TÜRKİYE'DE EĞİTİMLİ İNSANLARIN BİLİŞİM SUÇLARINA YAKLAŞIMI

Hikmet DİJLE

YÜKSEK LİSANS TEZİ
ELEKTRONİK-BİLGİSAYAR EĞİTİMİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2006
ANKARA

TÜRKİYE'DE EĞİTİMLİ İNSANLARIN BİLİŞİM SUÇLARINA YAKLAŞIMI

Hikmet DİJLE

YÜKSEK LİSANS TEZİ
ELEKTRONİK-BİLGİSAYAR EĞİTİMİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2006
ANKARA

Hikmet DİJLE tarafından hazırlanan TÜRKİYE'DE EĞİTİMLİ İNSANLARIN BİLİŞİM SUÇLARINA YAKLAŞIMI adlı bu tezin yüksek lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Nurettin Doğan
Tez Yöneticisi

Bu çalışma, jürimiz tarafından Elektronik Eğitimi Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. Çetin Elmas

Üye : Prof. Dr. Ömer Faruk Bay

Üye : Yrd. Doç. Dr. Ayhan Erdem

Üye : Yrd. Doç. Dr. Nursal Arıcı

Üye : Yrd. Doç. Dr. Nurettin Doğan

Tarih : 08/05/2006

Bu tez, Gazi Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

HİKMET DİJLE

TÜRKİYE'DE EĞİTİMLİ İNSANLARIN BİLİŞİM SUÇLARINA YAKLAŞIMI
(Yüksek Lisans Tezi)

Hikmet DİJLE

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Mayıs 2006

ÖZET

Bilgisayar ve iletişim teknolojilerindeki gelişmeler, eğitimden ticarete, devlet sektöründen özel sektöre, eğlenceden alışverişe kadar birçok alanda yerleşik anlayışı değiştirmiş ve yeni bir yaşam tarzı getirmiştir. Bu olumlu gelişmelere paralel olarak suç kavramı da gelişmiş ve bilişim suçları da diğer suçların arasında yerini almıştır. Bilişim suçları ciddi suçlardır ve dünya için büyük bir tehlike arz etmektedir. İnternet sayesinde eylemler dünyanın herhangi bir yerinde gerçekleştirilebildiğinden çok çabuk bu denli yaygın olmayı başarmışlardır. Bu nedenle bilişim suçları ve onlarla mücadele hakkında bilimsel çalışmaların yapılması gerekmektedir. Yapılan bu çalışma ile bilişim suçları çeşitli yönleri ile incelenmiş ve bilişim suçlarının kapsamı, tanımlaması ve sınıflandırılması açıklanarak, hukuki boyutu, polisiye uygulamaları üzerinde durulmuştur. Türkiye'de bilgisayar ve İnternet ile profesyonel olarak daha çok öğretim elemanları ve üniversite öğrencilerinin ilgilendiği düşünülerek öğretim elemanları ve üniversite öğrencilerine bir anket uygulanmıştır.

Bu anket bilişim ile ilgili olduğundan e-posta ile adresi duyurularak bir web sitesi vasıtasıyla uygulanmıştır. Böylece eğitimli insanların bilişim suçu ve bilişim suçları ile mücadele hakkındaki görüşleri değerlendirilmeye çalışılmıştır.

Bilim Kodu :**702.6.004**
Anahtar Kelimeler :**Bilişim suçu, bilgisayar suçu, dijital delillendirme, siber terör, internet suçları**
Sayfa Adedi :**59**
Tez Yöneticisi :**Yrd. Doç. Dr. Nurettin Doğan**

APPROACHES OF THE EDUCATED PEOPLE TO THE CRIMES OF INFORMATIC IN TURKEY
(M.Sc. Thesis)

Hikmet DİJLE

GAZİ UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY
May 2006

ABSTRACT

The developments in informatics and communication technologies have brought in a new style of life and also changed the common beliefs in various fields such as from education to trade, from state sector to private sector, from entertainment to shopping. Parallel to these positive developments, the concept of crime has developed and the crime of informatics has taken its place among the other types of crimes. Informatic crimes are serious crimes and they pose a great world-wide threat. Thanks to the internet, these crimes may be realized in any part of the world and that is why it has spread so much throughout the world. For this reason, research about informatic crimes and about the measures to be taken against them should be made. With this study, informatic crimes have been analysed from different aspects.The scope, definition and classification of these crimes have been discussed and its legal dimension as well as its detectionability have been focused on. Taking into consideration the fact that the internet users in Turkey are mostly educated people, university staff and university students, a survey has been made among them.

Since this survey is concerned with informatics, it has been made by means of a web site and announced through e-mail. With this, the opinions of educated people on the crime of informatics and the struggle against these crimes were tried to be evaluated.

Science Code :702.6.004
Key Words :Information technologies crimes, computer crimes, digital proofing, cyber terror, internet crimes
Page Number :59
Adviser :Assist. Prof. Dr. Nurettin Doğan

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Yrd. Doç. Dr. Nurettin Doğan'a, yardım ve desteklerini esirgemeyen arkadaşlarım Mehmet Ali İlhan ve Melek Yıldır'a, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli aileme ve tüm çalışma arkadaşlarıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
ASSK	Avrupa Siber Suçlar Konvansiyonu
ATM	Asychrone Transfer Mode (Eşzamansız İletim Modu)
DOS	Disk Operation System (Disk İşletim Sistemi)
GPRS	General Packed Radio Service (Genel Radyo Servisi)
GSM	Küresel mobil haberleşme sistemi
IP	İnternet Protokol
İ.S.S	İnternet Servis Sağlayıcılar
IT	Information Technologies (Bilişim Teknolojileri)
STK	Sivil Toplum Kuruluşları
SMS	Sistem Yönetim Sunucusu
TBMM	Türkiye Büyük Millet Meclisi
TCK	Türk Ceza Kanunu
YTCK	Yeni Türk Ceza Kanunu

1. GİRİŞ

Bilişim sektörünün gelişmesine paralel olarak, insanlarında bu durumdan yararlanması kaçınılmaz olmuştur. Günlük hayatta neredeyse her alanda bilişim teknolojisinin nimetlerinden yararlanılmaktadır. Bilişim teknolojileri gelişmesini sürdürürken bu olumlu gelişmeyi kendi çıkarları için kullanmayı düşünen insanlarda boş durmamakta ve bu teknolojiyi bir suç aracı olarak kullanmaktadır. Bu teknoloji ne kadar gelişirse bu tür insanlar da o kadar bilişim teknolojilerini bir suç aracı olarak kullanmak isteyecektir.

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 vadede birçok planlama yapılmış bunların bir kısmı gerçekleştirilmiş bir kısmı da devam etmektedir [1]. Türkiye hızla her alanda e-dönüşüm projesi içinde yer alırken bu konuya paralel olarak gelişen bilişim suçları ile ilgili olarak ta bilişim suçları kanunu yürürlüğe konmuştur. Ancak bilişim suçları ile ilgili birçok çalışma yapılmalıdır. Yapılacak bu çalışmalar konunun hukuki yönünün dışında bu tür tehditlerden korunmak için alınacak tedbirler, halkın bilinçlendirilmesi gibi çalışmalar da olabilir.

"Bilişim suçu" bilgisayarı da kapsayan ancak daha geniş bir alanda, bilişim sistemlerine karşı veya bilişim sistemleri ile işlenen suçları ifade eder. Bazen bu tür suçlardan bahsederken "Bilgisayar suçları" terimi de kullanılmaktadır. Bunların yanında siber suçlar, dijital suçlar, internet suçları, ileri teknoloji suçları vs. tanımlamaları ile de karşılaşılmaktadır. Uluslararası literatürde ise computer crimes, cyber crimes, IT crimes (Information technologies – bilgi teknolojileri), crime of networks gibi terimler kullanılmaktadır. Kullanılan bu terimler bu tür suçların sadece bir kısmını tanımlamaktadır. Bütün bunların yerine "Bilişim suçları" terimini kullanmak daha uygundur [2].

Genel olarak bilişim suçlarını aşağıdaki gibi sınıflandırmak mümkündür.

1. Bilgisayar sistemlerine ve servislerine yetkisiz erişim ve dinleme
2. Bilgisayar sabotajı
3. Bilgisayar yoluyla dolandırıcılık
4. Bilgisayar yoluyla sahtecilik
5. Kanunla korunmuş bir yazılımın izinsiz kullanımı
6. Yasadışı yayınlar
7. Diğer bilişim suçları : Ticari sırların çalınması, verilerin suistimali, sahte kişilik oluşturma ve kişilik taklidi vb. bilişim suçlarıdır [3].

Bilişim suçları ciddi suçlardır ve dünya için büyük bir tehlike arz etmektedir. İnternet sayesinde eylemler dünyanın herhangi bir yerinde gerçekleştirilebildiğinden çok çabuk bu denli yaygın olmayı başarmışlardır. Dallas'taki Suç Komisyonunun verdiği rakamlara göre, ABD siber suçlar yüzünden her yıl 15 milyar dolar zarara uğramaktadır [4]. Web sitenizin çökertilmesi, bilgisayarınızdaki bütün bilgilerin silinmesi, binlerce kişinin kredi kartı bilgilerinin çalınması, kamu kurumlarının ve özel şirketlerin önemli bilgilerinin çalınması, silinmesi ve çeşitli faaliyetlerinin engellenmesi gibi eylemler bilişim suçlarının önemini ve ciddiyetini ortaya koymaktadır. Teknik konuların yanında günümüzde bilgisayar güvenliğinin ekonomik, mali ve risk yönetimi boyutları önem kazanmıştır.

Türkiye'de okuma yazma oranı %87, bilgisayar okur yazarlığı %5'tir. Bilgisayar sayısı 2004 yılı 7 milyon, 2005'de 9 milyon, internet abonesi 2004 yılı 6,9 milyon 2005'de 8,5 milyon, internet kullanıcı sayısı 14 milyon civarındadır. İnternet kullanımının %19 olduğu belirtilmiştir. Görüldüğü gibi ülkemizde bilgisayar ve internet kullanım oranları düşük seviyelerdedir fakat hızlı bir yükseliş söz konusudur. İnternet kullanım oranın 2010 yılında %51 olması beklenmektedir. Dünyadaki internet kullanıcısı sayısı 694 milyon, ABD'de ise 152 milyondur. Türkiye nüfusunun yüzde 77'si bilgisayar, yüzde 82.4'ü ise hiç internet kullanmamaktadır [5-6,8].

Business Software Alliance (BSA), International Data Corporation (IDC) firmasına Türkiye'nin de dahil olduğu 70 ülkede "Korsan yazılımın ülke ekonomilerine etkileri" konulu bir araştırma yaptırmıştır. Araştırma bulgularına göre Türkiye'deki bilişim teknolojileri sektörü 2,4 milyar dolar değerindedir. Sektördeki mevcut 6600 kuruluş, 50 bin kadar insana iş imkanı sağlamakta ve vergi gelirlerine yıllık 650 milyon dolar katkıda bulunmaktadır [7].

Yapılan bu çalışmada bilişim suçları kavramı hakkında genel bilgiler verilmeye çalışılmış, bilişim suçlarının özel bir alanına değinilmemiştir. Devlet Planlama Teşkilatının, Nisan- Haziran 2005 tarihlerinde yaptığı, Hane Halkı Bilişim Teknolojilerini Kullanımı Araştırması sonuçlarına göre, yüksekokul, fakülte ve daha üstü mezun olanların son üç ay içinde bilgisayar kullanım oranı %69,85 ve internet kullanım oranı %62,64'tür [8]. Bu oran diğer kademelerdeki okul mezunlarına göre daha yüksektir. 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.

Çalışmanın 2. Bölümünde genel olarak internette işlenen suçlar ve bu suçların işleniş yöntemleri üzerinde durulmuştur. 3. Bölümde bilişim suçlarının hukuki boyutu, emniyet teşkilatımızın konuyla ilgili yapılanması ve delillendirme sürecinde yaşanan sorunlar üzerinde durulmuştur. Yine bilişim suçlarıyla mücadele kapsamında bireysel ve kurumsal sorumluluklarımız ve eğitimin önemi açıklanmıştır. 4. Bölümde ülkemizdeki eğitimli insanların bilişim suçları kavramı hakkındaki görüşlerini öğrenebilmek için üniversite öğretim elemanları ve öğrencilerine bir anket uygulanmıştır. Anket internet üzerinden gerçekleştirilmiş, deneklere kendileriyle ilgili bilgiler haricinde 30 soru yöneltilmiştir. Anket 766 kişiye uygulanmış veriler SPSS 11 programı kullanılarak değerlendirilmiştir.

2. GENEL OLARAK İNTERNETTE İŞLENEN SUÇLAR

İnsanlar her zaman hızlı bir değişim içinde bulunmuş ve kendi doğası içinde hep yeni şeyler arayışı içinde olmuşlardır. İnsanoğlunun eski alışkanlıklarını bıraktığı ve hızla çağa ayak uydurduğu şu günlerde, bunu en güzel yansıtan şey ise şüphesiz internettir. İnternet toplum yaşamında köklü değişiklikler meydana getirmiştir. Bu bilgi denizi sayesinde, kafanıza takılan herhangi bir sorunun cevabına çok kısa sürelerde ve çok farklı kaynaklardan cevap bulunabilinir. Daha önce günlerle ölçülen sürelerde gerçekleştirilen bilgi iletişimini saniyelerle ölçülen sürelerde ve miktar kısıtlamasına tabi tutulmaksızın yapabilir, piyasaya yeni çıkan müzikleri dinleyebilir, kitap okuyabilir ve istediğiniz daha pek çok şeyi gerçekleştirebilirsiniz.

90'lı yılların sonundan başlayarak ülkemizde de yaygın bir şekilde kullanılmaya başlanan internet, günümüz kitle iletişim araçları içerisinde yerini almıştır. İnternetin, gündelik iş yaşamından devlet kurumlarına, ekonomiden ticarete, bankalardan hastanelere, medyadan adliyelere, hastanelerden daha adını sayamayacağımız kadar çok alana yayılmış olması ve bilgilere bir klavye tuşuna dokunarak ulaşmak isteyen insanların varlığı bu iletişim aracının kullanıcı sayısını her geçen gün daha da artırmaktadır. Bilişim sistemlerinde meydana gelen gelişmeler, bu sistemlerin maliyetini düşürmüş, düşen maliyetler fiyatlarda azalmaya yol açmış ve bunun doğal sonucu olarak bilişim sistemleri normal gelir düzeyine sahip insanlar tarafından kullanılabilir olmuştur.

Bilişim sistemleri kullanımı toplum hayatında büyük etkiler meydana getirmiştir. Bu etkilerin bir kısmı yukarıda izah edildiği gibi toplum hayatını kolaylaştırmaya, üretimi ve kaliteyi artırmaya yönelik olumlu etkilerdir. Bilişim sistemleri kullanımının toplum hayatında yaygınlaşması ile beraber, bu yaygın kullanımın sonucu olarak bazı olumsuz etkiler de görülmeye başlanmıştır. Bilişim sistemleri kullanımının yaygınlaşmasının, daha önce insan gücüne dayanan alanlarda otomasyonu getirip, insan gücüne ihtiyacı azaltacağından, işsizlik

yaratacağı muhakkaktır. Ancak bu olumsuz etki, bilişim sistemlerinin kullanımına karşı olanların İddia ettiği ölçüde olmayacaktır. Nitelikli işgücüne her zaman ihtiyaç bulunacaktır.

Bilişim sistemlerinin, toplum hayatında meydana getireceği diğer bir olumsuz durum ise; insanların uzun süre bu sistemler ile uğraşacağı, bu durumun sosyal yaşamlarını olumsuz etkileyeceği, yüz yüze sosyal ilişkilerin gerileyeceği yönündedir.

Kişilerin özel hayatına müdahale kapsamında da, bilişim sistemlerinin getirdiği olumsuz etkiler görülmektedir. Kamu kurumları, bankalar, finans şirketleri, kredili mal satan firmalar, belirli işlemler için, özel bilgilere ihtiyaç duymakta ve ilgili kişilerden bu bilgileri almaktadırlar.

İnternetin toplum yaşamında giderek daha fazla yer alması ve kullanım alanının günden güne genişlemesi, doğal olarak bazı hukuki sorunları da beraberinde getirmiştir.

Gerçekten, interneti iletişim, bilgi edinme ve paylaşım gibi iyi amaçlarla kullanan kullanıcıların varlığına karşılık, sabotaj veya karışıklık oluşturmak amacıyla çeşitli sistemlerin açıklarını bularak bu sistemlere atak yapan ve sisteme izinsiz girerek çeşitli hasarlar meydana getiren “Programcılar” ve “Korsanlar (Hackerlar)” ortaya çıkmıştır. Bilişim teknolojisinden faydalanarak terör örgütleri faaliyetlerini internet ortamına taşımışlardır. Ayrıca hırsızlık ve dolandırıcılık gibi suçların bu ortamda işlenmeye başlanması, internette izinsiz yayınlanan film, müzik ve oyunların oluşturduğu lisans hakları ihlalleri şeklindeki suçların genişlemesi, hakaret amaçlı sitelerin kurulması ve pornografi ve çocuk pornografisi gibi yasadışı yayınların giderek artması, internetin kötü amaçla kullanılabileceğini göstermiştir [9].

2.1. Bilgisayar Sistemlerine Yapılan Saldırılar

Bilişim suçlarını, klasik suçlardan ayıran özelliklerden belki de en önemlisi, bu suçların maddî hareketinin (modus operandi) tespitinin zorluğudur. Bilişim suçlarında, suçu oluşturan maddi hareket, çeşitli şekillerde oluşabilir. Bilişim sistemlerine karşı işlenen suçlarda, maddi hareket herhangi bir virüs, truva atı, zaman veya mantık bombası olabileceği gibi bilişim sistemine yönelen etkili bir eylem de olabilir. Bilişim suçlarını oluşturan maddi hareketin tespitinin zor olması, suçun işlenmesinden sonra arkada herhangi bir iz bırakılmamasından kaynaklanmaktadır. Ayrıca bu hareketlerin milisaniyelerle ölçülen zaman diliminde gerçekleştirilebilir olması söz konusu suç tipini oluşturan maddi hareketlerin özelliklerindendir.

Bu nedenlerden dolayı bilişim suçlarını oluşturan maddi hareketlerin tanımlanmasına ihtiyaç duyulmaktadır. Ancak bu tanımlama ve tespit işlemi, hiçbir zaman sınırlayıcı değil, örnekleyicidir. Çünkü bu alan yeni maddi hareketlere açık olduğu gibi, mevcut maddî hareketler de geçen zaman içinde şekil değiştirebilecektir. Örneğin, internetin gelişmesine kadar görülemeyen birçok maddi hareket, internetin gelişmesi İle bilişim suçları dünyasında kendini göstermeye başlamıştır. Bu konuda, çeşitli yöntemlerle işlenebilen web sayfası kaçırma yöntemi örnek olarak verilebilir.

Bilgisayar sistemlerine gerçekleştirilen başlıca saldırı yöntemleri şunlardır:

1. Çöpe dalma
2. Gizlice dinleme
3. Veri aldatmacası
4. Truva atı
5. Tarama
6. Süper darbe
7. Salam tekniği

8. Gizli kapılar
9. Eş zamansız saldırılar
10. Ağ solucanları
11. Bilgisayar virüsleri
    a. Boot virüsleri
    b. Dosya virüsleri
    c. Makro/Mail virüsleri
12. İstem dışı alınan elektronik iletiler
13. Web sayfası hırsızlığı
14. Sırtlama
15. Mantık bombaları
16. Yerine geçme
17. Tavşanlar
18. Bukalemun

Bilişim dünyasındaki teknolojik ilerlemeler bu hareketlerin, icra yöntemlerini ve işlenme sıklıklarını değiştirmektedir. Çarpıcı bir örnek, bilişim suçlarından sayılan virüslerin 1996 yılı başlarında en çok (%70) disketlerin bilişim sistemlerinde kullanılması yolu ile yayılmasına karşın, 1999 yılında en çok elektronik posta yolu ile yayılmaya başlamalarıdır [10].

2.2. Dolandırıcılık suçu

Dünyanın en büyük bilgisayar şirketi olan IBM'in 2 bin kadar güvenlik danışmanının katkısıyla 500 bin elektronik cihazdan alınan verilere dayandırılarak hazırlanan raporda, bilinen bilgisayar virüsü sayısının 2004'te 28 bin 327 artarak 112 bin 438'e ulaştığı belirtildi. 2002'de saptanan virüs sayısı ise 4 bin 551'di. Ayrıca 2004'te 147 milyar e-postanın tarandığı belirtilen raporda, bunların 16'da biri, ya da yüzde 6'sının virüs içerdiği kaydedildi. 2002'de bu oran sadece %0,5 olarak belirlenmişti. Araştırmada ayrıca, küresel internet ortamında dolaşan ortalama spam oranının %75 olduğu, bunun zaman zaman e-posta trafiğinin %95'ine

ulaştığı belirlendi. 2004'ün en hızlı büyüyen tehdidinin, balık avlama (phishing) yöntemi olduğu ve bu yöntemi amaçlayan e-postaların geçen yıl %5000 oranında arttığı ve 18 milyon balık avlama girişimi saptandığı kaydedildi [11].

Günümüzde dolandırıcılık fiilinin yoğun bir şekilde işlendiği, özellikle kredi kartı sahtekarlığındaki artış nedeniyle özellikle bankaların ciddi sıkıntı içerisinde olduğu gözlenmektedir. Elektronik ortamdaki kredi kartı sahtekarlığında kullanılan başlıca yöntemler şöyledir;

Sahte müracaat yönteminde; çalıntı kimlik bilgileriyle bankalardan kredi kartı çıkartılarak harcama yapılmakta, asıl kimlik sahibi ise kendi adına yapılan harcamalardan hakkında başlatılan icra takipleri sırasında haberdar olmaktadır.

Sahte kart yönteminde; Avrupa'da limiti yüksek kredi kartı bilgileri bir şekilde elde edilerek, elektronik şeritler Türkiye'deki banka kartlarının plastiklerine basılıp piyasada kullanılmaktadır.

Hacking yönteminde; korsanlar virüs programlarıyla banka kart ve müşteri bilgilerini çalabilmektedir. Bankalar önlem olarak sanal klavye kullanma yolunu seçmişlerse de korsanlar yeni geliştirdikleri ekran kopyalama usulü ile sanal klavyelerin şifrelerini de çözebilmektedirler.

Web bağlantı yönteminde; bankaların internet ortamındaki sayfaları kopyalanarak tuzağa düşürülen kullanıcılar kendi bankasının internet sitesine girdiğini zannederek hackerlerin denetimindeki sayfaya bankacılıkla ilgili tüm bilgilerini bırakabilmektedir.

Kablosuz internet hırsızlığı yönteminde ise, kablosuz internet erişimi sağlanan ortamlarda dizüstü bilgisayarlardan ya da ev bilgisayarlarından girilen bilgiler internet ortamında kopyalanabilmektedir [12].

Balık avlama yöntemi (phishing) denilen yani kısaca bankanızın, e-postanızın veya bunun gibi bilgi girmenizi gerektiren bir kuruluşun web sayfasının bir kopyasını yapıp kullanıcının hesap bilgilerini çalmayı amaçlayan bir internet dolandırıcılığıdır. İngilizce "balık tutma" anlamına gelen "fishing" sözcüğünün “f” harfinin yerine “ph” harflerinin konulmasıyla gelen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenerek oluşturulmuş ve uygulanmaktadır [13].

Kullanılan yöntemlerin başında e-posta ile gönderilen sahte mesajlar gelmektedir. Bu e-posta, bir ticari kurumdan (bankalar, alışveriş siteleri vb.) geliyormuş gibi bir izlenim oluşturur. Bu, kullanıcının kendisine ait bilgileri girmesi için kurumun internet adresine ilişkin bağlantıya tıklamasını içeren bir e-posta olabilir. E-posta içeriği kişisel bilgilerin güncellenmesi, sistemdeki yeniliklerin hesabınızda aktif olması için şifrenizi girin gibi mesajlardır.

Bunu gören kullanıcı e-posta ile gelen mesajdaki bağlantıya tıkladığında kurumun web sitesinin birebir kopyası olan başka bir sayfaya yönlendirilir. Burada girilen şifre gibi özel bilgiler artık başkasının eline geçer.

E-posta kullanım oranının çok yüksek olması bu tür online dolandırıcılık işlemlerinin e-posta yoluyla gerçekleşmesinde temel etmenlerden biridir. E-posta içeriğinde belirtilen bağlantı (genellikle ticari kurumların web sitelerine yönelik sahte gösterim) kullanıcıların aldanmasında büyük rol oynar. İnternet kullanıcısı, üyesi olduğu ticari bir kurum sitesine yönlendirildiğini sanıp kendisine belirtilen yönergeleri uygular. Sonuçta online dolandırıcılık işlemiyle gerçekleşir. Balık avlama ataklarındaki önemli artış internet tarayıcı (browser) uygulamalarının (İnternet Explorer, Mozilla Firefox, Opera vb.) güvenlik sorunlarını da ön plana çıkarmıştır [14].

Balık avlama yöntemi kullanarak bilgisayar kullanıcılarını tuzaklarına düşüren dolandırıcılar özellikle aşağıda belirtilen işlemleri çalıyorlar;

1. Kredi ve banka kartı numaraları
2. Şifreler ve parolalar
3. Hesap numaraları
4. İnternet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri [13].

Rastlanılan balık avlama ataklarının temel konusunu YTL güncelleme işlemi içermektedir. YTL güncelleme konusunda internet kullanıcılarına iki çeşit e-posta gönderilmektedir. İlk e-posta "YTL'ye geçiş işlemleriniz..." başlığı adı altında internet kullanıcılarına yollanmıştır. Bu e-postayı gönderen kişi "T.C. Merkez Bankası", gönderen e-posta adresi merkezbankasi@tcmb.gov.tr" görülmektedir. T.C. Merkez Bankasından gönderilmiş havası verilen bu e-postanın amacı tamamıyla kullanıcıyı yanıltmak. Kullanıcı, T.C. Merkez Bankasına ilişkin belirtilen web adresine tıkladığında http://www.onlinebanka.net/tcmb/ şeklinde belirtilen bir adrese yönlendirilecektir [14].

Balık avlama ataklarının büyük çoğunluğunu ticari kurumların internet sitelerine ilişkin konular işlemektedir.

Bazı gelen e-postalar da müşteriye kişisel bilgilerini güncellemesi gerektiği tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verebilmeleri için gerekli olduğu söylenmektedir.

Başka bir teknikte ise, bazı bankaların cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi bağlantısı verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istenmektedir.

Aşağıda kullanıcıya gönderilen bir e-posta görülmektedir.

Sayın Garanti Bank müşterisi...

Son dönem içerisinde yaşanan internet yolu ile dolandırıcılık girişimlerini engellemek amacıyla sizler için *şifrematik* sistemini Türkiye'de ilk defa kullanmaya başladık. Bu güvenlik sisteminin temelini tam olarak oturtmak amacıyla şimdi yaptığınız bütün işlemler ve anlık şifreniz cep telefonu numaranıza bildirilecektir. Bu yeni güvenlik sisteminin işleyişi su şekildedir; İnternet bankacılığına giriş yaptığınızda cep telefonu numaranıza anında bilgi mesajı SMS yolu ile ulaştırılır. Ve yaptığınız bütün Havale/Eft/Nakit Avans işlemleri seçiminize göre cep telefonunuza bildirilir. SMS aktivasyonu işlemini bütün müşterilerimizin yapması sizlerin güvenliği için zorunlu hale getirilmiştir.

Lütfen burayı tıklayarak web sitemiz üzerinden interaktif hesabınıza giriş yaparak uyarıların ulaşacağı cep telefonu numarasını müşteri bilgilerinize ekleyin.

İnternet şubesine ulaşmak için burayı tıklayın.

İnternet bankacılığı şifrenizi almak için burayı tıklayın.

Yine kullanıcıya gönderilen başka bir e-posta aşağıdaki gibidir.

Sayın müşterimiz

Son dönem içerisinde yaşanan internet yolu ile dolandırıcılık girişimlerini engellemek amacıyla SMS yolu ile bilgi servisini devreye sokmuş bulunmaktayız. Bu güvenlik sisteminin temeli; interaktif bankacılığı kullanarak yaptığınız bütün işlemler ve anlık şifreniz cep telefonunuza gelmesinden ibarettir. İsleyişi kısaca su şekildedir; internet bankacılığına giriş yaptığınızda cep telefonunuza anında bir bilgi mesajı SMS yolu ile ulaştırılır ve yaptığınız bütün *Havale/Eft/Nakit avans* işlemlerinde cep telefonunuza gönderilen bir SMS ile teyit alınır. Bu nedenle sistemimize girilen cep telefonu numaranızın doğru olması gerekmektedir. Lütfen aşağıdaki linki, ya da logomuzu tıklayıp bankamıza login olduktan sonra *"Tanımlamalar"* menüsünden "*Bilgi*

güncelleme” ye tıklayarak ortada çıkan *"Telefon ve fax bilgileri"* butonuna tıklayınız. Telefon numaralarınız karşınıza çıkacaktır. Oradaki cep telefonu numaranızı güncelleyiniz.

http://www.garanti-banka.com/

Eğer yukarıdaki linke tıklayamıyorsanız lütfen fare ile seçerek adres çubuğuna (copy+paste) kopyala yapıştır yaparak adrese ulaşın.

Dikkat: Lütfen Garanti Bankası üzerinden gelmeyen mailleri dikkate almayınız.

Bu e-postalar sayın müşterimiz ile başlamaktadır, oysa bankalar müşterilerinin isimlerini belirtirler. Yine bu e-postalarda belirtilen bağlantılara bağlanıldığında internet adresleri sayısal rakamlar içeren adreslerle karşılaşılmıştır. Halbuki web sitelerinde; adresler çoğunlukla adres kısmı, ardından firmanın ve şirketin ismine ek olarak, com, org, net gibi uzantılar ile biter.

2.3. Siber Terörizm

Konunun bir diğer yönünü ise siber terörizm oluşturmakta olup şu an tüm netliğiyle hissetmediğimiz bu kavram üzerinde durulması gereken bir diğer bölümdür.

Siber terörizm kavramının yazılı ve görsel medyada, ulusal ya da uluslararası arenada çok fazla kullanılmaya başladığı görülmektedir. Trojanlar, kurtçuklar, virüsler siber terörizmin basit araçları olarak görülebilir. Son yıllarda terör ve terörizm konularına çok büyük bir önem verildiği görülmektedir.

Hemen hemen bütün ülkelerin gitgide bilgisayar ve iletişim teknolojilerine kaçınılmaz olarak bağımlı olması, içinde bulundukları risk durumlarının da, buna bağlı olarak artmasına yol açmaktadır.
Bilgisayar ve internet kullanımının yaygınlaşmasıyla siber terör faaliyetleri de artacaktır. Aşağıda belirtilen noktalar bu tehlikeyle ilgili bazı ipuçları verecektir.

Teröristler siber terörizmle;

- Kentin bütün trafik ışıklarını durdurabilirler
- Telefonları felç edebilirler
- Elektrik ve doğalgazı kapatabilirler
- Bilgisayar sistemlerini karmakarışık hale getirebilirler
- Ulaşım ve su sistemlerini allak bullak edebilirler
- Bankacılık ve finans sektörünü çökertebilirler
- Acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilirler
- Hükümet kurumlarını alt üst edebilirler [2].

Gelişen teknoloji ile birlikte, terör yöntemleri de bu gelişen teknolojilere paralel olarak kabuk değiştirmekte ve dünya üzerindeki tüm ülkeleri bu yeni terör tipi, yani siber terör saldırıları tehdit etmektedir. 11 Eylül 2001 tarihinde ABD'de meydana gelen ve dünyayı etkileyen terör olayı, teröristlerin ve terör gruplarının internet ve teknoloji kullanarak sınır tanımayan bir şekilde eylemlerde bulunulabileceğini göstermiş ve tüm dünya ülkelerinin bu olaydan kendi kendilerine ders almalarını sağlamıştır. Globalleşen dünyada siber terör tehditlerini gün be gün daha iyi hisseden ülkeler, bu tehdit karşısında kendilerini daha iyi savunmak için çeşitli tedbirler almaya ve bu tehdide karşı gereken önemi vermeye başlayarak hazırlıklı bulunmaya çalışmaktadırlar. Siber terörizm kapsamında bazı ülkeler, kendi çıkarlarına ve propagandalarına hizmet etmesi amacıyla hacker'lar yetiştirmektedir.

İnternetin özellikle devletlerarası istihbarat faaliyetlerinde de yoğun şekilde kullanıldığı bilinmektedir. Bununla ilgili olarak Echelon projesi ve uygulaması bunların en önemli bir örneğidir. Echelon uydular aracılıyla yapılan tele haberleşme türlerinin küresel izlenmesi projesidir. Bu projenin uygulanmasında, ABD, İngiltere, Kanada, Avustralya ve Yeni Zellanda güvenlik ve istihbarat örgütleri işbirliği yapmaktadır. Echelon, muazzam bir istihbarat akışını işleyen teknolojiyi hizmete sokmuş bir projedir.

Echelon ile tüm dünyanın faks, telefon, telgraf, e-posta, cep telefonu ve internet ağı dinlenmektedir. Böylece, sistem sadece iletişimi kayıt etmekle kalmayıp, iletişimin koordinatlarını da belirlemektedir. ABD, Echelon vasıtasıyla tüm uluslararası ihaleleri takip edip rakiplerinin tekliflerini kendi ülkesinin katılımcılarına bildirmektedir. Bu durum, ticarette siber terör olarak nitelendirilebilir [15].

Siber terör faaliyetlerinin giderek artması karşısında temel yasal düzenlemelerin yapılmamış olması bazı ülkelerde sorunlar doğurmuştur. Bu sorunların çözümü için birçok ülke, kendi iç hukuklarına uygun uluslararası sözleşmeler çerçevesinde özel yasalar çıkarak siber terörün önüne geçmeye çalışmış, özel birimler kurarak bu tehlikeyle savaşma yoluna gitmiştir.

3. BİLİŞİM SUÇLARIYLA MÜCADELE

Gerek Türkiye'de gerekse diğer dünya ülkelerinde bilişim ve teknoloji araçları kullanılmak suretiyle işlenen suçlar her geçen gün artmaktadır. Bilişim suçları ile mücadelede, yeterli hukuki alt yapı, uluslararası işbirliği, bilgisayar programı ve bilgisayarlarda en son teknolojinin kullanılması ve iyi eğitilmiş personelin önemli rolü olduğu söylenebilir. Amerika Birleşik Devletleri başta olmak üzere Avrupa ülkelerinin birçoğunda olduğu gibi Türkiye'de de bu suçlarla etkin bir şekilde mücadele etmek halen birçok soru işaretini üzerinde bulundurmaktadır.

ABD'de San Francisco Federal Bürosu (FBI)'nun bilgisayara zorla girme ekibi ile Bilgisayar Güvenlik Kurumu (CSI) tarafından 10 yıldır bilgisayar suçları ve güvenlik araştırması yapılmaktadır. Bu yılki araştırma sonuçları devletlerdeki şirketlerden, devlet acentelerinden, mali ve tıbbi kurumlarından ayrıca üniversitelerden 700 bilgisayar güvenliği uygulayıcısının cevaplarına dayanmaktadır.

Katılımcılar şirket içerisinden suç işleyenlerin en az dışarıdan bilgisayarlara girmeye çalışanlar kadar fazla olduğunun farkındadır. Yıldan yıla farklılıklar görünse de bu olaylar içerden de ve dışardan da aynı sıklıkta gerçekleştiriliyor. Buradan çıkarılması gereken ders oldukça basittir, firmalar tüm çevrelerden gelecek saldırılara karşı hazırlıklı olmalıdır. Şifreler, biometrikler, anti-virüs yazılımları ve izinsiz girişi tespit eden sistemler gibi teknik bilgisayarlar güvenlik önlemlerinin kullanımı bir firmanın bilgisayar güvenliğini tamamen sağlayamadığı gibi bununla bağlantılı mali kaybı da ortadan kaldıramamaktadır. Bu nedenle, teknik güvenlik önlemlerine rağmen büyük ölçüde mali kayıp riski altında olan firmaların çözüm olarak sigorta şirketlerine başvurmamaları normaldir. Sigorta şirketlerinin henüz sanal güvenlik sigorta oranlarını dayandırabilecek güçlü verileri olmasa da, kimi şirketler bu tarz poliçeler sunmaktadır.

Araştırma sonuçlarını kısaca özetlersek;

- Virüs saldırıları mali kayıpların en önemli nedeni olmaya devam etmektedir.
- Katılımcılara göre yetkisiz bilgisayar sistemleri kullanımında çok az bir artış olmuştur.
- Diğer yandan, araştırmaya katılanlar sanal suçun neden olduğu dolar bazında toplam mali kayıpta düşüş olduğunu belirtmişlerdir.
- Web sitesi ile ilgili suçlarda bariz artış olmuştur.
- Devlet kurumları günümüzde tüm endüstri ve yönetim alanlarında çalışan işçiler için yatırım ve harcama yapan en büyük bilgi güvenliğine sahiptir.
- Bilgi sızdırma olaylarının geçen yılla neredeyse aynı olduğu görülmüştür.
- Sanal sigorta kullanımı düşüktür.
- Bilgisayarlara zorla giriş olaylarını yargıya intikal ettiren kurumların sayısı da kötü bir üne sahip olacakları korkusu ile büyük oranda azalmaktadır.
- Kurumların %87'sinden fazlası güvenlik denetlemeleri yürütmektedir [16].

Genel anlamda Türkiye'de bilişim ve teknoloji başlığı altında işlenen suçları mercek altına aldığınızda Türkiye'de iletişim, internet hizmetleri, e-devlet hizmetleri, e-ticaret hizmetleri ve buna benzer konularda faaliyet yürüten tüm kurum ve kuruluşlara çok önemli işler düşmektedir.

Modern toplumlarda sosyal düzenin sağlanması ve geliştirilmesinden sorumlu tutulan polis, günümüzde geleneksel suça müdahale edici yaklaşımını terk ederek, suç önlemeye yönelik çalışmalara odaklanmaktadır.

3.1. Kişilerin ve Kurumların Alması Gereken Önlemler

ABD'de yapılan bir araştırmaya göre pornografik içerikli sitelere girişler, mesai saatleri olan 9.00-17.00 arasında doruğa çıkmaktadır [17].

Bilişim suçlarıyla mücadelede alınması gereken önlemlerin ilki, kişilerin ve kurumların kullandıkları bilişim sistemlerinin güvenliğini sağlamalarıdır. Bununla kastedilen; sistemde bulunan verilerin ve sistemin kendisinin, gizliliği, bütünlüğü ve kullanıma yönelik her türlü tehlikelere karşı güvenliğin sağlanmasıdır .

ICQ sohbet programını kullanan ve online olan kullanıcıların ICQ kimlik numarasına (icq account number) dayanarak çeşitli yazılımlar ile IP no'ları tespit edilebilmektedir. IP no'larından kurumların bilgisayar ağlarına girmek ve birçok işlem yapmak mümkündür.

Bugün için en yaygın olan, uygulamada en çok başvurulan ve etkili olan önlemler ise; bilişim sistemlerinde güvenlik duvarı yazılımlarının bulundurularak yetkisiz erişimlerin önüne geçilmesi ve bilişim sistemlerine anti-virüs yazılımları yüklenerek ve bu yazılımlar internet üzerinden sürekli güncellenerek yeni virüslerin bilişim sistemine girmesinin önlenmesine, girenlerin ise temizlenmesine çalışılmasıdır. Bu güvenlik önlemleriyle, hem bilişim sistemleri için öngörülen güvenlik, hem sistemde bulunan verilerin gizliliği ve yetkisiz erişimlerin önlenmesi, hem de sistemin kesintisiz olarak çalışması sağlanmalıdır.

3.1.1. İnternet servis sağlayıcılar (İSS) ve cep telefonu servislerinin (GSM) yükümlülükleri

İnternete bağlanma ancak bir İSS üzerinden erişim yolu ile mümkündür. Bu her türden kullanıcılar açısından istisnasız bir kuraldır. İnternet bağlantısı dünyada var olan telefon hatları üzerinden sunulmaktadır.
Yapı olarak bu güne kadar internetten farklı bir çizgi üzerinde bulunan GSM servisleri birer internet servis sağlayıcısı özelliği kazanarak abonelerini internet temelli birçok uygulamayla buluşturmuşlardır.

Avrupa Birliği, üye devletler arasında ortak bir mevzuat oluşturmak amacı ile 1998 tarihli Avrupa Komisyonu Direktifi ismi verilen bir öneri metni yayınlamıştır. Prensip olarak bu metinde İSS için cezai sorumluluk öngörülmemiştir. Ancak eğer İSS, yasa dışı faaliyetten haberdarsa ve buna rağmen bir girişimde bulunmazsa ya da kanuna aykırı içerikli yayını öğrendikten itibaren, erişimini engellemek için gerekli önlemleri almaz ise cezai sorumluluktan muaf tutulmaz [18].

Ayrıca bazı internet servis sağlayıcıların internet aboneliği yaparken kişilerin gerçek bilgilerini almamakta, asılsız isim ve adreslerle kayıt yapmaktadırlar. Bu durumda bu İSS'lardan abonelik ve e-posta hizmeti alan kişiler işledikleri suçlarda tespit edilememektedir [19].

İSS'nin sadece internet erişimini sağlamayı vaat ettiği bir sözleşme sonucunda, kullanıcının o erişim ile gerçekleştireceği fiillerden İSS'yi sorumlu tutmak yanlış bir yaklaşım olacaktır. Kaldı ki teknik olarak da İSS'nin, kendi üzerinden erişim gerçekleştiren bütün abonelerinin internet ortamındaki hareketlerini takip etmesi mümkün değildir. Bu nedenle İSS'nin, bir bilişim suçunda faile yardım ve yataklık eden konumunda düşünülmesi doğru değildir. İnternet bağlantısı yolu ile gerçekleştirilen suçlarda failin kim olduğunun tespiti oldukça zor bir konudur. Ancak failin kimliğinin tespitinde İSS'nin önemi çoktur. İSS'nin kullanıcıya vermekte olduğu erişim hizmeti boyunca kullanıcının adres ve kimlik bilgilerini kontrol etmesi beklenmese de failin tespiti aşamasında İSS'nin işbirliği kesinlikle gerekeceğinden bu konuda sorumluluk altına alınmalıdırlar [18].

İnternet servis sağlayıcıların ne tür kayıtları ne kadar süre ile saklayacakları yasalarımızda belirtilmediği için bu konuda belirsizlikler ve değişik uygulamalar yaşanmaktadır. Cumhuriyet Baş Savcılıklarından edinilen bilgilere göre GSM servislerinin internet uygulamalarında (internet üzerinden melodi transferleri, mesajlaşmalar, kontür yükleme ve GPRS internet erişimi gibi) internet erişim kayıtlarını tutmadıkları anlaşılmıştır.

Yaşanılan bir olayda, bir GSM kullanıcısının internet üzerinden mesaj gönderme, melodi yükleme ve benzeri işlemleri yapmasını sağlayan kullanıcı kimlik ve şifre bilgileri üçüncü bir kişi tarafından elde edilerek şahısın cep telefonu hesabından altı milyar lira tutarında hakaret ve uygunsuz sözler içeren mesajlar değişik kişilere gönderilmiştir. Fakat ilgili GSM firması söz konusu internet kayıtlarını tutmadığı için şikayetçi kişi adına mesajları gönderen suçlu kişiye ulaşılamamıştır [19].

3.1.2. İnternet kafelerin sorumlulukları

İnternet hizmetlerinin sunulduğu ve sosyal hayatın bir parçası haline gelen internet kafeler, eğitim, bilgi, kültür ve araştırma amaçlı olarak kullanılabileceği hiçbir zaman göz ardı edilmemelidir. Sayıları hızla artan internet kafeleri genellikle çocuklarla gençlerin tercih ettikleri göz önüne alındığında internet kafelerin sağlıklı bir yapıya kavuşturulmaları, bilgi toplumuna katkı sağlamaları amacıyla eğitim amaçlı merkezler haline getirilmeleri ve suç unsuru mekanlardan uzak tutulmaları için bu mekanların denetlenmesi büyük önem teşkil etmektedir. Çünkü Cumhuriyet Baş Savcılıklarından intikal eden her üç suç dosyasından ikisinin buralar üzerinden işleniyor olması gerçeği dikkatlerin buralara çekilmesi için yeterli bir sebeptir. İnternet kafeler tarafından sağlanan denetimsiz ve anonim bağlantıya izin veren İnternet erişim modeli teröristler tarafından takip edilmelerini ciddi biçimde güçleştirdiği için tercih ediliyor. Günün yoğunluğu içinde kalabalığa karışarak bir bilgisayar terminalini kullanan teröristlerin fark edilmeleri ise neredeyse imkansız durumdadır. Batı ülkeleri, internet kafelerle ilgili olarak yasal düzenlemeleri yapmış ve halen iyileştirmeler yapmaktadırlar.

Kamu ve eğitim kurumları bilişim suçlarının işleniş yerleri arasında önemli bir yer almaktadırlar. Yapılan çalışmalarda konusu itibari ile tehdit, hakaret ve internet sitesi içeriğinin değiştirilmesi gibi şikayet dilekçelerinin aydınlatılması çalışmalarında suçlu olarak kamu kurumlarına veya eğitim kurumlarına

ulaşılmış ancak suçlu şahıslara ulaşılamamıştır. İnternet üzerinden işlenmesi muhtemel bütün suçları buralarda işlemek söz konusudur. Bu durum karşısında kurumların bu konuda mevcut sistemleri içerisinde bilgisayarlarda yapılan işlemlerin kayıtlarını tutması gerekmektedir [17].

3.2. Bilişim Suçları ile Mücadelede Hukuk

Bilgi toplumuna geçişte başlıca etken olan bilişim teknolojilerinin, hem ülke ekonomileri için öneminin giderek artması, hem de bu teknolojilerin toplumsal yaşama etkin bir şekilde girmesiyle birtakım sorunların yaşanmaya başlaması, ülkelerce çeşitli yasal düzenlemeler yapılmasını gerekli kılmıştır. Suçların teknik olarak engellenmesinin mümkün olmayacağı bu noktada, teknolojik suçlarla mücadelede hukukun tartışılmaz üstünlüğü ortaya çıkmaktadır. Bu yüzden en iyi çözüm hukuk alanında yapılacak değişimlerdir. Bilişim suçlarının alanına hangi faaliyetlerin girdiğinin tespiti uygulamanın ve yargılamanın başlıca sorunudur.

Mevcut hukuk sistemlerinin bu yeni teknolojiler karşısında yetersiz kalışı, yeni düzenleme ve yaklaşımları zorunlu kılmıştır. Bu sorun genel hatları ile değerlendirildiğinde suçun işlenmesinde bilgisayarın rolü önem kazanmaktadır. Suç bilgisayar kullanarak mı gerçekleştirilmiştir, yoksa bilgisayar o suçun işlenmesinde yardımcı bir unsur olarak mı kullanılmaktadır? Bankaların ATM uygulaması bilgisayar temelli olduğu için bilişim faaliyetidir. Çünkü bu sistem çöktüğünde bu faaliyet asla gerçekleştirilemez. Ancak radyo ve televizyon yayıncılığı bilgisayar sistemlerini faaliyetlerinin çeşitli aşamalarında kullanmakta ise de, bunların faaliyeti bilişim temelli değil, iletişim temellidir. Yararlanma, bu yayınları bilgisayar temelli hale getirmez.

Bilişim teknolojilerindeki gelişmeler bilgisayar ağları sayesinde milli sınırları aşmış, bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmıştır. Teknolojik gelişmeler ile globalleşen

dünyamızda; tüm ülkelerin işbirliği ile bu tip suçlara karşı mücadele etme gereği ortaya çıkmıştır. Bu yüzden bilişim suçları konusunda İnterpol, Birleşmiş Milletler ve Avrupa Birliği gibi büyük organizasyonlar tarafından yapılan birçok çalışma bulunmaktadır. Ayrıca özellikle ABD ve bazı Avrupa ülkeleri kendi bünyelerinde hukuki düzenlemelerinde ve polisiye yapılanmalarında büyük ilerlemeler göstermiştir [20].

3.2.1. Avrupa siber suçlar konvansiyonu

Siber uzayın bir parçası olarak internet ortamında işlenen suçlarla mücadele etmek amacıyla, 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan; Avrupa ülkeleri ile Kanada, Japonya, Güney Afrika ve ABD dahil 33 devlet tarafından imzalandığı halde Türkiye tarafından henüz imzalanmamıştır. Avrupa Konseyi Siber Suç Sözleşmenin hedeflerine baktığımızda aşağıdaki maddelerden oluştuğu görülmektedir:

1) Yeni teknolojilerin kullanımı ile ilgili suçlara ait, ortak tanımların oluşturulması,
2) Soruşturma yöntemlerinin tanımlanması (veriyi saklama, trafik verisini arama, toplama ve el konulması ile iletişim yetkisi).
3) Uluslararası işbirliği için yöntemlerin tanımlanması.

Ayrıca sözleşmenin metninde bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanımına açık bulunmasına yönelik suçlar bağlamında hukuka aykırı erişim, yasa dışı müdahale, verilere müdahale, sistemlere müdahale, cihazın kötüye kullanımı fiilleri açıklanmıştır. Bilgisayarla ilişkili suçlar çerçevesinde ise sahtecilik, dolandırıcılık, telif haklarının ve benzeri hakların ihlaline ilişkin fiiller ve içerikle ilişkili olarak çocuk pornografisine yönelik fiiller, cezalandırma konuları arasında sayılmış, bu hususlarda ulusal ve uluslararası alanda gerekli etkin yaptırım ve işbirliğine ilişkin düzenlemeler belirtilmiştir [21].

3.2.2. Yeni Türk Ceza Kanunu'nda düzenlenen bilişim suçları

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.

Bilişim suçları, 5237 Sayılı Yeni Türk Ceza Kanununda şu numara ve başlıklar altında yer almaktadır:

"Topluma Karşı Suçlar", kısmının onuncu bölümünde "Bilişim Alanında Suçlar" başlığı altında 243. maddede "Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalmaya devam etme suçu". 244. maddede "Bilişim sisteminin işleyişini engelleme, verileri bozma, verileri yok etme, verileri değiştirme, verileri erişilmez kılma, sisteme veri yerleştirme, sistemdeki verileri başka yere gönderme, bilişim sistemi aracılığı ile çıkar sağlama suçları". 245. maddede "Banka veya kredi kartlarının kötüye kullanılması suçu" düzenlenmiştir.

"Kişilere karşı suçlar" kısmının dokuzuncu bölümünde "Özel hayata ve hayatın gizli alanına ilişkin suçlar" başlığı altında 135. maddede "Kişisel verilerin kaydedilmesi suçu", 136 ve 137. maddelerde "Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu", 138. maddede "Verileri yok etmeme suçu",

Yeni Türk Ceza Kanunundaki bu düzenlemelerin yanında, bilişim sistemleri ile işlenebilecek ancak tek başlarına tamamen bilişim suçu olarak adlandırılamayacak suç tipleriyle ilgilide düzenlemeler yapılmıştır. Bunlar : 81 ve 82. maddelerde "Kasten öldürme suçu", 105. maddede "Cinsel taciz suçu", 106. maddede "Tehdit suçu", 107. maddede "Şantaj suçu", 123. maddede "Kişilerin huzur ve sükununu bozma suçu", 124. maddede "Haberleşmenin engellenmesi", 125. maddede "Hakaret suçu", 132.

maddede “Haberleşmenin gizliliğini ihlal suçu”, 133. maddede “Kişisel konuşmaların dinlenmesi ve kayda alınması suçu”, 134. maddede “Özel hayatın gizliliğini ihlal suçu”, 142. maddenin 2. fıkrasının (e) bendinde “Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu”, 157 ve 158. maddelerde “Dolandırıcılık suçu”, 225. maddede “Alenen cinsel ilişkide bulunmak ve teşhircilik suçları”, 226. maddede “Müstehcenlik suçu”, 227. maddede “Fuhuşa teşvik ve aracılık suçları”, 228. maddede “Kumar oynanması için yer ve imkan sağlama suçu”, 237. maddede “Fiyatları etkilemek amacıyla yalan haber veya havadis yayma suçu”, 239. maddede “Ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi ve belgelerin açıklanması suçu”, 267. maddede “İftira suçu”, 281. maddede “Suç delillerini yok etme, gizleme veya değiştirme suçu”, 286. maddede “Soruşturma ve kovuşturma işlemleri sırasındaki ses veya görüntülerin yetkisiz olarak kayda alınması veya nakledilmesi suçları”, düzenlenmiştir. Burada sayılan suçlar bilişim sistemleri aracılığı ile de işlenebilecek suçlardır.

244. maddenin 4. fıkrasında bu suç tipi açısından, “Başka bir suç oluşturmaması halinde” ifadesi kullanılarak aynı eylemlerin gerçekleştirilerek hukuka aykırı yarar elde edilmesi ancak bunun bir başka suç tipinde düzenlenmiş olması halinde bu suç tipinin uygulanmayacağı belirtilmiştir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir [22].

Avrupa Siber Suçlar Konvansiyonunda yer alan çocuk pornografisi ile ilgili düzenlemelerin yeni TCK’da yer almaması bir eksiklik olarak göze çarpmaktadır. Çocuk pornografisi, mevzuatımızda başka şekillerde örneğin TCK’da genel ahlaka karşı fiiller bölümünde, müstehcenlik ve fuhuş suçlarını düzenleyen maddelerde yer almaktadır. Telif hakları konusundaki suçlar ile ilgili olarak mevzuatımızda TCK yerine Fikir ve Sanat Eserleri Kanunu yer almakta ancak bu kanun da özellikle bilişim sektöründeki gelişmelerin gerisinde kalmaktadır [23].

3.3. Bilişim Suçları Konusunda İdari Yapılanma

Sanal alemdeki suç, polisi de harekete geçirdi ve ülkeler suçları soruşturmak, iz sürmek, delil toplamak amacıyla polis teşkilatlarının içinde özel birimler oluşturmaya başladı.

Türk polisi ise sanal alemle ilk olarak 1997 yılında tanıştı. Başlangıçta kendi güvenliğini sağlamak amacıyla yola çıkan polis, zamanla çalışmalarını Bilgisayar suçlarına doğru kaydırdı. 2001 yılı içerisinde idari yapısı değiştirilerek "İnternet ve Bilişim Suçları Şube Müdürlüğü" ismini alan birim, organize suçlar, terörle mücadele, kaçakçılık gibi farklı birimler ya da savcılıktan gelen yardım taleplerini karşılayarak, teknik olarak yol göstermektedir [24].

Bilişim suçları konusu şu an itibariyle herhangi bir daire başkanlığının tam olarak görev alanına girmemektedir. Emniyet teşkilatı aşağıdaki yapılanmayı gerçekleştirerek ihtiyaca cevap vermeyi planlamaktadır.

1. Bilgi İşlem Daire Başkanlığı altında kurulacak İnternet ve Bilişim Suçları Araştırma ve Koordinasyon Merkezi Şube Müdürlüğü
2. Merkez birimlerinde kurulacak Bilgi İşlem ve Bilişim Suçları Şube Müdürlükleri
3. Taşra teşkilatında ilgili birimlerde kurulacak Bilgi İşlem ve Bilişim Suçları Büro Amirlikleri [3].

3.4. Bilişim Suçlarının Delillendirilmesi

Bilişim suçları ile mücadele kavramı, özellikle Türkiye için oldukça yeni bir kavramdır. Mücadele anlamında gerek hukuki gerekse teknik anlamda bazı sıkıntılar bulunmaktadır. Bu bir nevi sanal bir ortamı fiziksel bir ortam olarak ele almak anlamına gelmektedir. Bilişim suçlarında suçluların yakalanması geleneksel suçlardan farklı olarak çok daha zor olmaktadır. Suçların tespiti ve

yargılanmasındaki en önemli husus delillendirmedir. Geleneksel suçlarda “parmak izi v.b.” gibi deliller, bilişim suçlarında “Veriler ve bilgiler” olarak karşımıza çıkmaktadır. Dolayısıyla da bu kanıtların delil niteliği taşıması için sağlam bir yapıda ve değiştirilemeyecek nitelikte olması gerekir. Ancak bu bilgiler kullanıcılar tarafından istenildiği gibi değiştirilebilmektedir [25].

Delillendirme kısaca, bir suç ile ilgili o suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir. Dijital delil ise;

Shinder’e göre [26].

“Bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil”

denilmektedir.

Chisum ise dijital delilleri [27].

“Bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler”

olarak tanımlamıştır.

Son olarak Casey’in tanımına bakarsak dijital deliller [28].

“Bir suçun işlendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler”

olarak karşımıza çıkmaktadır.

Bilişim suçu sanıkları, genellikle orta seviyenin üzerinde ve hatta ileri seviyede zekaya sahip özellikler taşıyabilmektedir. Bunun sonucu olarak da,

işledikleri bilişim suçlarının delillendirilmesini engelleyici, zeka ürünü olan yanıltmalar, engellemeler, delilleri kaybettirici aldatmalar ve akla gelmedik pek çok yönteme başvurabilirler [29].

3.4.1. Delillerin elde edilmesi

Toplanan her delil soruşturma süresince polise ışık tutacak ve mahkeme aşamasında önemli sonuçlar ortaya koyacaktır. Bilgisayar suçlarında delil niteliği teşkil eden bilgiler ise; yine bilgisayar ortamında tutulmuş olan kayıtların olacağı da aşikardır. Bu kayıtların delil niteliği teşkil edebilmesi için sağlam ve değiştirilemez bir yapıya sahip olması gerekmektedir. Ancak bilgisayarın kullanıcısı tarafından belirlenen yöntemlerle kaydedilen bilgiler yine bilgisayarın kullanıcısı tarafından değiştirilebilme ihtimali taşımaktadır. Böyle olunca sağlam bir delil olmaktan çıkmaktadır. Bilişim suçlarında delil niteliği olan sadece bu kayıtlı bilgiler olduğundan dijital delillerin hukuki durumu tartışılması en önemli konulardan biri olmalıdır.

Delillerin elde edilmesi önemli bir problem olarak karşımıza çıkmaktadır. İnternete bağlanmak için bir internet servis sağlayıcıdan hizmet almak gerekmektedir. Böyle durumda internet üzerinden suç işleyen kişiye ait bilgiler sadece buralardan bulunabilir. Ancak ülkemizdeki internet servis sağlayıcıları ve özellikle de internet kafeler düzenli kayıt tutma işleminin masraflı olmasından dolayı bu sistemleri kurmamaktadırlar. Bu yüzden emniyet tarafından takip edilen bir soruşturma da kayıtların elde edilmesi aşamasında problem yaşanmaktadır. Bu durum, suçların yaygınlaşmasında önemli bir rol oynamaktadır [30].

3.4.2. 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 baslar. Bilgisayar delillendirme de bilgisayarı güvene aldıktan sonra ilk yapılacak şey, bilgisayarın bütün bilgilerinin yedeklemesinin, üzerinde çalışmadan ve tekrar gözden geçirmeden yapılmasıdır. Eğer suçu ilk fark eden kişinin bu alanda yeterli bilgisi yoksa çok önemli bilgi ve delilleri istem dışı yok edebilir.

Bilişim suçlarının yasal manada takibini yapan emniyet birimlerinin bu konuda özel bir eğitim almaları gerekmektedir. Emniyet birimlerinin eğitimi, suçlarla mücadelede ve suçluların yakalanmasında bilgisayar sistemlerini ve ileri teknoloji ürünlerini çok iyi derecede kullanarak ve olaya anında müdahale ederek kaybı çok kolay olan suç kanıtlarına ve suçlulara hızlı ulaşılmasını sağlayacaktır [29].

4. ANKET ÇALIŞMASININ DEĞERLENDİRMESİ

Bilgisayar güvenliğinin ihlallerinin nedenleri ve sonuçları ile ilgili ne kadar çok bilgiye sahip olursak bilgisayar güvenliği alanında o kadar gelişme kaydederiz.

4.1. Araştırmanın Amacı

Bilgisayar teknolojisinin hızlı gelişimi, insan hayatına getirdiği kolaylıkların yanında suç kavramına da yeni bir boyut kazandırmıştır. Suç bilgisayar ve internet sayesinde çok daha kolay işlenebilir olmuştur. Emniyet Genel Müdürlüğünün verilerine göre ülkemizde 2001 yılında 11, 2002'de 47, 2003'de 98 ve 2004'ün 11 aylık diliminde ise 224 bilişim suçu işlenmiştir [31]. 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 şikayete bağlı suçlar olduğu, delillendirmedeki güçlükler, emniyet teşkilatının bu konudaki yetersizlikleri düşünüldüğünde işlenen bilişim suçunun çok daha fazla olduğu anlaşılmaktadır. 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.

Bu nedenle ülkemizdeki eğitimli insanların bilişim suçları kavramı hakkındaki görüşlerini öğrenebilmek için bir anket uygulanmıştır.

Anket Türkiye'de yüksekokul, fakülte ve daha üstü mezun olanların bilgisayar kullanım oranlarının daha yüksek olması ayrıca bilgisayar ve internet ile profesyonel olarak daha çok öğretim elemanları ve üniversite öğrencilerinin ilgilendiği düşünülerek üniversite öğretim elemanları ve öğrencilerine uygulanmıştır. Bu anketin sadece üniversite ile sınırlı tutulmasının sebeplerinden biri bu konudaki akademik bakışı değerlendirebilmektir.

4.2. Araştırmanın Yöntemi

Bu bölümde veri toplama araçları, verilerin toplanması, verilerin çözümlenmesi ve yorumlanması konusunda bilgi verilmiştir.

4.2.1. Veri toplama aracı

Araştırma verileri, anket yöntemiyle kaynak gruplardan toplanmıştır.

Katılımcılara aşağıdaki sorular yöneltilmiştir;

I. Cinsiyetiniz

a) Kadın b) Erkek

II. Ait olduğunuz yaş kategorisini işaretleyiniz.

a. 20'nin altında
b. 20-29
c. 30-39
d. 40-49
e. 50'nin üstü

III. Üniversitedeki konumunuz

a. Öğrenci
b. Öğretim Elemanı

IV. Bölümünüz hangi alanla ilgili?

a. Fen Bilimleri
b. Sosyal Bilimler
c. Sağlık Bilimleri

1. Kaç senedir bilgisayar kullanıyorsunuz?
   a) 1,2 yıl b) 3,4 yıl c) 5,6 yıl d) Daha fazla
2. Hiç bilgisayar eğitimi aldınız mı?
   a) Evet b) Hayır
3. Günde ortalama kaç saat bilgisayar kullanıyorsunuz?
   a) 0-1 saat b)1-3 saat c) 3 saatten daha fazla

4. Sürekli kullanma imkanına sahip olduğunuz bir bilgisayar var mı?
   a) Evet b) Hayır (lütfen 11.sorudan devam ediniz)
   evetse
5. Antivirüs programı kullanıyor musunuz?
   a) Evet b) Hayır
6. Bilgisayarınızda lisanssız yazılım (program) var mı?
   a) Evet b) Hayır (cevabınız hayırsa lütfen 11. sorudan devam ediniz.)
   evetse
7. Lisanssız yazılım kullanma sebebinizi belirtiniz?
   a) Ucuz olduğundan b) Kolay bulunduğundan c) Hepsi
8. İşletim sisteminiz lisanslı mı?
   a) Evet b) Hayır
9. Lisanssız yazılım kullanmak sizi vicdanen rahatsız ediyor mu?
   a) Evet b) Hayır
10. Kullandığınız lisanssız yazılımları nereden elde ediyorsunuz?
    a) İnternetten
    b) Arkadaşlarımdan kopyalıyorum
    c) Kopya satan yerlerden satın alıyorum
    d) Hepsi
11. İnternetten müzik, film, oyun dosyaları indiriyor musunuz?
    a) Evet b) Hayır
12. İnternetten müzik, film, oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu biliyor musunuz?
    a) Evet b) Hayır (lütfen 14. sorudan devam ediniz)
    evetse
13. İnternetten müzik, film, oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunun farkındaysanız neden yapıyorsunuz?
    a) Kullandığım programları profesyonel olarak ve sürekli olarak kullanmadığım için
    b) Denetim olmadığından
    c) Maliyeti düşük olduğu için
    d) Hepsi

14. Sizce lisanssız yazılım kullanmaya karşı gerekli yaptırımın yeterince uygulanamamasının en önemli nedeni nedir?
    a) Yazılım şirketlerinin hakkını aramaması
    b) Devletin ilgili birimlerinin yeterince ciddiye almaması
    c) Yasaların yetersiz kalması veya uygulanamaması
    d) Hepsi
15. Kullandığınız bazı yazılımların, bilgilerinizi internet üzerinden başkalarına iletebileceğini biliyor musunuz?
    a) Bilmiyorum
    b) Evet bunu yapabilir ancak güvenlik programım beni korur
    c) Evet bunu yapabilir
    d) Hayır bunu yapamaz çünkü açık kod kullanıyorum yazılıma tamamen hakimim
16. Bilişim suçu kavramını daha önce duydunuz mu?
    a) Evet b) Hayır
17. Size göre aşağıdaki bilişim suçlarından en tehlikelisi hangisidir?
    a) Lisans hakları
    b) Dolandırıcılık (ATM, kredi kartı vb.)
    c) Yasa dışı yayınlar (pornografi, hakaret vb.)
    d) Bilgisayar sabotajı
18. Size göre en çok işlenen yasa dışı yayın suçu hangisidir?
    a) Pornografi b) Çocuk pornografisi
    b) Hakaret d) Siber terör
19. İnterneti en çok hangi amaç için kullanıyorsunuz?
    a) Araştırma yapmak için b) Arkadaş edinmek için
    b) Haberleşmek için
20. Yeterli bilgi ve birikime sahip olsaydınız hackerlık yapar mıydınız?
    a) Evet b) Hayır
21. İnternet bankacılığı sizce güvenli mi?
    b) Evet b) Hayır
22. İnternet üzerinden alış veriş yapıyor musunuz?
    a) Evet b) Hayır (lütfen 24. sorudan devam ediniz)

evetse

23. İnternet üzerinden alışveriş yaparken herhangi bir güvenlik problemi ile karşılaştınız mı?
    a) Evet b) Hayır
24. Size banka bilgilerinizi güncelleştirme için bankanızdan geldiği bildirilen bir e-posta (phishing olayı) geldi mi?
    a) Evet b) Hayır
25. Bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ilerde büyük tehlikelere yol açacağını düşünüyor musunuz?
    a) Evet b) Hayır
26. Bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesini olumlu karşılar mısınız?
    a) Evet b) Hayır
27. Bilişim suçlarını önlemek amacıyla internette gözetlenmeyi olumlu karşılar mısınız?
    a) Evet b) Hayır
28. Size göre önemli gördüğünüz bir bilişim suçuna şahit olursanız bunu ihbar etmeyi düşünür müsünüz?
    a) Evet b) Hayır
29. Bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmalarını yeterli buluyor musunuz?
    a) Yeterli b) Yetersiz c) Kesinlikle yetersiz d) Fikrim yok
30. Bilişim suçlarıyla ilgili yasalarımızı yeterli buluyor musunuz?
    a) Yeterli b) Yetersiz c) Kesinlikle yetersiz d) Fikrim yok

4.2.2. Verilerin toplanması

Anket internet üzerinden gerçekleştirilmiştir. *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.

4.2.3. Verilerin çözümlenmesi

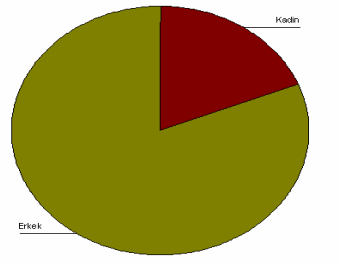
Anket kapsamında 766 kişinin görüşleri alınmıştır. Bu gruplardan toplanan veriler, istatistik yöntemlerle [frekans (f), yüzde (%), ki kare analizi] çözümlenerek değerlendirilmiş ve yorumlanmıştır. Değerlendirme SPSS 11 programı kullanılarak yapılmıştır.

4.3. Araştırmanın Bulguları

Ankete 1050 kişi katılmış fakat 766'sı anketi doğru ve eksiksiz olarak doldurduğundan değerlendirme 766 kişiye göre yapılmıştır.

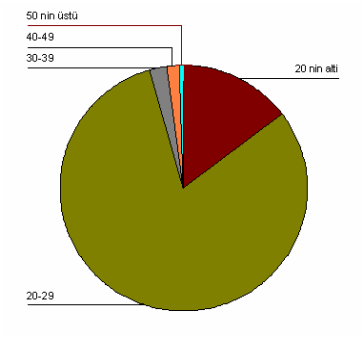
4.3.1. Grupların cinsiyet ve yaş dağılımları

Katılımcıların 177'si kadın (%23,1), 589'u erkektir (%76,9).



Şekil 4.1. Katılımcıların cinsiyet durumları

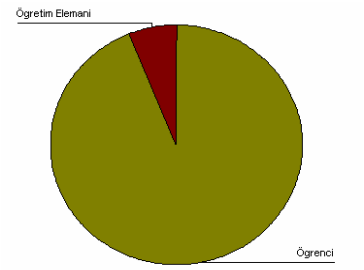
113 kişi (%14,8) 20 yaş altı, 618 kişi (%80,7) 20-29, 19 kişi (%2,5) 30-39, 12 kişi (%1,5) 40-49 ve 4 kişi de (%0,5) 50 yaş üstü gruplarındandır.



Şekil 4.2. Katılımcıların yaş durumları

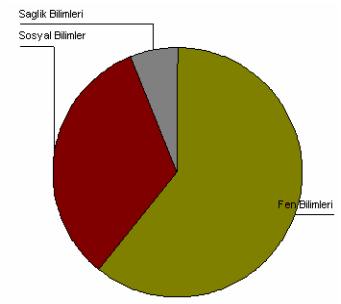
4.3.2. Grupların üniversitedeki konumları

766 katılımcının 47'si öğretim elemanı (%6,1) ve 719'u (%93,9) öğrencidir.



Şekil 4.3. Katılımcıların üniversitedeki konumları

Katılımcıların 467'si (%61) fen bilimleri, 252'si (%32,9) sosyal bilimler ve 47'si (%6,1) sağlık bilimleri alanlarına mensuptur.



Şekil 4.4. Katılımcıların üniversitedeki bölümleri

Cinsiyete göre değerlendirme yapıldığında, kadınlarla erkekler arasında önemli bir fark görülmemiştir. Öğretim elemanları ve öğrenciler arasında ise sadece önemli farklılıklar olan sorularda değerlendirme yapılmıştır.

4.3.3. Anket sorularının değerlendirilmesi

Çizelge 4.1. Bilgisayar kullanım süreleri

Kaç senedir bilgisayar kullanıyorsunuz?	f	%
1-2 yıl	63	8,2
3-4 yıl	142	18,5
5-6 yıl	160	21
Daha fazla	401	52,3
Toplam	766	100,0

Katılımcıların %52,3'ü 6 yıldan daha fazla süredir bilgisayar kullanmaktadır.

Çizelge 4.2. Bilgisayar eğitimi durumları

Bilgisayar eğitimi aldınız mı?	f	%
Evet	508	63,3
Hayır	258	37,7
Toplam	766	100,0

Katılımcıların %63,3'ü daha önce bilgisayar eğitimi almış durumdadır.

Çizelge 4.3. Günlük bilgisayar kullanım süreleri

Günde ortalama kaç saat bilgisayar kullanıyorsunuz?	f	%
0-1 saat	236	30,8
1-3 saat	261	34,1
3 saatten fazla	269	35,1
Toplam	766	100,0

Katılımcıların %35,1'i günde 3 saatten fazla bilgisayar kullanmaktadır.

Çizelge 4.4. Bilgisayara sahip olma durumları

Sürekli kullanma imkanına sahip olduğunuz bir bilgisayar var mı?	Öğrenci		Öğretim Elemanı		Genel	
	f	%	f	%	f	%
Evet	537	74,7	45	95,7	582	76,0
Hayır	182	25,3	2	4,3	184	24,0
Toplam	719	100,0	47	100,0	766	100,0

Katılımcıların %76'sının bilgisayarı vardır. Bu oran öğretim elemanları arasında %95,7'ye yükselirken, öğrenciler arasında %74,7 olmaktadır.

Çizelge 4.5. Antivirüs programı kullanma durumu

Antivirüs programı kullanıyor musunuz?	Genel		Bilgisayar Eğitimi Almayanlar	
	f	%	f	%
Evet	468	80,4	141	78,8
Hayır	114	19,6	38	21,2
Toplam	582	100,0	179	100,0

Sürekli kullanma imkanına sahip olduğu bir bilgisayarı olmayan 184 kişi bu soruyu cevaplamamıştır. Soruyu cevaplandıran 582 katılımcının %80,4'ü antivirüs programı kullandığını belirtmiştir. Bilgisayar eğitimi almayanlarda bu oran %78,8'e düşmektedir.

Çizelge 4.6. Lisanssız yazılım kullanım durumu

Bilgisayarınızda lisanssız yazılım (program) var mı?	Öğrenci		Öğretim Elemanı		Genel		Bilgisayar Eğitimi Almayanlar	
	f	%	f	%	f	%	f	%
Evet	393	73,2	29	64,4	422	72,5	133	74,3
Hayır	144	26,8	16	35,6	160	27,5	46	25,7
Toplam	537	100,0	45	100,0	582	100,0	179	100,0

Sürekli kullanma imkanına sahip olduğu bir bilgisayarı olmayan 184 kişi bu soruyu cevaplamamıştır. Katılımcıların %72,5'i lisanssız yazılım kullanmaktadır. Bu oran öğretim elemanlarında %64,4, öğrencilerde %73,2, bilgisayar eğitimi almayanlarda %74,3 olmaktadır.

Çizelge 4.7. 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	35,8
Kolay bulunduğundan	35	8,9	7	24,1	42	10,0
Hepsi	216	55,0	13	44,8	229	54,3
Toplam	393	100,0	29	100,0	422	100,0

Sürekli kullanma imkanına 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.

Çizelge 4.8. İşletim sisteminin lisanslı olma durumu

İşletim sisteminiz lisanslı mı?	f	%
Evet Lisansız yazılım kullanmayan	171 160	56,9
Hayır	251	43,1
Toplam	582	100,0

Yine bu soruyu bilgisayarı olmayan 184 kişi cevaplamamıştır. Katılımcıların %43,1'inin işletim sisteminin lisansız olduğu anlaşılmıştır.

Çizelge 4.9. Lisanssız yazılım kullanmanın vicdani boyutu

Lisanssız yazılım kullanmak sizi vicdanen rahatsız ediyor mu?	f	%
Evet	149	35,3
Hayır	273	64,7
Toplam	422	100,0

Bu soruyu da bilgisayarı olmayan ve lisanssız yazılım kullanmayan 344 kişi cevaplamamıştır. Lisanssız yazılım kullanmaktan dolayı vicdani rahatsızlık duyanların oranı %35,3'te kalmaktadır.

Çizelge 4.10. 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

Bilgisayarı olmayan ve lisanssız yazılım kullanmayan 344 kişinin cevaplamadığı bu soruya göre katılımcıların %19,9'u lisansız yazılımları arkadaşlarından kopyalamaktadır.

Çizelge 4.11. İnternetten müzik, film, oyun dosyaları indirilme durumu

İnternetten müzik, film, oyun dosyaları indiriyor musunuz?	Öğrenci		Öğretim Elemanı		Genel		Bilgisayarı olmayanlar	
	f	%	f	%	f	%	f	%
Evet	461	64,1	26	55,3	487	63,6	79	43,4
Hayır	258	35,9	21	44,7	279	36,4	103	56,6
Toplam	719	100,0	47	100,0	766	100,0	182	100,0

Katılımcıların %63,6'sı internetten müzik, film, oyun dosyaları indirmektedir. Bu oran öğretim elemanlarında %55,3'e, bilgisayarı olmayanlarda %43,4'e düşmektedir.

Çizelge 4.12. İnternetten müzik, film, oyun dosyalarını indirmenin ve lisanssız yazılım kullanmanın suç olma durumu

İnternetten müzik, film, oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu biliyor musunuz?	Bilgisayarı Olmayanlar		Bilgisayar Eğitimi Almayanlar		Genel	
	f	%	f	%	f	%
Evet	100	54,9	172	66,7	539	70,4
Hayır	82	45,1	86	33,3	227	29,6
Toplam	182	100,0	258	100,0	766	100,0

Katılımcıların %29,6'sı internetten müzik, film, oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu bilmemektedir. Bu oranlar bilgisayar eğitimi almayanlarda %33,3 ve bilgisayarı olmayanlarda %45,1'e yükselmektedir.

Çizelge 4.13. 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	19,7
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.

Çizelge 4.14. 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	13,6
Yasaların yetersiz kalması veya uygulanamaması.	191	24,9
Hepsi	417	54,4
Toplam	766	100,0

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

Çizelge 4.15. Kullandığınız yazılımların bilgilerinizi 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

Kullandığınız bazı yazılımların, bilgilerinizi internet üzerinden başkalarına iletebileceğini biliyor musunuz? Sorusuna katılımcıların %51,7'si evet bunu yapabilir cevabı vermiştir.

Çizelge 4.16. Bilişim suçu kavramının daha önce duyulma durumu

Bilişim suçu kavramını daha önce duydunuz mu?	Öğrenci		Öğretim Elemanı		Bilgisayarı olmayanlar		Genel	
	f	%	f	%	f	%	f	%
Evet	455	63,3	38	80,9	91	50,0	493	64,4
Hayır	264	36,7	9	19,1	91	50,0	273	35,6
Toplam	719	100,0	47	100,0	182	100,0	766	100,0

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.

Çizelge 4.17. En tehlikeli bilişim suçları

Size göre aşağıdaki bilişim suçlarından en tehlikelisi hangisidir?	f	%
Lisans hakları	104	13,6
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

Katılımcıların %61'i dolandırıcılık suçunu bilişim suçlarının en tehlikelisi olarak göstermiştir.

Çizelge 4.18. 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

En çok işlenen yasa dışı yayın suçu olarak %45,6 oranında pornografi seçilmiştir.

Çizelge 4.19. 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

Katılımcıların %73,9'u interneti en çok araştırma yapmak için kullanmaktadır.

Çizelge 4.20. Hackerlık yapar mısınız sorusuna verilen cevaplar

Hackerlık yapar mısınız?	Öğrenci		Öğretim Elemanı		Genel		Bilgisayar Eğitimi Almayanlar	
	f	%	f	%	f	%	f	%
Evet	311	43,3	12	25,5	323	42,2	119	46,1
Hayır	408	56,7	35	74,5	443	57,8	139	53,9
Toplam	719	100,0	47	100,0	766	100,0	258	100,0

Katılımcıların %42,2'si yeterli bilgi ve birikime sahip olsaydı hackerlik yapabileceğini belirtmiştir.

Çizelge 4.21. İnternet bankacılığının güvenilirlilik durumu

İnternet bankacılığı sizce güvenli mi?	Öğrenci		Öğretim Elemanı		Genel	
	f	%	f	%	f	%
Evet	185	25,7	23	48,9	208	27,2
Hayır	534	74,3	24	51,1	558	72,8
Toplam	719	100,0	47	100,0	766	100,0

İnternet bankacılığını güvenilir bulmayanların oranı %72,8 olmuştur. Öğretim elemanlarında bu oran %51,1'dir.

Çizelge 4.22. İnternet üzerinden alışveriş yapma durumu

İnternet üzerinden alış veriş yapıyor musunuz?	f	%
Evet	143	18,7
Hayır	623	81,3
Toplam	766	100,0

Katılımcıların %81,3'ü internet üzerinden alışveriş yapmamaktadır.

Çizelge 4.23. İnternet üzerinden alışveriş yaparken herhangi bir güvenlik problemi ile karşılaşma durumu

İnternet üzerinden alışveriş yaparken herhangi bir güvenlik problemi ile karşılaştınız mı?	f	%
Evet	17	11,9
Hayır	126	88,1
Toplam	143	100,0

İnternet üzerinden alışveriş yaparken herhangi bir güvenlik problemi ile karşılaşanların oranı %11,9 olmuştur.

Çizelge 4.24. Phishing olayı ile karşılaşma durumu

Size banka bilgilerinizi güncelleştirme için bankanızdan geldiği bildirilen bir e-posta (phishing olayı) geldi mi?	f	%
Evet	107	14,0
Hayır	659	86,0
Toplam	766	100,0

Katılımcıların %14'ü phishing olayı ile karşılaşmıştır.

Çizelge 4.25. Bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ilerde büyük tehlikelere yol açma durumu

Bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ilerde büyük tehlikelere yol açacağını düşünüyor musunuz?	f	%
Evet	466	60,8
Hayır	300	39,2
Toplam	766	100,0

Katılımcıların %60,8'i bilgisayar ve internet kullanımının çok hızlı bir şekilde artmasının ilerde büyük tehlikelere yol açacağını düşünmektedir.

Çizelge 4.26. Bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesine bakış

Bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesini olumlu karşılar mısınız?	Öğrenci		Öğretim Elemanı		Genel	
	f	%	f	%	f	%
Evet	269	37,4	13	27,7	282	36,8
Hayır	450	62,6	34	72,3	484	63,2
Toplam	719	100,0	47	100,0	766	100,0

Bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesine katılımcıların %63,2'si karşı çıkmaktadır, öğretim elemanlarında bu oran %72,3'e çıkmaktadır.

Çizelge 4.27. Bilişim suçlarını önlemek amacıyla internette gözetlenme durumuna bakış

Bilişim suçlarını önlemek amacıyla internette gözetlenmeyi olumlu karşılar mısınız?	Öğrenci		Öğretim Elemanı		Genel	
	f	%	f	%	f	%
Evet	213	29,6	12	25,5	225	29,4
Hayır	506	70,4	35	74,5	541	70,6
Toplam	719	100,0	47	100,0	766	100,0

Katılımcıların %70,6'sı bilişim suçlarını önlemek amacıyla internette gözetlenmeyi kabul etmemektedir.

Çizelge 4.28. Önemli görülen bir bilişim suçuna şahit olunduğunda bunu ihbar etme durumu

Size göre önemli gördüğünüz bir bilişim suçuna şahit olursanız bunu ihbar etmeyi düşünür müsünüz?	Öğrenci		Öğretim Elemanı		Genel	
	f	%	f	%	f	%
Evet	499	69,4	36	76,6	535	69,8
Hayır	220	30,6	11	23,4	231	30,2
Toplam	719	100,0	47	100,0	766	100,0

Katılımcıların %69,8'i önemli gördüğü bir bilişim suçuna şahit olduğunda ihbar edebileceğini belirmiştir.

Çizelge 4.29. 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	1,4
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

Bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmalarını yeterli bulanların oranı %1,4 olmuştur.

Çizelge 4.30. Bilişim suçlarıyla ilgili yasalarımız

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

Bilişim suçlarıyla ilgili yasalarımızı yeterli bulanların oranı ise %3 olmuştur.

4.4. Tartışma

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

Katılımcıların %76'sının sürekli kullanma imkanına 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. Oysa Devlet Planlama Teşkilatının, Nisan- Haziran 2005

tarihlerinde yaptığı, Hane Halkı Bilişim Teknolojilerini Kullanımı Araştırması sonuçlarına göre evlerdeki bilgisayar sayısı oranı %11,89 olmuştur [6].

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.

Business Software Alliance (BSA)'ın, araştırma sonuçlarına göre ülkemizde lisanssız yazılım kullanım oranı %66 olarak belirlenmiştir. Ayrıca bu oranın %56'ya indirilmesi, bilişim teknolojileri sektöründe ek 3 000, tüm sektörlerde ek 36 000 istihdamın açılmasına, ekonominin 4 yıllık bir süreçte 1 milyar dolar büyümesine ve yıllık 600 milyon dolar ek vergi kazancının elde edilmesine katkıda bulunacağı hatta dünya genelinde %10 oranındaki bir düşüşün tüm dünyada 67 milyar dolar değerinde ek vergi geliri oluşturabileceği belirtilmiştir [5].

İnternetten müzik, film, oyun dosyaları indirenlerin oranı ise %63,6'dır. 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 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.

Bilişim suçlarının en tehlikelisi %61 ile bilgisayar yoluyla dolandırıcılık (ATM, kredi kartı vb.) olmuştur. Emniyet Genel Müdürlüğünün 2001 yılı verilerine göre bilgisayar yoluyla dolandırıcılık suçlarının dağılımı kredi kartı dolandırıcılığı %67, ATM dolandırıcılığı %21 ve hırsızlık %12 şeklindedir.

En çok işlenen yasa dışı yayın suçu ise %45,6 ile pornografi olarak belirlenmiştir. Pornografi suçunu %25,2 ile çocuk pornografisi, %19,8 ile terör ve %9,4 ile hakaret suçları izlemiştir. Yine Emniyet Genel Müdürlüğünün verilerine göre yasa dışı yayın suçlarının dağılımı ise %40 çocuk pornografisi, %30 terör, %25 pornografi, %5 hakaret şeklindedir [32].

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 sempati 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. Yine Devlet Planlama teşkilatının raporuna göre insanların internet üzerinden alışveriş yapmama nedenlerinin başında İhtiyaç duymamak, güvenlik nedeniyle kredi kartı detaylarını vermek istememek, kişisel bilgileri İnternet üzerinden vermek istememek, ürünü yerinde görerek almayı tercih etmek, satış yapılan yere bağlılık ve alışkanlıklar gelmektedir [6].

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;

- Uyuşturucu ticareti
- Sahtekarlık, özellikle sahte faturalar
- Entelektüel mülk hırsızlığı
- Gerçek yüz veya ID hırsızlığı ve yanlış temsil
- Casusluk

- Elektronik izleme
- Çocuk pornografisi
- Organize suç
- Kopyalama suçları
- DOS (servis kullanımı engelleme) saldırıları
- Şantaj
- Web sitesi değiştirme

gibi suçların işlendiği 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 giderme yoluna gitmektedirler. Bilişim konusunda işlenen suçlarla ilgili vatandaşlarımızın şikayetlerini ve mağduriyetlerini iletebilecekleri bir birim bulunmamaktadır.

Genellikle bu tür konularda şikayeti olan insanlar Bilgi İşlem Şube Müdürlüklerine yönlendirilmektedir.

Üzerinde düşünülmesi gereken anketin önemli verilerinden bir diğeri bilişim suçlarıyla mücadelede emniyet teşkilatının çalışmalarını yeterli bulanların oranının %1,4, bilişim suçlarıyla ilgili yasalarımızı yeterli bulanların oranının ise sadece %3 olmasıdır. Oysa Türkiye Avrupa Konseyi Siber Suç Sözleşmesine imza atmamasına rağmen bu sözleşme hükümlerini kabul etmiş ve YTCK'da önemli düzenlemeler yapılmıştır. Ülkemizde kolluk kuvvetleri geleneksel suçlardaki durumun aksine, bilişim suçları konusunda sistemlerimizi koruyacak kadar yeterli bilgi ve kapasiteye sahip değildir. Üstelik çoğu bilişim suçu farkına bile varılmadan vuku bulmaktadır. 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.

5. SONUÇ VE ÖNERİLER

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. Bilgisayar ve internetin gelişimi insanlara bir çok kolaylık getirmekle birlikte, kötü niyetli kişilerin bu imkanlardan 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 da, ileride bu suçlar ile daha çok karşılaşacağımız anlamına gelmektedir. Bazı bilgisayar meraklıları ve büyük kurumlar haricinde, bilişim suçları ve güvenliği çok ciddiye alınmamakta, yeterince yatırım yapılmamaktadır. 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. Ancak suçun işlenmeden önlenebilmesi veya işlenmesine engel olunması için de çalışmalar yapılmalıdır.

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. Tedbir alınabilmesi için konunun iyi anlaşılması, insanların bilişim suçları hakkındaki bilgilerinin öğrenilmesi, bu suçu işleyenleri bu suçu işlemeye iten sebeplerin araştırılması gerekir. Bu sebeple bu tez çalışmasında eğitimli insanların bilişim suçu kavramı hakkındaki görüşlerini değerlendirebilmek amacıyla bir anket çalışması yapılmıştır. Anketin değerlendirilmesi dördüncü bölümde ayrıntılı olarak anlatılmıştır.

Anket sonuçlarına 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. Bir bilgisayarı kullanabilmek için en temel yazılım işletim sistemi yazılımıdır ve bilgisayarı olan her insanın mutlaka işletim sistemi yazılımına ihtiyacı vardır. Ancak piyasada kişisel bilgisayarlarda neredeyse tekel haline gelen Microsoft Windows işletim sistemi satın alındığında bilgisayara hatırı sayılır şekilde maliyet külfeti getirmektedir. Üstelik bir bilgisayar satın alındığında sadece işletim sistemi yazılımı o bilgisayardan istenildiği gibi yararlanılabilmesi için yeterli olmamaktadır. Böylece bütün yazılımları satın almak isteyen bir insan donanımdan daha çok yazılıma para ayırmak zorunda kalacaktır. Üstellikte çoğu zaman bilgisayarına kurmak ve kullanmak istediği programların bir kısmını ya bir sefer ya da birkaç sefer kullanacaktır. Bu sebepler ve lisanssız yazılımların elde edilmesinin kolaylığı insanları lisanssız yazılım kullanmaya itmektedir. Lisanssız yazılım kullanımının azaltılması için işletim sistemi yazılımları ucuzlatılmalı, her zaman kullanılması gerekmeyen ancak yine de bir bilgisayarda olduğunda kullanıcının işlerini kolaylaştıran programlar bir paket halinde daha ucuza pazarlanması sağlanmalıdır.

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 hakim olduğu görülmektedir. Ayrıca büyük bir çoğunluk bilişim suçlarıyla ilgili yasalarımızı ve emniyet teşkilatımızın çalışmalarını yetersiz bulmaktadır. 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 suçları ile mücadelede, yeterli hukuki alt yapı, uluslararası işbirliği, bilgisayar programı ve bilgisayarlarda en son 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,

e-Dönüşüm Türkiye Projesi 2005 Eylem Planında belirtildiği gibi, güvenli internet kullanımı ile ilgili olarak tanıtım filmleri ve eğitim materyallerinin hazırlanması, işgücü içindeki okur yazarlık düzeyini yükseltirken, aynı zamanda bilgisayar okur yazarlığının da her kesime kazandırılması bir zorunluluktur. Eğitim sistemlerinin bilgi teknolojilerine, dayalı olarak

yenilenmesi ve yaygınlaştırılması, okullarda öğretmenler ve öğrencilerin internete ve çoklu ortam kaynaklarına uygun düzeyde erişimi, öğretmen, öğrenci, silah altında bulunan er ve erbaşlar ile kamu çalışanlarının yeni teknolojileri kullanma becerilerini artırmaları ve güvenli internet kullanımı hakkında bilgi toplumunun gerektirdiği insan kaynağı planlamasının bir an önce yapılması gerekmektedir.

Bilişim suçları ve bilişim suçları ile mücadele konuları oldukça geniş konulardır. Bu tez çalışmasında konu hakkında genel bir değerlendirme yapılmaya çalışılmıştır. Bu konunun alt başlıkları ile ilgili olarak daha ayrıntılı çalışmalar yapılabilir.

KAYNAKLAR

1. Devlet Planlama Teşkilatı "e-Dönüşüm Türkiye projesi 2005 eylem planı değerlendirme raporu", ***DPT Rapor 1***, Ankara,1 (2005).

2. İnternet: "Bilişim suçları" http://mali.iem.gov.tr/Library/makale/BILISIM%-20SUCLARI.pdf (2005).

3. Emniyet Genel Müdürlüğü, "Bilgisayar suçları ve bilgi güvenliği kurulu", ***EGM Rapor 1***, Ankara, 5-12 (2001).

4. İnternet: "İnternet ve Ağ Güvenliği" http://support.infonet.com.tr/tr-/presales/konsept.htm (2003).

5. İnternet: "Türkiye internet raporu 2005" http://www.internethaftasi.org.tr-/hafta06/docs/turkiye-internet-raporu.pdf (2005).

6. İnternet:Tübider E Dergi http://www.tubiderbd.com/index.php?module-=news&news_id=5056&catid=1 (2006).

7. İnternet: "IDC-BSA Global Araştırma Sonucu" http://www.bsa.org.tr -/haberodasi.html (2006).

8. DİE, "Hanehalkı Bilişim Teknolojileri Kullanımı Sonuçları" 16 Kasım, ***Devlet İstatistik Enstitüsü Haber Bülteni***, 179 (2005).

9. İnternet:"Bilişim suçları içerisinde çocuk pornografisi" http://www.hukuki-.net/portal_ARTICLES.asp ? whichpage = 1 & catid=40&test=40 & area-= 3 (2004).

10. Mungo P., Clough B., Approaching Z., "Sıfıra doğru, veri suçları ve bilgisayar yeraltı dünyası", Data Crime and the Computer Undcnvorld, Emel Kurma, ***İletişim Yayınları,*** İstanbul, 154-176 (1999).

11. İnternet: "IBM'den uyarı: Bilgisayar virüsü ve spam'de büyük artış var" http://www.milliyet.com.tr/content/teknoloji/tek014/tekno29.html (2005).

12. İnternet: "Bilişim suçlarının Türk Ceza Kanunu ve tasarısındaki hükümler yönünden mukayeseli değerlendirilmesi-öneriler" http://www-.hukuki.net/portal_articles.asp?catid=40&cattitl (2005).

13. İnternet: "Sanal dolandırıcılık" http://www.iem.gov.tr/iem/?idno=147 (2005).

14. İnternet:"Türkiye'de phishing" http://www.olympos.org/article/articleview-/1403/1/10 (2005).

15. İnternet: “Siber terör (I,II,III,IV,V)” http://turk.internet.com/haber/yazigos - ter.php3?yaziid=8838 (2005).

16. İnternet:“Crıme And Securıty Survey”http://i.cmpnet.com/gocsi/db_area- /pdfs/fbi/FBI2005.pdf (2005).

17. Beyhan, Cem, Temmuz-Aralık, ***Polis Bilimleri Dergisi***, 3-4(4): 12(2002).

18. İnternet: “İnternet servis sağlayıcısının cezai Sorumluğu” http://www.martiyazilim.com.tr/marti.php?yol=haberler/fikirbahcesi/görüş rüşler/servissaglayici.htm (2005).

19. İnternet: “Bilişim suçları ve mücadelede taşra teşkilatında karşılaşılan problemler ve çözüm önerileri” http://www.caginpolisi.com.tr/24/43-44- 45-46.htm (2005).

20. İnternet: “Bilişim suçlarının delillendirilmesinde Amerikan uygulaması” http://bilisim.izmirpolis.gov.tr/dokuman/Bilişim%20Suçları%20delillendir- me%20süreci.pdf (2005).

21. İnternet: “İnternet ve hukuk” http://www.medyasoft.com.tr / MedyaSoft- /kaynaklar/makaleler/Read_News.cfm?NEWS_ID=371 (2005).

22. Dülger, M. V., “Yeni Türk Ceza Kanunu’nda düzenlenen bilişim suçları ve bu suçlarla mücadelede alınması gereken önlemler”, ***Emniyet Genel Müdürlüğü 2. Polis Bilişim Şurası***, Ankara, 1-10 (2005).

23. Nizam, F., “Avrupa Siber Suçlar Konvansiyonu ve Türk Ceza Kanunundaki bilişim suçlarının karşılaştırılması” ***Emniyet Genel Müdürlüğü 2. Polis Bilişim Şurası***, Ankara, 2-8 (2005).

24. Emniyet Genel Müdürlüğü, “Bilgisayar suçları ve bilgi güvenliği kurulu”, ***EGM, Rapor 2***, Ankara, 24 (2001).

25. İnternet: “Türkiye’de bilişim suçları” http://www.caginpolisi.com.tr/32/8- 9.htm (2005).

26. Shinder, D. L., “Scene of Cybercrime - Computer Forensics Handbook”, ***Syngress Publishing***, USA, 4 (2002).

27. Chisum J. W., "Crime Reconstruction and Evidence Dynamics", ***Presented at the Academy of Behavioral Profiling Annual Meeting***, Monterey, CA. 12 (1999).

28. Casey E., “Digital Evidence and Computer Crime”, ***Academic Pres,*** London, 6 (2000).

29. Karagülmez, A., "Bilişim suçlarında delil toplamayı etkileyen başlıca konular", ***Emniyet Genel Müdürlüğü 2.Polis Bilişim Sempozyumu***, Ankara, 1-3 (2005).

30. İnternet: "Ülkemizde bilişim suçları ve mücadele yöntemleri" http://www.dokurer.net/documents/bursa.pdf (2004).

31. Kazu, İ., Y., "Emniyet Teşkilatı personelinin bilişim teknolojilerinden yararlanma düzeyleri ve bilişim teknolojilerine ilişkin görüşleri (Gaziantep ili örneği)" ***Emniyet Genel Müdürlüğü 2.Polis Bilişim Sempozyumu***, Ankara, 3 (2005).

32. İnternet: "Ülkemizde işlenen bilişim suçları istatistikleri" http://www.egm-.gov.tr/docs/istatistikler.pdf (2004).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: DİJLE, Hikmet
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 15.08.1971 Düzce
Medeni hali	: Bekar
Telefon	: 0 (380) 681 70 34
Faks	: 0 (380) 524 58 93
e-mail	: hdicle@mynet.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Gazi Üniversitesi Elektronik Eğt. Bölümü	1997
Lise	Düzce Lisesi	1989

İş Deneyimi

Yıl	Yer	Görev
1997-1999	Adıyaman/Kahta ÇPL	Elektronik Öğretmeni
1999-2006	Düzce A.T,T.L Ve E.M.L	Elektronik Öğretmeni

Yabancı Dil

İngilizce