğunda, failin kastına (saikine) bakılacaktır. Eğer, failde, "kendi veya başkasına ekonomik bir menfaat temin etmek kötü niyeti veya dolandırıcılık niyeti" söz konusu ise, 4. madde değil, 8. madde esas alınacaktır.

Bilişim dolandırıcılığının üzerinde anlaşma sağlanabilmiş ortak bir tanımı olduğunu söylemek mümkün değildir. Bu suçun en temel özelliği dikkate alındığında bilişim dolandırıcılığı, bilgisayar bağlantısıyla yapılan her türlü dolandırıcılık fiilleri olarak tanımlanabilir. Esasında, bilişim dolandırıcılığının bu genel tanımını, özelleştirmek de, bilişim teknolojisindeki ilerlemeler karşısında yerinde bir yaklaşım olmayacaktır.[208] Nitekim, Sözleşmenin 8. maddesinde de, bu yaklaşım sergilenmektedir.

---

[208] Aynı görüş için bkz.: Peter Quest , **Computer Fraud**, (The Computer Law and Security Report, September-October 1990-91, 3 CLSR), s.19

Bilişim ve özellikle internet, klâsik dolandırıcılık suçlarında ve bu alana özgü dolandırıcılık suçlarında çok sayıda olanaklara açık bir yapı oluşturmaktadır. Özellikle, bilişim alanında kişisel (gizli) bilgilerin elde edilmesinde dolandırıcılık fiilleri en sorunlu konulardandır. Bilişim suçlarının türleri arasında da, bilgisayar bağlantılı dolandırıcılık suçları önemli bir yer tutmaktadır. Kredi kartlarına yönelik dolandırıcılık fiilleri ise en çok ilgi çekici alanlardandır.[209]

Internet dolandırıcılığı, dolandırıcılık fiillerinin bütün şekillerini içermektedir ve beyaz yaka suçlarının en yaygın olarak internette işlenen suç türünü oluşturmaktadır. İnternete, neredeyse sıfır maliyetle milyonlarca insanın anında girebilmesi, hem internete girilen ülkede ve hem de dünya çapında anında iletişim ve ulaşım olanakları, dolandırıcılık maksadı olan kötü niyetli kişiler için inanılmaz çekici suç ortamı sağlamaktadır.[210]

İnternetteki dolandırıcılıkların % 60'ı nakit ağırlıklıdır ve çek, ödeme emri, kredi kartı gibi ödeme araçları söz konusudur.[211] Para, dolandırıcıların uhtesine geçtikten sonra, artık geri alınabilmesi neredeyse imkânsız gibidir. İnternetteki (kredi kartıyla ödemeli) mal satımına yönelik dolandırıcılıklarda, satın alınan mallar, ya hiç gelmemekte veya ayıplı ya da satış ilanındaki niteliklere uygun olmayan şekilde gelmektedir.[212]

---

[209] Gordon Stevenson, **a.g.e.**, s.13; saunders, Kurt M.-ZUCKER, Bruce, *"Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deference Act"*, International Review of Law Computers & Technology, Vol.13, No.2,1999, s.183-185; LYNNE, s.1-5; PHILIPPSOHN, s.7-9

[210] Bruce Swartz,**a.g.e.**, s.1-2

[211] Internet ortamında, "elektronik para" kavramı ortaya çıkmıştır. Elektronik para, "chip kart (somut) veya bilgisayara (virtüel) kopyalanabilen ve ödeme vasıtası olarak kabul edilen bir para birimi" veya "internet üzerinden para transferini mümkün kılan ödeme sistemleri" olarak ifade edilebilir; Leyla KESER-BERBER, **Elektronik Ödeme Araçları, Elektronik Paranın Merkez Bankasının Para Politikası ve Kara Para Aklama Açısından Değerlendirilmesi**, (Uluslararası internet Hukuku Sempozyumu, 21-22 Mayıs 2001, DEÜ.yayını, İzmir, 2002), s.229

[212] Laurent Belsie,**Two Best Defenses Againts Online Fraud: Caution and Credit**, (Christian Science Monitor, Vol.89, Issue 204, 9.16.1997), s.15

SONUÇ VE DEĞERLENDİRME

1.ÜLKEMİZDE İNTERAKTİF DOLANDIRICILIK İSTATİSTİKLERİ

S.N	İL	TOPLAM OLAY	FAİLİ BELLİ	FAİLİ MEÇHUL
1	ADANA	60	55	5
2	ANKARA	38	36	2
3	ANTALYA	50	49	1
4	BURSA	16	15	1
5	K.MARAŞ	17	14	3
6	KONYA	22	20	2
7	MERSİN	73	15	58
8	ESKİŞEHİR	3	3	0
9	İSTANBUL	787	609	178
10	İZMİR	16	15	1

TÜRKİYE GENELİ		
TOPLAM OLAY	FAİLİ BELLİ	FAİLİ MEÇHUL
1218	990	227

YAKALANAN TOPLAM:886							
T.C VATANDAŞI				YABANCI			
18 YAŞ ALTI		18 YAŞ ÜSTÜ		18 YAŞ ALTI		18 YAŞ ÜSTÜ	
ERKEK	KIZ	ERKEK	KIZ	ERKEK	KIZ	ERKEK	KIZ
6	0	783	79	1	0	11	6

Şekil 15: 2006 yılı Türkiye İnteraktif Dolandırıcılık verileri [213]

YORUM:

- Olayların bir çoğunun faili(şüphelisinin) tespit edildiği
- Bu dolandırıcılık eyleminin İstanbul, Adana,Mersin eksenli gerçekleştirildiği
- İzmir ve Ankara'da interaktif dolandırıcılık eyleminin fazla olmadığı,
- Suça genellikle 18 yaşından büyük ,cinsiyeti erkek ve ve uyruğu T.C olan şahısların iştirak ettiği,

[213] Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığından alınmıştır.

S.N	İL	TOPLAM OLAY	FAİLİ BELLİ	FAİLİ MEÇHUL
1	ADANA	71	70	1
2	ANKARA	31	28	3
3	ANTALYA	29	28	1
4	BURSA	18	17	1
5	K.MARAŞ	86	83	3
6	ADIYAMAN	37	31	6
7	MERSİN	122	81	41
8	G.ANTEP	73	67	6
9	İSTANBUL	1010	737	273
10	İZMİR	25	23	2

TÜRKİYE GENELİ		
TOPLAM OLAY	FAİLİ BELLİ	FAİLİ MEÇHUL
1743	1286	457

YAKALANAN TOPLAM:1067							
T.C VATANDAŞI				YABANCI			
18 YAŞ ALTI		18 YAŞ ÜSTÜ		18 YAŞ ALTI		18 YAŞ ÜSTÜ	
ERKEK	KIZ	ERKEK	KIZ	ERKEK	KIZ	ERKEK	KIZ
11	0	943	107	2	0	3	1

Şekil 16: 2007 yılı Türkiye İnteraktif Dolandırıcılık verileri

YORUM:

- 2005 yılına göre olay sayısının %50 oranında arttığı
- Faili belli olmayan olay sayısının %200 oranında arttığı
- Mersin ilinde %100'e yakın bir oranla olaylarda artış gözlemlendiği
- Dolandırıcılık eyleminin odağının İstanbul ilinde olduğu ülke genelinde gerçekleşen olayların yaklaşık olarak %70 nin bu ilimizde gerçekleştiği
- İşlenen suçun Doğu Anadolu Bölgesinde Adıyaman ilimiz ile keşfinin gerçekleşmesi
- 2005 yılına göre yakalanan şüpheli oranında %20 lik bir artışın olduğu, suça bayan katılımının arttığı,yabancı uyruklu katılımın azaldığı

S.N	İL	TOPLAM OLAY	FAİLİ BELLİ	FAİLİ MEÇHUL
1	ADANA	36	31	5
2	ANKARA	16	16	0
3	ANTALYA	28	26	2
4	BURSA	6	5	1
5	K.MARAŞ	11	9	2
6	ADIYAMAN	36	25	11
7	MERSİN	56	39	17
8	G.ANTEP	52	51	1
9	İSTANBUL	1789	1207	582
10	İZMİR	17	5	12

TÜRKİYE GENELİ		
TOPLAM OLAY	FAİLİ BELLİ	FAİLİ MEÇHUL
2224	1533	691

YAKALANAN TOPLAM:1226							
T.C VATANDAŞI				YABANCI			
18 YAŞ ALTI		18 YAŞ ÜSTÜ		18 YAŞ ALTI		18 YAŞ ÜSTÜ	
ERKEK	KIZ	ERKEK	KIZ	ERKEK	KIZ	ERKEK	KIZ
15	1	1046	149	3	0	10	2

Şekil 17: 2008 yılı Türkiye İnteraktif Dolandırıcılık verileri

YORUM:

- 2006 yılına göre olay sayısının %30 oranında arttığı
- Faili belli olmayan olay sayısının %50 oranında arttığı
- Suçun yoğun işlendiği Mersin ilinde oranda düşüşün gözlendiği
- İstanbul ilinde suçun giderek daha fazla işlenmeye başladığı
- İç Anadolu , Akdeniz , Ege bölgelerinde suçun kontrol altında tutulduğu
- 2006 yılına göre yakalanan şahıslarda %25 lik bir artışın gözlemlendiği, bayan katılımının artmaya devam ettiği

2.DEĞERLENDİRME VE ÖNERİLER

Ülkemizde istatistiklere bakıldığında İnteraktif Dolandırıcılık eyleminin teknolojik gelişime paralel olarak yaygınlaştığı görülmektedir.Bu konuyla ilgili polisiye tedbirler ne kadar fazla olursa olsun, teknolojinin getirdiği kolaylıklar ile suçluların saklanabilmesi kolaylaşmakta ve eylemin daha çoğalması görülmektedir. Bu bakımdan Teknolojik , Hukuki, Kavramsal tedbirlerin artık hayatımıza girmesi gerekmektedir. Bunlar sürekli olarak güncellenmeli ve hayatımızın birer parçası halinde gelmelidir.Tedbirlere ilişkin bir genelleneme yapacak olursak:

- Bilişim suçlarının tanımlaması, ve konuyla ilgili önlemlerin alınması amacıyla ülke düzeyinde uluslar arası ilişki yetkisine sahip teşkilatlanmanın gerçekleşmesi
- Bilişim suçlarında suçlu profilinin ve suçun kriminolojisinin irdelenmesi
- Bilişim suçları ile ilgili olarak kanunlar ile sınırlı kalınmayıp yönetmelikler hazırlanması
- İnteraktif bankacılık ve Online alışverişler ile ilgili olarak oluşturulan teşkilatlanmanın gizlilik kuralları içerisinde denetleme yetkisine sahip olması
- Dijital delillerin muhafazası
- Özellikle İnteraktif Dolandırıcılık konusunda adli mercilerde periyodik olarak bilgilendirme çalışmalarının yapılması
- İnteraktif bankacılık hizmeti veren bankalara ve online alışveriş imkanı sağlayan şirketlere kanuni olarak güvenlik önlemlerinin zorunlu hale getirilmesi
- İnteraktif dolandırıcılık ile ilgili Kitle İletişim Araçlarının bilgilendirici rolü üstlenmesi
- İnternet bankacılığı suçlarının aydınlatılmasında bilgisayar kimliği(IP adresi) ile kullanıcı kimliğinin birlikteliğinin tespiti oldukça önemlidir.
- İnternette banka dolandırıcılığının önüne geçilmesi amacıyla özellikle Avrupa ülkelerinde tanımlanan internet sujeleri (erişim sağlayıcı,içerik sağlayıcı.servis sağlayıcı vb)ve bunların cezai sorumluluğu ülkemizde de açık ve net biçimde belirlenmesi

- Internet bankacılığında kullanıcı şifresini koruma yükümlülüğünün bankaya ait olması
- İnternette banka dolandırıcılığının önlenmesi amacıyla internet cafelerde kayıtları tutan çeşitli programların kullanılması ve denetlenmesi,
- İnternette işlenen özellikle dolandırıcılık suçlarının usulüne ilişkin hukuki süreç Ceza Muhakemesi Kanununda yer almalıdır.

KAYNAKÇA

ESERLER

Adams, Jo-Ann M., **Comment Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet**, 12 Santa Clara Computer-High Tech.L.J., 1996,

Andreano, Frank, P., "The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem", AM. J. CRIM. L, Vol.27:81

Bequai, August, **Computer Crime**, Lexington Books, Massachusetts Toronto, 1978

Blıznyuk, I., **Legal Aspect Of Cyber-Crime**, Bulletin of the National Academy of the Ministry of Internal Affairs No 2, 1999

Burgess, R. C., Small, M. P. **Computer Security In The Workplace**, North Charleston, North Carolina: SEO Pres.2005

Busch, Ed, **Forensics - What To Do After The Break-In**, DSA (Data SystemsAnalysts), Information Technology Solutions for a Global Market, 2001

Berber Keser, Leyla, **Adlî Bilişim**, Yetkin Yayınevi, Ankara, 2004

Belsıe, Laurent, "Two Best Defenses Againts Online Fraud: Caution and Credit", Christian Science Monitor, Vol.89, Issue 204, 9.16.1997

Chandler, Amanda, "The Changing Definition and Image of Hackers in Popular Discourse", International Journal of the Sociology of Law, 24, 1996,

Campbell, Diane Sears, "Focus on Cyber-Fraud", The Internal Auditor, 59, No 1, Şubat 2002,

Carter, David, L, "Computer Crime Categories How Techno-criminals Operate", FBI Law Enforcement Bulletin, v.64, Temmuz 1995

Casey , Eoghan,**Digital Evidence and Computer Crime : Forensic Science and Internet** , Academic Pres, London 2000

Conley, John M.-Bryan, Robert M,, "A Survey of Computer Crime Legislation in the United States, Information & Communications Technology Law", Mart 1999, Vol.8, Issue 1

Comsec, International and Technical Resourc Center, **Computer Forencics and Cyber Investigations**, (power point sunumu), 2004

Castano, S., Fugını Mg., **Database Security**, Milan, Addison-Wesley & ACM Pres,1995

Cohen, Fred, "Computer Fraud Scenarios", Computer & Security, Volume 2003, Issue 1, Ocak 2003,

Codina, Rosa ,**Information Age Crime** ,Haziran 2003

Carrier, Brian, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers", International Journal of Digital Evidence, Volume 1, Issue 4, Ocak 2003

Campbell, Diane Sears, "Focus on Cyber-Fraud", The Internal Auditor, 59, No 1, Şubat 2002

Duff ,Liz – Gardiner ,Simon,**Computer Crime in Global Village: Strategies for Control adn Regulation –in Defence of the Hacker** , International Journal of the Sociaology of Law ,24,1996

Dönmezer, Sulhi, **Ceza Adalet Reformunun İlkeleri** (Ceza Adalet Reformu İlkeleri Sempozyumu, 24-26 Şubat 1972), İstanbul, 1972

Dönmezer, Sulhi, **Toplum bilim**, 11 bası, İstanbul, 1994

Dıtzıon, Robert - Geddes, Elizabeth , Rhodes, Many, "Computer Crimes", American Criminal Law Review, 40 no2, Eylül 2003,

Denning ,Dorothy, **Activism, Hactivism and Cyberterrorism**,Santa Monica,2002

Dokurer, Semih, **Ülkemizde Bilişim Suçlan ve Mücadele Yöntemleri**, www.dikey8.com, (29.06.2004)

Değirmenci, Olgun, **Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi**, LHD., Kasım 2003,

Dolanbay, C., **e-ticaret Strateji ve Yöntemler**, Meteksan Sistem Yayınları Ankara, 2000

Ceza Muhakemesi Usul Kanunu

Ceza Muhakemesi Kanunu

Edwin H. Sultherland-C.E. Gehlke, **Crime and Punishment** (Recent Social Trends in the United States, New York, 1933, s.1116 ve son. Zikreden Reckless, 20)

Etter, Barbara, **Leadership in the Hi-Tech Crime Environment**, Australasian Centre For Policing Research To 2/2002 Pelp At The Aipm Sydney, 14 Ağustos 2002,

Erdönmez, Erhan, **Investigation Of Computer Crimes**, Yayınlanmamış Yüksek Lisans Tezi, University of North Texas, Ağustos 2002,

Erem, Faruk-Danışman, Ahmet-Artuk, Mehmet Emin, **Ceza Hukuku Genel Hükümler**, Seçkin Yayınevi, Ankara, 1997

Ferrara, Gerald R.-Lichtenstein, Stephen D.-Reder, Margo E. K.-August, Ray-Schiano, William T., **Cyber LAW Text and Cases**, South-Westem Colege Publishing, United States, 2001

Ferguson., Aaron J. , **Fostering e-mail security awareness: The West Point carronade**. Educause Quarterly, 28(1), 2005

Gates, Bill; **Dijital Sinir Sistemiyle Düşünce Hızında Çalışmak**, Çeviren:Ali Cevat Akkoyunlu, Doğan Kitapçılık, 4.Baskı, İstanbul, Nisan.1999.

Goodman, Marc D.- Brenner, Susan W., **The Emerging Consensus on Criminal Conduct in Cyberspace**, UCLA Journal of Law and Technology, 3, 2002,

Garfinkel, S., Spafford, G., And Schwartz, A., **Practical Unix & Internet Security**, O'Reilly & Associates, 3rd edition, 2003.

Gabrilovich, E. And Gontmakher, A., **The Homograph Attack**, Communications of the ACM, 45(2):128, Şubat 2002

Ghosh, Ajoy, Guidelines for the Management of IT Evidence, APEC Telecommunications and Information Working Group 29th Meeting 21-26 March 2004 | Hong Kong, China, This paper is a presentation of the recently published Standards Australia handbook

Hatcher, Michael-Mcdannel, Jay-Ostfeld, Stacy, "Computer Crimes", American Criminal Law Review, Vo.36, no.397, 2001

Hosmer, Chet, "Proving the Integrity of Digital Evidence with Time", International Journal of Digital Evidence, Spring 2002 Volume 1

Ippolıto ,Carlo Sarzana, **Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması ,İtalya'daki Durum**(Çev. Vesile Sonay DARAGENLİ) İHFM,Sayı 3,1997

İçel ,Kayıhan - Sokullu/Akıncı ,Füsun - Özgenç ,İzzet - Sözüer ,Adem - Mahmutoğlu ,Fatih S. - Ünver ,Yener, **İçel Suç Teorisi**

Javıer, Montes, **Confronting Cyber-Crime**, Americas, Eylül/Ekim 2003, Vol.55, Issue 5

Ksander, Scott L, **INFORENSICS**, Purdue Univesity, Calvin College Seminar, (power point sunumu), 2003

Kishore Subramanyam, Charles E. Frank, Donald H. Galli **Keyloggers: The Overlooked Threat to Computer Security**

Kurose ,James. F., Ross , Keith W., **Computer Networking**, 2003 Pearson Education, 2. Edition

Keskin, Serap, **Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi**, HFM.,. Sayı 1-2, 2001,

Loren ,D. - Mercer , M.F.S., "Computer Forensic Charasteristics and Presevatyion of Digital Evidence" , Vol 73 ,Number 3, Mart 2004

Loundy, David J., **Computer Crime, Information Warfare and Economic Espionage**, Carolina Academic Press, USA., 2003,

Metchık, Eric, *"A typologyof crime on the internet"*, Security Journal 9, 1997

Moıtra, Soumyo D., **Analysis And Modelling of Cybercirme : Prospects And Potential**, Max Planck Enstitute, 2004

Önemli, Murat, **İnternet Suçlarıyla Mücadele Yöntemleri**, (yayımlanmamış yüksek lisans tezi) TODAİE, Ankara, Nisan 2004, s.4

Öztop ,Esra, **İnternet'in Bireye ve Sosyal Hayata Etkileri,Türkiye'deki Durum,**2002

Özdemir Mehmet- **Bilişim Suçları Ve Mücadelede Karşılaşılan Problemler ve Çözüm Önerileri**

Özen, Muharrem, **Ceza Hukukunda Objektif Sorumluluk**/ US-A Yayıncılık, Ankara, 1998

Quest, Peter, **Computer Fraud**, The Computer Law and Security Report, September-October 1990-91

Potaczala, Michael, **Computer Forensics**, CHS5937 Topics in Forensic Science, 12.6.2001

Reckless, **The Crime Problem**, second edit, New York, 1955,

Romıg Steve, **Forensic Computing**, November 4, 1999, romig@acm.org/(2.4.2004);

Sırabaşı , Volkan, **Internet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (internet Rejimi)**, Adalet Yayınevi, Ankara, 2003

Sultherland ,Edwin H. , Gehlke , C.E., **Crime and Punishment** (Recent Social Trends in the United States, New York, 1933),

Stevenson ,Gordon, "Computer Fraud: Detection and Prevention", Computer Fraud & Security, Volume 2000, Issue 11,1 Aralık 2000

Shelley, I., Louise, "Crime and Corruption in the Digital Age", Journal of International Affairs 51 Vol.2, no.605, Eylül 1998

Shinder ,Debra Littlejohn, **Scene of Cybercrime – Computer Forensics Handbook**, Syngress Publishing, USA, 2002

Stephenson, Peter, **Structured Investigation of Digital Incidents in Complex Computing Environments**, Information Systems Security, Temmuz/Ağustos 2003

Sinar, Hasan, **internet ve Ceza Hukuku**, Beta Basım, İstanbul, 200*r

Swartz ,Bruce, **Internet fraud** , FDCH Congressional Testimony,2001

Toroslu, Nevzat, **Ceza Hukuku**, Savaş Yayınevi, Ankara, 2001,

Tezcan, Durmuş, **Internet Karşısında Özel Hayatın Korunması ve Adlî Yardımlaşma**", Uluslararası Internet Hukuku Sempozyumu, 21-22 Mayıs 2001, DEÜ.yayını, İzmir, 2002

Türk Dil Kurumunun Hazırlamış Olduğu Türkçe Sözlük

Türk Ceza Kanunu

Wall, S. David, **Cathing Cybercriminals : Policing the Internet, International Review of Law Computers**, Volume 12, Number 2,1998,

Widdison, Robin (1997), **Electronic Law Practice: An Exercise in Legal Futurology**", Modern Law Review, N: 60

Wolfe, Henry B., **An Introduction to Computer Forensics: Gathering Evidence in a Computing Environment**, Informing Science Challenges to Informing Clients: A Transdisciplinary Approach, Haziran 2001

Volonıno ,Linda, **Electronnic Evidence And Computer Forensics**, 2003

Yayla, Mehmet, **Uluslararası Platformda ve Türkiye'de Bilişim Suçları: Ankara İl Jandarma Komutanlığında Alan Çalışması**, Kara Harp Okulu Savunma Bilimleri Enstitüsü, (yayımlanmamış yüksek lisans tezi) Ankara, 2004,

İNTERNET ADRESLERİ

http://inet-tr.org.tr/inetconf4/inet98-akgul.html (1.3.2005)

http://www.webhocam.net/konuizle.asp?t=1769 (3.3.2008)

http://www.gencbilim.com/odev/odevgoster.php?il=eskisehir&id=18202 (1.2.2006)

http://www.sayfa.com/forum/showthread.php?t=4086 (2.2.2005)

http://www.haberdefteri.com/haberbak.php?id=9049 (1.7.2006)

http://forum.iyinet.com/guncel-konular-haberler/54386-turkiyede-internet-14-yasinda.html (2.2.2008)

http://www.muttrafik.8m.com/sucpsik.html (1.2.2008)

http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/s/Simmons:G=_J=.html,Çankaya,Ayhan – Bilişim Suçları (2.5.2007)

http://www.bilisimterimleri.com/?arananterim=bilişim&dil=tr (3.4.2007)

http://www.bilisimterimleri.com (3.6.2007)

http://www.caginpolisi.com.tr/24/43-44-45-46.htm,Özdemir Mehmet-Bilişim Suçları Ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler Ve Çözüm Önerileri (1.7.2007)

http://ferruh.mavituna.com/article/?218 (2.5.2007)

http://www.baskent.edu.tr/~cigir/emafya.htm (1.5.2007)

http://www.tbmpd.org.tr/modules.php?name=Sections&op=viewarticle&artid=10&page=1 (2.5.2006)

http://www.olympos.org/article/articleview/261/1/10-Yılmaz,Murat (5.7.2007)

http://www.hp.uab.edu/image_archive/ug/ | http://f27.parsimony.net/forum66647 (2.8.2006)

http://www.fuartakip.com/haberler/index.asp?ID=51 (3.3.2008)

http://www.kom.gov.tr/turkce/gundem.aspx?idd=32 (1.2.2006)

http://www.crime-research.org/articles/Internet_fraud_0405 (3.3.2005)

http://www.keyghost.com (5.3.2007)

http://www.zabforum.com/showthread.php?t=290 (3.6.2007)

http://www.gartner.com/5 about/press releases/asset 71087 11.jsp, (1.4.2007).

http://www.anti-phishing.org/Phishing-dhs-report.pdf, (1.1.2007)

http://securityresponse.symantec.com/avcenter/venc/data/vbs.loveletter.a.html, (3.5.2001)

http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=38&Itemid=28 (3.4.2007)

http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=114&Itemid=34 (1.1.2006)

http://ileriseviye.org/arasayfa.php?inode=phishing.html (3.3.2005)

http://www.olympos.org/article/articleview/1518/1/9/sahte_google_sayfalarina_dikkat (1.7.2006)

http://bilisim.istanbul.edu.tr/makaleler/casusyazilim.htm (3.2.2005)

http://www.akdenizforum.com/showthread.php/trojanlar-trojanlar-hakkinda-hersey-545.html (3.4.2006)

http://www.kom.gov.tr/turkce/gundem.aspx?idd=32 (3.4.2006)

http://www.8sutun.com/node/27841/print (2.9.2007)

http://www.tuncaykarakas.com/print_version.php?id=476 (3.1.2005)

http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=3513306&p=2 (4.4.2006)

http://www.suc.gen.tr/modules.php?name=News&file=article&sid=289 (5.4.2006)

http://www.eosb.org.tr/tr/duyurular.asp?id=680 (1.8.2007)

http://www.bitpipe.com/detail/RES/1129646348_201.html] (26.12.2007)

http://ferruh.mavituna.com/makale/sql-injection-a-giris-ve-sql-injection-nedir/ (25.11.2007)

http://www.forumklas.org/archives.php/Sql-injection-Anlatimi-/5154 (21.10.2007)

http://www.php.net/manual/en/ (22.10.2007)

http://www.bilgiportal.com/v1/idx/50/717/Hukuk/makale/Internette-Biliim-Sularnda-Kullanlan-Metotlar-.html (3.3.2007)

http://www.haylazturk.com/mail-yardim/37167-phishingden-sonra-simdi-de-vhishing-moda.html (3.3.2007)

http://www.sabote.com/archives.php/kablosuz-aglarda-saldiri-ve-guvenlik/6857 (1.1.2008)

http://teknokeyif.wordpress.com/2007/02/08/dns-saldirisi/ (1.11.2007)

http://www.geyikmerkezi.com/coskunoglundan-ulastirma-bakanina-tt-sorularifo-bilisim_haberi_son_haberler4932.html (3.5.2006)

http://en.wikipedia.org/wiki/Internet_fraud (1.11.2007)

http://www.indirsek.com/program.php?progID=1427/Advanced-ZIP-Password-Recovery-4.0 (1.9.2006)

http://www.vbmaster.org/sorular-cevaplar/424-veritabanenda-saklanan-uifrelerin-gvenliri.html (2.2.2007)

http://www.isbank.com.tr/sss/foSikcaSorulanSorular.asp?iKodSikcaSorulanSoru=306 (2.2.2007)

http://www.turkeyhack.org/ssl-security-hakkinda-her-8364-y-t1249.html?s=2b56506afc3aba1ae932525d4677e6d1& (3.4.2006)

http://www.bilgi-yarismasi.com/sanalklavye.html (1.1.2008)

http://www.akbank.com/1125.aspx (2.4.2007)

http://www.eticaretgaranti.com.tr (3.5.2006)

http://www.adambilgisayar.com.tr/ticaret.html (3.5.2006)

http://www.bilisimsurasi.org.tr/home.php?golink=rapor, (18.08.2002), s.293-300

http://www.madran.net/?p=15(2.4.2005)

http://www.computer-forensic.com/(1.3.2005)

http://newfirstsearchoclc.org/images/ WSPL/wsppdf1/ HTML/03, (4.12.2004)

http://www.taylorwessing.com/topical/dispute_resolution/efraud_and3fisdiction_wi nter2001.html+computer+crirne+court+jurisdiction+dispute&hl=tr(5.9.2004)

http://www.kentlaw.edu/cyberlaw/resources/interjuris.html+computer +crime+jurisdiction&hl=tr (11.11.2004)

http://www.unodc.org/ palermo/corein.doc (3.3.2005).

http://conventions.coe.int (20.10.2004)

http://conventions.coe.int (20.10.2004)

http://www.bayar.edu.tr/baum/dokumanlar/bilisimsuclari.pdf

http://www.fbi.gov/ucr/whitecollarforweb.pdf (12.3.2005)

http://www2.als.edu/faculty/dmoriarty/wccdescription.html+%22 white+collar+crime%22+descripti on&hl=tr (3.3.2005),

http:// \AMw.writing-world.c»m/mystery/forensics.shtml+vvhite+collar+crirninal%27s+related+ with+computer+crime&hl=tr (25.1.2005).

http://www.bitpipe.com/detail/RES/1129646348_201.html

http://www.turkhukuksitesi.com/ hukukforum/art_showarticle (2.2.2005)

http://www.nwfusion.com/news/2002/0709schmidthtml (1.10.2004)

http://www2.als.edu/faculty/dmoriarty/wccdescription.html+%22white+collar+crime %22+descripti on&hl=tr (3.3.2005)

http:www.inter.criminology. org.ua/jetspeed_eng/materials/orlovskaya/en/cyber-crime.htm+%22 cyber+crime+concept%22+&hl=tr (10.1.2005)

http://www.law. ankara.edu.tr/yazi, (18.8.2004).

http://rr.sns.org/incident/legal-standarts.php (7.9.2004)

http://css.sfu.ca/update/ethical-hacking.html (2.1.2006)