T.C.
ÇUKUROVA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ
ADLİ TIP ANABİLİM DALI

BİLİŞİM SUÇLARI VE ADANA İLİNDE 2006-2009 YILLARI ARASINDA MEYDANA GELEN BİLİŞİM SUÇLARININ DEĞERLENDİRİLMESİ

KEZBAN ATALIÇ TAŞ

YÜKSEK LİSANS TEZİ

DANIŞMANI
Prof.Dr. Necmi ÇEKİN

Tez No:

ADANA-2010

T.C.
ÇUKUROVA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ
ADLİ TIP ANABİLİM DALI

BİLİŞİM SUÇLARI VE ADANA İLİNDE 2006-2009 YILLARI ARASINDA MEYDANA GELEN BİLİŞİM SUÇLARININ DEĞERLENDİRİLMESİ

KEZBAN ATALIÇ TAŞ

YÜKSEK LİSANS TEZİ

DANIŞMANI
Prof.Dr. Necmi ÇEKİN

Bu tez Çukurova Üniversitesi Bilimsel Araştırma Projeleri Birimi Bütçesinden TF2009YL5 nolu proje olarak desteklenmiştir.

Tez No:

ADANA-2010

Adli Tıp Yüksek Lisans Programı Çerçevesinde yürütülmüş olan **Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi** adlı çalışma aşağıdaki jüri tarafından Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Savunma Tarihi:

Yukarıdaki tez, Yönetim Kurulun …….2009 tarih ve…….....sayılı kararı ile kabul edilmiştir.

TEŞEKKÜR

Tezimin oluşum ve çalışma aşamasında bilgi ve deneyimleri ile desteklerini esirgemeyen tez danışmanım Prof. Dr. Necmi Çekin'e,

Eğitim ve tez dönemim içerisinde gösterdikleri ilgi ve destekleri için Anabilim Dalı Başkanı Prof. Dr. Mete Korkut Gülmen ile Öğretim Üyeleri Prof. Dr. Behnan Alper, Doç. Dr. Ahmet Hilal ve Yrd. Doç. Dr. Selim Kadıoğlu, Dr. Kimya Mühendisi Nebile Dağlıoğlu, Dr. Biyolog Ayşe Serin, Dr. Biyolog Hüsniye Canan'a,

Bu tezin hazırlık aşamasında verilerin hazırlanmasında yardımları için Adana İl Emniyet Müdürlüğü ve İl Jandarma Komutanlığı personeline,

Çalışmalarımın her aşamasında bana her türlü anlayışı gösteren, yardım ve teşviklerini esirgemeyen Osmaniye 2. Ağır Ceza Mahkemesi Başkanı Hakim Gökçe Yıldırım, Seyhan İlçe Emniyet Müdür Yardımcısı 4. Sınıf Emniyet Müdürü İsmail Bilen, Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü Bilişim Suçları Büro Amiri Başkomiser Onur Sürücü ve Bilgisayar Öğretmenim Hülya Önaldı'ya,

Her zaman yanımda olan ve benden desteğini esirgemeyen Sevgili Eşim Engin Taş'a,

TF2009YL5 nolu proje olarak bu çalışmanın gerçekleştirilmesinde maddi katkı sağlayan Çukurova Üniversitesi Bilimsel Araştırma Projeleri Birimine teşekkür ederim.

Kezban Atalıç Taş

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

ÖZET

Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi

Teknolojinin gelişmesiyle birlikte hayatımızın her alanına giren bilgisayar ve bilgisayar sistemleri, bu yolla oluşabilecek suçları da beraberinde getirmiş ve karşımıza ulaşılması ve takibi zor olan bilişim suçlarını çıkarmıştır.

Bu çalışmada bilişim suçlarının nasıl işlendiği ve soruşturmada kullanılan teknik cihazlar araştırılmıştır.

Çalışmada Adana İl Emniyet Müdürlüğü kayıtlarına yansıyan 648 olay ve 1872 şüpheli incelenmiştir. İnternet üzerinden işlenen suçların ilk sırasında dolandırıcılık olduğu, suç işlemede en çok zararlı yazılım yönteminin kullanıldığı, şüphelilerin %89'unun erkek ve 21-30 yaş aralığında olduğu saptanmıştır.

Bilim ve teknolojideki gelişmeler aynı zamanda suçluların kullandıkları teknik ve yöntemlerin de gelişmesine neden olmaktadır. Bu yüzden tüm Adli Bilim uzmanları gibi Bilişim Suçu uzmanları da kendi alanlarındaki yenilikleri takip ederek gelişmelere uyum sağlamak zorundadırlar.

Anahtar Sözcükler: Bilgisayar, Bilişim Suçu, Suçla Mücadele, Adli Bilimler, Adli Bilişim.

ABSTRACT

Computer Crimes and Analysing Computer Crimes Which were Perpetrated in Adana Between 2006-2009.

Computers and computer systems, which penetrate into every aspect of our lives with the development of technology, have brought the resulting crimes together and faced us with computer crimes that are difficult to reach and trail.

This study presents how to perpetrate cyber crimes and the equipment that is used for investigation.

In this study, 648 incidents and 1872 suspects which were registrated by the Adana National Police Departmant have been examined. In the conclusion of the research, fraud is in the first rank of internet crimes and malware is in the first rank of methods and in respect of suspect number % 89 were men and their ages are between 21 and 30.

The tecniques and methods that criminals use change and improve at the same time the advances in science and technology. Therefore, as all forensic sciences experts, cyber crimes expert need to follow all innovations about their branch and carry them out their works.

Key words: Computer, Cyber Crime, Crime struggling, Forensic Sciences, Computer Forensics.

1. GİRİŞ VE AMAÇ

İnsanın var olduğu her ortamda suça rastlamak mümkündür. Suç işleme yaşının 12'ye kadar düştüğü günümüzde suç, bazı yerlerde suç olmaktan çıkmış ve bir yaşam tarzı haline gelmiştir. Öyle ki; geçimini dolandırıcılık, hırsızlık, vs ile sağlayan bir kesim dahi ortaya çıkmıştır. Dünya nüfusunun artması, kaynakların yetersiz hale gelmesi ve cezaların yetersizliğiyle de birlikte suç işleme oranı artmış ve suç yaygınlaşmıştır.

Teknolojinin gelişmesi, küreselleşme, artan bilgisayar sayısı ve internetin yaygın kullanımıyla beraber toplumsal ilişkiler değişmiştir. Daha içe kapalı, yüz yüze temas olmadan gerçek yaşamdan sanal ortama hızla geçişle birlikte; gerçek veya tüzel kişiler, özel veya kamu sektöründeki pek çok birime kadar (bankalar, okullar, muhtarlıklar, vs) her yerde işlemler bilgisayar sistemleri ile yürütülür hale gelmiştir.

Bilgi teknolojilerindeki gelişme yeni yaşam biçimleriyle beraber yeni suç türlerini yaşamımıza katmaktadır. Buna paralel olarak da bilişim suçlarının mağdur ve şüpheli sayısında artış gözlenmiştir. 2007 ve 2006 yıllarını kıyaslarsak: Türkiye'de işlenen bilişim suçu oranı %600 artmıştır. Asayiş suçlarının %64, narkotik madde kullanımı ile ilgili suçların %35, kaçakçılık mali suçlarda %36, terör suçlarında %14[1] artış olurken bilişim suçlarındaki bu artış, bilişim suçunun ne denli yaygınlaştığını ve acil önlemler alınması gerektiğini göstermektedir. Zevk için virüs gönderen iyi internet kullanıcıları yerlerini interneti suç işleyebilecekleri yeni bir ortam olarak değerlendiren suçlulara bırakmıştır.

Suçluların tespiti ve yargılanmasındaki en önemli husus delillendirmedir. Bilişim suçu işlenmesi kolay, çözülmesi-delillendirilmesi zor olan önemli bir suç türüdür. Delillendirmedeki en büyük sıkıntı, dijital delillerin diğer delillere göre çok daha fazla bilgi içermesi ve kolay bozulabilirliğidir. Bilişim suçlarında kullanılan dijital delillerin bütünlüğünü ve güvenilirliğini ispat konusu önemlidir, mahkeme esnasında gerçekten delil niteliğini taşımasını sağlamak için teknik ve hukuki bilgilerin çok iyi kullanılması gerekmektedir.

2005 yılında yürürlüğe giren Türk Ceza Kanunu bilişim suçlarına da yer vermiştir. Bunlar: madde 243 Bilişim Sistemine Girme; madde 244 Sistemi Engelleme, Bozma,

Verileri Yok Etme veya Değiştirme; madde 245 Banka veya Kredi Kartlarının Kötüye Kullanılması; madde 246 Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması; madde 158 Nitelikli Dolandırıcılık f bendi (Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık)tır. Bununla beraber bilişim suçu tek başına bir suç oluşturabileceği gibi diğer suçlarla da iç içe geçebilmektedir; bir cinsel taciz ya da cinayet suçunda cep telefonu, dijital kamera vs görüntüleri olması gibi. Haliyle bilişim suçu oldukça geniş bir alanı kapsamaktadır.

Bu çalışmada, Adana ilinde Emniyet Müdürlüğü'ne intikal eden olayların verilerinden yola çıkılarak; bilişim suçlarının nasıl işlendiği, nasıl soruşturulduğu anlatılarak bilişim suçlarını önlemeye yönelik neler yapılabileceğine dair çözüm önerileri sunulması planlanmaktadır.

2. GENEL BİLGİLER

2.1. Bilişim Suçunun Tanımı

Bilişim suçlarında teknoloji esastır. Ancak çok karmaşık ve kapsamlı bir konu olduğundan pek çok tanımla karşılaşmamız mümkündür. Bunlardan birkaçı:

"Ceza kanununu ihlal eden, işlenmesinde veya araştırılmasında bilgisayar teknolojisi bilgilerini içeren her suç bilişim suçu" olarak kabul edilmektedir[2].

"Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenilen suçlardır"[3].

"Bilgisayarları da kapsayan, ancak sadece bilgisayarlarla kısıtlı olmayıp bu alandaki bütün cihaz ve araçlara karşı veya bunlar marifetiyle işlenen suçlar"[4].

"Bilişim alanındaki gelişmelere paralel artış gösteren ve teknolojinin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar verecek davranışlarda bulunmaktır"[5].

Bilgisayar ve türevi teknolojik aletlerin kullanılmasıyla işlenen her suç bilişim suçu gibi görünse de bunların pek çoğu bilişim sistemleri kullanılarak işlenen geleneksel suçlardır. Bir suçun bilişim suçu olması için;

- "İşlenmesinde ve soruşturmasında teknik bilgi gerekir, bilgi paylaşımı son derece hızlı ve geniş kapsamlıdır,
- Soruşturma aşamasında kanuni ve teknik zorluklar kaçınılmazdır,
- Olası suç yöntemleri hayal gücü ile sınırlıdır,
- Sınır ötesi suçlardan olduğu tartışılmazdır"[6].

2.2. Bilişim Suçunun Türleri

Bilişim suçlarını farklı kategorilere ayırmak oldukça güçtür. Tek başına bir bilişim suçu olabileceği gibi, birleşerek veya birbirlerini kapsayarak da bir diğer bilişim suçunu oluşturabilirler.

2.2.1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Olarak Girme, Dinleme ve Engelleme

Düzenli olarak birbirleriyle etkileşen, birbirine bağlanmış bilgisayarların oluşturduğu topluluğa bilgisayar sistemleri denilmektedir. Bu networklerin ortak kullanımını sağlayan modem ve dağıtıcılara (hub) yetkisiz olarak internet (global network) üzerinden girmek, buralardan bilgi ve datalara ulaşmak, bunları izinsiz olarak kopyalamak, silmek, değiştirmek ve sisteme bağlı bilgisayarların kendi aralarındaki iletişimini engellemek bu suçların kapsamına girmektedir.

Erişim sistemin bir kısmına veya bütününe, bilgisayar ağına ya da içerdiği verilere, programlara; yine programlar, casus yazılımlar, virüsler vb. ile ulaşma anlamındadır. Günümüzde özel hayatın gizliliğinin korunması için kanunlarda gerekli müeyyideler konulması ile birlikte dinlemeler, erişimler, izinsiz olarak özel ve şirket bilgisayarlarına ve sistemlerine girmek suç olarak kabul edilmiştir[7].

Erişim haricinde, haberleşme amacıyla kurulu iki bilgisayar sisteminin iletişiminin dinlenmesi de aynı şekilde değerlendirilmektedir. İletişimin dinlenmesi, sadece bilgisayar başındaki iki kişinin birbiri ile görüşmesi olarak düşünülmemelidir. Birbirine bilgi gönderen ve uyum içinde çalışan bilgisayarların ağ içinde göndermiş oldukları bilgilerin izlenmesi de dinleme olarak değerlendirilmelidir[8].

Bu konu Türk Ceza Kanununun 243. maddesinin 1. ve 2. fıkralarında düzenlenmiştir.

2.2.2. Bilgisayarlara Fiziksel veya Mantıksal Yollar ile Zarar Verme

Bu suç türü iki şekilde karşımıza çıkmaktadır.

Birincisi: Bilgisayar teknolojileri kullanılarak sistemine sızılan bilgisayardaki bilgilerin silinmesi ve değiştirilmesidir.

İkincisi: Hedef alınan sisteme uzaktan erişerek değil de bilakis fiziksel zarar vererek ya da sistem başında bulunarak bilgisayardaki bilgileri silerek veya değiştirerek zarar verilmesi şeklinde karşımıza çıkmaktadır.

Burada önemli olan mala verilen zarardan ziyade içindeki bilgilere verilen zarardır. Yetkisiz erişimin aktif sahası olarak da nitelendirilen bu suç türü, yalnız

sisteme erişmekle kalmayıp sistemin içerdiği bilgileri silme veya değiştirme olarak ifade edilmekte ve ele geçirilen bu bilgiler kanun dışı kullanılmak üzere satılabilmektedir[9].

Bu konu Türk Ceza Kanununun 243. maddesinin 3. fıkrası ile 244. maddesinin 1. ve 2. fıkralarında düzenlenmiştir.

2.2.3. Bilgisayar Yoluyla Dolandırıcılık

Kişi veya kurum bilgisayarlarına yetkisiz olarak girerek kişilerin banka, kredi kartı hesap numaraları ve şifresi gibi önemli bilgilerinin ele geçirilmesiyle yapılan dolandırıcılık türüdür. Bunun için bilgisayarda yazılan herşeyi kopyalayan yazılımlar üretilmiştir. Bu yazılımlara "keylogger" (klavye kopyalayıcısı) örnek verilebilir. Klavye kopyalayıcıları, kişinin internet üzerinden şahsi veya kurum banka hesaplarına girmesi esnasında klavyede bastığı her tuşu kaydederek yazılan şifreyi hafızasına kopyalayıp dolandırıcılığı yapmak isteyen şahsın mail adresine göndermesi şeklinde çalışmaktadır. Hackerlar son olarak bunların bir üst versiyonu olan "screen logger"ı (ekran kopyalayıcısını) üretmişlerdir. Screen logger programı, kendisinden istenilen zaman aralıklarında ekran görüntüsünü kaydederek hackera mail atmaktadır.

İnternet üzerinden özel veya resmi kurum sistemlerine girerek veri tabanları ve verilerine ulaşılması yoluyla da gerçekleştirilebilir. Gerçekleştirilmesi en zor olan bu dolandırıcılık türüne bir banka veri tabanına ulaşılarak yapılan bakiye değişiklikleri örnek verilebilir.

Sahte mail veya web adresleri ya da gerçekte var olan bir kurumun mail veya web adreslerinin taklitleri aracılığıyla yapılanı bilinen en yaygın türüdür. Örneğin; bazı şahsi bilgiler yanlış girildiğinden banka veya sigorta işlemlerinin yapılamadığı ve bilgilerin güncellenmesi gerektiği yönünde bir mesajla kişi taklit siteye yönlendirilebilir ve şifre vb bilgileri ele geçirilebilir.

Bu konu Türk Ceza Kanununun 158. maddesinin 1. fıkrasının f bendi, 244. maddesinin 3. fıkrası ve 245. maddesinin 1. fıkrasında düzenlenmiştir.

2.2.4. Bilgisayar Yoluyla Sahtecilik

Bilgisayarlar ve diğer dijital aletler geleneksel suçları işlemede kullanılabilirler. Bilgisayar yoluyla sahteciliği, sahteciliğin bir bilgisayar ya da diğer elektronik kaynaklarla yapılması şeklinde tanımlayabiliriz. Bazı yazılım programlarının erişim kolaylığı sağlaması ve internet ağının küresel etkisiyle bilgisayar yoluyla sahtecilikte her geçen gün artış görülmektedir[10].

2.2.5. Lisans Haklarına Aykırı Olarak Bir Yazılımın İzinsiz Kullanımı

Bu konu 5846 Sayılı Fikir ve Sanat Eserleri Kanunu ile düzenlenmiştir. Buna göre, film, müzik CD'leri, yazılım programı vs her türlü eseri tamamen veya kısmen kopyalama, çoğaltma; çoğaltılmış nüshalarını kiralama, ödünç verme, satma ve diğer yollarla dağıtma hakkı sahibine aittir. İzinsiz olarak bunları kullanmak, kopyalamak, dağıtmak ve satmak suçtur. Bunun yanı sıra, bir bilgisayar programının yetkisi olmayan kişilerce çoğaltılmasını önlemek amacıyla oluşturulmuş programları etkisiz hale getiren program veya teknik donanımları üretmek ve satmak da suçtur.

2.2.6. İnternet Üzerinden Yasadışı Yayın Yapma

İnternet geçmişe ulaşma, günümüz ve geleceğe yönelik pek çok kolaylık ve güzelliği içerisinde barındırmakla beraber, hayatımıza yönelik maddi manevi zararlara yol açacak, özellikle çocukların gelişimi ile ilgili tehditleri de içermektedir. Terör içerikli sempatizan kazandırıcı, silah kullanımı ile ilgili bilgiler içeren yayınlar, uyuşturucu kullanımını teşvik eden yayınlar, porno (özellikle çocuk pornosu) içerikli yayınlar, vs...

2.2.6.1. Terör İçerikli Yayınlar

Terör örgütlerinin yasadışı unsurların yayınlanması ve dağıtılması maksadı ile bilgisayar sistem ve ağlarını kullanmasıdır. Kendilerinin oluşturduğu web sayfalarında linkler vererek terör eğitimi konusunda sempatizanlarını eğitmektedirler. Bu sitelerde teröristin el kitabı, teröristin yemek kitabı gibi yazılarda bomba yapımı en ince detayları

ile anlatılmakta ve bir teröristin bilmesi gereken birçok konuda ayrıntılı bilgiler yer almaktadır[11].

2.2.6.2. Pornografik Yayınlar (Çocuk Pornosu Yayınları)

Pornografik yayınları yapanlar da diğer yasadışı yayınlardaki gibi daha geniş kitlelere ulaşmak için internetten faydalanmakta ve internetten önce sınırlı sayıdaki insanları etkilerken günümüzde bu sayı milyonlara ulaşmaktadır. Bunun sonucu insanların aile yaşantısı büyük ölçüde zarar görürken daha da vahim olanı ise çocukların da porno sektöründe yer almalarıdır. Burada mağdur olan çocukların ileriye dönük psikolojik ve sosyolojik yapıları bozulduğundan gelecekte sağlıksız nesillerin yetişmesi söz konusu olmaktadır.

2.3. Siber Terörizm

Siber terörizm, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır.

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

Bilgisayar yoluyla internet üzerinden çok daha geniş kitlelere ulaşma imkanına sahip olan teröristler, kendi web sayfalarını oluşturarak sempatizan toplayabilmekte ve dünyanın her yerindeki yandaşlarıyla her türlü (açık ya da şifreli) iletişimi rahatlıkla sağlayabilmektedirler. Bunun yanı sıra, pek çok dolandırıcılık, kara para aklama, hırsızlık, vb suçlar aracılığıyla ele geçirdikleri parayı sahte kimliklerle veya yandaşları aracılığıyla internet üzerinden yurtiçi veya yurtdışı herhangi bir banka hesabına yatırarak kolayca ekonomik yardım alabilmektedirler.

Bilgisayar sistemleri ve internet kullanımıyla yandaşlarıyla iyi ilişkiler kurmanın yanında, kendilerinin karşısında olanlara karşı da kolay, ucuz ve etkili yoldan korku salarak sindirme politikası uygulayabilmektedirler. Devletlerin e-devlet uygulamalarındaki zayıf yanları keşfederek hükümete, kolluk kuvvetlerine ve diğer özel ya da resmi kurumlara gözdağı vererek zor durumda bırakabilirler. Mesela; bir hastane-

nin bilgisayar sistemine girebilir ve korku salmak veya intikam amacıyla bir hastaya verilecek ilacın dozunu değiştirebilir ve kişinin ölümüne sebep olabilirler[14].

2.4. Bilişim Suçu İşlemede Kullanılan Yöntemler

2.4.1. Zararlı Yazılımlar (Malware)

"Malware" İngilizce açılımıyla "Malicious Software" zararlı yazılımların genel adıdır[15]. Zararlı yazılımlar aracılığıyla bilgisayar ve sistemlerine zarar vermenin yanında yalnızca erişim sağlamak da yeni Türk Ceza Kanunu hükümlerince suç sayılmıştır.

Windows İşletim Sistemlerinin her geçen gün yeni sürümlerinin çıkması ve koruyucu yazılımların varlığı, bilgisayar ve sistemlerine ulaşmayı her ne kadar zorlaştırsa da yeni sistemin açıklıkları bulunmakta ve erişim bir şekilde sağlanmaktadır. Bu da en çok zararlı yazılımlar aracılığıyla yapılmaktadır.

2.4.1.1. Virüs

Virüsler, çoğunlukla zarar verme amaçlı yazılan, ancak zararsız biçimde de var olabilen bilgisayar programlarıdır. Bilgisayardaki verileri kaydedebilir, değiştirebilir ya da silebilirler. Kendilerini diğer programlara veya özellikle exe, com, scr gibi uzantıları olan çalıştırılabilir dosyalara ekleyerek, otomatik olarak çoğalabilirler. Diğer yazılımları denetleyebilir ve flash disk vb donanımlarla veya internet üzerinden yayılabilirler. Bulaştıkları bilgisayarların çalışmasını engelleyebilir, hatta bozabilirler. Ancak, disk sürücüleri ve monitör gibi donanımlara zarar vermezler[16,17].

Bugünkü bildiğimiz anlamıyla, ilk gerçek virüs 1981 yılında "Elk Cloner" ismiyle ortaya çıkmıştır. Disketler aracılığıyla yayılan bu virüs zararsız olarak yazılmıştır. İlk zararlı virüs ise, 03.11.1983 günü deneysel çalışmalarla ortaya çıkarılmış ve "virüs" adı ilk kez kullanılmıştır[18,19,20].

Microsoft Güvenlik İstihbarat Raporu'nu ilk kez Türkçe yayınladı. Buna göre dünya genelinde araştırılan 26 ülkeden Türkiye 2009 yılının ikinci yarısında her 1000

bilgisayardan 20sine tehlikeli virüs bulaşmasıyla birinci sırada yer aldı. İkinci sırada Brezilya ve sonrasında İspanya Türkiye'yi takip eden ülkeler arasında[21].

2.4.1.1.1. Virüs Çeşitleri

2.4.1.1.1.1. Dosya Virüsleri

Çalıştırılabilir dosyalara tutunan ve tutunduğu program çalıştırılınca faaliyete geçen kod parçacıklarıdır. Genellikle com, exe gibi uzantıları olan dosyaları tercih etmekle beraber sys, drv, bin, ovl, ovy gibi uzantılı dosyalara bulaşanları da vardır. Dosya virüslerinin çoğu, kendisini sistem hafızasına yükler ve sürücüdeki diğer programları araştırır. Programları kendi kodunu da içerecek ve kendisini etkinleştirecek şekilde değiştirir. Bu şekilde yayılmasıyla birlikte, tahrip edici bir yöne de sahiptir. En çok bilinen dosya virüsleri "Randex, Meve ve MrKlunky"dir[18,19,20].

2.4.1.1.1.2. Önyükleme (Boot) Sektörü Virüsleri

"Boot işlemi" bilgisayarı açma şeklinde tanımlanabilir. Hard diskteki tüm verilerin saklandığı ve işletim sisteminin başlatıldığı yere "disk boot sektörü" denir. Burada sistem dosyalarını yükleyen programlar vardır ve bu programlara bulaşan virüslere "Önyükleme Sektörü Virüsleri" denilmektedir.

Boot sektörü virüsleri bellekte kalıcı ve aktif haldedirler, bilgisayara takılan her diskete bulaşırlar. 1996 yılına kadar en yaygın virüs tipi olan bu tür, günümüzde sayıca yok denecek kadar azalmıştır.

2.4.1.1.1.3. Çok Parçalı Virüsler

Dosya ve boot sektörü virüslerinin birleşmesiyle ortaya çıkmıştır. Virüsler disket, CD, DVD ile bilgisayarın önyükleme sektörüne gelir, oradan da çalıştırılabilir dosyalara bulaşırlar. En bilineni Ywinz'dir[20].

2.4.1.1.1.4. Makro Virüsler

Microsoft Office programı tarafından yaratılan Word, Excel, Powerpoint, Access vb uygulama programlarının diliyle yazılan ve bu uygulama ve programlara bulaşarak yayılan virüs türleridir. İlk makro virüsü, 1995'te Microsoft Word için yazılan virüstür. Çoğalma açısından solucanlara benzerler[18,19,20].

2.4.1.1.1.5. Eşlik Virüsleri

Bu türdeki virüsler, kendilerini MS-DOS, IQ.SYS, COMMAND.COM gibi önemli sistem dosyalarının uzantıları şeklinde kopyalayabilmektedir. Yani, dosya virüsleri gibi dosyalara tutunmaz, exe (uygulama) dosyalarına ait isimleri kullanan genelde com, nadiren exd uzantılı yeni dosyalar oluşturur. Bilgisayara komut verildiğinde aktif hale geçerler. Virüslü olan dosyalarda işlem yapmak olmayana göre daha uzun sürer[18,19,20].

2.4.1.1.1.6. Ağ Virüsleri

Herhangi bir hedefe yönelik yaratılmamışlardır. Diğer türlerin bulaştığı her dosyaya bulaşabileceği gibi, çoğunlukla çalıştırılabilir ve paylaşılan dosyaları tercih ederler. Bazen Truva atı gibi de kullanılabilirler. Anti-virüs programlarına yakalanmamak için bazı özel gizlenme teknikleri kullanırlar. Yerel ağ ve internet üzerinden gönderildiğinden en hızlı yayılan tiptir ve ele geçirdiği sistemlerde ağır zararlara yol açabilir[18].

2.4.1.1.1.7. Cross-site Scripting Virüsleri

Aslında bir virüs değil, sistem açığıdır. Yayılmak için web tarayıcı açıklıklarını kullanır. HTML, JavaScript, ActiveX, Java, Flash ve diğer kodlarla açıklık çağrılabilir. Bu açıklık bazı internet sitelerinde de olduğundan dikkatli olunmalıdır[22].

2.4.1.2. Truva Atları

Truva atı yazılımına, ünlü "Truva Atı" hikâyesinden esinlenilerek bu ad verilmiştir. Nitekim trojan da gayet masumane görünen içinde zararlı programları barındıran bir programdır ve kullanıcı tarafından çalıştırılmadıkça etkinleşmez[20].

Trojan, mağdur olan kişinin bilgisayarının belirli bir portunu açarak uzaktan erişim sağlanmasına ve verilerde tahribat yapılmasına olanak sağlayabilir. Buna göre trojanın yapabilecekleri:

1. Uzaktan erişime olanak verme
2. Veri gönderme
3. Veri tahribatı
4. Zararlı yazılım bulaşmış sistemi saklama (Proxy Trojans)
5. Zararlı bilgisayardan dosya ekleme ya da kopyalama (ftp trojans)
6. Güvenlik yazılımını devre dışı bırakma
7. Sistemi engelleme saldırıları (DOS)[23].

Trojanların ilk ortaya çıkışı kötü niyetli değildir. 90'lı yılların başında şirketlerde çalışan insanlar akşam işlerini bitiremeyince evden işyerindeki bilgisayara bağlanarak çalışmalarını tamamlamayı amaçlamışlardır. Ancak zamanla kötü niyetli kimseler bunu yasadışı amaçlar için kullanmış ve bu yönde geliştirmeye devam etmişlerdir[24].

Truva atı çoğunlukla internet üzerinden özellikle e-mail yoluyla bulaşır. Bu nedenle tanınmayan kişilerden gelen veya tanınan kişilerden beklenmeyen e-postalar açılmamalıdır. İnternet sitelerinden mümkün olduğunca bedava içerik indirilmemelidir.

2.4.1.3. Mantık Bombaları

Mantık bombaları trojanların bir alt kümesi kabul edilebilir.

Mantık bombası belirli şartlar oluşana dek etkisiz olarak bekleyen bir program veya program parçasıdır. Bu haliyle gerçek dünyadaki mayına benzetilebilir.

Bir mantık bombası için en yaygın harekete geçirme faktörü tarihtir. İlgili sisteme girdiğinde sistem tarihini kontrol eder ve önceden planlanmış tarih ve saate ulaşana dek hiçbir şey yapmaz, vakti gelince harekete geçer. Örneğin; ABD'de çalışma vizesi almış bir Hintli olan Fannie Mae Şirketi müteahhidi 31.01.2010 günü şirketin 4000 sunucusundaki bilgileri yok etmeye programlanmış bir mantık bombası tasarladı. Aynı şirkette çalışan Unix İşletim Sistemleri Mühendisi tarafından 29.01.2010 tarihinde fark edildi. Zamanında farkına varılmasaydı, şirket milyonlarca dolar kaybetmenin yanı sıra hükümet desteğiyle aldığı parayı ödeyemeyeceğinden kapanacaktı[25].

Aynı zamanda programcıdan belirli bir mesajın gelmesini beklemeye yönelik de programlanabilir. Örneğin; bir mantık bombası, belirli bir mesaja göre, bir web sitesini haftada bir kontrol edebilir. Çok geniş bir yelpazedeki başka değişkenlere göre de programlanabilir. Mesela; bir veritabanının belirli bir büyüklüğe ulaştırılması ya da kullanıcının ana dizininin silinmesi gibi[26].

Mantık bombası, yazılması çok kolay olduğundan kendisini çoğaltacak şekilde yazılmaz. Bu aynı zamanda istenmeyen kurbanlara yayılımını da önler.

Mantık bombasının en tehlikeli olanı hiçbir şey yapılmadığında faaliyete geçenidir. Bir ay içerisinde belirli bir siteye giriş yapılmaması durumunda bilgisayardaki tüm verilerin silinmesi gibi. En klasik kullanımı ise, bir yazılıma para ödenmesini sağlamaktır. Ödemenin belirli bir tarihe kadar yapılmaması halinde mantık bombası harekete geçer ve yazılım kendini otomatik olarak siler[27].

Bilişim sistemlerini kullanırken hiçbir zaman %100 güvenlik söz konusu olamaz. Bu nedenle istenmeyen durumların oluşmasını önlemek için koruyucu programlar kullanmanın yanı sıra, en iyisi, sürekli olarak veri yedeklemesi yapmak olacaktır.

2.4.1.4. Keylogger

Bir çeşit trojandır. En basit tanımıyla keylogger, klavyedeki tuş vuruşlarını takip eden, bilgileri bir dosyaya kaydedip saldırgana gönderen zararlı bir yazılım türüdür.

Keylogger tüm tuş vuruşlarını kaydetmek amaçlı ya da çok özel durumlarda aktive olacak şekilde kurulabilir. Mesela; yalnızca banka hesaplarına girildiğinde aktif hale geçip kullanıcı adını ve şifreyi ele geçirenler gibi. Bazı keyloggerlar ticari amaçla

da satılabilmektedir. Bir ebeveyn çocuklarının internette neler yaptığını, hangi sitelere girdiğini takip etmek için bilgisayara bu yazılımları yükleyebilir[28].

Keylogger ve trojanın diğer uzaktan erişim formları istenen bilgiyi çalmak adına kararlı bir şekilde ilerler ve "Rootkit"i kullanırlar. Rootkit: "Çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubudur. Amacı yayılmak değil bulunduğu sistemde varlığını gizlemektir"[20].

Bazı siteler "keylogger"ı önlemek amacıyla sanal klavyeyi geliştirmiştir. Ancak monitöre yazılan herşeyi kopyalayan "screenlogger"ın ortaya çıkmasıyla bu da yetersiz kalmıştır.

2.4.1.5. Solucanlar

Solucanlar, çok hızlı üreyerek çoğalır ve internet vb ağları tıkayabilir, hatta bilgisayarın çökmesine neden olabilir. Otomatik olarak çoğalır, ancak herhangi bir programa tutunmaya ihtiyaç duymadığından, bağımsız çalışmasıyla virüslerden ayrılır.

Bir trojan gibi bilgisayarların uzaktan erişimine ve kumanda edilmesine neden olabilir. Fakat çalışması için kullanıcı eylemine ihtiyaç duymadığından ve sisteme doğrudan zarar vermemesi ile trojanlardan ayrılır[29].

Solucanlar da diğer kötü yazılımlar gibi, taşıyıcı bellekler aracılığıyla ve daha çok kaynağı güvenli olmayan web sitelerine girip porno, bedava oyun, film, müzik içeriklerinin indirilmesiyle ve e-postalar aracılığıyla bulaşır.

2.4.1.6. Adware

Adware, İngilizce açılımı "advertising-supported software" olan reklam destekli yazılım. Bazı firmaların reklamının başka bir programın içinde gizlenmesi şeklinde yapılan ve program kullanımdayken otomatik olarak gösterme ve indirme yapan bir yazılımdır[20,26].

2.4.1.7. Spyware (Casus Yazılım)

Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır[30].

Spyware, bir yandan firmaların reklamını gösterirken bir yandan da kendisinden istenen kullanıcının şahsi bilgilerini sahibine gönderir. Bu internette hangi sitelere girildiği gibi bilgilerin yanı sıra kredi kartı ve banka hesap numaraları ile şifrelerine kadar elzem bilgileri içerebilir.

Casus yazılımlardan korunma konusundaki bir yanlış düşünce, anti-virüs yazılımlarının bilgisayarı koruyacağı inancıdır. Ancak bu programlar kesinlikle yeterli değildir. Casus yazılımlara karşı anti-spyware yazılımlar kullanılmalıdır[20].

2.4.1.8. Şifre Kırıcılar

Şifre kırıcılar üç temel mantık üzerine çalışırlar.

- *"Decrypt:* Şifreleme algoritmasının bir zayıflığından yararlanarak şifreyi çok kısa sürede kırabilirler.
- *Sözlük saldırısı:* (Dictionary Attack) Bir sözlük kullanarak geçen kelimelerin denemesi ile şifrenin bulunma ihtimalini kısa sürede artırmaktadır.
- *Kaba Kuvvet Saldırısı:* (Broute Force) Belli bir düzen içerisinde bütün olasılıkların denenmesi üzerine dayalıdır. En uzun süren ve zahmetli şifre kırma yöntemi budur"[31].

2.4.1.9. Zararlı Yazılımların Tarihçesi

Disketlerin ortaya çıkmasıyla ilk virüs ortaya çıktı. 1980li yılların başı internet üzerinden ilk büyük yayılma oldu.

- **1972-** Bilgisayarlarla ilgili bilinen ilk virüs, David Gerrold tarafından yazılan "When H.A.R.L.I.E. Was One" adlı bir bilim kurgu romanında geçmektedir.

- The Creeper virüsü ilk olarak Arpanet'te 1970'lı yılların başında tespit edilmiştir. Tenex işletim sistemi yoluyla yayılmış ve bilgisayara bağlı modemi diğer bilgisayarlara bağlanmak ve onları enfekte etmek için kullanmıştır. "I'm The Creeper: Catch Me If You Can." mesajını ekranda göstermiştir.
- **1982-** İlk virüs olduğu düşünülen (ancak yanlış bilinen) "Elk Cloner" Rich Skrenta tarafından yazıldı. Disketler aracılığıyla yayılarak Apple DOS 3.3 türünden bilgisayarları etkiledi.
- **1983-** Güney Kaliforniya'daki Fred Cohen Üniversitesi'nde "Bilgisayar virüsü" ilk kez terim olarak kullanıldı.
- **1986-** "Brain" adı verilen ilk boot sektörü virüsünün bir Pakistanlı tarafından yaratılması.
- **1987-** Büyük ölçüde command.com uzantılı sistem dosyalarını etkileyen ilk "dosya virüsü"nün ortaya çıkışı.
- **1988-** Robert Morris tarafından yazılan "Arpanet" isimli solucanın ağ üzerindeki 6000 bilgisayarı devre dışı bırakması.
  - Ünlü "Friday the 13th" virüsü de bu yıl ortaya çıkmıştır.
  - "Cascade" isimli MS-DOS sistemine etki eden ilk virüs keşfedildi.
- **1989-** Trojanın ortaya çıkması
- **1990-** Anti-virüs yazılımları ortaya çıktı.
- **1991-** Symantec firması tarafından "Norton" anti-virüs yazılımı yayınlandı.
- **1992-** 1000'den fazla virüs çeşidinin bilindiği tarih.
- **1994-** "Good Times" adıyla bilinen ilk büyük virüs aldatmacası
- **1995-** "Concept" adyla bilinen ilk büyük "Word" virüsü
- **1999-** David L.Smith tarafından yazılan "Melisa" virüsü binlerce bilgisayarı bozarak tahmini 80.000.000 $ hasara yol açtı. Bu virüs, Microsoft Outlook adres bölümünde bulunan adreslere kendi kopyalarını göndermek suretiyle kendini çoğaltı. Bundan ötürü David L. Smith 20 ay hapse mahkum oldu.

- **2000-** Bu yılın Mayıs ayında Filipinli bir öğrenci tarafından yazılan "I Love You" virüsü milyonlarca bilgisayarı etkiledi. "Melissa" virüsüne benzer, ancak bu virüs ağ üzerinden şifreleri de geri gönderebilir.
- **2001-** Bu yılın Temmuz ayında "Code Red" isimli solucan Windows NT/2000 model sunucuları etkileyerek 2.000.000.000 $ zarara sebep oldu.
- **2003-** Bugüne kadar var olanların içinde en hızlı oranda yayılan "Slammer" isimli solucan bu yılın Ocak ayında ortaya çıkar ve yüzbinlerce bilgisayara bulaşır.
- **2004-** Ocak ayında "MyDoom" solucanı mail üzerinden en hızlı yayılan solucan ortaya çıktı.
  - Şubat ayında e-mail yoluyla yayılan ve kendini kopyalayarak çoğalma özelliğiyle ağ trafiğini tıkayan "Netsky" solucanı keşfedildi.
  - Mart ayında internet güvenlik sistemi ürünlerinin açıklarını bulan Witty solucanı yaratıldı.
  - Ağustos ayında "Nuclear Rat" isimli Truva atı Windows 2000, XP ve 2003 sistemlerini etkiledi.
  - Ağustos ayında casus yazılımların internet üzerinden yayılmasına ve özellikle Google ve Facebook sitelerine ulaşılmasını engelleyen (Denial of Service Attacks) "Vundo" isimli Truva atı ortaya çıktı.
  - Aralık ayında İlk web solucanı olarak bilinen "Santy" ortaya çıktı, Google arama motoru filtreler içermeden önce onun üzerinden 40.000 siteyi etkiledi.
- **2005-** Kasım ayında "Samy XSS" en hızlı yayılan solucan olarak kabul edildi.

  ActiveX kontrollerini kullanan "Zlob" isimli Truva atı keşfedildi.
- **2006-** Mail yoluyla yayılan "Nyxem" solucanı, "Mac OS X" isimli malware yazılımı, "OSX/Leap-A" veya "OSX/Oompa" adıyla bilinen düşük seviyede tehdit içeren trojan ve "Stration" isimli solucan ortaya çıktı.
- **2007-** "Storm" isimli botnet ağını kuran aynı isme sahip solucan e-mail yoluyla yayıldı. İlk etapta 1,7 milyon bilgisayarı etkilerken bu sayı üç ay içerisinde 10 milyona ulaştı. Merkezi Rusya'da olan bu botnet ağı bulaşırken haber, film içerikli bir e-mail gibi davranıyordu.

- **2008-** Windows programlarını etkileyen, anti-virüs programlarını kapatan ve kullanıcıların şifresi vb özel verileri çalan "Torpig" isimli Truva atı ortaya çıktı.
  - "Bohmini" isimli trojan, Windows XP'ye uyumlu Adobe 9.0, İnternet Explorer 7.0 ve Firefox 2.0 sürümlerinde güvenlik zafiyetine sebep oldu.
  - "Conficker" isimli solucanın beş farklı sürümü (A, B, C, D, E) ortaya çıktı. Fransız Ordusu, İngiltere Başkanlık Koruma (savaş gemileri ve denizaltıları da dâhil), Sheffield Hastanesi, Alman Ordusu ve Norveç Polisi bilgisayarlarının da aralarında bulunduğu Windows 2000 ve Windows 7 sürümlerini kullanan 9 milyondan 15 milyona ulaşan sayıda bilgisayarı etkiledi.
- **2009-** "W32.Dozor" isimli solucanla Amerika Birleşik Devletleri'ne ve Güney Kore'ye siber saldırı yapıldı.
- **2010-** Microsoft tarafından 18 Şubat'ta "Alureon" isimli trojanın sebep olduğu Salı günü güncelleştirmelerinden kaynaklanan BSoD (Blue Screen of Death - Ölümün Mavi Ekranı) probleminin olabileceği ilan edildi[32,33,34].

2.4.2. Phishing Yöntemi

Kredi, ATM kart numaraları, müşteri numaraları, hesap numaraları, internet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri ve benzeri bilgileri ele geçirmek üzere kişinin banka ve benzeri bir kurumdan gelmiş izlenimi verilen kurumun elektronik posta servisinin bir kopyasının e-posta olarak gönderilmesi ve kişinin oradaki linki tıklayarak işlem yapması sonucu dolandırılması yöntemidir. İngilizce "Balık tutma" anlamına gelen "Fishing" sözcüğünden esinlenerek oluşturulan bu terime "oltalama" da denir[34,35].

Bu konuyla ilgili Banka ve Kredi Kartları Kanununun 8. maddesinin 5. bendinde: "Kart çıkaran kuruluşlar, kartların kullanılması bir kod numarası, şifre ya da kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa, bu tür bilgilerin gizli kalması amacıyla gerekli önlemleri almak ve harcama ve alacak belgesinin müşteri nüshası üzerinde ve yazışmalarda kart numarasının açıkça yer almasını engellemekle yükümlüdür" denilmektedir. Bu nedenle banka ve benzeri kurumlar e-posta gibi yollarla şifre, kod numarası istememektedir.

2.4.3. Sosyal Mühendislik

Sosyal mühendisliği, bir sisteme yetkisiz erişim sağlama ve sistemdeki önemli bilgileri elde etme adına, hackerın hileli davranışlarda bulunarak insanların güvenini kazanması, şeklinde tanımlayabiliriz. Sosyal mühendisliğin amacı: ağ saldırıları, endüstriyel casusluk, kimlik hırsızlığı ya da sahtekârlık için bilgi toplamak yahut sadece sistemlere veya bilgilere yetkisiz erişim sağlamak olabilir[36,37,38].

İnternet, sosyal mühendislik için mükemmel bir ortam olabilir. Hacker e-posta yoluyla ya da sohbet ortamlarında kullanıcıların bilgisayarına zararlı yazılım yükleyebilir ya da ikna yoluyla kullanıcının bizzat kendisinden önemli bilgileri edinebilir[39,40].

2.4.4. Dumpster Diving (Çöpe Dalma)

Sosyal mühendisliğin bir türüdür. Bilgisayar atıklarında şirket telefon rehberleri, şirket politika kılavuzları, giriş adları ve şifreler gibi önemli bilgiler bulunabilir ve bunlar hacker tarafından kullanılabilir[41,42,43].

2.4.5. Denial of Service Attacks (Sistemi Engelleme Saldırıları)

Bu saldırı tekniğinde, herhangi bir şeyin ele geçirilmesi hedeflenmez; yalnızca belirli bir sistemi engelleme söz konusudur[44].

2.4.6. IP Aldatmacası

IP numarası, bilgisayarın kimliği şeklinde yorumlanabilir. IP aldatmacası, bilgisayarın hangi kaynağa bağlı olduğunun bulunmasını engellemek amacıyla ve TCP/IP protokolleri üzerindeki IP adresini yanlış göstermek suretiyle yapılır. IP aldatmacası iki şekilde yapılabilir.

1. Proxy/Socks sunucularını kullanarak,
2. IP paketlerinde düzenlemeler yaparak,

Proxy/Socks sunucularını kullanmak daha basit bir yöntemdir. IP paketlerinde düzenlemeler yapmak ise çok daha etkilidir. IP aldatmacası en çok sistemi engelleme saldırılarında kullanılır[45,46,47].

2.4.7. Sniffing (Paket Koklama)

Sniffing, ağ üzerindeki açıkları tespit etmek ve verileri ele geçirmek için bazı araçlar kullanmak suretiyle ağ trafiğini denetlemek ve ağ üzerinden iletilen verilerin çalınma işlemidir. Sniffing, bir problem oluşması dâhilinde sistem yöneticisinin müdahalesini sağlamak amacıyla yapıldığından içeriden gelebilecek saldırılara karşı da hazırlıklı olunmalıdır[48].

2.4.8. Spam

Spam, internet üzerinden aynı mesajın büyük miktarlarda kopyasının istenmediği halde gönderilmesidir. Çoğu reklam içerikli ticari amaçlı olmasına karşın, politik bir görüşün propagandasını yapma ya da başka herhangi bir konuda kamuoyu oluşturma amacı ile de gönderilebilir. Spamlar, e-posta gelen kutusunu fazlasıyla doldurarak kullanıcıların istediği haberi alamamasına ve vakit kaybına neden olmaktadır[49].

2.4.9. Botnet

Botnet, çok sayıda bilgisayarın tek kişi tarafından kötü amaçlara hizmet doğrultusunda yönetilmesidir[50]. Özellikle internet sohbet sitelerinde veya e-posta yoluyla farkında olmadan bulaştırılan zararlı yazılımlar aracılığıyla bilgisayarın kontrolü ele geçirilmekte ve kontrolü ele geçirilen bu bilgisayarlar diğerlerini etkileyip ağı genişletmede de kullanılmaktadır.

Botnet ağına katılan bilgisayarlar, dolandırıcılık ve sahtecilikten karapara aklamaya kadar akla gelen her türlü yasadışı eylemde kullanılabilirler. Kimi zaman bu ağ ya da ağı yaratmada kullanılan programlar da para karşılığı satılabilirler[51,52].

Botnetle yapılan saldırıların şüphelisi farkında olmadan o ağa dahil olan bilgisayarın kullanıcısı olduğundan, botnetteki bilgisayarlar terörizm gibi pek çok ağır suçun işlenmesinde de kullanılarak faillerinin belirlenmesini zorlaştırır[53].

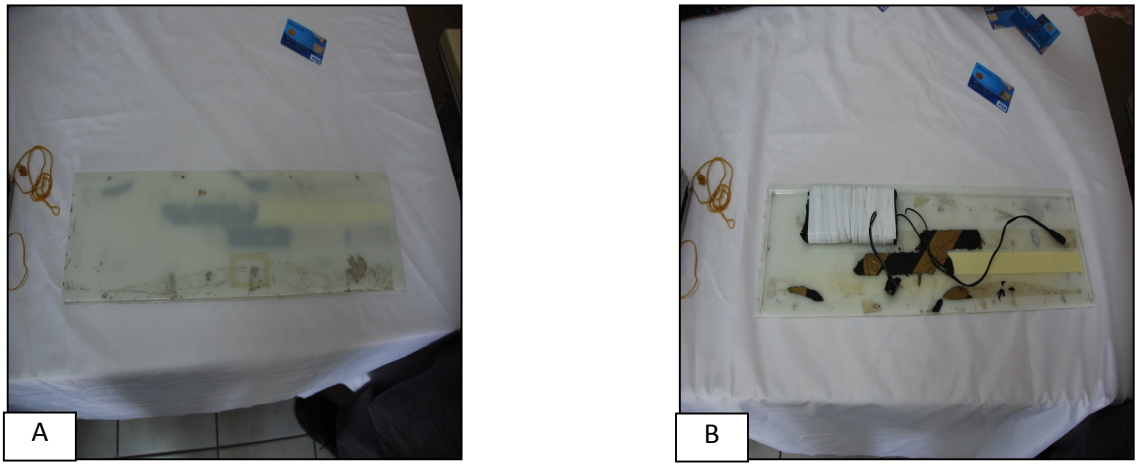
Botnet, zararlı yazılımlar kullanılarak oluşturulduğundan ve koruyucu programları sürekli olarak güncellenmeyen bilgisayarları hedef aldığından; koruyucu programlar kullanılarak ve sürekli güncelleyerek önemli derecede bundan korunulabilir. Ayrıca sohbet ortamlarında ya da e-posta eklentilerinde karşıdan yüklenecek olan yazılımlara da dikkat edilmelidir[54,55].

2.4.10. Banka ve Kredi Kartlarının Kötüye Kullanılması

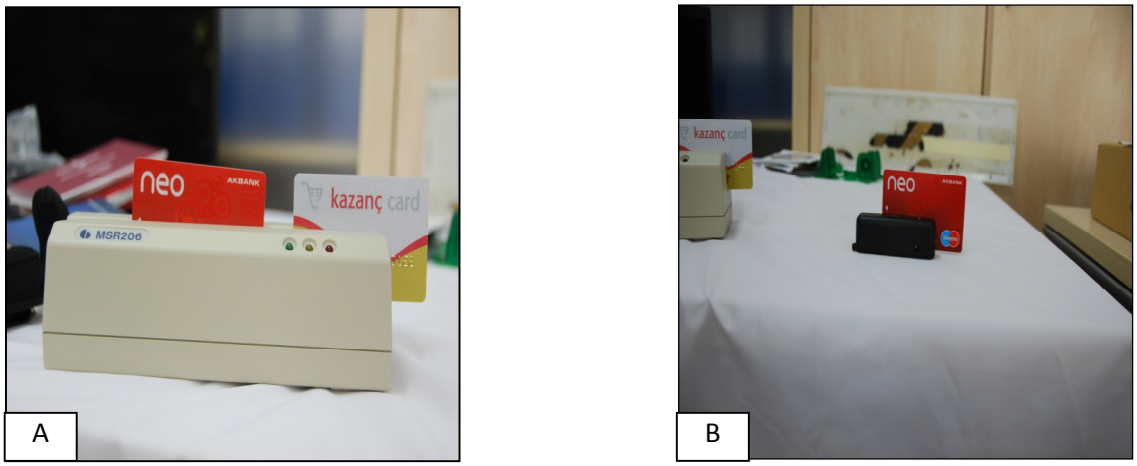
Banka ve kredi kartlarıyla ATM veya BTM cihazlarından para çekme veya yatırma işlemleri esnasında bu cihazlara kurulan sahte tuş takımı, sahte kart okuyucu gibi düzenekler kullanılarak ya da ödeme yapılması esnasındaki sahte cihazlar ve gerçek cihazların ucuna takılan bir aparat yardımıyla kart bilgileri ele geçirilebilmektedir. Ele geçirilen kart bilgileri boş bir karta yazılarak asıl kartın bir ikizi yapılabilmekte ve bu da büyük miktarlarda para kaybına neden olabilmektedir. Türkiye ve Adana bilişim suçları istatistiklerinde kredi kartı ve banka dolandırıcılığı suçu birinci sırada yer almaktadır.

Adana KOM Şube Müdürlüğü Tarafından Gerçekleştirilen Bir Operasyonda Ele Geçirilen Düzeneklerin Resimleri

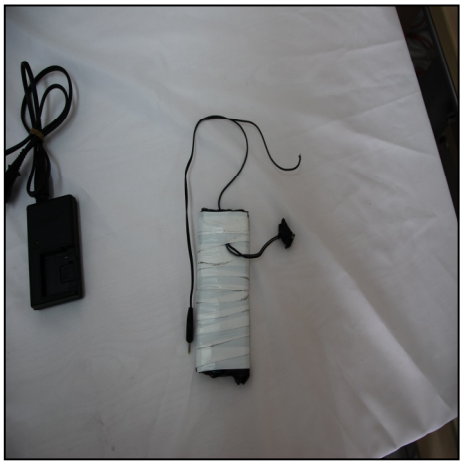
Şekil 1. ATM cihazına takılan kablosuz kamera sistemi



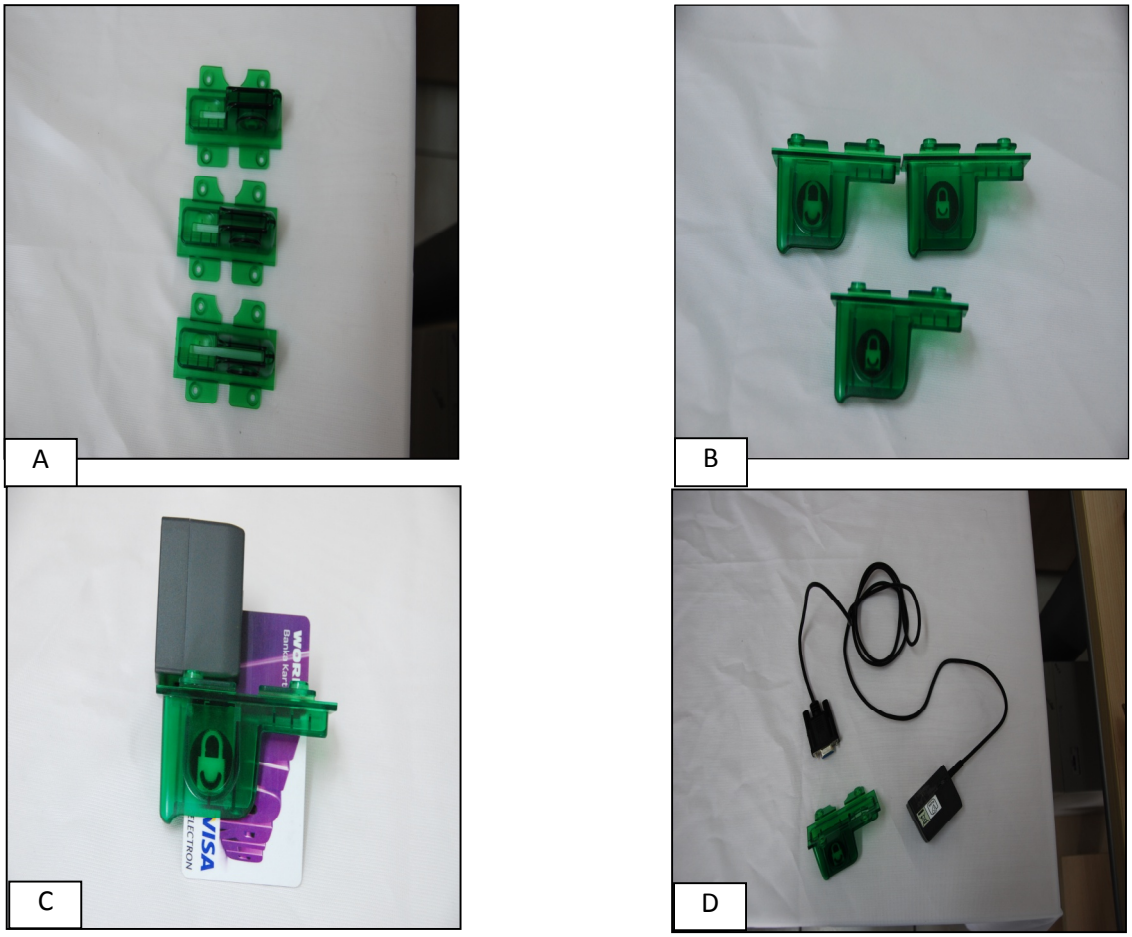
Şekil 2. ATM flüoresan lamba içine yerleştirilmiş kamera sistemi: A. Kapalı, B. Açık hali



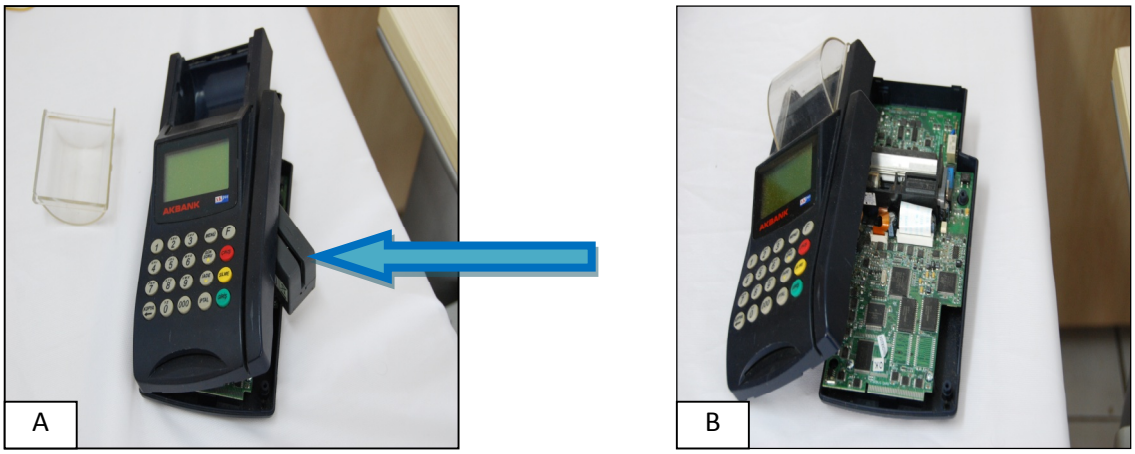
Şekil 3. En Coder cihazı (Papağan): A. Büyük tasarım, B.Küçük tasarım



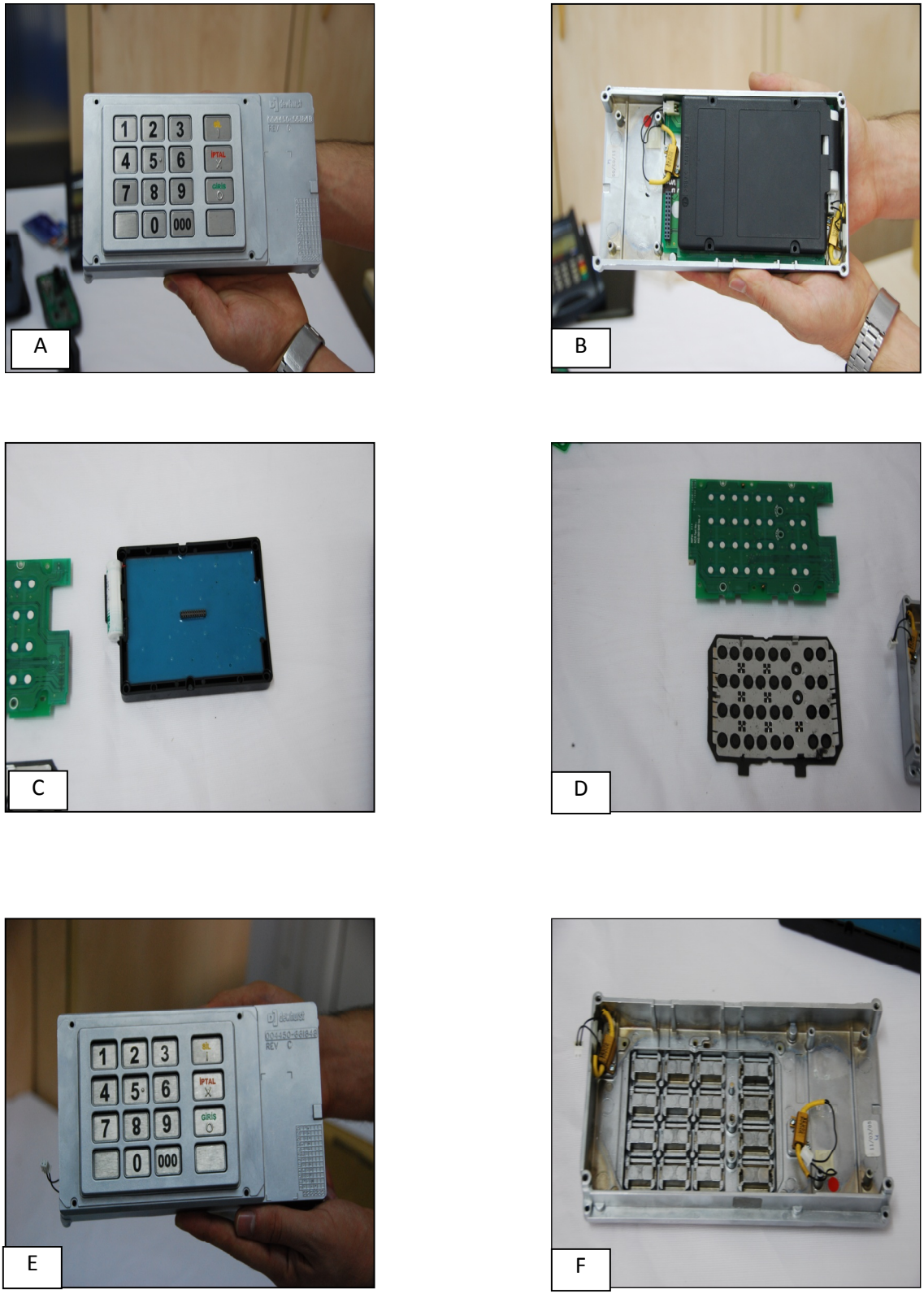
Şekil 4. Kameranın uzun süre çalışması için güçlendirilmiş batarya



Şekil 5. ATM Kart yuvası: A. Düz, B. Çıkıntılı, C. ATM'deki tam monteli hali
D. ATM kart yuvası kablo giriş yeri



Şekil 6. POS Cihazı: A. POS cihazı içine şifre kopyalama cihazı yerleştirilmiş, B. Sökülmüş hali



Şekil 7. Sahte tuş takımının sırasıyla sökülme aşamaları A, B, C, D, E, F.

Şekil 8. Dolandırıcılık olaylarında kullanılan program CD'leri

Şekil 9. Operasyonda ele geçirilen aletlerin tamamı

2.5. Geçmişten Günümüze Bilişim Suçları

Her ne kadar dünyada abaküs ilk bilgisayar olarak kabul edilse de, gerçek anlamda ilk bilgisayar 1941 yılında Berlin'de Konrad Zuse tarafından geliştirilendir[56].

Bilgisayarlar konusunda en önemli ve hızlı gelişmeler 2. Dünya Savaşı'ndan sonra başlamıştır. İlk geniş ölçekli otomatik, elektromekanik bilgisayar, 1944'te IBM ile işbirliği yapılarak meydana getirilen ve delikli kartlar kullanılarak veri alış verişi yapılabilen MARK I'dir[56,57]. Bunu 1945'te askeri amaçlar için geliştirilen ENIAC isimli bilgisayar takip etti[57].

Ticari amaçlarla kullanılabilen ve seri halde üretimi yapılan ilk bilgisayar, UNI-VAC I, 1960 yılında ve aynı yıllarda IBM 701 bilgisayarı piyasaya çıktı[56,57].

1964 ve 1970 yılları bilgisayar alanındaki gelişmelere ivme kazandırmış; daha hızlı, güvenilir ve maliyeti daha ucuz bilgisayarlar üretilmeye başlanmıştır. Özellikle 1993 yılından itibaren ortaya çıkan bilgisayarlar bugün kullanmış olduğumuz bilgisayarların eski modelleri sayılabilir[57].

İnternet fikri, Amerika'nın en büyük üniversitelerinden biri olan Massachusetts Institute of Tecnology'de (MIT) 1962 yılında J.C.R. Licklider'in tartışmaya açtığı "Galaktik Ağ" kavramıyla ortaya çıktı. Nükleer bir savaş esnasında telefon hatlarının tahrip olması durumunda bilgisayar ile iletişiminin sürdürülmesi düşüncesiyle, 1966'da Amerikan askeri araştırma projesi olan "İleri Savunma Araştırma Projesi (DARPA - Defense Advanced Research Project Agency)" ile Arpanet ortaya çıktı[58,59].

1969 yılında Amerika'da veri haberleşmesindeki tekniklerin öğrenilmesi amacı ile Arpanet çerçevesinde ilk bağlantı dört merkezle yapıldı. 1972'de 40 bilgisayardan oluşan bir Arpanet ağı kuruldu ve aynı yıl elektronik posta (e-mail) ilk defa kullanıldı. 1975 yılında işlevsel bir ağ konumunu alan Arpanet'e birçok organizasyon katıldı[58,59].

1980'li yılların ortasında Savunma Bakanlığı'na bağlı Amerikan askeri bilgisayar ağı, Arpanet'ten ayrıldı ve Military Net adı ile kendi ağını kurdu[59].

1983 yılında, Internetworking Working Group (INWG) TCP/IP'ye temel halini verdi. TCP/IP protokolleri de askeri standart olarak (MIL STD) uyarlanmıştır. Aynı yıllarda Internet terimi yaygın olarak kullanılmaya başlanmıştır. TCP/IP protokolünün

Unix işletim sistemine eklenmesinin ardından, 1984 yılında DNS (Domain Name System) tanıtılmıştır[58].

1990 yılında ARPANET varlığını yitirmiş ve internet tam anlamıyla doğmuştur[58].

Türkiye'de internet çalışmaları 1991'de ODTÜ ve TUBİTAK tarafından oluşturulan TR-NET adı altındaki proje grubu ile başlatıldı. İlk bağlantı ise 1993 yılında ODTÜ-Washington (Türkiye-ABD) arasında gerçekleştirildi[60].

1960 yılında Amerika'daki MIT(Massachusetts Institute of Technology) laboratuarlarında çalışan araştırma görevlileri Fortran'da ilk kez "bir yazılım veya sistemin yapabileceklerini öteye taşımak" anlamında "hacker" deyimini kullandı[61]. İlk bilgisayar hackerları aynı yıl MIT'te ortaya çıktı. Amaçları ise enstitü içinde elektrikle çalışan trenlerin daha hızlı yol kat etmesini sağlamaktı[62].

1967 yılında, 3000 kredi kartının kaybolması olayı ile adını duyurarak bilgisayarı araç olarak kullanarak, ilk bilgisayar suçunu işleyerek 620.000 $ zarara sebep olan ve 1969 yılında bu suçtan dolayı yargılanan ilk kişi Amerikalı Alfonse Confessore olmuştur[63].

1972 yılında John Draper, Captain Crunch marka şekerlemeler içinden çıkan düdüğün telefonla uzak mesafe görüşmeleri için gerekli sinyal ile aynı olduğunu keşfederek bedava görüşmeler yapmıştır[61].

1982'de Kevin Mitnick Kuzey Amerika Hava Savunma Komutanlığı bilgisayarına girdi. Ayrıca Kaliforniya'daki tüm telefon anahtarlama merkezlerine erişti ve Manhattan'daki üç adet merkezi telefon şirketinin kontrolünü geçici olarak ele geçirdi[64].

1986 yılında Kaliforniya Üniversitesi'ndeki network uzmanı hesaplardaki 75 centlik kayıpların sorumlusu olan beş Alman hackerı tespit etti ve aynı yıl Amerikan Kongresi bilgisayar sistemlerine izinsiz girişi suç sayan yasayı onayladı[61].

1987'de "Shadow Hawk" olarak bilinen 17 yaşındaki lise öğrencisi olan Herbert Zinn ABD Savunma Bakanlığı, NATO ve cep telefonu operatörü AT&T'nin bilgisayarlarına girdi, bir milyon dolarlık yazılımı çaldı ve bazı verileri yok etti. Bunun sonucu dokuz ay hapis ve 10.000 $ para cezası aldı[65].

Robert Morris, 1988 yılında yazdığı ve kendi adını verdiği Morris solucan yazılımıyla Arpanet'e bağlı 60.000 bilgisayarın 6.000'den fazlasını çökertti[62].

Kevin Mitnick 1988 yılının Aralık ayında Digital Equipment firmasının bilgisayarına girerek bir milyon dolarlık yazılımı çaldı ve bilgisayar sistemlerinde dört milyon dolarlık hasara sebep oldu[64].

1990 yılında "dark dante" takma adıyla bilinen Kevin Poulsen, Pacific Bell telefon şirketini hackleyerek KISS -FM adındaki radyo istasyonunun düzenlediği yarışmada 102. arayan olmayı başararak Porsche 944 S2 kazanmıştır[66].

1993 yılında Kaliforniya eyalet polisi Kevin Mitnick hakkında tutuklama müzekkeresi çıkardı. Mitnick, Kaliforniya Motorlu Araçlar Departmanı'nın veritabanlarından sürücü belgelerini çalmakla suçlanıyordu[67].

28 Mart 1994 tarihinde "Datastream Cowboy" ve "Kuji" takma adlarını kullanan iki hacker Roma Laboratuarları'na ve Güney Kore Atom Araştırmaları Enstitüsü'nün sistemlerine girerek tüm bilgileri indirdi[67].

1996'da "Johnny [Xchaotic]" adını kullanan bir hacker, 40 kadar politikacı, iş adamı ve çeşitli enstitülerin liderlerini e-posta bombardımanına tutmuştur[62]. Aynı yıl NASA ve ABD donanmasına bileşenler üreten Omega Engineering firmasında çalışan bir kişi, kovulduktan sonra firmanın sistemine girip, kendi yazdığı 6 satırlık kodu sisteme eklemiş ve tüm sistemi çökertmiştir[66].

1998 yılında "Analyzer" adıyla bilinen İsrailli Ehud Tenenbaum, NASA, Pentagon ve İsrail Parlamentosu'nun bilgisayarlarını hackledi. Aynı yıl üç arkadaşıyla birlikte Kanada ve ABD'deki ele geçirdikleri banka ve kredi kartı bilgilerini kullanarak ön ödemeli banka hesaplarından 1.800.000 $ çektiler[68].

1999'da Norveçli bir hacker gurubu olan Masters of Reverse Engineering (More), DVD kopya korumasını kırarak DVD'lerdeki korumaları kaldıran bir yazılımı internet üzerinden dağıtmışlardır[69].

2000 yılı DDOS saldırılarının yılı kabul edilmektedir. Özellikle Amazon ve Yahoo gibi sitelere bol miktarda istek gönderilerek siteler yavaşlatıldı. Aynı yıl "I LOVE YOU" virüsü ortaya çıktı. Ayrıca Microsoft'un sunucularına sızan hackerlar yeni Windows ve Office yazılımlarına ait kaynak kodları çaldılar[61].

28.10.2000 tarihinde güvenlik web sitesi Anti Online, dokuz milyon kez saldırıya uğradığı halde zarar görmeyince sitenin sahibi John Vranesevich, siteyi hacklenemez

ilan etti. Bunun üzerine saldırıları arttıran hackerlardan Avustralyalı "n1nor" lakaplı kişi siteyi hackledi[70].

2001'de Los Angeles Times gazetesinde yer alan habere göre Çin kaynaklı olduğu düşünülen hackerlar Kaliforniya elektrik sistemini kontrol eden bilgisayar ağına saldırarak 17 günlük bir krize sebep oldu[62].

2001-2002 yıllarında "Solo" lakabını kullanan Gary Mckinnon, Amerikan Savunma Bakanlığı (Pentagon) ile Amerikan Uzay ve Havacılık Dairesi (NASA) bilgisayarlarını hackledi ve Amerikan hükümetinin bir milyar dolar zarara uğramasına sebep oldu[71].

2002 yılında Amerika'da yetmiş beş milyon dolarlık yazılımı ele geçiren Lisa Chen dokuz yıl hapse mahkûm edildi[72].

2004'te Myron Tereshchuk adlı hacker, uluslar arası patent şirketini DDOS saldırısı yoluyla gizli bilgilerini açığa çıkaracağı yönünde tehdit ederek on yedi milyon dolar dolandırdı. [73]

2005 yılı içerisinde 20 yaşındaki Jeanson James Ancheta Amerikan ordularına ait bilgisayarların kontrolünü ele geçirerek botnet olarak satışa çıkarmış ve bilgisayarların DDOS saldırıları ve spam göndermede kullanılmasına sebep oldu, ayrıca bu bilgisayarlar üzerinden dolandırıcılık ve kara para aklama suçu işledi[74].

2006 yılında "İskorpitx" lakaplı bir Türk hacker tek seferde 21.549 internet sitesini çökertti[73].

2007'de bir Türk hacker grubu Birleşmiş Milletler internet sayfasını değiştirerek "Hey İsrail ve Amerika, çocukları ve başka insanları öldürmeyin. Sonsuza kadar barış, savaşa hayır" yazısını eklediler[72]. Aynı yıl FBI'nın yaptığı bir operasyonla bir milyon bilgisayarın bulunduğu botnet şebekesi çökertildi[73].

2008 yılı içerisinde 20 Çinli hacker Pentagon gibi önemli birimlerin bilgisayarlarını hacklediler. Ayrıca "Jeopardy" lakaplı bir Türk hacker, Amerikan Bankası'nın sistemlerine girerek 85.000 kredi kartı bilgilerini çaldı[73].

2010 yılı içinde Türk hackerlar İsrail'in resmi internet sitelerinin çoğuna saldırmışlardır[75]. Aynı yıl içerisinde "Google" internet sitesi Çin kaynaklı hackerların saldırısına uğradı[73].

2.6. Bilişim Suçlarının Hukuki İncelemesi

Bilgisayar – hukuk ilişkisi ilk olarak 1972 yılında yazılımların korunması konusunun ABD mahkemelerinde yer almasıyla gündeme gelmiştir. ABD'yi sırasıyla 1976 yılında Almanya, 1981 yılında İngiltere, 1982 yılında İtalya ve Fransa takip etmişlerdir[76]. Türkiye'de ise bu konu 07.06.1995 tarihinde 4110 sayılı kanunla 5846 sayılı Fikir ve Sanat Eserleri Hakkındaki Kanun'da yapılan değişiklikle Türk hukukundaki yerini almıştır[77].

Bilgisayarların kötüye kullanılması ve uluslar arası veri alış verişinin sebep olacağı sıkıntılar üzerine ilk araştırma 1977 yılında İsveç tarafından yapılmıştır[78]. Aynı yıl bilişim suçları ile ilgili ilk kapsamlı kanun teklifi, Senatör Ribikoff tarafından Amerikan Kongresi'ne sunulmuştur. Bu teklif Kongre tarafından kabul edilmemesine rağmen, bu suç grubunun dünya çapında tanınmasını sağlamıştır[79]. ABD 1980'de Telif Hakları Kanunu'nda bilgisayar programlarını da konu edinmiştir[80].

1985 yılında Avrupa Topluluğu Suç Problemleri Avrupa Komitesi, bilgisayar suçları ve çözümü konusunda araştırma yapmak üzere bir komisyon kurdu. Aynı yıl Norveç'te ve 1989'da Hollanda'da benzeri çalışmalar yapıldı[78].

1991'de Avrupa Konseyi, üye ülkelere bilgisayar programlarının korunması konusunda milli kanunlarında yapmaları gereken değişiklikleri gösteren bir yönerge göndermiştir. Almanya ve Fransa ise 1985 yılında Avrupa Konseyi'nden önce bu çalışmaları kendi ülkelerinde yapmışlardır[80,81].

2.6.1. 765 Sayılı Eski Türk Ceza Kanunu'nda Bilişim Suçları

Bilişim suçu kavramı, Türk Ceza Hukuku'na ilk defa 1991 yılında 3756 sayılı kanunla girmiştir ve "Bilişim Alanında Suçlar" başlığı altında T.C.K.'nın 525. maddesinin (a-b-c-d) bentlerindeki düzenlemeler ile bilişim alanı ihlalleri bilişim suçu olarak ifade edilmiştir. 525. maddenin (d) bendi, bilişim suçu işleyenler hakkında verilmesi gereken cezalarla ilgilidir. (a), (b) ve (c) bentlerinde tarifi yapılan beş ayrı suç tipi şunlardır:

- (a-1), sistemde yer alan ve sır teşkil eden bilgiyi hukuka aykırı olarak elde edip öğrenmek,
- (a-2), başkasına zarar vermek için sistemde bulunan bilgileri kullanmak, nakletmek, çoğaltmak,
- (b-1), başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadı ile sistemi ve unsurlarını tahrip etmek, değiştirmek, silmek, sistemin işlemesine engel olmak, yanlış biçimde işlemesini sağlamak,
- (b-2), sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamak, dolandırıcılık,
- (c), sistemi kullanarak sahtecilik yapmaktır[82].

2.6.2. 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Alanında Suçlar

Eski TCK' da tek maddede "Bilişim Alanında Suçlar" başlığı adı altında düzenlenen bilişim suçları, 26.09.2004 tarihinde kabul edilip 01.06.2005 tarihinde yürürlüğe giren 5237 Sayılı Türk Ceza Kanunu ile daha da genişletilmiş ve "Bilişim Alanında Suçlar" başlığı altında onuncu bölümde açıklanmıştır.

- **Madde 243 - Bilişim Sistemine Girme**

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

- **Madde 244 - Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme**

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

• **Madde 245 - Banka veya Kredi Kartlarının Kötüye Kullanılması** (Değişik madde: 29/06/2005-5377 S.K./27.mad)

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) (Ek fıkra: 06/12/2006 - 5560 S.K.11.md) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.

- **Madde 246 - Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması**

Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Bilişim alanında suçlar bölümünde açıklanmasa da kanunun 142. ve 158. maddelerinde açıklanan "nitelikli hırsızlık" ve "nitelikli dolandırıcılık" suçları da bilişim sistemleri aracılığıyla işlendiğinde bilişim suçu kapsamına girmektedir.

Madde 142 –Nitelikli Hırsızlık

(1) Hırsızlık suçunun;

a) Kime ait olursa olsun kamu kurum ve kuruluşlarında veya ibadete ayrılmış yerlerde bulunan ya da kamu yararına veya hizmetine tahsis edilen eşya hakkında,

b) Herkesin girebileceği bir yerde bırakılmakla birlikte kilitlenmek suretiyle ya da bina veya eklentileri içinde muhafaza altına alınmış olan eşya hakkında,

c) Halkın yararlanmasına sunulmuş ulaşım aracı içinde veya bunların belli varış veya kalkış yerlerinde bulunan eşya hakkında,

d) Bir afet veya genel bir felâketin meydana getirebileceği zararları önlemek veya hafifletmek maksadıyla hazırlanan eşya hakkında,

e) Adet veya tahsis veya kullanımları gereği açıkta bırakılmış eşya hakkında,

f) Elektrik enerjisi hakkında,

İşlenmesi hâlinde, iki yıldan beş yıla kadar hapis cezasına hükmolunur.

(2) Suçun;

a) Kişinin malını koruyamayacak durumda olmasından veya ölmesinden yararlanarak,

b) Elde veya üstte taşınan eşyayı çekip almak suretiyle ya da özel beceriyle,

c) Doğal afetin veya sosyal olayların meydana getirdiği korku, kargaşadan yararlanarak,

d) Haksız yere elde bulundurulan veya taklit anahtarla ya da diğer bir aletle kilit açmak suretiyle,

e) Bilişim sistemlerinin kullanılması suretiyle,

f) Tanınmamak için tedbir alarak veya yetkisi olmadığı hâlde resmî sıfat takınarak,

g) Barınak yerlerinde, sürüde veya açık yerlerde bulunan büyük veya küçük baş hayvan hakkında,

İşlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur. Suçun, bu fıkranın (b) bendinde belirtilen surette, beden veya ruh bakımından kendisini savunamayacak durumda olan kimseye karşı işlenmesi halinde, verilecek ceza üçte biri oranına kadar artırılır.

(3) Suçun, sıvı veya gaz hâlindeki enerji hakkında ve bunların nakline, işlenmesine veya depolanmasına ait tesislerde işlenmesi hâlinde, ikinci fıkraya göre cezaya hükmolunur. Bu fiilin bir örgütün faaliyeti çerçevesinde işlenmesi hâlinde, onbeş yıla kadar hapis ve onbin güne kadar adlî para cezasına hükmolunur.

(4) (Ek fıkra: 06/12/2006 - 5560 S.K.6.md) Hırsızlık suçunun işlenmesi amacıyla konut dokunulmazlığının ihlâli veya mala zarar verme suçunun işlenmesi halinde, bu suçlardan dolayı soruşturma ve kovuşturma yapılabilmesi için şikâyet aranmaz.

• Madde 158 - Nitelikli Dolandırıcılık

(1) Dolandırıcılık suçunun;

a) Dinî inanç ve duyguların istismar edilmesi suretiyle,

b) Kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan yararlanmak suretiyle,

c) Kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle,

d) Kamu kurum ve kuruluşlarının, kamu meslek kuruluşlarının, siyasî parti, vakıf veya dernek tüzel kişiliklerinin araç olarak kullanılması suretiyle,

e) Kamu kurum ve kuruluşlarının zararına olarak,

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,

g) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle,

h) Tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında,

i) Serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle,

j) Banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla,

k) Sigorta bedelini almak maksadıyla,

İşlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur. (Ek cümle: 29/06/2005-5377 S.K./19.mad) Ancak (e), (f) ve (j) bentlerinde sayılan hâllerde hapis cezasının alt sınırı üç yıldan, adlî para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz.

(2) Kamu görevlileriyle ilişkisinin olduğundan, onlar nezdinde hatırı sayıldığından bahisle ve belli bir işin gördürüleceği vaadiyle aldatarak, başkasından menfaat temin eden kişi, yukarıdaki fıkra hükmüne göre cezalandırılır.

2.6.3. 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemleri Aracılığıyla İşlenen Suçlar

- 106. madde "Tehdit", 107. madde "Şantaj", 125. madde "Hakaret", 132. madde "Haberleşmenin Gizliliğini İhlal", 133. madde "Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması", 134. madde "Özel Hayatın Gizliliğini İhlâl", 135. madde "Kişisel Verilerin Kaydedilmesi", 136. madde "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme", 137. madde "Nitelikli Haller", 138. madde "Verileri Yok Etmeme", 103. madde "Çocukların Cinsel İstismarı", 226. madde "Müstehcenlik", 190. madde "Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma", 228. madde "Kumar Oynanması için Yer ve İmkân Sağlama".

Bu bölümde anlatılan suçlar başlı başına bir bilişim suçu olmamakla birlikte, bilişim sistemleriyle işlendiğinde neredeyse bilişim suçundan ayırt edilemeyecek şekilde zihinleri karıştırabilmektedir. Türk Ceza Kanunu'nun kapsadığı hemen hemen

her suça bilişim sistemleri dâhil edilebilir. Bununla birlikte, bazen bilişim suçu bazen de normal suçlar işleniş yönü, vs itibariyle birbirini kapsayabilir ya da birbiriyle ilişkilendirilebilir. TCK 243. maddede belirtilen "Bilişim sistemine girme" suçunun aynı zamanda 134. maddedeki "Özel hayatın gizliliğini ihlal" suçunu oluşturması gibi.

2.6.4. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'ndaki Düzenleme

Madde 72 - Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri (Değişik madde: 03/03/2004-5101/18.mad; Değişik madde: 23/01/2008-5728 S.K./139.mad)

Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır.

2.6.5. 5816 Sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun

Madde 1 - Atatürk'ün hatırasına alenen hakaret eden veya söven kimse bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

Atatürk'ü temsil eden heykel, büst ve abideleri veyahut Atatürk'ün kabrini tahrip eden, kıran, bozan veya kirleten kimseye bir yıldan beş yıla kadar ağır hapis cezası verilir.

Yukarıdaki fıkralarda yazılı suçları işlemeye başkalarını teşvik eden kimse asıl fail gibi cezalandırılır.

Madde 2 - Birinci maddede yazılı suçlar; iki veya daha fazla kimseler tarafından toplu olarak veya umumi veya umuma açık mahallerde yahut basın vasıtasıyla işlenirse hükmolunacak ceza yarı nispetinde artırılır.

Birinci maddenin ikinci fıkrasında yazılı suçlar zor kullanılarak işlenir veya bu suretle işlenmesine teşebbüs olunursa verilecek ceza bir misli artırılır.

2.6.6. 7258 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun

Madde 5 - (Değişik madde: 22/02/2007-5583 S.K./3.mad; Değişik madde: 23/01/2008-5728 S.K./256.mad)

Kanunun verdiği yetkiye dayalı olmaksızın, spor müsabakaları ile ilişkili olarak sabit ihtimalli veya müşterek bahis oynatanlar, oynanmasına yer veya imkân sağlayanlar, bir yıldan üç yıla kadar hapis ve on bin güne kadar adlî para cezasıyla cezalandırılır.

Yurt dışında oynatılan her çeşit bahis veya şans oyunlarının internet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkân sağlayan kişiler, iki yıldan beş yıla kadar hapis cezasıyla cezalandırılır.

Her türlü bahis veya şans oyunlarıyla bağlantılı olarak para nakline aracılık eden kişiler, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adlî para cezasıyla cezalandırılır.

Kişileri, reklam vermek ve sair surette, her türlü bahis veya şans oyunlarını oynamaya teşvik edenler, altı aydan iki yıla kadar hapis ve üç bin güne kadar adlî para cezasıyla cezalandırılır.

Bu maddede tanımlanan suçlarla bağlantılı olarak, her türlü bahis veya şans oyunlarının oynanmasına tahsis edilen veya oynanmasında kullanılan ya da suçun konusunu oluşturan eşya ile bu oyunların oynanması için ortaya konulan veya oynanması suretiyle elde edilen her türlü mal varlığı değeri, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun eşya ve kazanç müsaderesine ilişkin hükümlerine göre müsadere edilir.

Bu maddede tanımlanan suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Bu maddede tanımlanan suçlarla ilgili olarak, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun erişimin engellenmesine ilişkin hükümleri uygulanır.

2.6.7. 5271 Sayılı Ceza Muhakemesi Kanunu'ndaki Düzenleme

Madde 134 - Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

2.6.8. 5070 Sayılı Elektronik İmza Kanunu

Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir. Burada bizi ilgilendiren kanunun üçüncü kısmı, denetim ve ceza hükümleri ile ilgili maddeleri.

- **Madde 15 – Denetim**

Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir.

Kurum, gerekli gördüğü zamanlarda elektronik sertifika hizmet sağlayıcılarını denetleyebilir. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

• **Madde 16 - İmza Oluşturma Verilerinin İzinsiz Kullanımı** (Değişik madde: 23/01/2008 - 5728 S.K./525.mad)

Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

• **Madde 17- Elektronik Sertifikalarda Sahtekârlık** (Değişik madde: 23/01/2008 - 5728 S.K./526.mad)

Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

2.6.9. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik

04.05.2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'

a dayanılarak hazırlanan bu yönetmeliğin amacı; içerik sağlayıcıların, yer sağlayıcıların ve erişim sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir.

- **Madde 4 – İlkeler**

(1) Yayınlar;

a) İnsan onuruna, temel hak ve hürriyetlere saygılı olmalıdır.

b) Gençlerin ve çocukların fiziksel, zihinsel ve ahlakî gelişimini zedeleyecek türden içeriklere yer vermemelidir.

c) Ailenin huzur ve refahını sağlayan hususlara zarar verecek nitelikte olmamalıdır.

ç) Kişileri, uyuşturucu madde bağımlılığı, fuhuş, müstehcenlik ve kumar gibi kötü alışkanlıklara teşvik edici olmamalıdır.

(2) Herkesin kendisine yönelik haklarını ihlal eden internet yayınlarının içeriklerinden dolayı cevap ve düzeltme hakkı olmalıdır.

- **Madde 5 - Bilgilendirme Yükümlülüğü**

(1) Ticari veya ekonomik amaçlı içerik sağlayıcıları, yer sağlayıcıları ve erişim sağlayıcıları, aşağıda belirtilen tanıtıcı bilgilerini, kendilerine ait internet ortamında, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve iletişim başlığı altında, doğru, eksiksiz ve güncel olarak bulundurmakla yükümlüdür:

a) Gerçek kişi ise; adı ve soyadı, tüzel kişi ise; unvanı ve sorumlu kişiler, vergi kimlik numarası veya ticaret sicil numarası,

b) Yerleşim yeri, tüzel kişi ise merkezinin bulunduğu yer,

c) Elektronik iletişim adresi ve telefon numarası,

ç) Sunduğu hizmet, bir merciin iznine veya denetimine tabi bir faaliyet çerçevesinde yapılıyor ise, yetkili denetim merciine ilişkin bilgiler.

(2) Ticari veya ekonomik amaçlı içerik sağlayıcı, birinci fıkradaki bilgilerle birlikte, yer sağlayıcıya ilişkin tanıtıcı bilgileri, doğru, eksiksiz ve güncel olarak ana sayfasında bulundurmakla yükümlüdür.

- **Madde 6 - İçerik Sağlayıcının Sorumluluğu**

(1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

(2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur.

- **Madde 7 - Yer Sağlayıcının Yükümlülükleri**

(1) Yer sağlayıcı;

a) Yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, Kanun ve ilgili mevzuat hükümlerine göre Başkanlık, adli makamlar veya hakları ihlal edilen kişiler tarafından haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla,

b) Sunucu barındırma hizmeti dâhil, yer sağlamakla ilgili hizmetlerinde (a) bendindeki hükümlere uymakla,

c) Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlüdür.

(2) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

- **Madde 8 - Erişim Sağlayıcının Yükümlülükleri**

(1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, Kanun ve ilgili diğer mevzuat hükümlerine göre, Başkanlıkça haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemekle,

b) Sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla ve ilgili diğer mevzuatla verilen görevlerini yerine getirebilmesi için; erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle, internet trafik izlemesinde Başkanlığa gerekli yardım ve desteği sağlamakla, faaliyet belgesinde yer alan Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirmekle ve ticari amaçla internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP adres planlaması yapmakla ve bu bloktan IP adresi vermekle,

c) Faaliyetine son vereceği tarihten en az üç ay önce, durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmekle, Kuruma bildirilen kapanma tarihinden geriye doğru bir yıllık süredeki trafik bilgilerine ilişkin bütün kayıtları metin dosyası olarak, log formatlarını açıklamalarıyla birlikte, abone kütük bilgilerini Başkanlığa CD, DVD gibi optik medya ortamında teslim etmekle,

ç) Faaliyete başlamasından itibaren her ay düzenli olarak, her erişim yöntemine ilişkin kullanacağı erişim numaralarını ve toptan hizmet verdiği abonelere ilişkin bilgileri Başkanlığa göndermekle,

d) Başkanlık ile aralarındaki bağlantıdan erişimi engellenecek adreslere ilişkin gönderilecek bilgileri kendi sistemlerinde derhal uygulanabilmesi için, gerekli olan donanım ve yazılımı kurarak lazım olan düzenlemeleri yapmakla,

e) Kullanıcılarına vekil sunucu hizmeti sunuyor ise; vekil sunucu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle yükümlüdür.

(2) Erişim sağlayıcı, verdiği hizmeti kullananlara ilişkin bilgilerin başkaları tarafından elde edilmesini ilgili mevzuatta belirlenen esas ve usullere uygun olarak engeller.

(3) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadığını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

- **Madde 9 - İdari Para Cezaları**

(1) Bu Yönetmeliğin 5 inci maddesinde belirtilen yükümlülüğü yerine getirmeyen içerik sağlayıcı, yer sağlayıcı veya erişim sağlayıcıya Başkanlık tarafından ikibin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar idarî para cezası verilir.

(2) Bu Yönetmeliğin 8 inci maddesinin birinci fıkrasının (b) ve (c) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına, Başkanlık tarafından on bin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir.

- **Madde 10 - İçeriğin Yayından Çıkarılması ve Cevap Hakkı**

(1) İçerik nedeniyle hakları ihlâl edildiğini iddia eden kişi, içerik sağlayıcıya, buna ulaşamaması halinde yer sağlayıcıya, internet ortamından veya bizzat başvurarak, kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasını isteyebilir. İçerik veya yer sağlayıcı, kendisine ulaştığı tarihten itibaren iki gün içinde talebi yerine getirir. Bu süre zarfında talep yerine getirilmediği takdirde reddedilmiş sayılır.

(2) Talebin reddedilmiş sayılması halinde, kişi on beş gün içinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkarılmasına ve yayındaki kapsamından fazla olmamak üzere, hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasına karar verilmesini isteyebilir. Sulh ceza hâkimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hâkiminin kararına karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(3) Sulh ceza hâkiminin kesinleşen kararının, birinci fıkraya göre yapılan başvuruyu yerine getirmeyen içerik sağlayıcıya veya yer sağlayıcıya tebliğinden itibaren iki gün içinde, içerik yayından çıkarılarak hazırlanan cevabın yayımlanmasına,

kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve tekzip başlığı altında başlanır.

- **Madde 11 - Cezai Yaptırım**

(1) Sulh ceza hâkiminin kararını, 10 uncu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İçerik veya yer sağlayıcının tüzel kişi olması halinde, bu fıkra hükmü yayın sorumlusu hakkında uygulanır.

- **Madde 12 - Erişimin Engellenmesi Kararının Konusunu Oluşturan Suçlar**

(1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228) suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

- **Madde 13 - Koruma Tedbiri Olarak Erişimin Engellenmesi Kararı**

(1) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar

verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmi dört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır.

(2) Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara, Başkanlıkça ve Ceza Muhakemesi Kanunu hükümlerine göre ilgililer tarafından itiraz edilebilir.

- **Madde 14 - İdari Tedbir Olarak Erişimin Engellenmesi Kararı**

(1) İçeriği 12. maddede belirtilen suçları oluşturan yayınlarda, içerik sağlayıcının veya yer sağlayıcının yurt dışında bulunması halinde veya içerik sağlayıcı veya yer sağlayıcı yurt içinde bulunsa bile, içeriği Türk Ceza Kanununun 103. maddesinin birinci fıkrasında yer alan çocukların cinsel istismarı veya aynı Kanunun 226. maddesinde yer alan müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesine Başkanlıkça resen karar verilir. Türk Ceza Kanununun 103. maddesinin birinci fıkrasında yer alan çocukların cinsel istismarı veya aynı Kanunun 226. maddesinde yer alan müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak içerik veya yer sağlayıcının yurt içinde bulunması durumunda bu karar, yirmi dört saat içinde hâkimin onayına sunulur ve hâkim kararını en geç yirmi dört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Başkanlık tarafından derhal kaldırılır ve erişim sağlayıcılara bildirilerek gereğinin yerine getirilmesi istenir.

(2) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Cumhuriyet başsavcılığına suç duyurusunda bulunulur. Başkanlık, suç duyurusuna esas teşkil edecek verilerin elde edilebilmesi için kamu kurum ve kuruluşlarından bilgi ve belge talep edebilir.

2.6.10. 26687 Sayılı İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik

01.11.2007 tarihinde yürürlüğe giren bu yönetmelik, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun' a dayanılarak hazırlanmıştır ve internet toplu kullanım sağlayıcıları ve ticari amaçla internet toplu kullanım sağlayıcılarının

yükümlülükleri ve sorumlulukları ile denetimlerine ilişkin esas ve usulleri düzenlemeyi amaçlar.

- **Madde 4 - İnternet Toplu Kullanım Sağlayıcılarının Yükümlülükleri**

(1) İnternet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:

a) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.

b) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.

- **Madde 5- Ticari Amaçla İnternet Toplu Kullanım Sağlayıcılarının Yükümlülükleri**

(1) Ticarî amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:

a) Mülki idare amirinden izin belgesi almak.

b) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak.

c) Başkanlık tarafından onaylanan içerik filtreleme yazılımını kullanmak.

ç) Erişim sağlayıcılardan sabit IP almak ve kullanmak.

d) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek.

e) Başkanlık tarafından verilen yazılım ile, (d) bendi gereğince kaydedilen bilgileri ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri bir yıl süre ile saklamak.

2.6.11. 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu

- **Madde 8 - Kart Çıkarma ve Buna İlişkin Yükümlülükler**

Kart çıkaran kuruluşlar, talepte bulunmayan veya sözleşme imzalamayan kişiler adına hiçbir şekil ve surette kart veremezler. Bu kuruluşlarca genel müdürlük veya şube haricinde kredi kartı talebi toplanabilecek yerler Kurumun uygun görüşü alınarak Türkiye Bankalar Birliği ve Türkiye Katılım Bankaları Birliği tarafından müştereken belirlenir.

Asgarî tutarın son ödeme tarihini takip eden üç ay içinde ödenmemesi durumunda kart çıkaran kuruluşça kart hamiline yapılacak bildirimden itibaren bir aylık süre içerisinde bu tutarın ödenmemesi ya da banka kartı ile kredi kartı kullanımından dolayı

adli cezaların uygulanması halinde, ilgili kart çıkaran kuruluşça kart hamiline verilen kredi kartları iptal edilir ve borcun tamamı ödeninceye kadar yeni kredi kartı düzenlenemez.

Kart çıkaran kuruluşlar, kartların düzenli ve güvenli kullanımı ile bildirim, talep, şikâyet ve itirazlara ilişkin gerekli tedbirleri almaya yönelik sistemi kurmak ve kesintisiz olarak açık tutmakla yükümlüdür.

Kart çıkaran kuruluşlar, kartın verilmesi anında kart hamilini yeteri derecede bilgilendirmek ve talep edilmesi halinde, gerçekleştirilmiş işlemlere ait kayıtları otuz günü geçmemek üzere işlemin mahiyetine uygun bir süre zarfında sağlamakla yükümlüdür. Yurt dışı işlemlerinde bu süre altmış gün olarak uygulanır.

Kart çıkaran kuruluşlar, kartların kullanılması bir kod numarası, şifre ya da kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa, bu tür bilgilerin gizli kalması amacıyla gerekli önlemleri almak ve harcama ve alacak belgesinin müşteri nüshası üzerinde ve yazışmalarda kart numarasının açıkça yer almasını engellemekle yükümlüdür.

Kart çıkaran kuruluşlar, banka kartı ve kredi kartlarının asıl kart hamiline teslim edilmesini sağlayacak önlemleri almak, reşit olmayan ek kart hamilleri adına düzenlenen banka ve kredi kartlarının asıl kart hamillerine teslimini sağlamakla yükümlüdür.

- **Madde 16 - Bildirim Zorunluluğu**

Kart hamili, kendisine tevdi edilen kartı ve kartın kullanılması bir kod numarası, şifre veya kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa bu bilgileri güvenli bir şekilde korumak ve başkaları tarafından kullanılmasına engel olacak önlemleri almak, kartın kaybolması, çalınması veya iradesi dışında gerçekleşmiş herhangi bir işlemi öğrenmesi halinde kart çıkaran kuruluşu derhal haberdar etmek zorundadır.

Kart hamili adresinde meydana gelen değişiklikleri, değişiklik tarihinden itibaren on beş gün içinde kart çıkaran kuruluşa bildirmekle yükümlüdür.

- **Madde 23 – Bilgilerin Saklanması**

Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür.

Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür.

- **Madde 32 – İdari Para Cezaları**

Kurul kararıyla ve gerekçesi belirtilmek suretiyle bu Kanun kapsamındaki kuruluşlara, bu Kanunun;

a) 8 inci maddesinin birinci, ikinci ve üçüncü fıkralarına aykırılık halinde ikibin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar,

b) 9 uncu maddesinin birinci fıkrasına aykırılık halinde iki bin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar, ikinci fıkrasına aykırılık halinde beş bin Yeni Türk Lirasından az olmamak üzere, aykırılık oluşturan tutarın yüzde biri tutarına kadar,

c) 10 uncu maddesi ve 11 inci maddesinin birinci fıkrasına aykırılık halinde iki bin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar,

d) 14 üncü maddesi hükümlerine aykırılık halinde on bin Yeni Türk Lirasından elli bin Yeni Türk Lirasına kadar,

e) 18 inci maddesinin ikinci fıkrasına aykırılık halinde iki bin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar,

f) 24 üncü ve 25 inci maddelerine aykırılık halinde iki bin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar,

g) 27 nci maddesinin birinci fıkrasına aykırılık halinde on bin Yeni Türk Lirasından elli bin Yeni Türk Lirasına kadar,

h) İlgili maddelerine göre, Kurul tarafından bu Kanuna dayanılarak alınan kararlara, çıkarılan yönetmelik ve tebliğlere ve yapılan diğer düzenlemelere uyulmaması halinde iki bin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar veya aykırılık teşkil eden tutarın yüzde biri oranına kadar idarî para cezası uygulanır.

Bu Kanunda belirtilen para cezaları her yılbaşında 5326 sayılı Kabahatler Kanununun ilgili hükümleri uyarınca artırılır.

- **Madde 36 – Sahte Belge Düzenlenmesi**

Gerçeğe aykırı olarak harcama belgesi, nakit ödeme belgesi ya da alacak belgesi düzenlemek veya bu belgelerde ne surette olursa olsun tahrifat yapmak suretiyle kendisine veya başkasına yarar sağlayanlar, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılırlar.

- **Madde 37 - Gerçeğe Aykırı Beyan, Sözleşme ve Eki Belgelerde Sahtecilik**

Banka kartı veya kredi kartını kaybettiği ya da çaldırdığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar bir yıldan üç yıla kadar hapis ve iki bin güne kadar adlî para cezası ile cezalandırılırlar.

Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler.

- **Madde 38 – İzinsiz Kart Çıkarma**

Bu Kanunun 4 üncü maddesinde belirtilen izinleri almaksızın kartlı sistem kuran, kredi kartı çıkaran veya üye işyeri anlaşması yapan veya ticaret unvanları, her türlü belgeleri, ilân ve reklamları veya kamuoyuna yaptıkları açıklamalarda bu işlerle uğraştıkları izlenimini yaratacak söz ve deyimleri kullanan gerçek kişiler ile tüzel

kişilerin görevlileri bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılırlar.

Birinci fıkraya aykırılık halinde Kurumun, ilgili Cumhuriyet Başsavcılığını muhatap talebi üzerine sulh ceza hâkimince, dava açılması halinde davaya bakan mahkemece işyerlerinin faaliyetleri ve reklamları geçici olarak durdurulur, ilânları toplatılır. Bu tedbirler, hâkim kararı ile kaldırılıncaya kadar devam eder. Bu kararlara karşı itiraz yolu açıktır.

- **Madde 39 - Bilgi Güvenliği Yükümlülüğüne Aykırı Davranılması**

Bu Kanunun 8 inci maddesinin beşinci fıkrası ve 23 üncü maddesi hükümlerine kasten aykırı hareket eden kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişiler, bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılırlar.

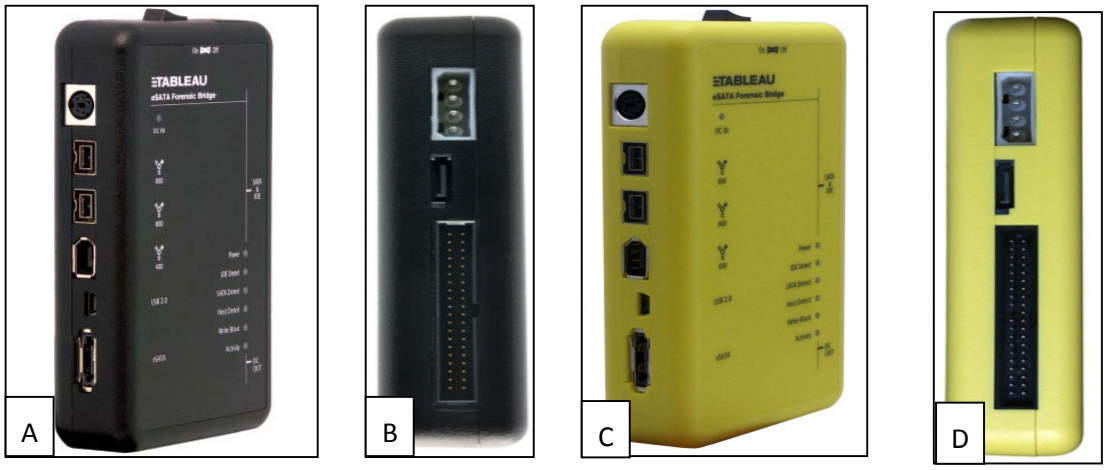
Kartların kullanılması için zorunlu olup gizli kalması gereken kod numarası, kart numarası, şifre ya da kimliği belirleyici başka bir yöntemin dikkatsizlik veya tedbirsizlik veya meslekte yetersizlik veya emir ve kurallara aykırılık nedeniyle açığa çıkmasına neden olan kart çıkaran kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevli ve ilgili mensupları bin güne kadar adlî para cezası ile cezalandırılırlar.

Bu Kanunun 31 inci maddesine aykırı davrananlar hakkında bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası uygulanır.

2.7. Bilişim Suçlarında Delillendirme

Bilişim suçlarında delillendirme, oldukça fazla dikkat gerektiren, hassas bir uzmanlık konusudur. Olay yerinde ilk müdahale dâhil tüm işlemler eğitim almış, konusunda uzman kişilerce yapılmalıdır. Bilişim suçlarıyla mücadele eden birimlerce delillendirmede kullanılan birkaç tane cihaz ve program vardır. Avrupa Birliği'ne üye ülkeler tarafından kullanılan Drag cihazları, bunun bir örneği olmakla birlikte, bazen yetersiz kalmaktadır. Türk Polis Teşkilatı, Amerika Birleşik Devletleri Hava Kuvvetleri ve FBI'ın da kullandığı delilin hash değerlerinin değiştirilmesini önleyerek üzerinde

oynanmasını engelleyen Write Blocker, Imager, Tableu gibi cihazlar, delilin aynen muhafaza edilmesini sağlayarak soruşturma veya mahkeme aşamasında değiştirildiği yönündeki iddiaların asılsızlığını ortaya koymaktadır. Bozulmadan saklanan deliller, EnCase veya FTK (Forensic Toolkit) programlarıyla incelenerek içindeki bilgiler mahkemeye sunulmaktadır[83].



Şekil 10. Delillendirmede kullanılan Tableau cihazı A, C önden; B, D arkadan görünüşü.

A, B Tableau cihazının eski modeli; C, D yeni modeli.

2.8. Emniyet Teşkilatı'nda Bilişim Suçlarıyla Mücadele ile İlgili Gelişme

Ülkemizde Emniyet Teşkilatı bilişim ile 1 Temmuz 1982 tarihinde Bilgi İşlem Daire Başkanlığı'nın kurulmasıyla tanıştı. 1987 yılında ODTÜ danışmanlığında çalışmalarına başlanan polis bilgisayar ağı, 29.07.1998 tarihinde 81 ilde "Bilgi İşlem Şube Müdürlüğü" adı altında faaliyete geçirilmiştir.1997 yılında Bilişim Suçları Bürosu'nun kurulmasının ardından 2001 yılında bu büronun adı "İnternet ve Bilişim Suçları Şube Müdürlüğü" olarak değiştirilmiştir. Ayrıca merkez teşkilatı içinde bir Bilgisayar Suçları ve Bilgi Güvenliği Kurulu ve Üst Kurul oluşturulmuştur. 01.04.1981 tarihinde kurulan Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, 26.06.2000 tarihinde Birleşmiş Milletler ile ortaklaşa kurulan TADOC (Turkish Academy Against Drug and Organised Crime) bünyesinde, 2001 yılında "Bilişim Suçları Araştırma Merkezi" oluşturulmuştur. Başkanlık bünyesinde faaliyetlerine devam eden Bilgi İşlem Büro Amirliği, 20.04.2003 tarihinden itibaren "İleri teknoloji Suçları Bilişim Sistemleri Şube Müdürlüğü" adını almış, 03.01.2006 tarihinde "Bilişim Suçları ve Sistemleri Şube Müdürlüğü" şeklinde yeniden yapılandırılmıştır[84,85,86].

Adana Bilgi İşlem Daire Başkanlığı'na bağlı bilişim sistemleri hizmetleri yönünden 10 Bölge Merkezi'nden biridir. Ancak Bilişim Suçları Büro Amirliği, Asayiş Şube Müdürlüğü Ahlak Büro Amirliği bünyesinde bu birimde görevlendirilen 2 memur ile Ekim 2006 tarihinde, Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü bünyesinde ise 2007 yılının Temmuz ayında faaliyete geçirilmiştir. KOM Şube Müdürlüğü'nde ilk zamanlar tüm işlemler tek kalemde yapılırken 2009'da Adli Bilişim ve Teknik Takip Büro Amirliklerinin de kurulmasıyla delil inceleme, şüphelinin gizlice izlenmesi ve dinlenmesi ile soruşturma işleri ayrı ayrı yapılmaya başlanmıştır. Asayiş Şube Müdürlüğü Bilişim Suçları Büro Amirliği ise Ahlak Büro Amirliği bünyesinde faaliyet göstermekte olup, ayrı büro olarak faaliyet göstermesi planlanmaktadır.

3. GEREÇ VE YÖNTEM

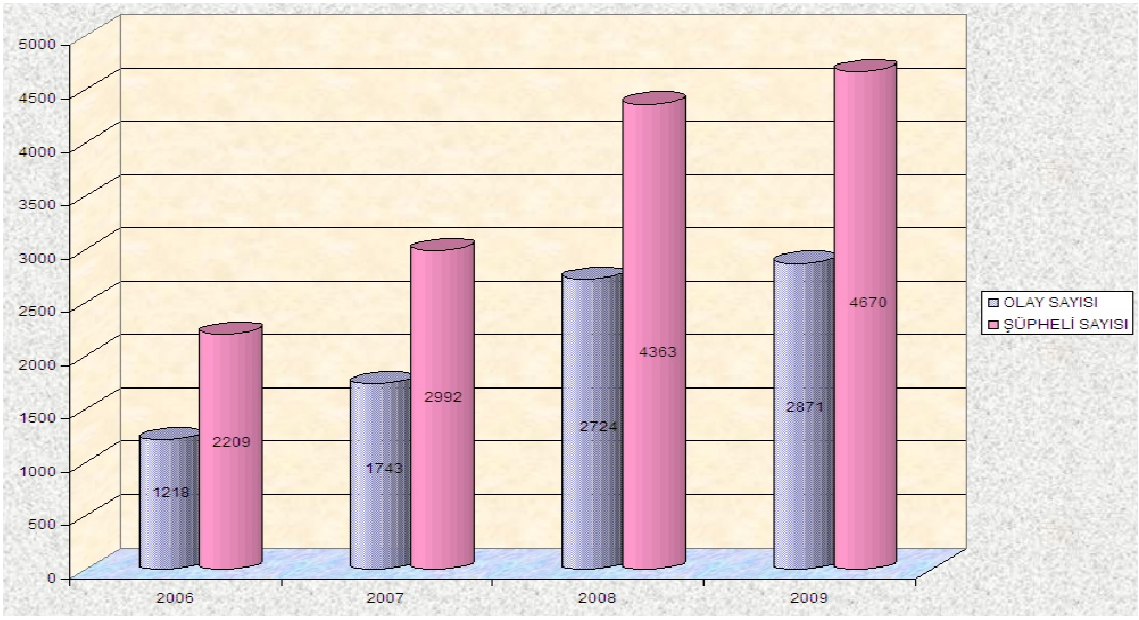
Bu araştırma, 2006-2009 yılları arasında Adana ilinde meydana gelen ve Emniyet Müdürlüğü ile İl Jandarma Komutanlığı kayıtlarına yansıyan bilişim suçlarının türleri, işleniş yöntemleri, toplu suç olup olmadığı, suçun işlendiği yer ile bu suçları işleyenlerin yaş, cinsiyet ve yaşadıkları bölge açısından olayların olduğu yıllara göre incelenmesini kapsayan bir çalışmadır.

Bu araştırmadaki veriler, Adana Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü, Asayiş Şube Müdürlüğü ile Çocuk Şube Müdürlüğü arşiv kayıtlarındaki toplam 648 olay ve 1872 kişi üzerinde inceleme yapılarak elde edilmiştir. Ayrıca 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'na aykırı durumlarla ilgili Güvenlik Şube Müdürlüğü kayıtlarındaki istatistikî bilgilere de yer verilmiştir.

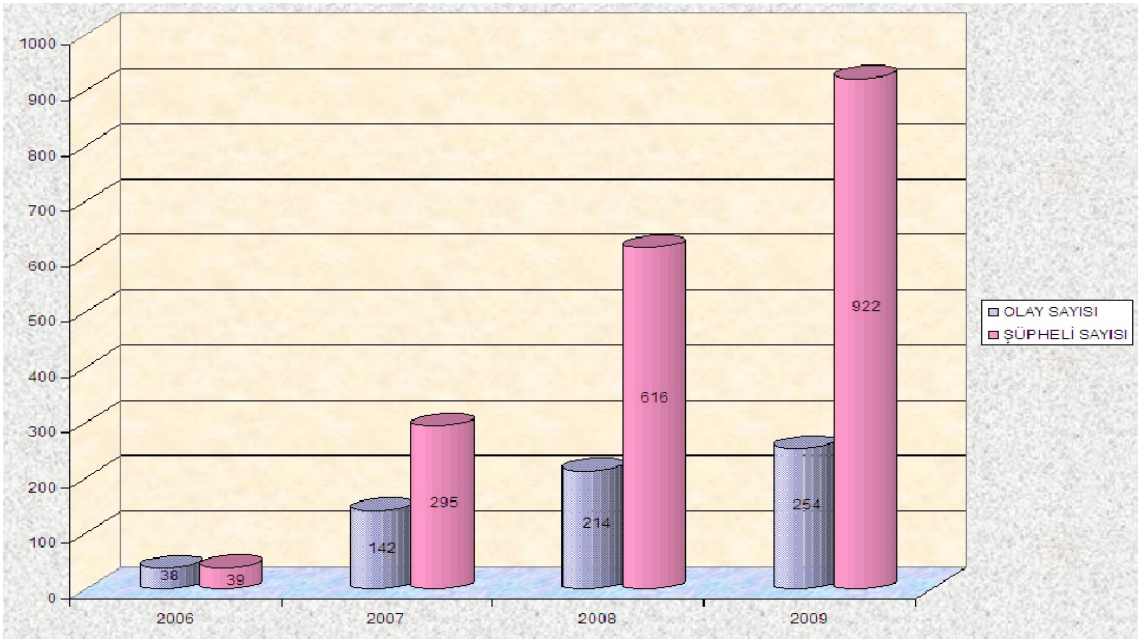
İl Jandarma Komutanlığı arşiv kayıtları da incelenmiş ve bilişim suçlarıyla ilgili olarak yalnızca 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'na aykırı olayların varlığı öğrenilmiş ve çalışmamızda bu bilgilere de yer verilmiştir.

4. BULGULAR

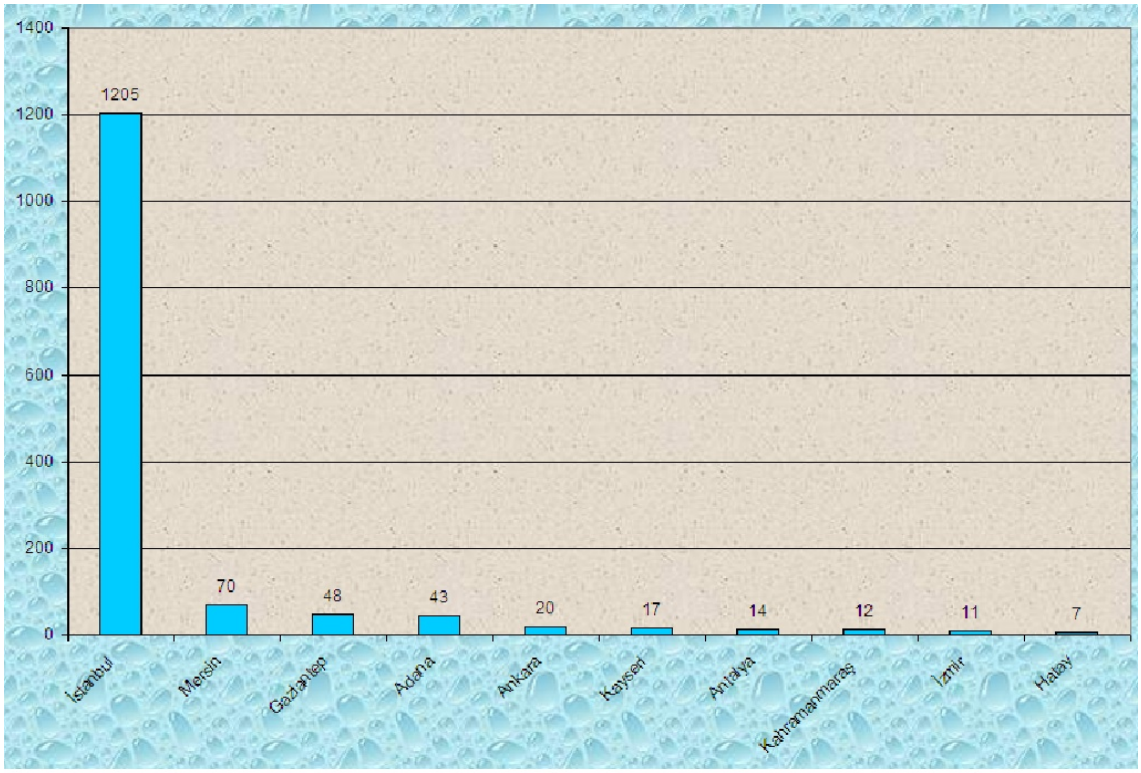
Bu bölümde araştırmadan elde edilen verilerin istatistiksel analiz sonuçları yer almaktadır.



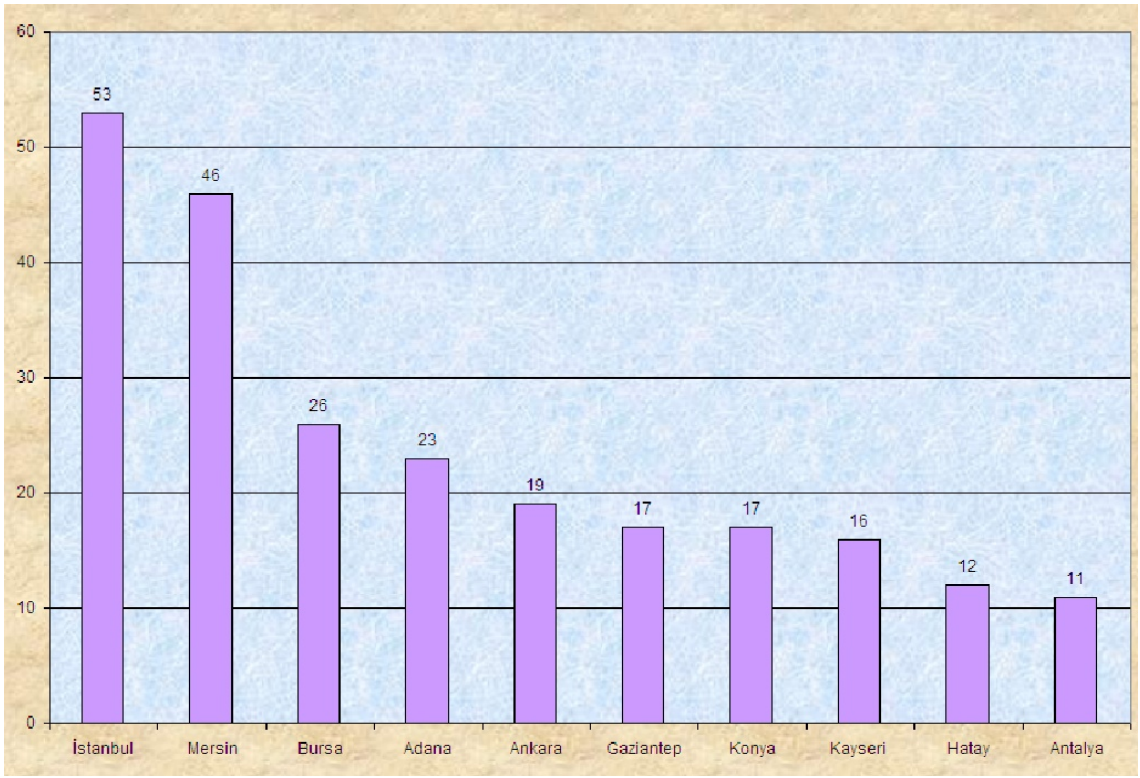
Şekil 11. 2006-2009 yılları içerisinde Türkiye genelinde meydana gelen bilişim suçu olay ve şüpheli sayısının yıllara göre dağılımı[87,88].



Şekil 12. 2006-2009 yılları içerisinde Adana ilinde meydana gelen bilişim suçu olay ve şüpheli sayısının yıllara göre dağılımı.

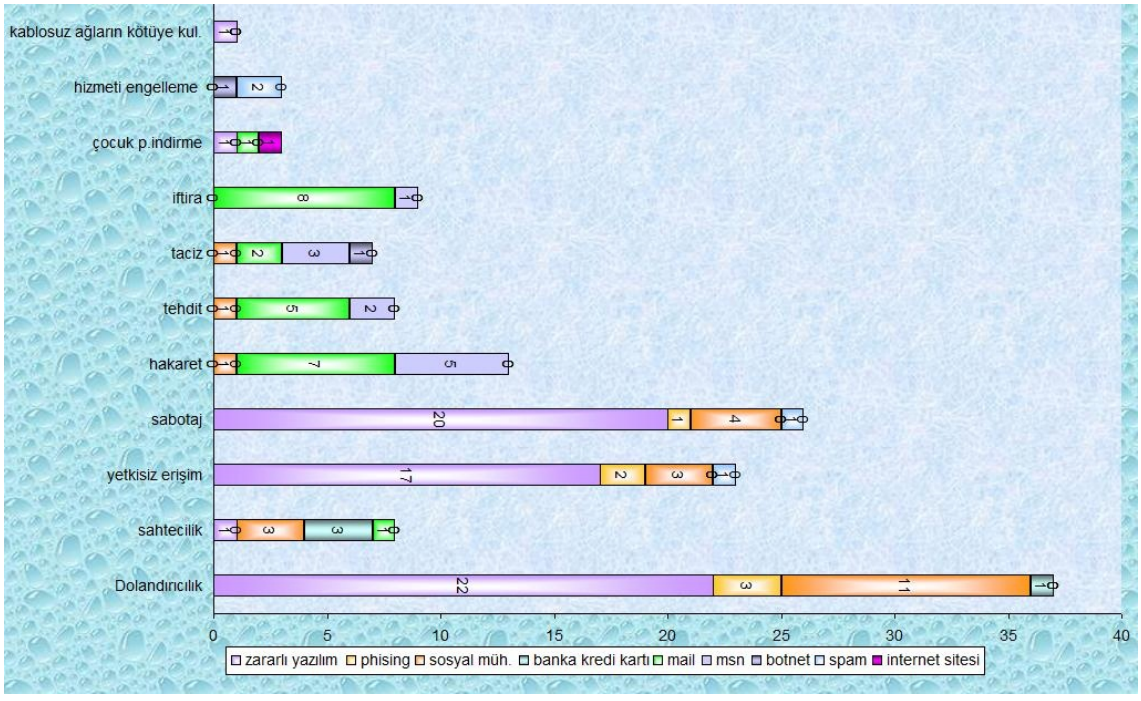


Şekil 13. 2009 yılı Banka ve Kredi Kartı Dolandırıcılığı suçu olay sayılarına göre ilk on il[88].

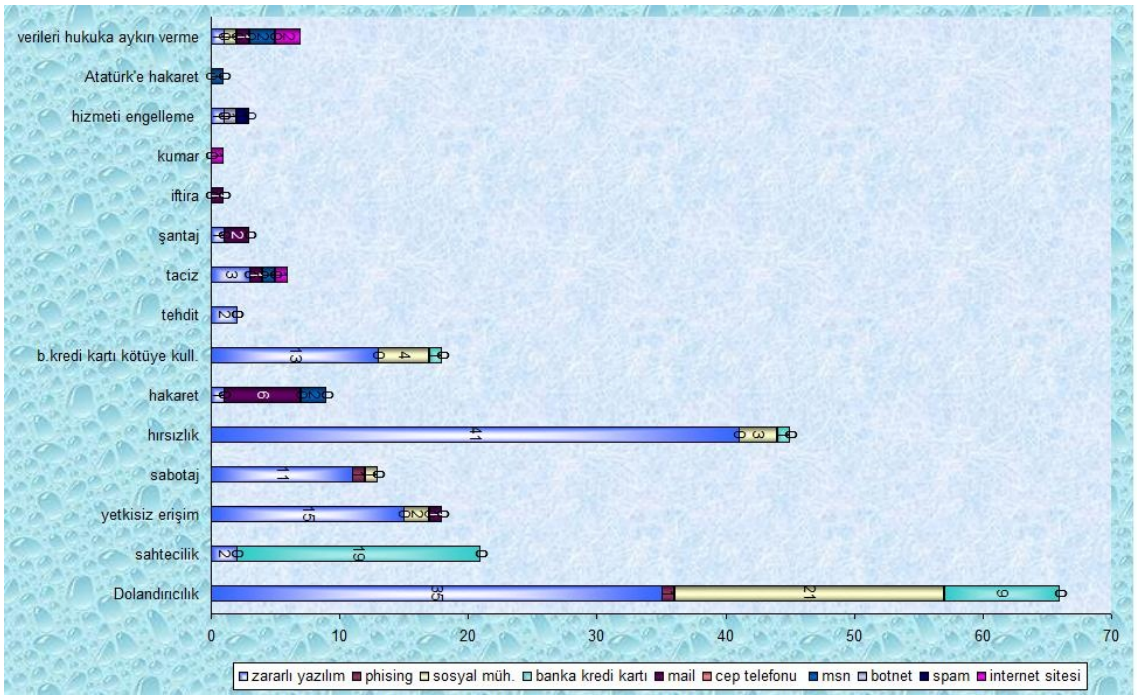


Şekil 14. 2009 yılı Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme, Değiştirme suçları olay sayılarına göre ilk on il[88].

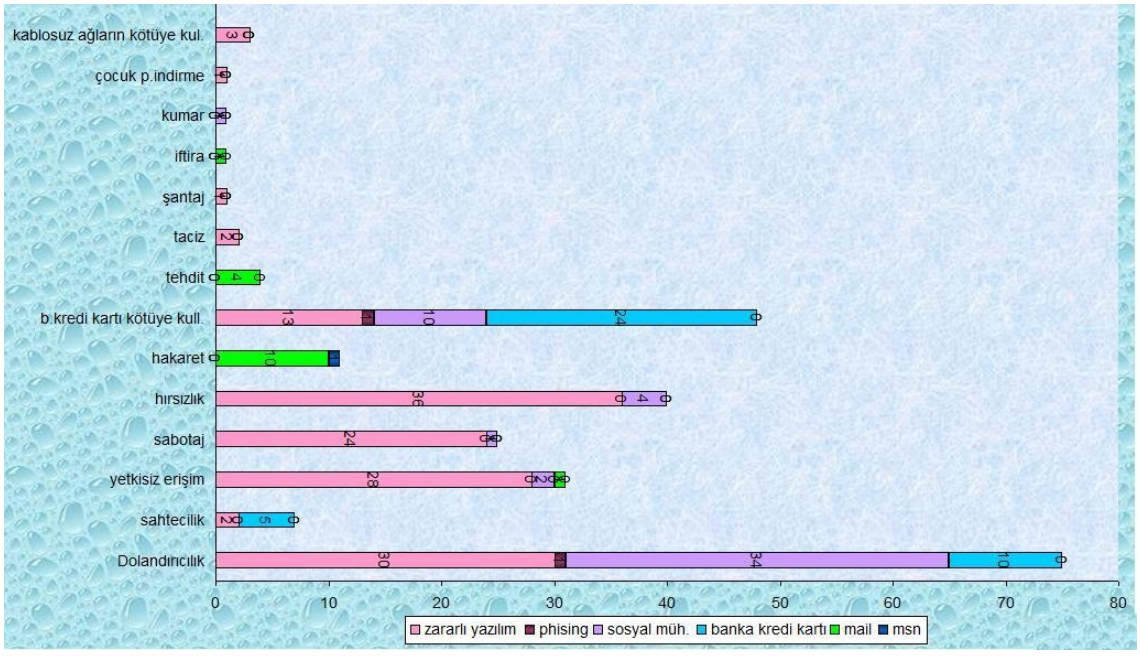
Şekil 15. 2006 yılında Adana ilinde meydana gelen bilişim suçlarının işleniş yöntemlerinin suç türüne göre dağılımı.



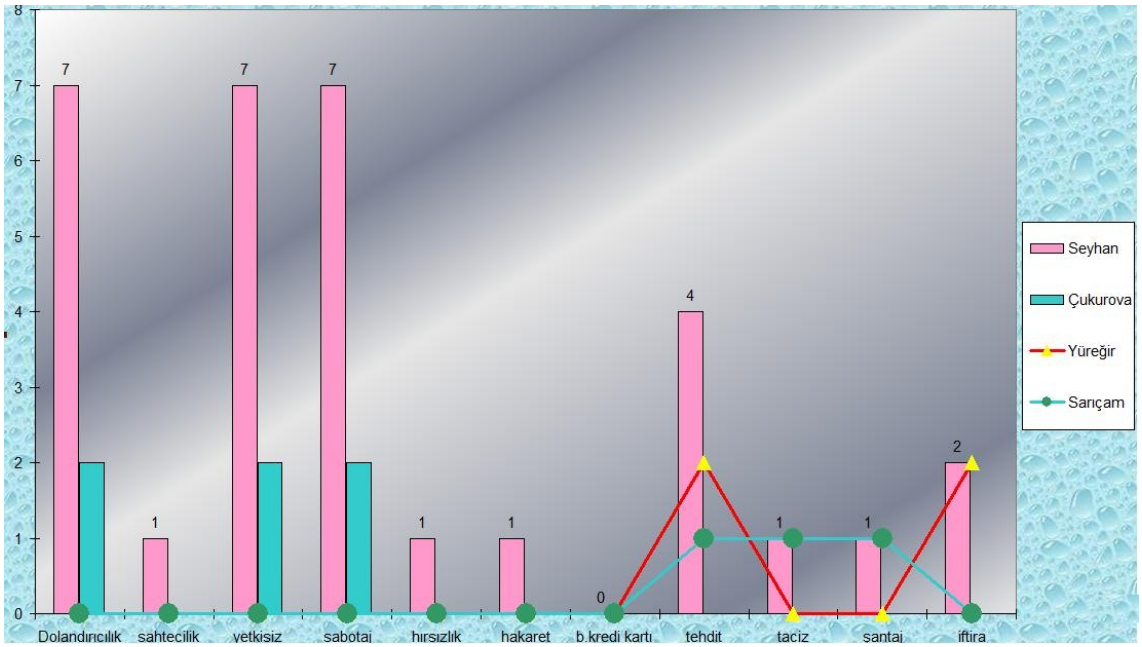
Şekil 16. 2007 yılında Adana ilinde meydana gelen bilişim suçlarının işleniş yöntemlerinin suç türüne göre dağılımı.



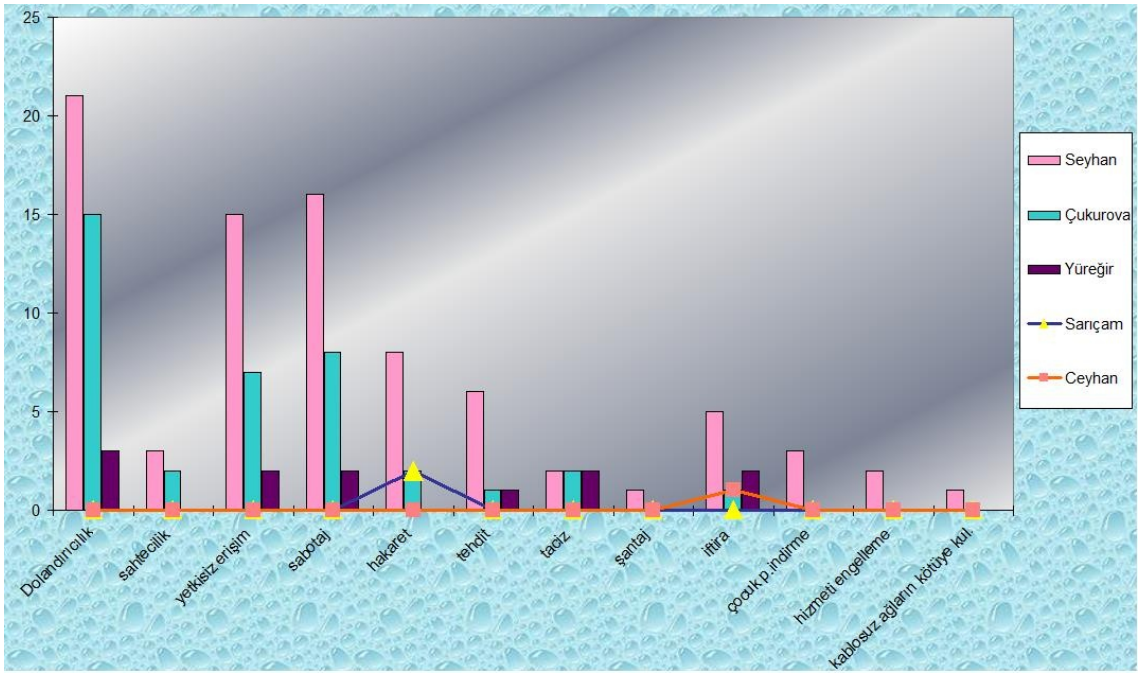
Şekil 17. 2008 yılında Adana ilinde meydana gelen bilişim suçlarının işleniş yöntemlerinin suç türüne göre dağılımı.



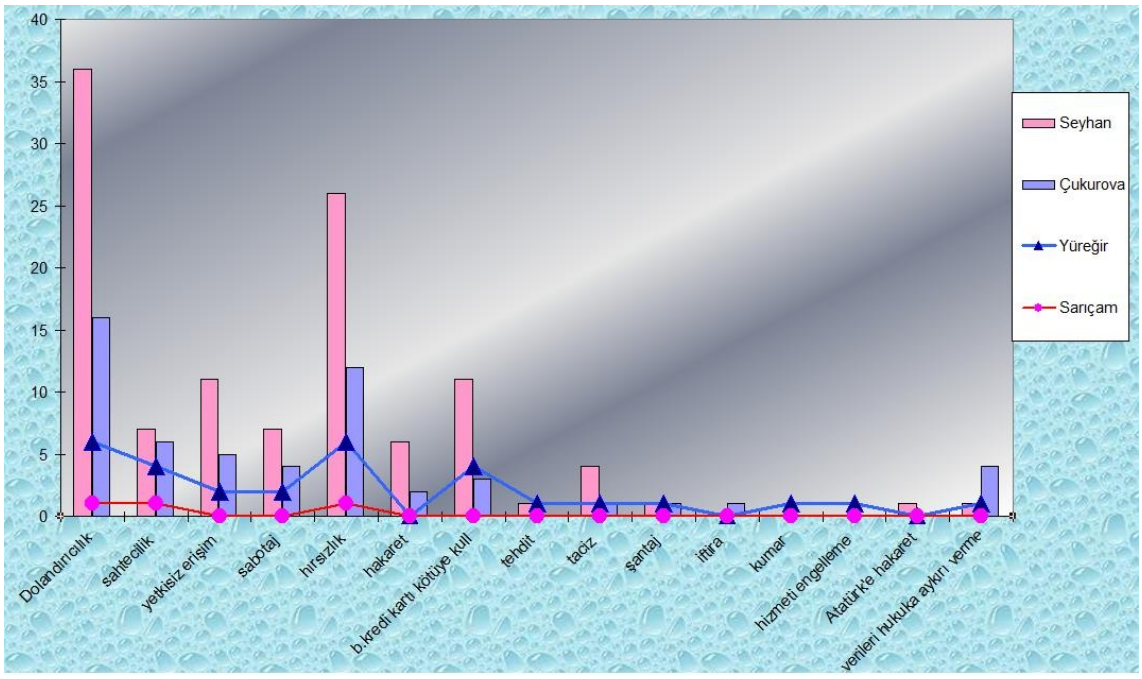
Şekil 18. 2009 yılında Adana ilinde meydana gelen bilişim suçlarının işleniş yöntemlerinin suç türüne göre dağılımı.



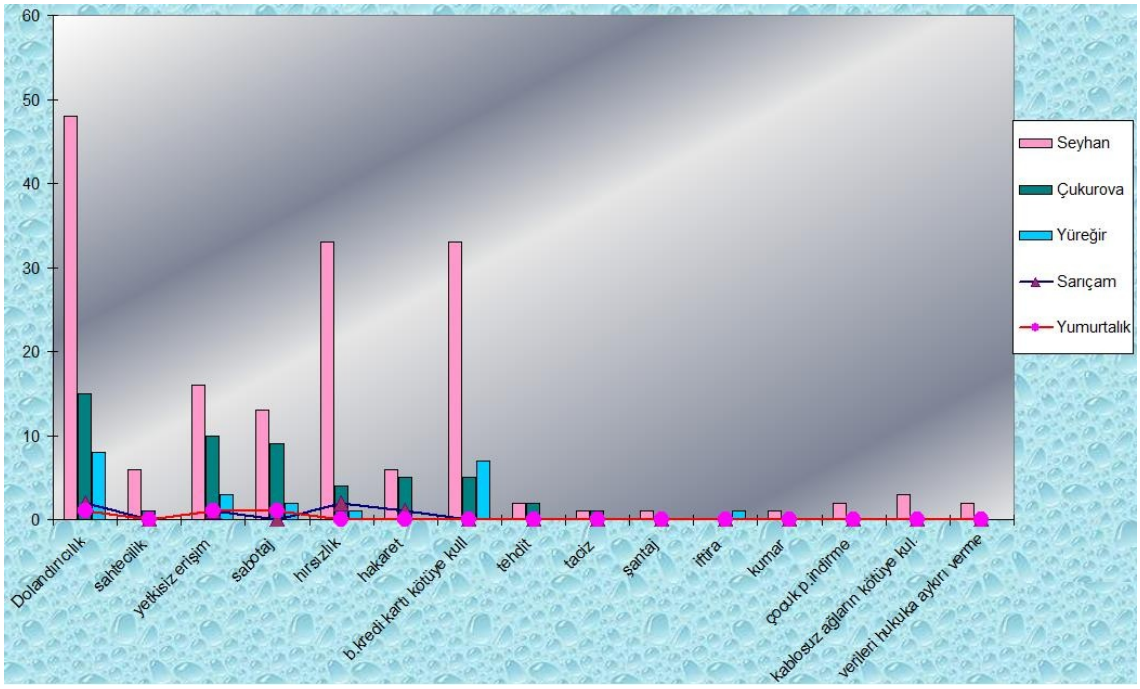
Şekil 19. 2006 yılında Adana ilinde meydana gelen bilişim suç türlerinin suçun işlendiği yere göre dağılımı



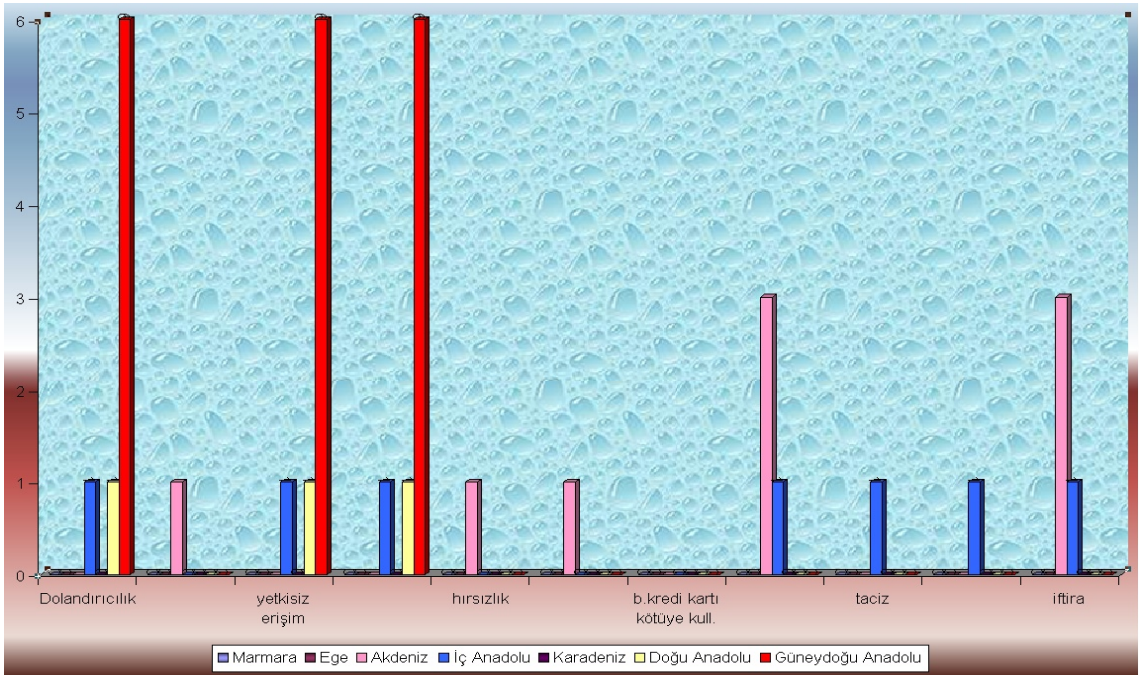
Şekil 20. 2007 yılında Adana ilinde meydana gelen bilişim suç türlerinin suçun işlendiği yere göre dağılımı



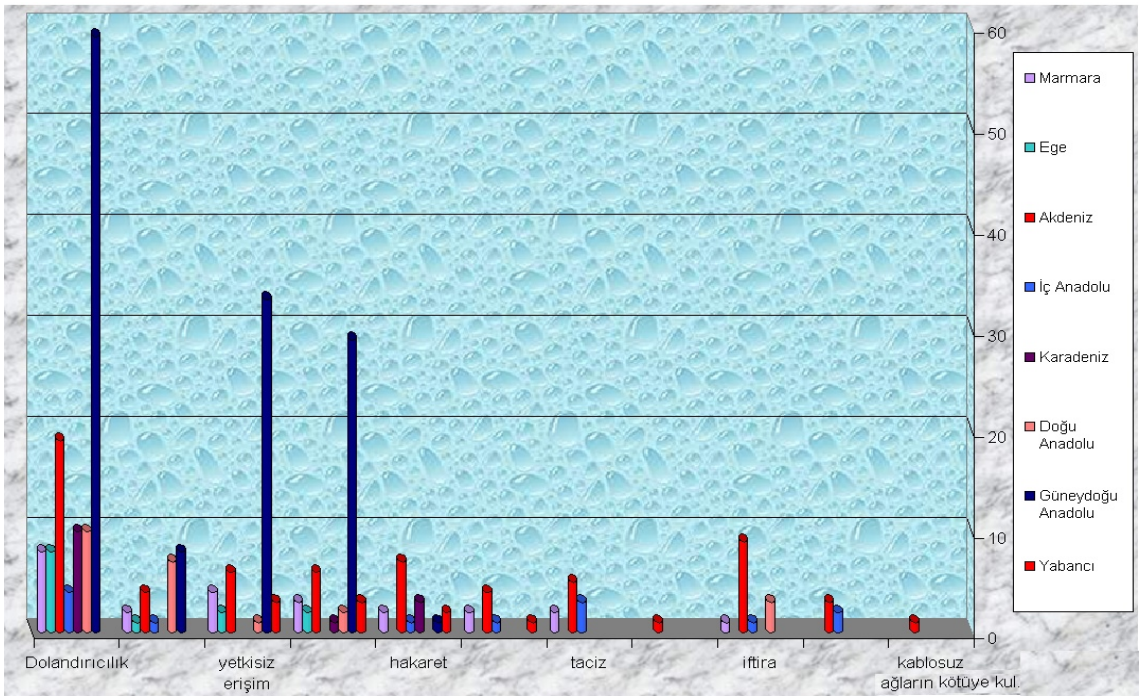
Şekil 21. 2008 yılında Adana ilinde meydana gelen bilişim suç türlerinin suçun işlendiği yere göre dağılımı



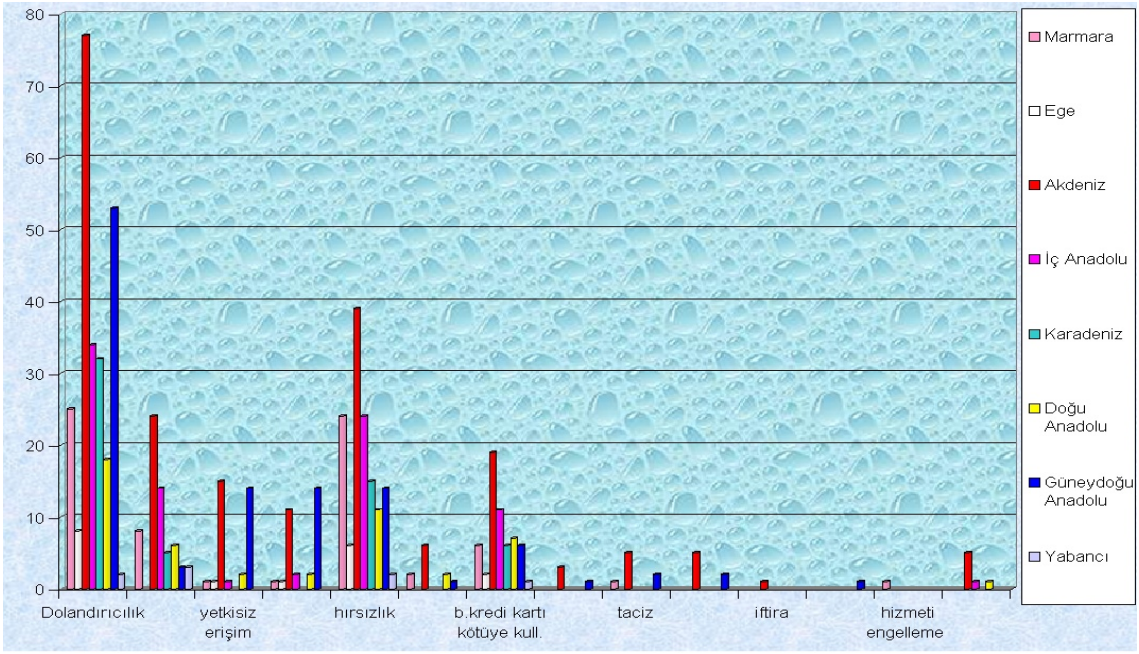
Şekil 22. 2009 yılında Adana ilinde meydana gelen bilişim suç türlerinin suçun işlendiği yere göre dağılımı



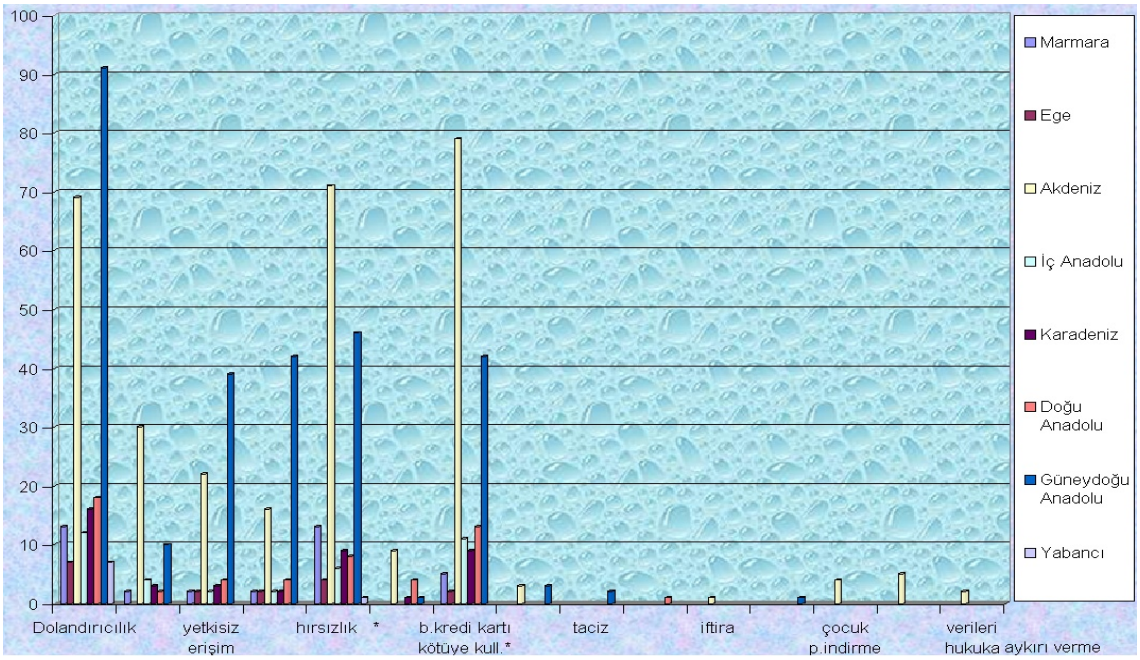
Şekil 23. 2006 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin yaşadıkları bölgelere göre dağılımı



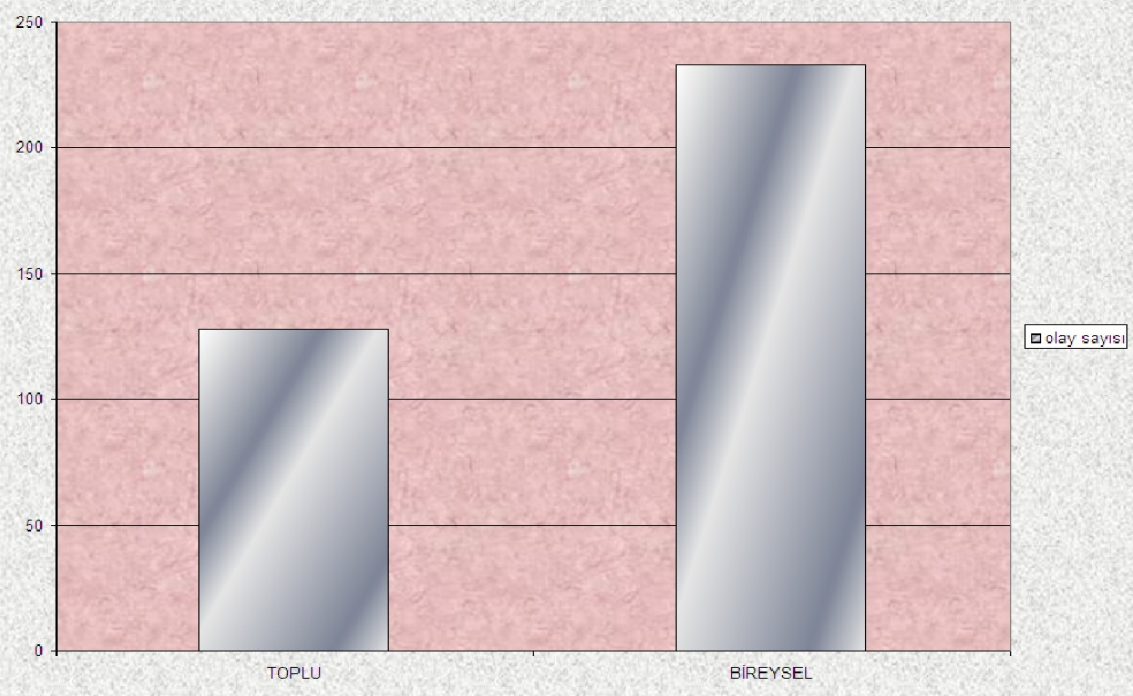
Şekil 24. 2007 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin yaşadıkları bölgelere göre dağılımı



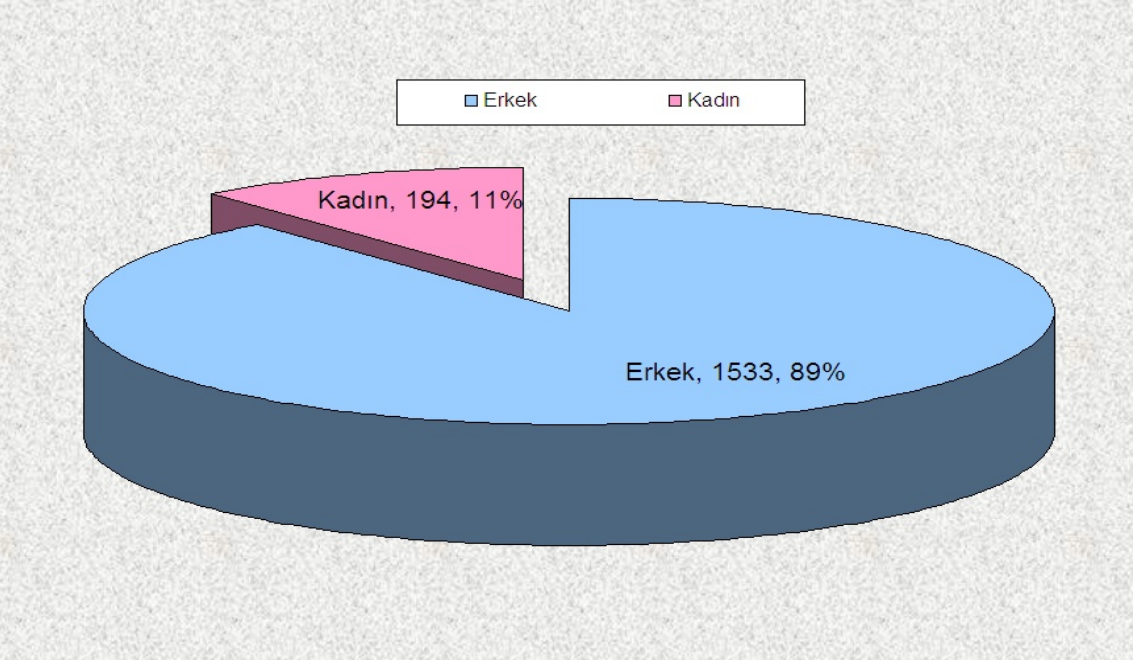
Şekil 25. 2008 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin yaşadıkları bölgelere göre dağılımı



Şekil 26. 2009 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin yaşadıkları bölgelere göre dağılımı



Şekil 27. 2006-2009 yılları içerisinde Adana ilinde meydana gelen bilişim suçlarının işleniş biçimlerine göre dağılımı



Şekil 28. 2006-2009 yıllarında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin cinsiyetlerine göre dağılımı.

YAŞ ARALIKLARI	≤20		21-30		31-40		41-50		51-60		≥61		**39**
TOPLAM	2	0	12	4	18	1	0	0	2	0	0	0	
SUÇ TÜRÜ	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**TOPLAM**
Dolandırıcılık	0	0	3	1	4	0	0	0	0	0	0	0	
Sahtecilik	0	0	0	0	0	0	0	0	1	0	0	0	
Yetkisiz Erişim	0	0	3	1	4	0	0	0	0	0	0	0	
Sabotaj	0	0	3	1	4	0	0	0	0	0	0	0	
Hırsızlık	0	0	1	0	0	0	0	0	0	0	0	0	
Hakaret	0	0	1	0	0	0	0	0	0	0	0	0	
Tehdit	0	0	0	1	4	1	0	0	0	0	0	0	
Taciz	0	0	0	0	1	0	0	0	0	0	0	0	
Şantaj	0	0	0	0	1	0	0	0	0	0	0	0	
İftira	2	0	1	0	0	0	0	0	1	0	0	0	

Çizelge 1. 2006 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin cinsiyet ve yaş aralıklarının suçlara göre dağılımı.

YAŞ ARALIKLARI	≤20		21-30		31-40		41-50		51-60		≥61		
TOPLAM	16	0	131	20	77	7	32	6	3	0	2	1	**295**
SUÇ TÜRÜ	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**TOPLAM**
Dolandırıcılık	7	0	48	6	36	2	14	4	0	0	2	1	
Sahtecilik	3	0	9	1	5	0	0	0	0	0	0	0	
Yetkisiz Erişim	2	0	27	5	10	2	4	1	0	0	0	0	
Sabotaj	2	0	27	5	10	1	4	1	0	0	0	0	
Hakaret	1	0	5	1	3	1	3	0	2	0	0	0	
Tehdit	0	0	3	1	2	0	2	0	0	0	0	0	
Taciz	1	0	5	1	3	0	1	0	0	0	0	0	
Şantaj	0	0	1	0	0	0	0	0	0	0	0	0	
İftira	0	0	4	0	5	1	3	0	1	0	0	0	
Çocuk Pornosu İndirme	0	0	2	0	2	0	1	0	0	0	0	0	
Kablosuz Ağ. Kötüye Kul.	0	0	0	0	1	0	0	0	0	0	0	0	
Kendi İçinde (%) Oranı	6.1	0.0	50.2	58.8	29.5	20.6	12.3	17.6	1.1	0.0	0.8	2.9	
Toplam (%) Oranı	5.4	0.0	44.4	6.8	26.1	2.4	10.8	2.0	1.0	0.0	0.7	0.3	

Çizelge 2. 2007 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin cinsiyet ve yaş aralıklarının suçlara göre dağılımı.

YAŞ ARALIKLARI	≤20		21-30		31-40		41-50		51-60		≥61		
TOPLAM	26	2	205	24	188	15	89	13	34	2	16	2	**616**
SUÇ TÜRÜ	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	
Dolandırıcılık	9	1	90	12	77	5	30	8	8	2	5	2	
Sahtecilik	0	0	14	2	21	2	17	1	4	0	1	0	
Yetkisiz Erişim	4	0	10	0	10	2	1	0	3	0	1	0	
Sabotaj	2	0	12	0	10	2	1	0	3	0	1	0	
Hırsızlık	4	1	43	8	46	3	25	3	9	0	3	0	
Hakaret	1	0	4	0	4	0	2	0	1	0	0	0	
Banka Kredi Kart. Kötü. Kul.	2	0	25	0	20	1	7	1	1	0	3	0	
Tehdit	1	0	1	0	0	0	1	0	1	0	1	0	
Taciz	1	0	1	1	0	0	2	0	2	0	1	0	
Şantaj	1	0	3	0	0	0	2	0	1	0	0	0	
İftira	0	0	1	0	0	0	0	0	0	0	0	0	
Kumar	0	0	1	0	0	0	0	0	0	0	0	0	
Sistemi Engelleme Saldırısı	0	0	1	0	0	0	0	0	0	0	0	0	
Verileri Hukuka Aykırı Olarak Verme	1	0	2	1	0	0	1	0	1	0	0	0	
Kendi İçinde (%) Oranı	4.7	3.4	36.7	41.4	33.7	25.9	15.9	22.4	6.1	3.4	2.9	3.4	
Toplam (%) Oranı	4.2	0.3	33.3	3.9	30.5	2.4	14.4	2.1	5.5	0.3	2.6	0.3	

TOPLAM

Çizelge 3. 2008 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin cinsiyet ve yaş aralıklarının suçlara göre dağılımı.

YAŞ ARALIKLARI	≤20		21-30		31-40		41-50		51-60		≥61		
TOPLAM	40	3	382	15	223	12	115	8	31	2	15	1	**847**
SUÇ TÜRÜ	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	**E**	**K**	
Dolandırıcılık	12	3	136	15	67	12	34	8	9	2	6	1	
Sahtecilik	1	0	23	3	18	2	7	1	2	0	0	0	
Yetkisiz Erişim	3	0	36	4	18	3	9	4	3	1	1	0	
Sabotaj	3	0	35	3	16	3	8	4	1	1	1	0	
Hırsızlık	10	0	65	10	44	8	29	4	9	1	4	1	
Hakaret	0	0	4	2	6	1	2	0	0	0	0	0	
Banka Kredi Kart. Kötü. Kul.	9	0	75	7	48	5	21	2	7	1	3	0	
Tehdit	1	0	0	1	2	1	1	0	0	0	0	0	
Taciz	0	0	2	0	1	1	0	1	0	0	0	0	
Şantaj	0	0	1	0	0	0	0	0	0	6	0	2	
İftira	0	0	1	0	0	0	0	0	0	0	0	0	
Kumar	0	0	0	0	1	0	0	0	0	0	0	0	
Çocuk Pornosu İndirme	0	0	3	0	0	0	1	0	0	0	0	0	
Kablosuz Ağ. Kötüye Kul.	1	0	0	0	2	0	2	0	0	0	0	0	
Verileri Huk. Aykırı Olarak Ver.	0	0	1	0	0	0	1	0	0	0	0	0	
Kendi İçinde (%) Oranı	5.0	2.6	47.4	38.8	27.7	31.0	14.3	20.7	3.8	5.2	1.9	1.7	
Toplam (%) Oranı	4.3	0.3	41.4	4.9	24.2	3.9	12.5	2.6	3.4	0.7	1.6	0.2	

TOPLAM

Çizelge 4. 2009 yılında Adana ilinde meydana gelen bilişim suçlarını işleyenlerin cinsiyet ve yaş aralıklarının suçlara göre dağılımı.

	SİYASİ YAYIN	KORSAN CD	KORSAN DVD	KORSAN KİTAP	PORNO VİDEO KASETİ	PORNO CD	YAKALANAN ŞAHIS SAYISI
2006	694	397,485	0	6,230	89	2,584	292
2007	2,748	387,749	0	7,644	0	1,269	548
2008	4,909	255,016	83,127	4,286	0	1,416	489
2009	8649	153,011	109,493	11,065	0	1,916	395

Çizelge 5. 2006-2009 yılları arasında Adana İl Emniyet Müdürlüğü Güvenlik Şube Müdürlüğü kayıtlarında yer alan 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'na aykırı durumların yıllara göre dağılımı[89].

	KORSAN CD	YAKALANAN ŞAHIS SAYISI
2006	0	0
2007	1282	7
2008	2812	3
2009	0	0

Çizelge 6. 2006-2009 yılları arasında Adana İl Jandarma Komutanlığı kayıtlarında yer alan (bilişim suçlarının) 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'na aykırı durumların yıllara göre dağılımı[90].

5. TARTIŞMA

Gelişen teknolojiyle beraber yedisinden yetmişine toplumun her kesiminin ilgisini çeken ve yaşamımıza nüfuz eden bilgisayarlar, hayata renk katıp işlerimizi kolaylaştırmasıyla birlikte yeni suç türlerinin ortaya çıkması ve gelişmesine de katkıda bulunmuştur.

Sanal ortamda arkadaşlıklar ve alış verişlerin yaygınlaşmasıyla birlikte; bilgisayar sabotajı, telefon dinleme, özel hayatın gizliliğini ihlal, hırsızlık, bilgisayar yazılımlarıyla yapılan belge sahteciliği gibi olayların artması ve bunların toplumsal yaşama zarar vermesiyle oluşan sanal suçlar hayatımıza yakın zamanda girmiş olmakla beraber dünyada ve ülkemizde hızla artan ve büyük zararlar veren bir suç alanı olmuştur.

Bilişim suçları takibi şikâyete bağlı suçlardandır ve çoğu insan maruz kaldığı durumun bir suç teşkil ettiğini dahi bilmemektedir. Bazılarının ise yalnızca önemsemediğinden suçun gerçek boyutlarını gözler önüne sermek oldukça zordur. Para kaybının büyük olmadığı durumlarda veya bankaların suçun oluşmasında sorumlu olarak paranın bir kısmını ödemesi sonucu kişi şikâyette bulunmayınca ve bankaların da itibarını kaybetme korkusu yüzünden bildirimde bulunmaması sonucu suçların pek çoğu açığa çıkmamaktadır.

Bilişim suçlarında olay sayısının yıllara göre dağılımı incelendiğinde; Türkiye genelinde ve Adana'da her yıl bir öncekine oranla artış gözlenmesiyle birlikte, Adana'da 2006-2007 yılları arasındaki farkın büyüklüğü göze çarpmaktadır. Bu suç grubuyla özel olarak ilgilenen birimlerin, Bilişim Suçları Büro Amirliklerinin, Asayiş Şube Müdürlüğü Ahlak Büro Amirliği bünyesinde Ekim 2006 tarihinde, Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü bünyesinde de 2007 yılının Temmuz ayında kurulması nedeniyle kayıtlar bu denli artmıştır.

Adana'da 2006 ve 2009 yılları arasında suç sayısı oranları kıyaslandığında %568,4 oranında artış görünmektedir. Ancak 2006 yılı bilişim suçları açısından Adana ili için tam bir başlangıç sayılamayacağından 2007 ve 2009 yılları suç oranları kıyaslandığında Adana'da % 78,8, Türkiye'de % 64,7 ve Amerika'da % 62,7 oranlarında artış olmuştur[91].

2009 yılı ülkemiz geneli "dolandırıcılık" ve "bilişim sistemlerine girme, sistemi engelleme, bozma, verileri yok etme, değiştirme" suçları olay sayıları incelendiğinde İstanbul birinci, Adana ise dördüncü sırada yer almaktadır. Adana'daki olay ve şüpheli sayılarının artış oranı Türkiye geneliyle benzerlik göstermektedir.

Adana'da 2006 yılında %22'lik oranla yetkisiz erişim ve sabotaj birinci, dolandırıcılık ikinci; 2007-2009 yılları arası ise dolandırıcılık suçu birinci sırada yer alırken Amerika'da 2006-2007 yıllarında dolandırıcılık birinci, 2008-2009 yıllarında ise ülkemiz kanunlarında henüz bilişim suçu olarak dahi bahsedilmeyen "internet üzerinden yapılan alış verişlerde malların teslim edilmemesi veya paranın ödenmemesi" suçu birinci, dolandırıcılık suçu ikinci sırada yer almaktadır[91,92].

90'lı yıllarda banka ve kredi kartı dolandırıcılığı ve sahteciliği ile gündeme gelen İsrail, 2000'li yıllarda da en çok zararlı yazılım kullanan ülke olarak adını duyurmuştur[93,94]. 2006-2009 yılları içerisinde işlenen bilişim suçlarında kullanılan yöntemlerde Amerika'da en çok sosyal mühendislik kullanılırken; Adana'da zararlı yazılım birinci, sosyal mühendislik ikinci sırada yer almaktadır. Bununla birlikte 2008 ve 2009 yıllarında banka ve kredi kartlarının kötüye kullanılması ile işlenen suçların artarak üçüncü sırada yer almasının en büyük nedeni de şüphesiz banka ve kredi kartlarının kullanımının her geçen gün artmasıdır.

Bilişim suçları içinde en çok işlenenin dolandırıcılık olması, bunun da en çok bankalar kullanılarak işlenmesine istinaden; bankaların güvenlik bölümü çalışanları özellikle internet bankacılığında daha güvenli hizmet verme açısından araştırmalar yapmakta ve müşterilerini koruma konusunda gün be gün gelişme göstermektedir. Bunlar phising saldırılarından korunmak için "Güvenlik Resmi" veya "Güvenlik Kodu" uygulamaları, şifrematikler, keylogger programlarına karşı "Keypad yani Mini Klavye" ve sanal Mouse gibi bankanın sabit uygulamaları olabileceği gibi; "IP Kısıtlama", "Kullanım Periyodu Tanımlama" "Para Transferi Kapatma veya Uyarısı" ile "Hesap-Kart Tanımlama" gibi müşterilerin isteğe bağlı gerçekleştirebileceği kişisel uygulamalar olabilmektedir[95,96].

Bankaların bir bilişim suçuyla karşı karşıya kalması durumunda saygınlığını kaybetme korkusuyla paranın bir kısmını karşılama yoluna giderek polise bilgi vermemesi de suçların çözümsüzlüğünde önemli rol oynayan etkenlerden biridir. ATM'den yapılan

kartsız işlemler sonucu ya da kartın sahte bir ikizi oluşturularak çekilen paraların kaybı ile ilgili ATM'ye kayıtlı bir kamera sistemi ile suç önlenemese bile çözümünün kolaylaşabileceği düşünülmektedir. "Mail order" yöntemiyle yapılacak alış verişlerde ise güven vermeyen yerlerde ve sonunda verilen imzalı ödeme emri olmadan işlem yaptırılmaması bu suçtan korunma anlamında önemli bir adım olacaktır.

2006-2009 yılları bilişim suçlarının işlendiği yer açısından değerlendirildiğinde; Seyhan ilçesinin birinci, Çukurova ilçesinin ikinci sırada yer aldığını görmekteyiz. Diğer ilçelerin suç oranları bu denli azken özellikle Seyhan ilçesinin büyük farkla birinci olmasının nedeni ise bilişim suçları içinde en çok işlenenin dolandırıcılık suçu olması ve bankaların da en çok Seyhan'da yer almasıdır.

Bilişim suçlarıyla ilgili Türkiye sıralamasında dördüncü sırada yer alan Adana ili büyükşehir olmasının da etkisiyle her kesim insanı ve dolayısıyla suç türünü birlikte barındırır. 2006-2009 yılları içerisinde Adana ilinde işlenen bilişim suçlarını işleyenlerin yaşadıkları bölgelere göre dağılımı incelendiğinde; 2006-2007 yıllarında Güneydoğu Anadolu, 2008-2009 yıllarında ise Akdeniz Bölgesi en çok bilişim suçu işlenen bölgeler olarak kayıtlara geçmiştir. 2006-2007 yılları içerisinde Güneydoğu Anadolu'nun birinci sırada yer almasının nedeni; Adana'da yaşayan insanların çoğunluğunun göçle gelmesi ve en çok göçü Güneydoğu'dan almasıdır. Bununla beraber, 2007 ve 2008 yılları içerisinde KOM Daire Başkanlığı tarafından Şanlıurfa ve Suruç ilçesi merkezli yapılan "Virüs" ve "Kontör Yolla" adlı operasyonlarla pek çoğunun yakalanması da ikinci önemli nedendir[87].

2006-2009 yılları içerisinde Adana ilinde meydana gelen bilişim suçlarının çoğunluğunun toplu suç oluşturmadığı, bireysel olarak işlendiği gözlemlenmiştir.

Çalışmanın arşiv kayıtları ile sınırlı olması, bilişim suçlarının şehirler hatta ülkeler arası işlenmesi sebebiyle bilişim suçunu işleyenlerin eğitim ve mesleki durumları vs, tüm verilere ulaşılamamış olması çalışmada elde edilen verilerin sınırlı kalmasına yol açmıştır.

2006-2009 yılları içerisinde meydana gelen bilişim suçlarını işleyenlerin cinsiyetlerine göre dağılımı incelendiğinde; Adana'da bilişim suçunu işleyenlerin % 89'u, Amerika'da yapılan bir çalışmada ise %76,6'sının erkek olduğu saptanmıştır. Dolayısıyla bu

alanda Amerika'daki kadın suçluların yoğunluğu Adana'dan fazla olmakla birlikte, erkeklerin bilişim suçları dağılımında çok daha fazla suç işlediği görülmektedir[91].

2006-2009 yılları içerisinde Adana ilinde bilişim suçu işleyenlerin yaş dağılımları incelendiğinde; sayıları erkeklere oranla ne kadar az olsa da bilişim suçu içerisinde de kendine yer edinen kadınların en çok 21-30 yaş aralığında oldukları göze çarpmaktadır. Erkeklerden 2006 yılında suç işleyenlerin çoğu 31-40 yaş aralığında iken 2007, 2008, 2009 yıllarında suç işleyenlerde 21-30 yaş aralığında olanlar çoğunluktadır. Bilişim suçlarının çoğu yetişkinlerce işlense de 2007'de 16 yaşında bir, 2008'de 16 yaşında iki ve 2009'da 17 yaşında bir kişi olmak üzere toplam dört tane çocuk suçlu bulunmaktadır.

Teknolojiye olan merakın artmasına paralel bilgisayar kullanımının artması, internete erişmenin daha kolay ve hızlı hale gelmesi, bilişim suçu işlemek için gerekli olan bilgilerin internet ortamında rahatlıkla bulunabilmesi bu ortamı suç işlemek için en uygun ortam haline getirmiştir.

Bilişim suçlarının belirlenmesi ve çözümü oldukça zordur. İnternet gibi kalabalık ve bilinmeyen bir ortamda kişiler lakap kullanarak gerçek kimliklerini kolayca gizleyebilmektedirler. Ayrıca bu suç, şehirler hatta uluslar arası işlenebilen bir suçtur. Klasik anlamdaki bir hırsızlık olayında şüpheli, mağdur ve çalınan değer hep bir arada olurken ve olay yeri tekken; bilişim yoluyla hırsızlık olayında şüpheli, mağdur ve kaybedilen değer çok farklı farklı yerlerde olabileceğinden suç yerini belirlemek oldukça güçtür. Kurumlar arası irtibatsızlık da bir diğer sorundur. Bilişim suçunda zaman çok önemlidir ve kurumların suçu bildirme ile suç sonrası yapılan yazışmalara geç cevap vermesi de suçun çözümünü zorlaştırıcı etkenlerdendir. Bununla birlikte Facebook ve Yahoo gibi yabancı kaynaklı siteler yalnızca kendi ülkelerinin mahkeme kararlarını ve kolluk güçlerini tanıdığından bu sitelerle ilgili bir sıkıntı olması durumunda suçlar çözümsüz kalmaktadır. Yabancı kaynaklı olsa da Türkiye temsilciliği bulunan Hotmail gibi sitelerle fazla sorun yaşanmadığından uluslar arası ilişkileri geliştirmek bu sorunun çözümü için yeterli olacaktır.

Avrupa Birliği üye ülkeleri tarafından 12 Nisan 2002'de sunulan ve 2005'te Konsey tarafından kabul edilen önerideki üç madde AB'ye üye olma yolunda yaptığı çalışmalarda ülkemiz tarafından da benimsenmiş ve yeni Türk Ceza Kanunu'nda yapılan değişikliklerde örnek alınmıştır. Bunlar: "(madde 2) Bilişim sistemlerine illegal erişim",

"(madde 3) Bilişim sistemlerine müdahale" ve "(madde 4) İllegal şekilde bilgiye müdahale veya engelleme"dir[97].

Mayıs 2007'de ise AB Komisyonu "Siber Suçlarla Mücadelede Genel Önlemler" adı altında bir toplantı yaptı. Avrupa ülkelerinde giderek artmakta olan siber suçlar; Estonya'da sistemlere müdahale, İspanya'da kimlik hırsızlığı, Avusturya, Almanya, İtalya ve İngiltere'de çocuk pornosu olmakla beraber acil önlemlerin alınması gerektiği tartışıldı. Buna göre, AB Yasası'nın "Halkı terör için tahrik etmek", "Terörist faaliyetler için insan temin etmek" ve "Terörist eğitimi" adı altında üç yeni suç içereceği ve suçla mücadelede işbirliği yapılacağı kararlaştırıldı[97].

Bilişim suçları; diğer suçlara göre bilgi ve yöntemlerin çok hızlı geliştiği ve değiştiği suçlardır. Bu nedenle; bilimsel gelişme, yenilik ve uygulamaya yansımalarının yakın olarak takip edilmesi büyük önem taşımaktadır. Diğer ülkelerde bilişim suçlarıyla hukuksal anlamda mücadelenin 70'li yıllarda başlayıp 90'lı yılların sonunda çok yol kat ettiğini göz önünde bulundurursak, ülkemizdeki mücadelenin 1997 yılında başlaması ve 01.04.2005 tarihinde yürürlüğe giren Türk Ceza Kanunu'nun hukuki anlamdaki eksiklikleriyle de birlikte hem çok gecikmiş hem de yetersiz olduğu görülmektedir.

Suçla mücadele alanında uzman personel yetiştirmek en önemli faktörlerden biridir. Dolayısıyla bilişim suçları büro amirliklerini bünyesinde barındıran birimler, bahse konu bürolarda çalışacak personelin eğitimini de üstlenmek zorundadır. Buna göre; Asayiş ve KOM Daire Başkanlıkları tarafından yılda 2-3 kez olmak üzere temel branş kursu verilmesinin yanı sıra, yılın belli dönemlerinde FBI ve diğer yabancı devlet kurumlarıyla birlikte hazırlanan yeni suç türleri ve yöntemlerinin öğretilmesi ile delil inceleme aletlerinin tanıtımı ve kullanımı gibi konularda da eğitim programları düzenlenmektedir.

Amerika'da 2000 yılının Haziran ayında National White Collar Crime ve FBI'nın ortak çalışması olarak kurulan Internet Crime Complaint Center (IC3) "İnternet Suçları Şikayet Merkezi"nde internet üzerinden işlenen suçlarla ilgili federal, eyalet, yerel veya uluslar arası güvenlik güçlerine yansıyan olaylar toplanarak, raporların sonucu ortaya çıkan istatistiki bilgilere göre suçların işlenme şekilleri ve yoğunlukları ortaya koyulmaktadır[91].

Kanunları, internet suçlarını adlandırmada yaşanan güçlüklere karşı geliştirmek amacıyla tasarlanmış ve Avrupa Birliği çatısı altında kurulması planlanan Cybercrime

Task Force biriminde de yer alan, internet suçlarıyla mücadele eden federal, eyalet, yerel veya uluslar arası kanun koyucu ve düzenleyici organlara yol göstermektedir[91].

14-15 Haziran 2010'da ise Avrupa Birliği üye ülkelerin temsilcilerinin katılımıyla yapılan bir toplantıya göre, 2010-2014 yıllarını kapsayan çalışmalar sonucu Avrupa Birliği Siber Suç Hizmet Gücü (European Union Cybercrime Task Force) adı altında AB'ye üye ülkeler arası işbirliği, bilişim suçu olayları, özel kurumlarla işbirliği, yeni kanunlar gibi çalışmaların hayata geçirileceği bir organın kurulması planlanmaktadır[98].

Türkiye'de ise bilişim suçları ile özel olarak ilgilenen birimlerin tek çatı altında bulunmaması, ayrı bürolara dağılması suçla mücadelede aksaklıklara yol açmaktadır. Terörle ilgili bir bilişim suçu olması durumunda Terörle Mücadele Şube Müdürlüğü'nün, aynı suçlu grubun banka dolandırıcılığı yapması durumunda Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü'nün birbirinden bağımsız, ayrı ayrı soruşturması olayın bütünüyle görünemeyip suçluların yakalanmasını ve işledikleri suçların aydınlatılmasını zorlaştırmaktadır. Her birimde meydana gelen bilişim suçu olaylarının ortak bir havuza aktarılmasının bu tür suçlarla mücadelede daha etkin rol oynayacağı düşünülmektedir.

Suçların hızlı ve doğru şekilde aydınlatılması için kurumlar arası işbirliği oldukça önemlidir. Emniyet, Telekom, Microsoft, Bankalar arası Kart Merkezi, bankalar ya da suça karışan herhangi bir internet sitesi ve diğer kurumlar ile yapılan yazışmaların daha kısa sürede cevaplanması çözümde büyük bir adım olacaktır.

Her suçun aydınlatılmasında zaman önemlidir. Ancak söz konusu bilişim suçu ise zaman en önemli şey denilebilir. Birimlerin farklı olması, mağdurun doğru birime ulaşmasına kadar geçen süre ile yaşanan zaman kaybı hem soruşturmanın geç başlamasına hem de kişinin ikinci kez mağdur olmasına yol açmaktadır.

Delil, bir suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte iz, eser ve emare olabilecek her türlü bilgidir. Delillendirme süreci, bir suçun aydınlatılmasını sağlayacak suçluların açığa çıkarılması ve yargılanması için en önemli aşamadır. Bilişim suçları kapsamında ise fiziksel delillerden ziyade, dijital deliller bulunmaktadır. Bu tür deliller, elektronik kayıtlar olduğundan üzerinde kolayca değişiklik yapılabileceği iddiaları göz önünde bulundurulmalı ve delilin değerinin azalması ya da hukuki geçerliliğini kaybetmesini önleyici tedbirler alınmalıdır. Delillerin doğru şekilde muhafaza

edilmemesi, suç ve suçlu yaratmaya veya bu yönde iddialara sebep olabileceğinden; dijital delillerin toplanması, incelenmesi ve yargı mercilerine iletilmesi aşamalarında uzman kişilerin çalışması ve özel cihazların kullanılması büyük önem arz etmektedir. Ayrıca Ceza Muhakemesi Kanunu'nun 134. maddesinde belirtildiği üzere bilgisayar ve türevi aletlerde arama, elkoyma, inceleme ve kopyalama işlemleri yalnızca hâkim kararı ile yapılabilmektedir. İnceleme işlemi hiçbir zaman asıl delil üzerinde yapılmamalı, daima inceleme yapılacak olan araç ve gereçlerdeki bilgiler yedeklenmeli ve bu kopyalar üzerinde çalışma yapılmalıdır. Şüpheli isterse çıkarılan kopyadan bir suret kendisine veya vekiline verilebilmektedir. Kopya çıkarma işlemi mümkün olduğunca el koymaksızın yapılmalıdır. Bilgisayarlara el koyma işlemi, ancak şifrenin çözülememesinden dolayı veya gizlenmiş bilgilere ulaşılamaması durumunda yapılabilmektedir ve gerekli kopyalar alındığında cihazlar gecikmeksizin iade edilmektedir.

Kişilerin bilişim suçundan korunması konusunda daha bilinçli kullanıcılar haline gelmesi oldukça önemlidir. Tanınmayan kişilerden gelen ya da tanıdığınız kişilerden beklenmeyen mesajlar olduğunda açmayarak; bağlanılacak internet sitesinin adresini adres çubuğuna yazarak; internet adresi olarak sayısal veriler içeren adresler ile karşılaşılması durumunda kontrol ederek; banka ve kredi kartı numaraları, şifreleri ve diğer kimlik bilgilerini internet üzerinden vermeyerek; daima lisanslı, orijinal yazılımlar kullanarak ve güncellemeye açarak; yalnızca virüs koruma programlarıyla yetinmeden casus yazılımlar için de ayrıca önleme programı ve firewall kullanarak alınacak birkaç şahsi önlem ile bilişim suçlarından büyük ölçüde korunmak mümkündür.

6. SONUÇ VE ÖNERİLER

1. Bu çalışma bilişim suçlarını önlemeye yönelik neler yapılabileceğinin araştırılması amacıyla yapılmıştır.

2. Adana Emniyet Müdürlüğü arşiv kayıtlarındaki toplam 648 olay ve 1872 kişi üzerinde inceleme yapılmıştır.

3. Bilişim suçlarındaki olay ve şüpheli sayılarındaki artış yönünden Adana'nın Türkiye geneli ile benzerlik göstermekle beraber, Adana'nın bilişim suçu işlenen ilk on il sıralamasında dördüncü sırada yer aldığı ortaya çıkmıştır.

4. Adana ilinde en çok işlenen bilişim suçunun dolandırıcılık olduğu belirlenmiştir.

5. Adana ili bilişim suçu işlemede kullanılan yöntemler açısından İsrail ile benzerlik göstermekte ve en çok zararlı yazılım kullanmakta iken, Amerika'da suçlar daha çok sosyal mühendislik yöntemiyle işlenmektedir.

6. Dolandırıcılık suçunun daha çok internet bankacılığı kullanılarak işlenmesi sebebiyle, bankalar müşterilerini korumak amacıyla pek çok yeni güvenlik önlemi almışlar, yaptıkları uygulamalar bilişim suçlarının azalmasında etkili olmuştur.

7. Bilişim suçlarının şehirler hatta uluslar arası işlenebilmesi ve Adana ilinin bir büyükşehir olması sebebiyle de suçluların yakalanması konusunda şehirlerarası iletişim ve uluslararası ilişkilerin geliştirilmesi suçun çözümü yönünden çok önemlidir.

8. Adana'da işlenen bilişim suçlarının çoğu toplu suç oluşturmamakta, bireysel olarak işlenmektedir.

9. Adana'da suç işleyen şüphelilerden 1533 (%89)'ü erkek, 194 (%11)'ü kadın olup, 21-30 yaş aralığında olanlar çoğunluktadır.

10. Bilişim suçlarının çoğu yetişkinlerce işlenmekle beraber, dört tane de çocuk suçlu bulunmaktadır.

11. Teknolojik ilerlemeler hayatı kolaylaştırdığı kadar suçlara da katkı sağlamakta olduğundan gelişmeler iyi takip edilmelidir.

12. Bilişim suçunda zaman çok önemli olduğundan kurumlar arası iletişim ve işbirliği en iyi şekilde sağlanmalı, yazışmalar ve haberleşmede zaman kaybı ortadan kaldırılmalıdır.

13. Türkiye temsilciliği bulunmayan yabancı kaynaklı sitelerle ilgili bir sıkıntı olması durumunda suçlar çözümsüz kaldığından uluslar arası ilişkiler geliştirilmelidir.

14. Suçların çözümünde hukuki gelişmelerin öneminin büyüklüğü göz önünde bulundurulmalı ve hukuksal anlamda gelişmelere de dikkat edilmelidir.

15. Suçla mücadele alanında uzman personelin katkısının artması açısından eğitime büyük önem verilmelidir.

16. Bilişim suçları ile özel olarak ilgilenen birimlerin tek çatı altında toplanmasının bu tür suçlarla mücadelede daha etkin rol oynayacağı kanısındayım.

17. Dijital delillerin hassaslığı göz önünde bulundurulmalı, delilin değerinin azalması ya da hukuki geçerliliğini kaybetmesini önleyici tedbirler alınmalıdır.

18. Bilişim suçlarını önleme adına en etkili çözüm kullanıcıların kendilerini korumasıdır. Bu sebeple medya, internet gibi etkenler de kullanılarak kullanıcılar bilinçlendirilmelidir.

7. KAYNAKLAR

1. Emniyet Genel Müdürlüğü Suç İstatistikleri
2. **Uzunay Y,** Dijital Delil Araştırma Süreci, http://caginpolisi.com.tr/50/14-15-16-17-18htm Erişim: 02.11.2009
3. http://web.ego.gov.tr/inc/newsread.asp?ID=247 Erişim: 28.01.2010
4. **Ersoy Y**, Genel *hukuki koruma çerçevesinde bilişim suçları, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* **1994**, 49:151.
5. **Tavukçuoğlu C**, Bilişim Terimleri Sözlüğü, Asil Yayıncılık, **2004**, s:56.
6. **Başoğlu K B**, Teknolojiye Boyun Eğmeyin, Bilişim Suçlarına Genel Bakış 1. Sempozyum, Ankara, **Ocak 2008.**
7. http://bulentozer.av.tr/hukuk/bilisim-hukuku/bilisim-sucları-turleri.html Erişim: 18.02.2010
8. http://www.uludagforum.com/hukuk-fakultesi/16743-bilisim-suclari.html Erişim:02.12.2009
9. www.kemalsener.av.tr/bilisim/bilisim-suclarinin-turleri.html Erişim:13.02.2010
10. **Kunz M, Wilson P**, Computer Crime and Computer Fraud, **2004,**
    http://www.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf Erişim: 09.05.2010
11. **Tulum İ**, Bilişim Suçları ile Mücadele, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Isparta, **2006**.
12. Cybercrimes: Infrastructure Threats from Cyberterrorist," Cyberspace Lawyer, 4 No 2. Cyberspae Law 23. Den aktaran Mehmet Özcan
13. **Özcan M**, Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu, http://www.bayar.edu.tr/bilisim/dokuman/siberteror.pdf Erişim: 14.11.2009
14. http://csciwww.etsu.edu/gotterbarn/stdntppr/Cyber Terrorism Erişim: 24.08.2009
15. http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177438-dialer-mantik-bombasi-nedir.html Erişim: 10.04.2010
16. http://www.microsoft.com/turkiye/athome/security/viruses/intro_viruses_what.mspx Erişim: 05.01.2010
17. **Bahtiyar Z**, Virüsler ve Güvenlik, Pusula Yayınları, **2009,** s:2.
18. http://www.cknow.com/cms/vtutor/virus-history-summary.html, Virus History Erişim: 26.10.2009
19. http://yunus.hacettepe.edu.tr/~bbm841/odev5.htm Erişim: 12,02,2010

20. http://tr.wikipedia.org/wiki/Bilgisayar_virusleri Erişim: 01.03.2010

21. http://www.hurriyet.com.tr/teknoloji/14593872.asp?gid=234 Erişim: 04.04.2010

22. http://projects.webappsec.org/Cross-Site-Scripting
WASC Threat Classification-Attack/WASC-8 Cross Site Scripting Erişim: 08.03.2010

23. http://www.webopedia.com/TERM/T/Trojan_horse.html Erişim: 15.03.2010

24. http://www.forumti.com/bilgisayara-sizma/20184-truva-ati-trojan-horse-nedir.html
Erişim: 18.03.2010

25. http://www.topbits.com/logic-bomb.html Discussing Technology Erişim: 22.04.2010

26. http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177438-dialer-mantik-bombasi-nedir.html
Erişim: 22.04.2010

27. http://www.informationweek.com/news/security/management/showArticle.jhtml
Erişim: 22.04.2010

28. http://antivirus.about.com/od/whatisavirus/a/keylogger.htm Erişim: 25.04.2010

29. http://www.microsoft.com/turkiye/athome/security/viruses/virus101.mspx Erişim: 25.04.2010

30. **Canbek G, Sağıroğlu Ş**, Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri,Grafiker Yayıncılık, **2006**:26.

31. **Hızır B**, Hacking Nedir, yayımlanmamış.

32. http://www.uekae.tubitak.gov.tr/uekae_content_files/EtkinlikWeb/BT_Guvenliginin_Gecmisi_ve_Gelecegi.pdf Erişim: 23.07.2010.

33. http://www.pc-history.org/pc-virus.htm The History of the PC Virus Erişim: 12.12.2009.

34. http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms#cite_note-12
Erişim: 12.12.2009.

35. http://www.mertada.com/ Erişim: 13.01.2010

36. **Mitnick K**, My first RSA Conference, Security Focus, 30.04.2001
http://www.securityfocus.com/news/199 Erişim: 21.11.2009

37. http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics
Erişim: 24.01.2010

38. **Verizon K**, PBX Social Engineering Scam, 2000
http://www.bellatlantic.com/security/fraud/pbx_scam.htm Erişim: 24.01.2010

39. **Tims R**, Social Engineering: Policies and Education a Must, SANS Institute**, 2001**

40. http://www.vigilante.com/inetsecurity/socialengineering.htm Erişim: 24.01.2010

41. Ameritech Consumer Information "Social Engineering Fraud,"
http://www.ameritech.com/content/0,3086,92,00.html Erişim: 17.12.2008

42. **Stevens G**, Enhancing Defenses Against Social Engineering, SANS Institute, **2001**

43. **Arthurs W**, A Proactive Defence to Social Engineering, SANS Institute, **2001**

44. **Berg A**, Al Berg Cracking a Social Engineer, LAN Times, **1995**

45. http://www.cyber-security.org/CW/Dokuman/Default.Asp?Data_id=504 Erişim: 10.06.2009

46. **Akgün F, Buluş E, Şen Ş**, Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek için Kullanılan Önemli Teknikler ve Korunma Yollarının İncelenmesi

47. **Tripunitara M, Dutta P**, A Middleware Approach to Asynchronous and Backward Compatible Detection and Prevention of ARP Cache Poisoning, 15th Annual Computer Security Applications Conference, **1999**, Phoenix, Arizona.

48. **Perring A, Song D, Yaar A**, StackPi: A New Defense Mechanism Against IP Spoofing and DDoS Attacks, Carnegie Mellon University, **2003**, Pittsburgh.

49. **Akarslan H**, Bilişim Suçu İşlenirken Kullanılan Metotlar ve "Adanalı Hacker" Örneği, Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Fakültesi, Ankara, **2006**.

50. http://www.spam.org.tr/nedir.html Erişim: 15.08.2009

51. http://www.turkdownload.gen.tr/haber/tehlikenin-adi-botnet/ Erişim: 13.03.2008

52. http://packetstorm.decepticons.org/docs/social-engineering/socintro.html Erişim: 19.09.2008

53. **Anonymous**, Social engineering: Examples and Countermeasures from the Real-world, Computer Security Institute, http://www.gocsi.com/soceng.htm Erişim: 30.04.2010

54. **Orr, C**, Social Engineering: A Backdoor to the Vault, SANS Institute, **2000**

55. **Palumbo J**, Social Engineering: What is it, why is so little said about it and what can be done?, SANS Institute, **26.07.2000**

56. http://www.serdarkalkan.com/bilgisayarin_icadi.htm Erişim: 23.06.2010

57. http://www.webhatti.com/donanim-bilesenleri/615-bilgisayar-tarihi.html Erişim: 23.06.2010

58. http://www.gencwebtasarim.net/bilgi/internetin-tarihcesi.html Erişim: 01.07.2010

59. http://www.meb.gov.tr/belirligunler/internet/internet_tarih.htm Erişim: 01.07.2010

60. http://www.yildiz.edu.tr/~inan/internet_notu.htm Erişim: 01.07.2010

61. **Karakaya A, Bozdoğan B, Konar B ve Çınar V.** Hacker Tarihi, Byte Plus Der, **2006;** 12: 6

62. http://blogir.net/hackerligin-tarihi.html Erişim: 23.07.2010

63. http://www.computer.org/portal/web/csdl/doi/10.1109/AFIPS.1970.89 Erişim:24.07.2010

64. http://www.webster.edu/philosophy/~umbaugh/courses/frosh/dairy/mitnick.htm Erişim: 23.07.2010

65. http://www.newsweek.com/2010/03/09/hacking-the-planet/shadow-hawk.ht Erişim: 23.07.2010

66. http://www.bildirgec.org/yazi/tarihin-ilk-hack-leri-ve Erişim: 23.07.2010

67. http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm Erişim: 23.07.2010

68. http://www.wired.com/threatlevel/2008/09/the-analyzer-su/ Erişim: 23.07.2010
69. http://www.fmgraphics.net/forum/internet-haberleri/28651-1960lardan-bu-yana-onemli-hack-olaylari.html Erişim:24.07.2010
70. http://www.antionline.com/showthread.php?threadid=278848 Erişim:24.07.2010
71. http://www.tumgazeteler.com/?a=835902 Erişim:24.07.2010
72. http://www.caferkara.org/hackerlarin-tarihcesi.html Erişim:24.07.2010
73. http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history#2000s Erişim:24.07.2010
74. http://www.justice.gov/criminal/cybercrime/anchetaArrest.htm Erişim:24.07.2010
75. http://www.kamuhaber.net/alt.php?tad=haberler&ic=haber&resim=haber_resim&no_h=23717 Erişim:24.07.2010
76. **Franceschelli V'den aktaran Yazıcıoğlu R,** Bilgisayar Suçları, Alfa Yayınları, **1997**: 52
77. **Yazıcıoğlu R,** Bilgisayar Suçları, Alfa Yayınları, **1997**: 52
78. **Sarzana C'den aktaran Yazıcıoğlu R,** Bilgisayar Suçları, Alfa Yayınları, **1997**: 54, 55
79. **Doğan E. A,** Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınları, **1992**: 14
80. **Topaloğlu M,** Bilişim Hukuku, Karahan Yayınları, **2005:** 16
81. **Harl N**, People Hacking: The Psychology of Social Engineering, Text of Harl's Talk at Access All Areas III, 1997
82. **Özkan T**, Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi, Yüksek Lisans Tezi, Anadolu Üniversitesi, Eskişehir, **2006**.
83. http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=135 Erişim: 10.05.2010.
84. www.bilisimpolisi.com/?p=105 Erişim: 02.08.2009
85. http://www.kom.gov.tr/Tr/KonuDetay.asp?id=0&BKey=21 Erişim: 17.08.2009
86. http://www.tadoc.gov.tr/tr/KonuDetay.asp?id=0&BKey=194 Erişim: 17.08.2009
87. Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı 2008 Raporu
88. Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı 2009 Raporu
89. Adana İl Emniyet Müdürlüğü Güvenlik Şube istatistikleri
90. Adana İl Jandarma Komutanlığı arşiv kayıtları
91. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf Erişim: 12.08.2010
92. http://www.csmonitor.com/USA/Justice/2010/0326/Card-hacker-Albert-Gonzalez-gets-20-years-but-cyber-crime-rising Erişim: 17.08.2010

93. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html Erişim: 23.08.2010

94. http://www.crime-research.org/analytics/cybercrime1302/ Erişim: 23.08.2010

95. www.garanti.com Erişim: 23.08.2010

96. www.akbank.com Erişim: 23.08.2010

97. http://www.cybercrimelaw.net/EU.html Erişim: 03.10.2010

98. http://www.europol.europa.eu/index.asp?page=news&news=pr100622.htm Erişim: 03.10.2010

ÖZGEÇMİŞ

Kezban Atalıç Taş 1984 yılında Kastamonu'da doğdu. İlk, orta ve lise öğrenimini Konya'nın ilçesi Akşehir'de tamamladıktan sonra, 2006 yılında Polis Akademisi Güvenlik Bilimleri Fakültesi'nden mezun olarak Komiser Yardımcısı rütbesi ile Adana Eskiistasyon Polis Merkezi Amirliği'nde göreve başladı.

2007 yılında Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü Adli Tıp Anabilim Dalı Yüksek Lisans eğitimine başladı.

2008 yılında Seyhan İlçe Emniyet Müdürlüğü'ne ataması yapıldı. Halen Seyhan İlçe Emniyet Müdürlüğü'nde Bürolar Amiri olarak görev yapmaktadır.