Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı

Hikmet DİJLE[1], Nurettin DOĞAN[2]

[1]Düzce Anadolu Teknik ve Endüstri Meslek Lisesi, Milli Eğitim Bakanlığı, Düzce, Türkiye
[2] Elektronik ve Bilgisayar Eğitimi Bölümü, Gazi Üniversitesi, Ankara, Türkiye
hdicle@mynet.com, ndogan@gazi.edu.tr
(Geliş/Received: 15.01.2011; Kabul/Accepted: 14.03.2011)

Özet— Bilişim teknolojilerinde meydana gelen gelişmeler birçok alanda insanların yaşam tarzını değiştirmiş ve buna paralel olarak da bilişim teknolojileri ile ilgili işlenen suçlar ortaya çıkmıştır. Böylece suç ve suçlu kavramları yeni boyutlar kazanmıştır. Bu çalışmada bilişim suçları hakkında genel bir bilgi verilmiştir. Dünyada ve Türkiye' de bilişim suçlarındaki artış ele alınmıştır. Daha sonra Türkiye' de eğitimli insanların bilişim suçu ve bilişim suçları ile mücadele hakkındaki görüşlerini öğrenmek için hazırlanan bir anketin sonuçları değerlendirilmiştir.

Anahtar Kelimeler— Bilişim suçu, bilgisayar suçları, internet suçları

View of Educated People in Turkey against Cyber Crimes

Abstract— Developments occurring in information technology have changed lifestyles of people in many areas and in parallel crimes related to information technologies have emerged. Thus, the concept of crime and criminals has gained new dimensions. In this study, general information about the cyber crimes is given. The increase in cyber crimes in World and Turkey is discussed. The results of a survey were evaluated to find out opinions of educated people in Turkey about cyber crimes and the fight against cyber crimes.

Keywords— Cyber crimes, computer crimes, internet crimes

1. GİRİŞ

Bilişim teknolojilerinde meydana gelen baş döndürücü gelişmelere paralel olarak bu alanla ilgili işlenen suçlarda da aynı oranda artış meydana gelmiştir. Böylece suç ve suçlu tarifi de değişmiştir. Bilişim teknolojileri kullanılarak veya bilişim teknolojilerini hedef alan suçlar bilişim suçu olarak tarif edilebilir. Bilişim suçlarının bir başka tarifi de "Bir bilgisayar, ağ veya bir donanım yardımıyla işlenen herhangi bir suç bilişim suçudur." [1] şeklindedir. Bilişim teknolojilerinin kullanıldığı bilişim suçlarında suç işlemek için bu teknolojiler bir araç olarak kullanılmaktadır. Bazen bir telefon, bazen bir bilgisayar, bazen de internet teknolojileri işlenen suç için bir araç olarak kullanılabilmektedir. Bu anlamda insanlığın yararı için geliştirilen bilişim teknolojileri, günümüzün modern suç aletleri haline gelmiştir. Bilişim teknolojilerini hedef alan suçlarda cep telefonları, bilgisayarlar, e-posta hesapları, banka hesapları, sunucular, web siteleri, özel ve kamu kuruluşların bilişim sistemleri ve kişisel veriler hedef olabilmektedir. Bu suçu işleyenlerin bir kısmı kendini tatmin için, bir kısmı intikam için, bir kısmı dolandırıcılık yaparak para kazanmak için yapmaktadır. Bazen de ülkelerin vatansever hackerları bazı önemli durumlarda diğer ülkelerin web sitelerine, kamu kurum ve kuruluşlarına, bankalarına ve önemli gördükleri ne kadar kuruluş varsa seri saldırılarda bulunabilmektedir. Bu duruma siber savaş adı verilmektedir. Bilişim suçlarını işleyen insanların bir kısmı gerçek hayatta suç işlemekten çekinen insanlar olduğu halde bilişim teknolojileri söz konusu olduğunda çok rahat suç işleyebilmekte ve bundan rahatsızlık duymamaktadır. Bunun en önemli sebebi siber uzayda kimliklerin kolaylıkla gizlenebilmesi, izlenmenin ve yakalanma ihtimalinin zor olmasıdır. Ancak dolandırıcılık gibi bilişim suçlarında suçu işleyen insanlar gerçek hayatta da suça meyilli olan insanlardır. Dünya gittikçe küreselleşmektedir ancak sanal dünya kürselleşmede gerçek dünyadan çok daha öndedir. Artık suç örgütleri internet üzerinden işlerini yapmaktadırlar. Elde ettikleri bilgileri diğer suç örgütlerine satarak diğer ülkelerdeki bilişim suçlarının artışına katkı sağlamaktadırlar. İnternet sayesinde dünyanın herhangi bir bölgesi ile rahatlıkla iletişim sağlandığından suçlular için artık ülke sınırı, polisten kaçmak için sınırı geçmek gibi problemler ortadan kalkmıştır.

Ülkemiz 90'lı yıllardan itibaren bilgisayar ve internetin kullanımına paralel olarak bir e- dönüşüm süreci içine girmiştir. Bu dönüşüm çerçevesinde önce ticari şirketler (özellikle bankalar) daha sonrada kamu kuruluşları dönüşümlerini tamamlama ve iyileştirme adımları atmaktadırlar. Bununla birlikte dünyada ve ülkemizde internet hizmetinin yaygınlaşmasıyla internete bağlı kişilerin sayısı her geçen gün artmaktadır.

Tablo 1. Dünyada İnternet Kullanımı İstatistiği

Dünya İnternet Kullanımı İstatistiği						
Dünyada Bölgeler	Nüfus	Internet Kullanıcıları	Internet Kullanıcıları	Penetrasyon	Büyüme	Kullanıcılar %
	(2010 Tahmini)	31 Aralık 2000	Son Veriler	(% Nüfus)	2000-2010	Tabloya göre
Afrika	1,013,779,050	4,514,400	110,931,700	% 10.9	% 2,357.3	% 5.6
Asya	3,834,792,852	114,304,000	825,094,396	% 21.5	% 621.8	% 42.0
Avrupa	813,319,511	105,096,093	475,069,448	% 58.4	% 352.0	% 24.2
Orta Doğu	212,336,924	3,284,800	63,240,946	% 29.8	% 1,825.3	% 3.2
Kuzey Amerika	344,124,450	108,096,800	266,224,500	% 77.4	% 146.3	% 13.5
Latin Amerika/Karayipler	592,556,972	18,068,919	204,689,836	% 34.5	% 1,032.8	% 10.4
Okyanusya/Australya	34,700,201	7,620,480	21,263,990	% 61.3	% 179.0	% 1.1
TOPLAM	6,845,609,960	360,985,492	1,966,514,816	% 28.7	% 444.8	% 100.0

Tablo 1' de 2010 yılı verilerine göre dünyada internet kullanımı istatistiği görülmektedir. Bu tabloya göre tüm dünyada internet kullanımı ortalama olarak 2000-2010 yılları arasında % 444.8 oranında artmıştır. Türkiye' de ise yine 2010 yılı verilerine göre 35 milyon kullanıcı ile Türkiye Avrupa'da ilk on ülke arasında yer almıştır. Türkiye' de internet kullanımı ortalama olarak 2000-2010 arasında % 1650 oranında artmıştır [2].

Bilgisayar ve internetin gelişimi insanlara birçok kolaylık getirmekle birlikte, kötü niyetli kişilerin bu imkânlardan faydalanarak ticari şirketleri, masum insanları ve dijital ortamda tutulan bütün kayıtları tehdit altında tutmalarına sebep olmaktadır. Çünkü elektronik cihazlar, bilgisayarlar ve diğer yüksek teknoloji ürünleri kullanılarak daha kolay ve ucuz suç işlenebilmektedir. Bu suçu işleyenleri izlemek ve ortaya çıkarmak daha zor olmaktadır. Bu da, ileride bu suçlar ile daha çok karşılaşacağımız anlamına gelmektedir [3]. Her geçen gün gelişen ileri teknoloji bu tür suçların işlenmesini kolaylaştırmakta, değişik yöntemlerin ortaya çıkmasını sağlamaktadır. Şimdiye kadar bu tür suçlar için "Siber Suçlar", "Dijital Suçlar", "İnternet Suçları", "Bilişim Suçları" tanımlamaları kullanılmıştır. Ancak bütün bunların hepsinin yerine "Bilişim Suçları" ifadesi kullanılmaktadır. Konu ile ilgili olarak ülkemizde 12.10.2005 tarihinde 5237 sayılı yeni Türk Ceza Kanunu bilişim suçlarını düzenleyen hükümler kapsamı ve hukuki tanımı genişletilerek yürürlüğe girmiştir. Ülkemizde 90'lı yıllardan bu yana bilgi toplumuna dönüşüm süreci ile ilgili çeşitli girişimler yapılmıştır. Bu doğrultuda atılan en son somut adım 58. ve 59. Hükümetlerin Acil Eylem Planında yer verdiği KYR-22 numaralı "e- Dönüşüm Türkiye Projesi" eylemidir. Bu proje kapsamında yakın ve uzak vade de birçok planlama yapılmış bunların bir kısmı gerçekleştirilmiş bir kısmı da devam etmektedir [4]. Bilgisayar ve internet kullanımının hızlı artışına paralel olarak bilişim suçlarının da hızla artması, başta gelişmiş ülkeler olmak üzere dünyanın ve tabi ki ülkemizin karşısında büyük bir tehlike oluşturmaktadır.

2. BİLİŞİM SUÇLARI

Bilgisayar teknolojilerinde hızlı gelişmeler neticesinde bilgisayar bilgisayarlı sistemler ve internet hayatımızın vazgeçilmez bir parçası olmuştur. Her geçen gün bilgisayarlar ve bilgisayarlı sistemlerin depoladığı ve işlediği veriler baş döndürücü bir şekilde artış göstermektedir. İnsanlar iletişimi, alışverişi, birbirleri ile görüşmelerini, duygularını paylaşmayı, arkadaşlıkları, dostlukları bilgisayarlar ve internet aracığı ile gerçekleştirmekteler. Bu sayede de sanal dünyanın nüfusu ülkelerin sınırlarını ve dil faklılıklarını da ortadan kaldırarak her geçen gün katlanarak artmaktadır. Suç kavramı insanlar ile ilgili bir kavram olduğundan bu sanal dünyada suç ve suçlu kavramı da kendine yer bulmuştur. Artık bilgisayar diğer yararlı yönlerinin dışında bir suç makinesi olarak da bilişim dünyasında yerini almıştır. Bilişim suçları daha nitelikli bilgiye ve eğitime dayanan suçlar olarak diğer suçlardan ayrılmaktadır.

"*Bilişim suçu sanıkları, genellikle orta seviyenin üzerinde ve hatta ileri seviyede zekâya sahip özellikler taşıyabilmektedir. Bunun sonucu olarak da, işledikleri bilişim suçlarının delillendirilmesini engelleyici, zekâ ürünü olan yanıltmalar, engellemeler, delilleri kaybettirici aldatmalar ve akla gelmedik pek çok yönteme başvururlar.*" [5].

Günümüzde gerçek dünyada işlenen birçok suçun bilişim suçları olarak da işlendiği görülmektedir. Siber suçlular dolandırıcılık yapmak için, hızsızlık yapmak için, haraç almak için ve diğer suç çeşitleri için bilgisayarı kullanmaktadırlar [6].

En sık rastlanan bilişim suçları Tablo 2'de görülmektedir [7,8,9]. Bilişim suçları içinde bilgisayar sistemlerine yapılan saldırılar önemli bir yer kaplamaktadır.

Tablo 2. En sık rastlanan bilişim suçları

Bireylere Karşı İşlenen Suçlar	Bireyin kendine karşı işlenen suçlar	e-posta ile taciz
		Siber takip
		Müstehcen malzemelerin dağıtılması
		İftira
		Bilgisayar sistemi üzerinde yetkisiz kontrol/erişim
		Ahlaksız teşhir
		e-posta ile kandırma
		Hile ve dolandırıcılık
	Bireyin mülkiyet haklarına karşı işlenen suçlar	Bilgisayar vandalizmi (kasten yok etmek veya başka bir mala zarar vermek)
		Virüs bulaştırma
		Bilgisayar sistemi üzerinde yetkisiz kontrol/erişim
		Fikri mülkiyet suçları
		İnternet saati hızsızlığı
Organizasyonlara karşı işlenen suçlar (Hükümet, Firma, şirket ve bireylerin oluşturduğu guruplar)	Bilgisayar sistemi üzerinde yetkisiz kontrol/erişim	
	Yetkisiz bilgi sahibi olma	
	Hükümet kuruluşlarına karşı siber terörizm	
	Korsan yazılım v.b. dağılımı	
Toplumun büyük bir kısmına karşı işlenen suçlar	Pornografi (temelde çocuk pornografisi)	
	Ahlaksız resimlerle gençliğin dejenarasyonu	
	Yasa dışı uygunsuz ticaret yapmak	
	Mali suçlar	
	Kaçak eşya satışı	
	Çevrimiçi kumar	
	Sahtecilik, kalpazanlık	

"*Var olan bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak; zafiyete uğratmak; kişileri doğrudan veya dolaylı olarak zarara uğratmak; sistemlere zarar vermek, sistemlerin işleyişini aksattırmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler, saldırı veya atak olarak adlandırılmaktadır.*" [10]. Başlıca saldırı türleri arasında, kaynak kod istismarı (code exploit), gizli dinleme (eavesdropping), hizmet aksattırma saldırıları (DoS), dolaylı saldırılar, arka kapılar (backdoor), doğrudan erişim saldırıları, sosyal veya toplum mühendisliği ve kriptografik saldırıları saymak mümkündür [10].

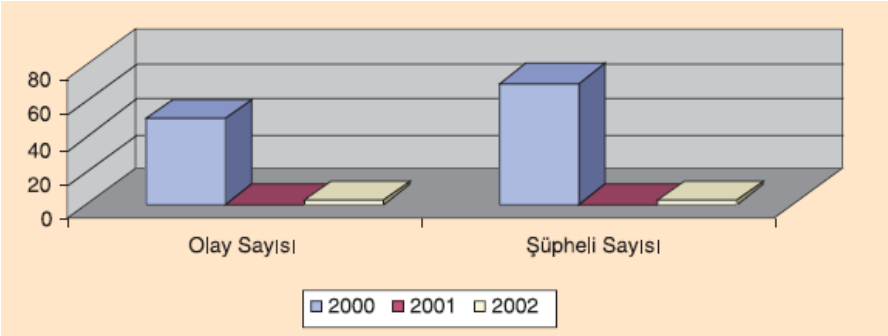
A.B.D.'de Bilgisayar Güvenlik Enstitüsü (CSI-Computer Security Institute) tarafından 14 yıldır bilgisayar suçları ve güvenlik araştırması yapılmaktadır. Enstitünün 14. yıllık raporuna göre araştırma sonuçları devletlerdeki şirketlerden, devlet acentelerinden, mali ve tıbbi kurumlarından ayrıca üniversitelerden 443 bilgisayar güvenliği uygulayıcısının cevaplarına dayanmaktadır. CSI' nın 2009 raporunda [11] saldırı türleri deneyimleri Tablo 3'te verilmiştir.

Türkiye'de bilişim suçlarını araştırmakla görevli birim Emniyet Genel Müdürlüğünde Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığıdır. Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığının her yıl yayınladığı raporda bilişim suçları da yer almaktadır. Bu raporlara göre ülkemizde 2002 yılında yayınlanan rapora göre 2000, 2001 ve 2002 yıllarında ortaya çıkarılan olay ve şüpheli sayısı Şekil 1' de verilmiştir [12].

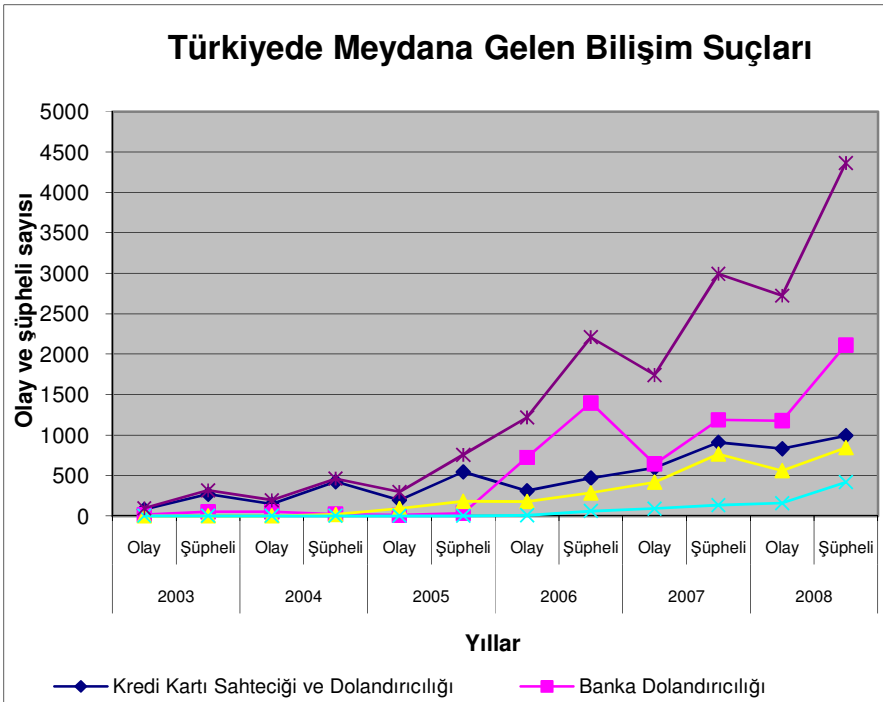
Şekil 1' de görüldüğü gibi ortaya çıkarılan bilişim suçları oldukça azdır. Ancak daha sonraki yıllarda ortaya çıkarılan bilişim suçları hem nitelik kazanmış hem de sayıları oldukça artmıştır. 2003-2008 yıllarında hazırlanan raporlara göre [13,14] bilişim suçları Şekil 2'de görülmektedir. Daha sonra hazırlanan 2009-2010 yıllarına ait raporlarda bilişim suçlarının sınıflandırılması değiştirilmiştir.

Tablo 3. Saldırı Türleri Deneyimleri

Atak Tipi	2005	2006	2007	2008	2009
Kötücül yazılım bulaşması	%74	%65	%52	%50	%64
Organizasyon içinde botlar/zombiler	2007 de eklendi		%21	%20	%23
Avlama mesajları (phishing) yoluyla sahtecilik	2007 de eklendi		%26	%31	%34
Şifre koklama (Password sniffing)	2007 de eklendi		%10	%9	%17
Dolandırıcılık	%7	%9	%12	%12	%20
Denial of service (DoS) atakları	%32	%25	%25	%21	%29
Gasp, saldırı veya çalınan verilerin serbest tehdidi ile ilgili şantaj	2009 de eklendi				%3
Web sitesi tahrifatı	%5	%6	%10	%6	%14
Halka dönük diğer web sitelerinin istismarı	2009 da değiştirildi				6%
Kablosuz ağların istismarı	%16	%14	%17	%14	%8
DNS Sunucularının istismarı	2007 de eklendi		%6	%8	%7
İstemci web tarayıcı istismarı	2009 de eklendi				%11
Kullanıcıların Sosyal ağ profili istismarı	2009 de eklendi				%7
Anlık mesajların kötüye kullanılması	2007 de eklendi		%25	%21	%8
Kurum içindekilerin internet erişimini veya e-postayı kötüye kullanması (pornography, korsan yazılım v.b.)	%48	%42	%59	%44	%30
Kurum içindekilerin yetkisiz erişimi veya ayrıcalık yükseltmesi	2009 da değiştirildi				%15
Dışarıdan sisteme sızma	2009 da değiştirildi				%14
Laptop veya mobil cihazların çalınması veya kaybolması	%48	%47	%50	%42	%42
Mobil cihaz hırsızlığı veya kaybı nedeniyle personel kimlik bilgilerinin (personal identification information –PII) veya korunan sağlık bilgilerinin (protected health information -PHI) çalınması veya yetkisiz erişim.	2008 de eklendi			%8	%6
Mobil cihaz hırsızlığı veya kaybı nedeniyle fikri mülkiyetin çalınması veya yetkisiz erişim.	2008 de eklendi			%4	%6
Diğer bütün nedenlerden dolayı personel kimlik bilgilerinin (personal identification information –PII) veya korunan sağlık bilgilerinin (protected health information -PHI) çalınması veya yetkisiz erişim.	2008 de eklendi			%8	%10
Diğer bütün nedenlerden dolayı fikri mülkiyetin çalınması veya yetkisiz erişim.	2008 de eklendi			%5	%8



Şekil 1. 2000, 2001 ve 2002 yıllarında ortaya çıkarılan olay ve şüpheli sayısı

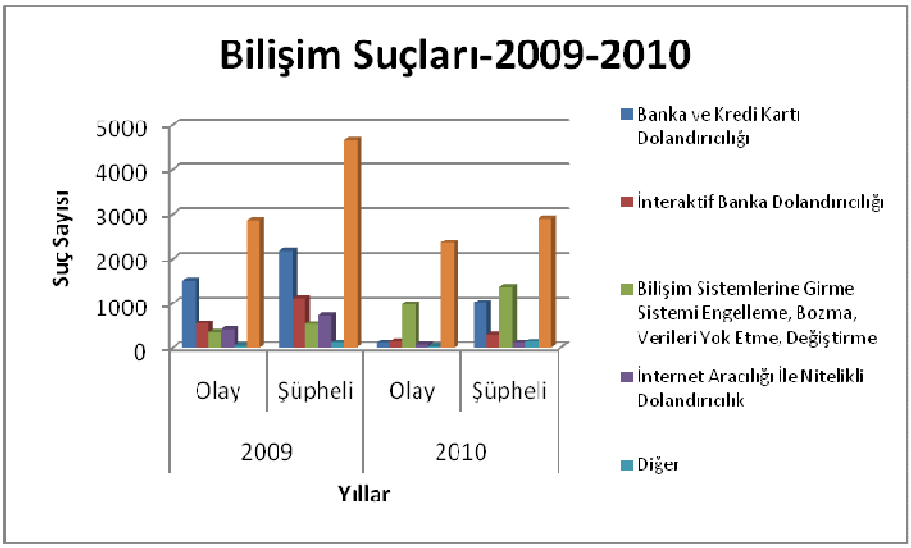


Şekil 2. 2003-2008 yıllarında Türkiye'de bilişim suçları

Bu yıllara ait suçlarla ilgili grafik Şekil 3'te görülmektedir. Görüldüğü gibi bu suçların işlenme oranları her yıl %100'den fazla artış göstermektedir ve bu rakamlar emniyete intikal etmiş suçların sayısını göstermektedir. Bu suçların takibi şikâyete bağlı suçlar olduğu, delillendirmedeki güçlükler, işlenen bilişim suçunun çok daha fazla olduğu anlaşılmaktadır.

3. AMAÇ VE YÖNTEM

Yapılan bu çalışmada bilişim suçları kavramı hakkında genel bilgiler verilmeye çalışılmış, bilişim suçlarının özel bir alanına değinilmemiştir. T.C. Başbakanlık Türkiye İstatistik Kurumunun 2009 yılı Nisan ayı içerisinde gerçekleştirdiği Hane Halkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre son üç ay içerisinde (Ocak-Mart) bireylerin % 35,6'sı bilgisayar, % 34,0'ı internet kullanmıştır. Bilgisayar ve İnternet kullanım oranlarının en yüksek olduğu yaş grubu 16-24 yaş grubudur. Bu oranlar tüm yaş gruplarında erkeklerde daha yüksektir. Eğitim durumuna göre incelendiğinde ise yüksekokul, fakülte ve üstü mezunları en yüksek bilgisayar ve İnternet kullanım oranlarına sahiptir [15]. Ülkemizdeki eğitimli insanların bilişim suçları kavramı hakkındaki görüşlerini öğrenebilmek için üniversite öğretim elemanları ve öğrencilerine bir anket uygulanmıştır. Bu anketin sadece üniversite ile sınırlı tutulmasının sebeplerinden biri bu konudaki akademik bakışı değerlendirebilmektir.



Şekil 3. 2009-2010 yıllarında Türkiye'de bilişim suçları

Araştırma verileri, anket yöntemiyle kaynak gruplardan toplanmıştır. Anket internet üzerinden gerçekleştirilmiştir. http://www.medyayin.com/anket adresinde yayınlanmış ve Gazi Üniversitesinin web sitesinin ana sayfasından duyurulmuştur. Ayrıca gruplar, e-posta ve bizzat görüşme yoluyla ankete katılmaları doğrultusunda yönlendirilmiştir.

4. BULGULAR

Ankete 1050 kişi katılmış, fakat 766'sı anketi doğru ve eksiksiz olarak doldurduğundan değerlendirme 766 kişiye göre yapılmıştır. Tablo 4'te katılımcılara sorulan bazı sorulara katılımcılardan evet cevabı verenler görülmektedir.

Tablo 4. Sorulara evet cevabı verenler katılımcılar

Soru	Evet %
Bilgisayarınız var mı?	76,0
Antivirüs yazılımı kullanıyor musunuz?	80,4
Bilgisayarınızda lisanssız yazılım (program) var mı?	72,5
Lisanssız yazılım kullanmak sizi vicdanen rahatsız ediyor mu?	35,3
İnternetten müzik, film, oyun dosyaları indiriyor musunuz?	63,6
İnternetten müzik, film, oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu biliyor musunuz?	66,7
Bilişim suçu kavramını daha önce duydunuz mu?	64,4
Hackerlık yapar mısınız?	42,2
İnternet bankacılığı sizce güvenli mi?	27,2
İnternet üzerinden alış veriş yapıyor musunuz?	18,7
İnternet üzerinden alışveriş yaparken herhangi bir güvenlik problemi ile karşılaştınız mı?	11,9
Size banka bilgilerinizi güncelleştirme için bankanızdan geldiği bildirilen bir e-posta (phishing olayı) geldi mi?	14,0
Bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ilerde büyük tehlikelere yol açacağını düşünüyor musunuz?	60,8
Bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesini olumlu karşılar mısınız?	36,8
Bilişim suçlarını önlemek amacıyla internette gözetlenmeyi olumlu karşılar mısınız?	29,4
Size göre önemli gördüğünüz bir bilişim suçuna şahit olursanız bunu ihbar etmeyi düşünür müsünüz?	69,8

Grupların cinsiyet ve yaş dağılımları; Katılımcıların 177'si kadın (%23,1), 589'u erkektir (%76,9). 113 kişinin (%14,8) yaşı 20'nin altındayken, 618 kişi (%80,7) 20–29, 19 kişi (%2,5) 30–39, 12 kişi (%1,5) 40–49 ve 4 kişi de (%0,5) 50'nin üstü yaş gruplarıdır. Grupların üniversitedeki konumları; 766 katılımcının 47'si öğretim elemanı (%6,1) ve 719'u (%93,9) öğrencidir. Katılımcıların 467'si (%61) fen bilimleri, 252'si (%32,9) sosyal bilimler ve 47'si (%6,1) sağlık bilimleri alanlarına mensuptur.

Öğretim elemanları ve öğrenciler arasında ise sadece önemli farklılıklar olan sorularda değerlendirme yapılmıştır. Bu gruplardan toplanan veriler, istatistik yöntemlerle frekans (f), yüzde (%) çözümlenerek değerlendirilmiş ve yorumlanmıştır. Değerlendirme SPSS 11 programı kullanılarak yapılmıştır. Tablo 5'te Lisanssız yazılım kullanma sebebi görülmektedir.

Sürekli kullanma imkânına sahip olduğu bir bilgisayarı olmayan 184 kişi ve lisanssız yazılım kullanmayan 160 kişi bu soruyu cevaplamamıştır. Cevaplayanların %35,8'i ucuz olduğu için lisanssız yazılım kullandığını belirtmiştir. Lisansız yazılım kullanma sebebi ile öğrenci öğretim elemanı arasında istatistiksel olarak anlamlı ilişki bulunmuştur. İlişki öğretim elamanlarının "kolay bulunması" seçeneğini daha yüksek oranda seçmesinden kaynaklanmaktadır.

Tablo 6' da Lisanssız yazılımların nereden elde edildiği görülmektedir. Bilgisayarı olmayan ve lisanssız yazılım kullanmayan 344 kişinin cevaplamadığı bu soruya göre katılımcıların %19,9'u lisansız yazılımları arkadaşlarından kopyalamaktadır.

Tablo 7' de İnternetten müzik, film, oyun dosyalarını indirmenin ve lisanssız yazılım kullanmanın sebepleri görülmektedir.

Tablo 5. Lisanssız yazılım kullanma sebebi

Lisanssız yazılım kullanma sebebinizi belirtiniz?	Öğrenci		Öğretim Elemanı		Genel	
	f	**%**	**f**	**%**	**f**	**%**
Ucuz olduğundan	142	36,1	9	31,0	151	35,7
Kolay bulunduğundan	35	8,9	7	24,2	42	10,0
Hepsi	216	55,0	13	44,8	229	54,3
Toplam	393	100,0	29	100,0	422	100,0

$(\chi^2 = 7.003, \quad p = 0.003)$

Tablo 6. Lisanssız yazılımların elde edilmesi durumu

Kullandığınız lisanssız yazılımları nereden elde ediyorsunuz?	**f**	**%**
İnternetten	51	12,1
Arkadaşlarımdan kopyalıyorum	84	19,9
Kopya satan yerlerden satın alıyorum	58	13,7
Hepsi	229	54,3
Toplam	422	100,0

Tablo 7. İnternetten müzik, film, oyun dosyalarını indirmenin ve lisanssız yazılım kullanmanın sebepleri

İnternetten müzik, film, oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunun farkındaysanız neden yapıyorsunuz?	**f**	**%**
Kullandığım programları profesyonel olarak ve sürekli olarak kullanmadığım için	106	19,6
Denetim olmadığından	49	9,1
Maliyeti düşük olduğu için	188	34,9
Hepsi	196	36,4
Toplam	539	100,0

Katılımcıların %34,9'u internetten müzik, film, oyun dosyaları indirmenin ve lisanssız yazılım kullanmalarının sebebi olarak maliyetin düşük olmasını göstermiştir. 227 kişi bu soruyu cevaplamamıştır.

Tablo 8'de Lisanssız yazılım kullanmaya karşı gerekli yaptırımın yeterince uygulanamamasının nedenleri görülmektedir.

Lisanssız yazılım kullanmaya karşı gerekli yaptırımın yeterince uygulanamamasının en önemli nedeni olarak %24,9 oranında yasaların yetersiz kalması veya uygulanamaması gösterilmiştir.

Tablo 9'da Kullanılan yazılımların bilgileri internet üzerinden başkalarına iletme durumu görülmektedir. "Kullandığınız bazı yazılımların, bilgilerinizi internet üzerinden başkalarına iletebileceğini biliyor musunuz?" Sorusuna katılımcıların %51,7'si evet bunu yapabilir cevabı vermiştir.

Tablo 10'da en tehlikeli bilişim suçları görülmektedir. Katılımcıların %61'i dolandırıcılık suçunu bilişim suçlarının en tehlikelisi olarak göstermiştir.

Tablo 11'de en çok işlenen yasa dışı yayın suçları görülmektedir. En çok işlenen yasa dışı yayın suçu olarak %45,6 oranında pornografi seçilmiştir. Tablo 12'de internetin kullanılma amaçları görülmektedir. Katılımcıların %73,9'u interneti en çok araştırma yapmak için kullanmaktadır. Tablo 13'te bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmaları görülmektedir. Bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmalarını yeterli bulanların oranı %1,4 olmuştur. İstatistiksel olarak anlamlı bir ilişki yoktur. Tablo 14'te bilişim suçlarıyla ilgili yasalarımızın yeterliliği ile ilgili görüş görülmektedir. Bilişim suçlarıyla ilgili yasalarımızı yeterli bulanların oranı ise %3 olmuştur. İstatistiksel olarak anlamlı bir ilişki yoktur.

Tablo 8. Lisanssız yazılım kullanmaya karşı gerekli yaptırımın yeterince uygulanamamasının nedenleri

Sizce lisanssız yazılım kullanmaya karşı gerekli yaptırımın yeterince uygulanamamasının en önemli nedeni nedir?	**f**	**%**
Yazılım şirketlerinin hakkını aramaması	54	7,0
Devletin ilgili birimlerinin yeterince ciddiye almaması	104	13,7
Yasaların yetersiz kalması veya uygulanamaması	191	24,9
Hepsi	417	54,4
Toplam	766	100,0

Tablo 9. Kullanılan yazılımların bilgileri internet üzerinden başkalarına iletme durumu

Kullandığınız bazı yazılımların, bilgilerinizi internet üzerinden başkalarına iletebileceğini biliyor musunuz?	**f**	**%**
Bilmiyorum.	219	28,6
Evet bunu yapabilir ancak güvenlik programım beni korur.	121	15,8
Evet bunu yapabilir.	396	51,7
Hayır bunu yapamaz çünkü açık kod kullanıyorum yazılıma tamamen hakimim.	30	3,9
Toplam	766	100,0

Tablo 10. En tehlikeli bilişim suçları

Size göre aşağıdaki bilişim suçlarından en tehlikelisi hangisidir?	**f**	**%**
Lisans hakları	104	13,5
Dolandırıcılık (ATM,kredi kartı vb.)	467	61,0
Yasa dışı yayınlar (pornografi, hakaret vb.)	81	10,6
Bilgisayar sabotajı	114	14,9
Toplam	766	100,0

Tablo 11. En çok işlenen yasa dışı yayın suçları

Size göre en çok işlenen yasa dışı yayın suçu hangisidir?	**f**	**%**
Pornografi	349	45,6
Çocuk pornografisi	193	25,2
Hakaret	72	9,4
Siber terör	152	19,8
Toplam	766	100,0

Tablo 12. İnternetin kullanılma amaçları

İnterneti en çok hangi amaç için kullanıyorsunuz?	**f**	**%**
Araştırma yapmak için	566	73,9
Arkadaş edinmek için	18	2,3
Haberleşmek için	182	23,8
Toplam	766	100,0

Tablo 13. Bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmaları

Bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmalarını yeterli buluyor musunuz?	Öğrenci		Öğretim Elemanı		Genel	
	f	**%**	**f**	**%**	**f**	**%**
Yeterli	10	1,4	1	2,1	11	1,5
Yetersiz	213	29,6	11	23,4	224	29,2
Kesinlikle yetersiz	210	29.2	17	36,2	227	29,6
Fikrim yok	286	39,8	18	38,3	304	39,7
Toplam	719	100,0	47	100,0	766	100,0

$(\chi^2 = 1,497 \quad p = 0.683)$

Tablo 14. Bilişim suçlarıyla ilgili yasalarımızın yeterliliği

Bilişim suçlarıyla ilgili yasalarımızı yeterli buluyor musunuz?	Öğrenci		Öğretim Elemanı		Genel	
	f	**%**	**f**	**%**	**f**	**%**
Yeterli	23	3,2	0	0	23	3
Yetersiz	238	33,1	15	31,9	253	33
Kesinlikle yetersiz	171	23,8	16	34,0	187	24,4
Fikrim yok	287	39,9	16	34,0	303	39,6
Toplam	719	100,0	47	100,0	766	100,0

$(\chi^2 = 3,809 \quad p = 0.282)$

5. TARTIŞMA

Anket sonuçları incelenirken öncelikle dikkat edilmelidir ki, katılımcılar üniversite öğrencileri ve öğretim elemanlarıdır. %63,3'ü bilgisayar eğitimi almıştır.

Katılımcıların %76'sının sürekli kullanma imkânına sahip olduğu bir bilgisayar varken, bu oran öğretim elemanlarında %95,7, öğrenciler arasında ise %74,7 olmaktadır. Türkiye'nin ekonomik durumu göz önüne alındığında, %76 oranı bir hayli yüksektir. Antivirüs programı kullanma oranı %80,4'tür. Bilgisayar eğitimi almayanlarda %78,8'e düşmüştür. Katılımcılar %72,5 gibi bir oranda lisansız yazılım kullanmaktadır. Yine bilgisayar eğitimi almayanlarda %74,3'e yükselmektedir. İşletim sistemi lisanslı olanların oranı (%56,9), lisansız olanların (%43,1)'dir.

İnternetten müzik, film, oyun dosyaları indirenlerin oranı ise %63,6. Bilgisayarı olmayanlar arasında bu oranın %43,4 olması internet kafe ve okul bilgisayarlarında bu ihlallerin gerçekleştirildiğini göstermektedir.

Katılımcıların %29,6'sı internetten müzik, film, oyun dosyaları indirmenin suç olduğunu bilmemektedir. Bu oranlar bilgisayar eğitimi almayanlar arasında %33,3, bilgisayarı olmayanlar arasında %45,1 olmaktadır. İnternet suçlarının artmasında ve daha önce adli suç işlememiş kişilerin internet aracılığıyla suç işler hale gelmesinde suç işlemenin kolaylaşmasının yanı sıra, kullanıcıların internet üzerinden gerçekleştirilen eylemlerin herhangi yasal bir yükümlülüğünün ve herhangi bir yasal düzenlemenin olmadığına dair yanlış bir yargının bulunmasıdır. Ancak, gerçekleştirdikleri eylemler ile bilişim sistemlerine zarar veren bu kişiler, bilişim suç yasaları ile cezalandırılmaktadır.

Katılımcıların %24,5'i ve lisansız yazılım kullanmanın ve internetten müzik, film, oyun dosyaları indirmenin suç olduğunu bilenlerin %34,9'u bu suçu işlemelerinin nedeni olarak maliyetin düşük olmasını göstermiştir. Görüldüğü gibi bu suçların işlenmesinin en büyük nedeni maddi yetersizlikler veya lisanslı yazılımların pahalı olmasıdır. Türkiye'nin gelişmekte olan bir ülke olduğu ve bu anketin katılımcılarının büyük çoğunluğunun öğrenciler olduğu düşünüldüğünde bu kusurların işlenme oranının yüksek olması pek de şaşırtıcı değildir.

Lisanssız yazılım kullanmaya karşı gerekli yaptırımın yeterince uygulanamamasının en önemli nedeni olarak %24,9 oranında yasaların yetersiz kalması veya uygulanamaması gösterilmiştir. Katılımcıların %35,6'sı bilişim suçu kavramını daha önce duymamıştır. Bu oran öğretim elemanları arasında %19,1'e düşerken, bilgisayarı olmayanlar arasında %50'ye çıkmaktadır.

Katılımcıların %73,9'u interneti en çok araştırma yapmak için kullanmaktadır. Katılımcılar öğrenciler ve öğretim elemanları olduğuna göre gayet normal bir sonuç olduğu anlaşılmaktadır.

Normal olmayan bir sonuç ise katılımcıların %42,2'sinin yeterli bilgi ve birikime sahip olsaydı hackerlık yapabileceğini belirtmeleridir. Bilişim suç faillerinin büyük bir kısmının herhangi bir suç kaydı bulunmayan, bilişim suçlarının ilk suçları olarak kayda geçen kişiler olduğu belirtilmektedir. Hackerların, genelde bir şeyler ispatlamaya çalışan zeki kişilerden oluşması kamuoyu ve medyanın söz konusu kişilere merak ve ilgi ile bakmasına sebep olmuştur. Bu durum araştırmadan elde edilen %42,2'lik sonucun gerçeği yansıttığını ortaya koymaktadır.

İnternet bankacılığı %75,3 oranında güvenilir bulunmazken, İnternet üzerinden alışveriş yapanların oranı %18,7'de kalmaktadır. Oysa internetten alışveriş yapanların %88,1'i herhangi bir problem yaşamadığını belirtmiştir.

Anket sonuçlarının önemli bir göstergesi de katılımcıların %60,8'nin bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ileride büyük tehlikelere yol açacağını düşünmesi olmuştur. Bilgisayar ve internet kullanımının katlanarak artması, bilgisayarlarla işlenen bilişim suçlarının her geçen çeşitlenerek artması ve bu suçların maliyetinin milyar dolarları bulduğu günümüzde insanların gelecek için endişelenmesi çok normal bir davranış olarak kabul edilmelidir. Asıl önemli olan bu tehlikeye karşı alınabilecek önlemlerin doğru tespit edilebilmesidir. Çünkü bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ileride büyük tehlikelere yol açacağını düşünenlerin oranının %60,8 olduğu katılımcıların %62,6'sı bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesine karşı çıkarken, %70,6'sı bilişim suçlarını önlemek amacıyla internette gözetlenmeye karşı çıkmaktadır. Elektronik bilgilere erişimin kolaylaşması ve yaygınlaşması bilgi edinme özgürlüğüne yeni bir boyut kazandırmıştır. Aynı zamanda elektronik ortamdaki kişisel bilgilerin (mali bilgiler, sağlık bilgileri vs.) gizliliği ve güvenliği de son derece önem kazanmıştır. Sadece kredi kartının takibi ile bir kişi hakkında, bankadaki para miktarı, borçları, aldıkları, yedikleri giydikleri vs. öğrenilebilir. Web sitelerinin, kullanıcının web istemcisine gönderdiği cookie'ler aracılığı ile sitenin en son hangi kısmını ve ne zaman ziyaret ettiğinizi takip etmesi ve kayıt altına alması mümkündür.

Katılımcıların %69,8'i önemli gördüğü bir bilişim suçuyla karşılaştığında ihbar edebileceğini belirtmiştir. Ülkemizde bilişim suçu mağdurlarının bu konuda nasıl müracaatta bulunacaklarını ve hangi kanunlarla korunduklarını bilemediklerinden kendi yöntemleri ile mağduriyetlerini gidermeye gitmektedirler. Bilişim konusunda işlenen suçlarla ilgili vatandaşlarımızın şikâyetlerini ve mağduriyetlerini iletebilecekleri bir birim bulunmamaktadır. Genellikle bu tür konularda şikâyeti olan insanlar. Bilgi İşlem Şube Müdürlüklerine yönlendirilmektedir.

Üzerinde düşünülmesi gereken anketin önemli verilerinden biri de bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmalarını yeterli bulanların oranının %1,4 bilişim suçlarıyla ilgili yasalarımızı yeterli bulanların

oranının ise sadece %3 olmasıdır. Bilişim suçlarında suçluların yakalanması geleneksel suçlardan farklı olarak çok daha zor olmaktadır. Kullanıcılar ve sistem yöneticileri çoğu zaman bir suçun varlığını bile ispatlayamamaktadırlar. Bilişim alanında işlenen suçlarla karakollarımızda ve diğer polis birimlerimizde yeterli bilgi birikimine sahip personel olmadığı için ideal manada mücadele edilememektedir. Şu an için yeterli düzeyde olmasa da emniyet teşkilatımız bilişim suçlarıyla mücadele kapsamında önemli çalışmalar yapmaktadır.

6. SONUÇ VE ÖNERİLER

Bilişim suçları hukuki bir konu gibi görünse de bilişim suçlarını suç oluşmadan önleyebilmek için alınacak tedbirlerin bilişim sektörü ile ilgili olması bu konunun sadece hukuki bir konu olmadığını göstermektedir. Yani bu konu ile ilgilenen araştırmacılar sadece hukukçular değil bilişim sektörünün ilgili alanlarında çalışan kişiler de olmalıdır. Elde edilen bulgulara göre insanların konuyla ilgili yeterli bilince sahip olmadıkları ve özellikle lisanssız yazılım kullanma oranının çok yüksek olduğu anlaşılmıştır. Bu ihlallerin işlenme sıklığı öğrencilerde ve bilgisayar eğitimi almamış olanlarda daha yüksektir. Özellikle maddi yetersizlikler, lisanslı yazılımların çok pahalı oluşu ve eğitimsizlik önemli faktörler olarak öne çıkmaktadır. Lisanssız yazılım kullanımının azaltılması için işletim sistemi yazılımları ucuzlatılmalıdır.

Lisanssız yazılım kullanımının önüne geçmenin yollarından birisi de açık kaynak kodlu yazılımların kullanılmasının teşvik edilmesidir. Üstelik bu yolla yazılım için ülkemizin yurt dışına ödediği para miktarı da önemli ölçüde düşecek, bu yazılımlarla ilgilenen insanlar daha çok araştırmacı olacak bu yolla ülkemizdeki yazılım sektörünün gelişmesine katkı sağlanmış olacaktır.
Katılımcıların önemli bir kısmı lisansız yazılım kullanmanın ve internetten müzik, film, oyun dosyaları indirmenin suç olduğunu bilmemektedir. Hatta katılımcıların birçoğu bilişim suçu kavramını daha önce duymamıştır. İnternet suçlarının artmasında ve daha önce adli suç işlememiş kişilerin internet aracılığıyla suç işler hale gelmesinde suç işlemenin kolaylaşmasının yanı sıra, kullanıcıların internet üzerinden gerçekleştirilen eylemlerin herhangi yasal bir yükümlülüğünün ve herhangi bir yasal düzenlemenin olmadığına dair yanlış bir yargının bulunmasıdır. Ancak, gerçekleştirdikleri eylemler ile bilişim sistemlerine zarar veren bu kişiler, bilişim suç yasaları ile cezalandırılmaktadır.

Bunun yanı sıra bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ileride büyük tehlikelere yol açacağı düşüncesinin hâkim olduğu görülmektedir. Bilişim suçlularının mağdurlara verdikleri zararlar ve aldıkları cezalar kamuoyuna duyurulmalı ve medyanın bu konuda yaptığı özendirici yayınlar engellenmelidir.

Bu yüzden Türkiye'nin bilişim suçları üzerine ciddi olarak eğilmesi gerekmektedir. Bilişim suçlarını sınıflandırarak takibini gerçekleştirecek kamu kuruluşları kurulmalı ve özel sektör kuruluşlarının kurulması teşvik edilmelidir. Bilişim suçları ile mücadele eden uluslar arası kuruluşlar daha etkin mücadele yöntemleri geliştirmelidir. Bilişim suçları ile mücadelede, yeterli hukuki alt yapı, uluslararası işbirliği, bilgisayar programı ve bilgisayarlarda son model teknolojinin kullanılması ve iyi eğitilmiş personelin önemli rolü olduğu söylenebilir.

İnternet üzerinden işlenen bilişim suçlarına maruz kalmamak için, antivirüs yazılımları, güvenlik duvarı gibi yazılımlar bilgisayarlarda yüklü olmalıdır. Bunun haricinde her gelen e-posta açılmamalı, her internet sitesine girilmemeli, internet üzerinden güvenli olmayan siteler üzerinden ve özellikle halka açık yerlerde internete bağlanıldığında banka kayıtları ve kişisel bilgiler gönderilmemelidir.

Örgün ve yaygın eğitim kurumları kullanılarak toplumun her kesimi bilişim suçları konusunda bilgilendirilmeli ve nasıl mücadele edileceği anlatılmalıdır.

TEŞEKKÜR

Yaptıkları katkılar ile bu çalışmayı daha değerli hale getiren hakemlere teşekkürü bir borç biliriz.

KAYNAKLAR

[1] S. Gordon, R. Ford, "On the definition and classification of cybercrime", *Journal in Computer Virology*, 2(1), 13–20, 2006.
[2] İnternet: World Internet Users and Population Stats http://www.internetworldstats.com/stats.htm, 2011.
[3] N. Doğan, "Türkiye'de Bilişim Suçlarına Bakış", *Popüler Bilim*, 8(3), 14-17, 2008.
[4] H. Dijle, **Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Yaklaşımı**, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, 2006.
[5] A. Karagülmez, "Bilişim suçlarında delil toplamayı etkileyen başlıca konular", **2.Polis Bilişim Sempozyumu**, Ankara, 1-3, 2005.
[6] S. W. Brenner, "Toward A Criminal Law for Cyberspace: Distributed Security", *Boston University Journal of Science & Technology Law,* 10(2), 1-105, 2004.
[7] J. Govil, "Ramifications of cyber crime and suggestive preventive measures", **IEEE International Conference on Electro/Information Technology**, Chicago, 610-615, 2007.
[8] B. Kit at all, "Cyber Crime–A new breed of criminal?", *Computer Law & Security Report*, 19(3), 222-227, 2003.
[9] İnternet: Cyber Crime by Parthasarathi Pati, http://www.naavi.org/pati/pati_cybercrimes_dec03.htm, 2011.
[10] G. Canbek, Ş. Sağıroğlu, "Bilgisayar Sistemlerine Yapılan Saldırılar Ve Türleri: Bir İnceleme", *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23(2), 1-12, 2007.
[11] R. Richardson, CSI Computer Crime and Security Survey, **CSI,** New York**,** 2009.
[12] T.C. İçişleri Bakanlığı, Bilişim Suçları, **Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı,** Ankara, 2003.
[13] T.C. İçişleri Bakanlığı, Bilişim Suçları, **Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı,** Ankara, 2005.
[14] T.C. İçişleri Bakanlığı, Bilişim Suçları, **Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı,** Ankara, 2008.
[15] Internet: 2009 Yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması Sonuçları. http://www.tuik.gov.tr/PreHaberBultenleri.do?id=4104, 2011.