SİBER SUÇLAR ÜZERİNE BİR ARAŞTIRMA
AFYONKARAHİSAR ÖRNEĞİ

YÜKSEK LİSANS TEZİ

Musa SÜRER
DANIŞMAN
Yrd. Doç. Barış GÖKÇE
İNTERNET VE BİLİŞİM TEKNOLOJİLERİ
YÖNETİMİ ANABİLİM DALI
Temmuz, 2014

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

SİBER SUÇLAR ÜZERİNE BİR ARAŞTIRMA AFYONKARAHİSAR ÖRNEĞİ

Musa SÜRER

Danışman: Yrd. Doç. Barış GÖKÇE

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
ANABİLİM DALI

Temmuz, 2014

TEZ ONAY SAYFASI

Musa SÜRER tarafından hazırlanan "**SİBER SUÇLAR ÜZERİNE BİR RAŞTIRMA: AFYONKARAHİSAR ÖRNEĞİ"** adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 24/07/2014 tarihinde aşağıdaki jüri tarafından oy birliği ile **Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.**

Danışman : Yrd. Doç. Dr. Barış GÖKÇE
AKÜ Teknoloji Fakültesi

Başkan : Prof. Dr. Şuayıp ÖZDEMİR
AKÜ İktisadi ve İdari Bilimler Fakültesi,

Üye : Yrd. Doç. Dr. Sinan YÖRÜK
AKÜ Eğitim Fakültesi

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../ 2014 tarih ve
..... sayılı kararıyla onaylanmıştır.

.....
Prof. Dr. Yılmaz YALÇIN
Enstitü Müdürü

i

BİLİMSEL ETİK BİLDİRİM SAYFASI

Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

30. 07. 2014

Musa SÜRER

ÖZET

Yüksek Lisans Tezi

SİBER SUÇLAR ÜZERİNE BİR ARAŞTIRMA
AFYONKARAHİSAR ÖRNEĞİ

Musa SÜRER
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı

Danışman: Yrd. Doç. Dr. Barış GÖKÇE

Bilgi iletişim teknolojilerinin ve bu teknolojilere erişilebilirliğin her geçen gün artmasına paralel olarak bu sistemlere yönelik suç türleri de artmaktadır. Sanal bir ortamda paylaşılan bilgiler bilinçsiz veya yetersiz güvenlik adımları uygulamalarıyla kötü niyetli kullanıcıların eline geçebilmektedir. İnternet kullanıcıları bazı mağduriyetler yaşayarak bilmeden adli bir konunun tarafı olabilmektedir. Bu noktada siber suçun insanlar tarafından nasıl algılandığı son derece önemlidir. Bu çalışmada Afyonkarahisar ölçeğinde lise öğrencilerinden yükseköğretim öğrencilerine ve kamu çalışanlarına kadar siber suç algısının temel düzeyde ölçümü yapılmıştır.

Afyonkarahisar örnekleminde kamu çalışanları ile öğrenim gören öğrencilere yönelik internet kullanım alışkanlıklarının tespiti, siber (bilişim) suça ilişkin görüşlerinin tesbiti ve suç farkındalıklarının ortaya konması amacıyla bir anket çalışması yapılmıştır. Anket sonuçları yorumlanarak katılımcıların internet kullanım araçları, amaçları, alışkanlıkları, siber suç bilgileri, tehdit algıları ve farkındalıkları, internet ortamında bireysel özgürlüklerin kullanımı ve korunması, güvenlik uygulamalarına yaklaşımları ve duyarlılıkları hakkında bir düzey ölçümü yapılmıştır.

2014, Temmuz + 129 sayfa
Anahtar Kelimeler: Siber Suç, Siber Suç Algısı, Siber Güvenlik.

ABSRACT

M.Sc. Thesis

A STUDY ON SIBER CRIME: AFYONKARAHİSAR SAMPLE

Musa SÜRER

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

Supervisor: Assist. Prof. Dr. Barış GÖKÇE

Types of cyber crimes are also increased along with developing information communication technologies and the accessibility. The information shared in a cyber environment can be passed into the hands of malicious users with unconscious or inadequate security steps. Internet users living some grievances may be a judicial side of the issue without knowing. At this point, people's perception of cyber crime is extremely important. In this study, cyber crime has been evaluated at a basic level of perception on the scale of Afyonkarahisar from high school students to university students and public employees

A survey study was conducted in a sample of Afyonkarahisar to public employee and students in order to determine internet usage habits, opinion on cybercrime awareness and cyber crime identification. Survey results are interpreted and made a level evaluation about participants' use of the internet tools, goals, habits, cyber crime information, threat perceptions and awareness, use and protection of individual freedoms in the internet environment and approach to security applications and sensitivities

2014, July + 129 pages

Key Words: Cybercrime, Cyber Crime Perception, Cyber Security.

TEŞEKKÜR

Bu çalışmanın konusu, kaynak araştırması, anket çalışmalarının gerçekleştirilmesi, sonuçların değerlendirilmesi ve yazım aşamasında yapmış olduğu değerli katkılarından dolayı tez danışmanım Yrd. Doç. Dr. Barış GÖKÇE'ye, değerli katkılarından dolayı Prof. Dr. Şuayıp ÖZDEMİR ve Yrd. Doç. Dr. Sinan YÖRÜK'e, analizlere katkılarından dolayı Yrd. Doç. Dr. Bülent Aydoğuş'a Anket çalışmalarına desteklerinden dolayı Afyonkarahisar Emniyet Müdürlüğü, Afyonkarahisar Defterdarlığı, Tapu Müdürlüğü, Ali Çağlar Anadolu Lisesi, Afyon Lisesi, Zübeyde Hanım Kız Meslek Lisesi ve Afyon Kocatepe Üniversitesi personel ve öğrencilerine ve her konuda öneri ve eleştirileriyle yardımlarını gördüğüm arkadaşlarıma teşekkür ederim.

Bu çalışma süresince maddi ve manevi fedakârlıklarından dolayı eşim Yasemin'e, oğlum Meriç Berkay'a ve kızım Elif'e teşekkür ederim.

Musa SÜRER

AFYONKARAHİSAR, 2014

İÇİNDEKİLER DİZİNİ

Sayfa

SİMGELER ve KISALTMALAR DİZİNİ

Kısaltmalar:

ABD	Amerika Birleşik Devletleri
ATM	Automatic Money Transfer
AET	Avrupa Ekonomik Teşkilatı
BKK	Bankalar ve Kredi Kartlar Kanunu
CIA	Central Intelligence Service
CMK	Ceza Muhakemeleri Kanunu
DNS	Domain Name Sistem
EFT	Elektronik Fon transferi
EGM	Emniyet Genel Müdürlüğü
EİK	Elektronik İmza Kanunu
FBI	Federal Buro Of Investigation
FTK	Forensic Tool Kit
GSM	Global System for Mobile
HSYK	Hâkim Savcılar Yüksek Kurulu
HTTPS	Secure Hypertext Transfer Protocol
IP	İnternet Protocol
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
RAM	Random Access Memory
SMS	Short Message Service
STK	Sivil Topluk Kuruluşları
STS	Saldırı Tespit Sistemleri
TCK	Türk Ceza Kanunu
TİB	Telekomünikasyon İletişim Başkanlığı
TUİK	Türkiye İstatistik Kurumu
URL	Uniform Resource Locator
UYAP	Ulusal Yargı Ağı
WAP	Wireless Access Point
YTCK	Yeni Türk Ceza Kanunu

ÇİZELGELER DİZİNİ

Sayfa

1.GİRİŞ

Bilgi iletişim teknolojilerinin ve bu teknolojilere erişilebilirliğin her geçen gün artmasına paralel olarak bu sistemlere yönelik suç arayışları da artmaktadır. Teknolojinin gelişmesiyle internet erişimli elektronik cihazların artışı ve ucuzlaması, buna bağlı olarak yaygınlaşan internet ve internet tabanlı uygulamaların kullanımı (İnt. Kyn.1), özellikle sosyal ağların hayatımızın her anını paylaşıma açması, kişiye özel hayatın gizliliğini ve kişiye özel verilerin güvenliğini ve korunmasını gündeme getirmiştir. Sanal bir ortamda paylaşılan bilgiler bilinçsiz veya yetersiz güvenlik adımları uygulamalarıyla kötü niyetli kullanıcıların eline geçebilmekte, internet kullanıcıları mağduriyetler yaşayarak bilmeden adli bir konunun tarafı olabilmektedir. Suçtan zarar gören (mağdur) ve kendi kimlik/ kullanıcı bilgileri ile suç işleyen veya aracılık eden konumuna gelebilmektedir.

Günlük hayatımızda iletişim, eğlence, arkadaşlıklar, eğitim, ticari faaliyetler, ödemeler gibi çok farklı amaçlar için kullanılan fiziksel ve sosyal sınırları olmayan siber ortam, kullanıcı mağdur sayılarındaki artış ve maddi kayıplar, özel bilgi, belge kayıpları, İnternet kullanıcılarında siber suça bulaşma veya mağdur edilme korkusu oluşturmuş, bu korku yeni ve farklı mağdur hikâyeleriyle artmaya devam etmektedir.

Teknolojideki hızlı gelişmenin yarattığı süreç değişimleri ve bilişim sistemlerinin mevcut süreçlere entegrasyonu, suç işleme niyetindeki bazı birey ve grupların teknolojiyi hem araç hem de hedef olarak kullanmasına yol açmış ve neticede siber suçlar günümüz modern toplumlarının önemli sorunlarından biri haline gelmiştir.

Türk Hukuk mevzuatında internet ortamındaki yayınlar düzenlenmiş olup internet aracılığıyla işlenen suçlarda Ceza Kanununda yerini almıştır. İnternet kullanımının hızlı yayılımına karşın sanal ortamlardaki hukuki ihlaller konusunda yeterli bilinç gelişiminin olmayışı, hangi fiil ve eylemlerin suç oluşturduğu, hangi durumlarda suç mağduru olarak adli birimlere müracaat edilmesi gerektiği, hangi durumlarda suç işleyen konumuna düşülebileceğinin bilinmeyişini ortaya çıkarmaktadır. Özellikle kullanıcı

profillerinin yaş ve eğitim düzeyine bağlı olarak ilkokul altı yaşlardan 80/90 lara kadar genişlemesi bilinç düzeylerinin farklılığını gündeme getirmektedir.

Hukuk ve teknoloji birbirine oldukça uzak mesafede duran iki disiplindir. Ancak bunların kesişim noktası "Siber suçlar" konusunda hukuksal düzenlemeler hem yeni, hem de dar kapsamlı olduğu, yapılan araştırma ve çalışmaların da yetersiz olduğu, artan ve çeşitlenen siber suç türlerini içermediği bilinmektedir. Her geçen gün gelişen ve değişen siber suçlar ve suç grupları günlük yaşamımızı tehdit etmeye devam etmektedir. Suçla mücadelede kolluk ve adli birimler açısından suçun unsurlarını tespitte yaşanan zorluklar, ülkeler arası adli yardımlaşma ve suç tanımlarındaki farklılıklar, adli bilişim uzmanlığı hizmetlerinin yeterince gelişmemesi suç işleyenlerin tespit edilmesini ve yakalanmasını zorlaştırmaktadır.

Öte yandan siber ortamdaki kullanıcı sayılarının çokluğu, erişimin ve ulaşımın kolaylığı yeni bir terör çeşidini ortaya çıkarmıştır. Dünya, toplumları çok hızlı manipüle edebilen, sokağa dökebilen, şiddete sürükleyen, yönetimleri zorlayan, tehdit eden, devlet güvenliğine ait kurumların veri bankalarına müdahale edebilen siber terörizmle tanışmıştır. Siber suç gruplarının yanında terör örgütlerince ve ülkelerin güç mücadelelerinde de bilişim teknolojileri etkili bir araç olarak profesyonelce kullanılmaya başlanmıştır. Özellikle Arap baharı olarak adlandırılan kuzey Afrika ülkelerindeki yönetim değişikliklerinde halkın mobilize edilmesi, protesto mitinglerin gerçekleştirilmesi, direnişlerin sürdürülmesinde sosyal medya baş aktör olmuştur. Yine ülkemizdeki taksim ağaç parkı direnişleri ve protesto mitingleri hep sosyal medya aracılığıyla sürdürülmüştür.

Mevcut hukuk kuralları modern teknolojinin yarattığı olumsuzlukları gidermede yetersiz kalmaktadır. Ahlaki değerleri, insanlığı ve ülkeleri tehdit eden siber suçlar tüm ülkelerin ortak problemi haline gelmiştir. Bu denli karmaşık ve çok yönlü yapıyla etkili mücadele için her fırsatta uluslararası işbirliği imkânları düşünülmelidir. Siber suçlar ile mücadelede, milli menfaatlerimiz ve ulusal güvenliğimiz için geleceğin teknolojilerine de cevap verilebilecek esnek çözümler üretilmeli, yasal mevzuatın uyarlanması yanı sıra, terör örgütlerinin veya taşeron örgütler üzerinden devletlerin

diğer ülkeler üzerine örtülü operasyonlar yapmasını engelleyecek tedbirlerin özgürlükleri kısıtlamadan geliştirilmesi sağlanmalı, e-devlet kapsamında kamu hizmetlerin sunumu kolaylaştırılırken bilgi güvenliği kapsamında her kurum ve kuruluş kendi içerisinde özel tedbirler geliştirmeli ve güvenlik kuralları asla ihmal edilmemelidir.

Günlük rutin hayatımızda, yaşam tarzlarımızın maruz bıraktığı yoğun teknoloji kullanımı karşısında bireysel olarak çevrimiçi yaşamda siber güvenliğin korunması ve siber suç mağduriyetlerinin yaşanmaması için siber tehlikenin varlığının farkında olunması, siber tehditlere karşı geliştirilen dijital güvenlik tedbirlerin aktif olarak kullanılması ve alışkanlık haline dönüştürülmesi taşınan riskin azaltılmasında önemli görülmektedir.

Bu tez çalışması dört bölümden oluşmakta olup birinci bölümde siber ve siber suç kavramı irdelenmiş olup, siber suçun farkı ve hedefleri anlatılmış, ikinci bölümde siber kavramının Türk hukuk literatürüne girişi, Türk ceza kanuınlarında yer alan siber suçlara değinilerek siber suçlar sınıflandırlmış, internet ortamındaki yayınları düzenleyen 5651 sayılı kanun detaylı olarak incelenerek, Avrupa birliği siber suçlar sözleşmesine bakılmış, siber suç tehdit ve işleme yöntemleri anlatılarak alınması gerekli güvenlik önlemlerine vurgu yapılmış, üçüncü bölümde bilgi iletişim teknolojilerinin suç kolaylaştırıcı yapısı ifade edilerek siber suç faillerinin ve mağdurlarının genel özellikleri anlatılmış, dördüncü bölümde ise Afyonkarahisar örnekleminde çalışan kamu görevlileri ile öğrenim gören kişilere yönelik internet kullanım alışkanlıklarının tespiti, siber (bilişim) suça ilişkin görüşlerinin tesbiti ve suç farkındalıklarının ortaya konması amacıyla Afyon Kocatepe Üniversitesi, Afyonkarahisar Milli Eğitim Müdürlüğüne bağlı lise okullarındaki öğrenciler ile Afyonkarahisar'da devlet memuru olarak kamu kurumlarında çalışan kişilere yönelik bir anket çalışması yapılmış olup, anket sonuçları eğitim seviyesi ve cinsiyet düzleminde yorumlanmış olup katılımcıların internet kullanım alışkanlıkları ile kendilerinin veya çevrelerindeki kişilerin suçla karşılaşma ve tecrübesel yaşamları, siber suç bilgileri, tehdit algıları ve farkındalıkları, internet ortamında bireysel özgürlüklerin kullanımı ve korunmasına yönelik güvenlik uygulamalarına yaklaşımları hakkında bir düzey ölçümü yapılmıştır.

2. LİTERATÜR

2.1 Siber Kavramı

"Siber" kelimesi Türk Dil Kurumunca henüz Türkçe karşılığı oluşturulmayan (İnt. Kyn.2) İngilizcedeki "Cyber" kelimesinden uyarlanarak kullanıma kazandırılan bir kelime olup, "Sanal Gerçeklik", "İnternete ait olan", "Bilgisayar ağlarına ait olan" anlamlarına gelmekte olup (İnt. Kyn.3) günümüzde bilişim ve iletişim ağlarının şekillendirdiği uzayı ifade etmektedir.

Sibernetik kökeninden gelen Siber terimi İlk olarak Sibernetik biliminin babası sayılan Louis Couffignal tarafından 1958 yılında, canlılar ve/veya makineler arasındaki iletişim disiplinini inceleme için kullanılmıştır (İnt. Kyn.4).

"Siber uzay" terimi ise ilk olarak 1984 yıllında "Neu romancer" adlı bilim kurgu romanında William Gibson tarafından kullanılmış olup, etimolojik açıdan siber ve uzay kelimelerinin bir araya gelmesinden oluşmaktadır. Sonrasında, siber uzay terimi akademik ortamda da kullanılmaya başlanmış ve teknolojinin gelişmesi ile birlikte tanımı da değişmiştir. İnternetin yaygın olarak kullanılmaya başlanması ile coğrafi kısıtlamalar ortadan kalkmış, insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan yeni bir dünya oluşmuştur. Bu dünya zamanla siber uzay olarak tanımlanmıştır (Whittekar 2004).

Birleşmiş Milletler Terimler Sözlüğünde siber uzay, ağ (web) olarak bilinen internete, iletişim altyapısına, online konferans kuruluşlarına, bilgi depolama ve işleme aygıtlarına bağlı global sistem olarak tanımlanmıştır (İnt. Kyn.5).

Amerikan Savunma Bakanlığı'nın Askeri Terimler Sözlüğü ise siber uzayı; internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol sistemleri gibi birbirine bağlı bilgi teknolojilerin altyapılarını kapsayan bilgi ortamı olarak tanımlanmıştır (İnt. Kyn.6)

Siber uzay, günümüzde tek bir homojen uzaydan oluşmamaktadır. Çok sayıda, hızla genişleyen, her biri farklı bir sayısal etkileşim ve iletişim yöntemi sağlayan uzayların bir birleşimidir. Siber uzayın bir merkezinin olmaması, sınırları olmayan, ağ biçimindeki yapısı onun tek bir devletin, dolayısıyla tek bir hukuk sisteminin egemenliği altında olmasına engel olmakta bu durumda farklı hukuk sistemleri açısından hangi fiillerin siber suç olduğu tanımını da zorlaştırmaktadır. Vatandaşlık, ulusal sınır gibi kavramların anlam ifade etmediği siber uzayda, ülkelerin egemenlik yetkilerini meşrulaştırmasına, başka bir deyişle hukuk kuralı koyma ve uygulama haklarını sağlam temeller üzerine oturtulmasına ihtiyaç duyulmaktadır. Siber uzayın yeni bir hukuk alanı olduğu genel kabul görmekle birlikte asıl üzerinde uzlaşmaya varılamayan konu, hukukun kim tarafından konulacağı ve nasıl uygulanacağı sorunudur. Her ne kadar siber uzay, ulusal devletlerin fiziki sınırları içinde bir kısım dijital alanı kapsıyorsa da aynı zamanda farklı ülkelerin de ulusal alanını işgal etmektedir. Gerçek dünya, insanlar tarafından binlerce yılın sonunda ulusal ve uluslararası hukuk kuralları ile yönetilirken siber uzay yapısı gereği hala üzerinde yeterince uluslararası uzlaşının oluşamadığı bir alandır (Yayla 2013).

2.2 Siber Suç Nedir

İnternet ve bilgisayar aracılığıyla işlenen suçları ifade etmede pek çok terim kullanılmaktadır. Bunlardan bazıları siber suç, bilgisayar suçları, internet suçları, bilgi teknolojileri suçları, bilişim suçları, yüksek teknoloji suçları gibi (Goodman & Brenner 2002).

Genel kullanımda “siber suç”, “bilgisayar suçları”, “bilişim suçları” terimleri tercih edilse de bu ifade suçun işlenmesinde kullanılan bilgisayar, internet ağı ve teknolojik cihazlara göre değişiklik gösterebilmektedir. “Bilgisayar suçları” internetin keşfedilmesinden önce ki dönemlerde kullanılan bir kavramdı, günümüzde kabul gören ve yaygınca kullanılan terim “siber suçlar” dır (Moitra 2005).

Bilgisayar suçu terimi genel olarak faillerin bir bilgisayarda veya bilgisayarı aracı kılarak suç işlemesini, “Siber suç” terimi ise sadece bilgisayarların değil bilgisayarlar

arası iletişim sağlayan ağların (internet, intranet) suçta kullanılmasını ifade eder (Moitra 2005).

Siber uzay suçları teriminin kullanımının da doğru olacağı vurgulansa da, "siber suç" terimi suç ve zararlı davranışın ağ teknolojisi aracılığıyla gerçekleşmesi ve dönüşümü ifade etme açısından bütün avantaj ve dezavantajlarına rağmen kabul gören ve yaygınca kullanılan bir kavram haline gelmiştir (Wall 2001).

Her halükarda "Siber suç" teriminin net bir tanımlaması, üzerinde ulusal veya küresel uzlaşı oluşmuş bir tanımı yoktur (Yar 2005, Moitra 2005, Goodman 1997, Brenner & Clarke 2005). Dahası "Siber suç" terimi yasal mevzuatlarda ifade edilen bir terimden öte politikacıların, akademisyenlerin, medya ve halk tarafından bilgisayar ve ağlar aracılığıyla gerçekleşen yasa dışı faaliyetleri ifade için kullanılmıştır (Clifford 2001, Wall 2001).

Oldukça yeni ve üzerinde uzlaşılmış bir tanımı bulunmayan Siber suç teriminin ne anlama geldiği ve bu siber suçu diğer suçlardan farklı kılan unsurların ne olduğunu açıklamak gerekmektedir. Bazı bilim adamları siber suçun yeni bir suç olmadığı, geleneksel suçların farklı bir şekilde işlenmesi olduğu, mevcut yasalarla soruşturulması, yargılanması ve cezalandırılması gerektiğini belirtmektedirler (Grabosky 2007).

Wall (2001) geniş bir yaklaşımla internetin keşfiyle suç faaliyetlerinin üç farklı şekilde geliştiğini belirtmektedir. Birincisi, internetin uyuşturucu kaçakçılığı, taciz ya da nefret söylemi gibi geleneksel suçlar için yeni bir iletişim ortamı yarattığı, ikinci olarak internetin uluslararası bir ortam yaratarak pedofili ya da dolandırıcılık gibi sapkın ve zararlı davranışlar için yeni fırsatlar sağladığı, üçüncü olarak İnternetin, hackleme, service hizmetlerini engelleme saldırıları, bilgisayar virüsleri yayma gibi suç faaliyetleri için tamamen yeni formlar yarattığını belirtmektedir. Hatta siber ortam içerisinde gerçekleşen zararlı yeni suç aktivitelerini "yeni üretilen şişesiz şarap" senaryosuyla ifade etmektedir.

Siber suçları yeni bir suç aktivitesi veya eski suçların yeni vasıtalar aracılığıyla işlenmesi olarak sınıflama yerine Yar (2006) önerisinde; siber suçu tek bir olgu olarak kavramaya çalışmak yerine bir dizi yasa dışı faaliyetlerin ortak paydası bilgi ve iletişim teknolojileri olan alan olarak tanımlamanın daha iyi olacağını.

Benzer bir bakış açısıyla, Moitra (2005) siber suçu " internet üzerinden yetkisiz veya sapkın ya da yasadışı faaliyet içeren aktivitenin, bir bilgisayar (veya bilgisayarlar) aracı kılınarak yine hedefi bilgisayar (veya bilgisayarlar) olan faaliyet" olarak tanımlar.

Goodman ve Brenner (2002) siber suçu iki ana başlık altında incelemektedirler. Birincisinde, bilgisayar suçun hedefi olan (bilgisayar odaklı suçlar), bu ağ gizlilik, bütünlük ve / veya saldırı gibi durumu. İkinci kategoride ise bilgisayar geleneksel suçları işlemede bir araç olarak kullanılır (bilgisayar destekli suç). Bu hırsızlık, dolandırıcılık ve sahtecilik gibi suçların bilgisayar ve bilgisayar ağ teknolojileri yardımı ile gerçekleştirilmesidir.

Türk literatüründe kavramsal olarak henüz yerini bulmayan, üzerinde görüş birliği oluşmayan "siber suç", "internet suçları", "bilişim suçları" veya "bilgisayar suçları" olarak adlandırılan suçlar için, Dünya'daki pek çok devlet tarafından temel kabul edilen düzenlemelerden biri olarak Avrupa Konseyi Siber Suç Sözleşmesi'nin adına uygun olması ve uluslararası hukukta ve literatürde yaygın olarak kullanılması nedeniyle "siber suç" ifadesi bu çalışmada kavramsal olarak tercih edilmiştir.

Siber suç, bir bilgisayar, ağ veya donanım cihazı kullanılmak suretiyle, elektronik ortamda hukuka aykırı olarak gerçekleştirilen her tür fiil olarak tanımlanabilir. 1980'li yıllardan sonra bilgisayar ve internet kullanımının yaygınlaşması ile ortaya çıkan siber suçlarla sadece ekonomik kayıpların yaşanmadığı aksine farklı değerler aleyhinde de işlendiği anlaşılmıştır. Bu nedenlerden dolayı da bu suçların ayrı bir disiplin altında incelenmesi gerekliliği ortaya çıkmıştır.

İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şubesi web sitesinde siber suçu "Bir bilişim sisteminin güvenliğini ve / veya buna bağlı verileri ve / veya kullanıcısını

hedef alan ve bilişim sistemi kullanılarak işlenen suçlar'' olarak tanımlamış, diğer suçlardan ayıran özellik olarak bir bilişim sistemi olmadan işlenememesi, bilgisayar ve internete özgü suçlar olarak da adlandırılması olarak vurgulamıştır (İnt. Kyn.7).

Siber suçu genel olarak internet ve/ya intranet ağ yapılarına bağlı bilgi iletişim teknolojileri kullanan birey ve sistemleri, sistem içindeki dataları, ağ ve sistem güvenliklerini hedef olarak ve/ya araç olarak kullanarak gerçekleştirilen hukuk dışı eylemler olarak tarif edebiliriz.

Avrupa Siber Suçlar Sözleşmesinde bir bilişim sistemine izinsiz olarak ve hukuka aykırı olacak şekilde ağları kullanarak girilmesi ve sonrasında yapılan eylemler siber suç olarak tanımlanmıştır.

2.2.1 Siber Suçu Farklı Kılan Nedir

Bilişim sistemleri aracı kılınarak tüm suçların işlenebilmesi mümkündür. Ancak her fiil siber suç olarak tanımlanamaz. Avrupa Siber Suçlar Sözleşmesi perspektifinde bir bilişim sistemine izinsiz olarak ve hukuka aykırı olacak şekilde ağları kullanarak girilmesi ve sonrasında yapılan eylemler siber suç olarak tanımlanmıştır. Burada hedef bir sistemin kendisi olabileceği gibi özel verilerle birlikte bir kişi de olabilir. Örneğin iletişimi izinsiz izleme ve kayıt etme, iletişimi engelleme, özel hayatın gizliliğine müdahale etme, sistemin kullanımını engelleme, bir sisteme girerek zarar verme, veri ekleme, verileri silme, ele geçirme, şifreleme gibi eylemler siber suç olarak değerlendirilen fiillerdendir (Avrupa Siber Suçlar Sözleşmesi).

Siber suçları, bilinen klasik anlamdaki suçlardan farklı yapan özelliklerden en önemlisi, bu suçların işlenme şekillerindeki (modus operandi) tespit zorluğudur. Bu tip suçlar, yepyeni ve çok farklı usullerle işlenebilmektedir (Turhan 2006).

Bir kişiye ait isim, adres, telefon, fotoğraf veya kimlik numarası veya aile hayatına ilişkin kişisel veriler çoğu kez veri sahibinin isteği ve bilgisi dışında yayılabilmektedir. Böyle durumlarda, bilgilerin web'e erişimi olan milyonlara hatta milyarlara iletilmesi ya

da çoğaltılması saniyelerle ifade edilmektedir. Klasik ceza hukukunda suç aracı olan herhangi bir vasıta gibi kişisel verilerin de, üçüncü kişilerin tasarrufuna girdiği anda suç aracı olarak kullanılma riski doğmuş olmaktadır. Klasik suça göre daha hızlı ve kolay işlenebilen siber suçun tespit edilmesi, bu suç tespit edilse bile suçta kullanılan araçlardan faile ulaşılması, fail belirlense bile yakalanması, fail yakalansa bile kişinin uğradığı zararın veya suça konu zararlı içeriğin web ortamından tamamen kaldırılması, alınan veya yayılmış üçüncü dördüncü taraflardaki kopyaların silinmesi, yok edilmesi mümkün olmayan bir durumdur.

Web üzerinde yayınlanmış suça konu bilgi, belge veya içerikler yayınlayanlar açısından suç oluşturmakla beraber erişerek kopya elde edenler açısından suç oluşturmayacaktır. Ancak bu kopyaların tekrar yayılması veya yayınlanması veya farklı amaçlar için kullanılması, beğenilmesi veya yorumlar eklenmesi suç oluşturma konusunu gündeme getirecektir.

Bir de siber suçların özelliği olarak suçtan zarar gören bazen de zarar görmese de ihlale uğrayan taraflar kendileri aleyhine işlenen suçlardan hiç haberdar bile olmayabilmektedirler. Bu durumlar ancak ihlali yapan faillerce itiraf edilmesi, başka bir yerde farklı bir zamanda deşifre edilmesi ile ortaya çıkmaktadır. Örneğin ‘’redhack’’ isimli bir hacker grubunun eylemlerini itiraf etmesi ile pek çok işletmenin web sitesi admin bilgilerinin, mail ve sosyal hesap şifrelerinin ele geçirildiği, pek çok kamu kurumunun yine aynı şekilde kurumsal hesap şifrelerinin ele geçirildiği yayınlanan paylaşımlarından anlaşılmaktadır (İnt. Kyn.8).

2.2.2 Siber Suçun Hedefleri

Gerçek dünyada işlenen suçlarda suçun hedefi ya parasal değer taşıyan somut bir varlıktır (taşınabilir elektronik, otomobil, mücevher veya nakit para) ya da gerçek bir kişidir. Fakat siberuzay da pek çok siber suçun hedefi dijital ortamda depolanan veya aktarılan soyut olan, elle tutulamayan bilgilerdir (Goodman 1997).

Gerçek dünyada her nesne benzersiz bir kimliğe sahip olup aynı zaman ve mekân içinde birden fazla yerde aynı eşsizlikle yer alamaz, ama siber uzayda her nesne aynı anda birden çok yerde aynı anda var olabilir (Geer 2007).

Bundan dolayı network ağına bağlı bir bilgisayarda depolanan bilgiler, erişim sağlayanlarca değiştirilme, silinme, kopyalanma veya çalınma gibi saldırılara karşı daha savunmasızdır. Ancak, elektronik bilgiler (0 ve 1) hammaddedir ve anlamlı bir kavram oluşturması için işlenmesi ve diğer bilgilerle ilişkilendirilmesi gereklidir ve bu işleme tabii olmadıkça tek başına bir değer ifade etmeyecektir (Cavelty 2007).

Bilginin doğadaki varlığı soyuttur ve belirginliği bazen dijital ortamda kayıtlı bazen de kâğıt üzerinde yazılı olarak ortaya çıkabilir. Siber uzaydaki "değer" anlamının ifadesi maddesel değerlerden ziyade bilgisel fikirlerin ifadesiyle ilgilidir (Wall 2001).

Siber suçun hedefi, taşınan değeri çözümleyerek bilgiyi elde etmektir. Siber uzayda bilgi bireyin kimlik numarası, banka hesap bilgileri, kredi kart bilgileri, özel hayatı ve iletişimi gibi kişiye özel veriler olabileceği gibi kişisel/kurumsal sosyal hesap şifreleri, bir şirketin ticari marka fikri mülkiyet bilgileri, geliştirilen bir ürün/ proje içeriği, banka güvenlik sistemleri, bir ülkenin askeri savunma planları veya ulusal veri bankalarındaki bilgiler veya sistemler de olabilir.

2.3 Türk Literatürüne Siber Kavramının Girişi

Türk Ceza Hukukunda siber suç kavramı henüz yer almamıştır. Türk Ceza kanunlarında 2005 yılında yenilenen Ceza Muhakemeleri Kanununda "bilişim suçları" başlığı tercih edilerek bu kavram kullanılmıştır.

TÜBİTAK içerisinde 2001 yılında kurulan Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bu alandaki faaliyetlerine ilk önce Türk Silahlı Kuvvetleri ile başlamıştır (İnt Kyn. 9).

Siber kelimesi ilk olarak 2012/3842 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan 20.10.2012 tarih ve 28447 sayılı Resmî Gazete 'de yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararla kullanılmıştır (İnt. Kyn.10).

2012 yılı aralık ayı içerisinde Türk Silahlı Kuvvetler bünyesinde "Siber Savunma Merkezi Başkanlığı" kurulmuş ve görev tanımını "TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunması yapma, siber olaylara 7/24 esasına göre müdahale etme, ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak etme, TSK çapında bilinçlendirme ve eğitim faaliyetleri yürütme, TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapma" olarak belirlemiştir (İnt. Kyn. 11).

28.02.2013 tarihinde Emniyet Genel Müdürlüğü bünyesinde 2011 yılında 2025 sayılı Bakanlar Kurulu Kararı ile kurulan Bilişim Suçlarıyla Mücadele Daire Başkanlığının ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiş ve illerde Siber Suçlarla Mücadele İl Şube Müdürlükleri oluşturulmuş ve 59 ilde kurulum tamamlamış, görev tanım ve çerçevesini "Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli daire başkanlıklarının ve taşra teşkilatındaki birimlerin dağınık yapısının tek bir çatı altında toplanması, mükerrer yatırımların önüne geçilmesi, siber suçlarla mücadelenin etkin ve verimli olarak yürütülmesini sağlamak" olarak belirlemiştir. Cumhuriyet Başsavcılıkları ve Mahkemelere adli bilişim uzmanlığı ekspertiz incelemeleri için 19 ilde Siber Şubeler içerisinde Adli bilişim bölge laboratuvarları oluşturulmuştur (İnt. Kyn.12).

25.03.2013 tarih ve 2013/4890 sayılı Bakanlar Kurulu Kararıyla 2013-2014 Eylem Planı hazırlanarak Ulusal Siber Güvenlik Stratejisi ortaya konmuştur (İnt. Kyn.13).

Yine 11.10.2013 tarih ve 28818 Sayılı Resmî Gazetede Ulaştırma, Denizcilik ve Haberleşme Bakanlığınca yayınlanan tebliğde, Siber Güvenlik Kurulu, (USOM) Ulusal Siber Olaylara Müdahale Merkezi ve (SOME) Kurumsal Siber Olaylara Müdahale Ekipleri kuruluş, çalışma ve eşgüdümü düzenlenmiştir (İnt. Kyn.14).

19 Şubat 2014 gün ve 28918 sayılı resmi gazetede yayınlanarak yürürlüğe giren 6518 sayılı Torba Kanun ile 06.02.2014 tarihinde kabul edilen 5651 sayılı İnternet ortamındaki Yayınları Düzenleyen kanun maddeleri ve ekleri üzerinde değişikliklerde 10. Maddeye yeni eklenen 6. fıkra ile ulusal siber tehditler gerekçe gösterilerek TİB'e ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesine yönelik içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlama, gerekli tedbirleri aldırma, bu doğrultuda faaliyet yürütme ve ihtiyaç duyulan çalışmaları yapma yetkisi ve tasarrufu verilmiştir (İnt. Kyn.15).

2.4 Türk Hukuk Mevzuatında Siber/Bilişim Suçları

Türk hukuk mevzuatı içerisinde TCK, CMK ve diğer kanunlarımızda siber kelimesi kullanılmamış olup bilişim alanında suçlar veya bilişim sistemleri aracılığıyla işlenen suçlar olarak yer almıştır.

2.4.1 YTCK' da Tanımlanan Siber/Bilişim Suçları

Bilişim suçları; 26.09.2004 tarihinde kabul edilip 12.10.2004 tarih ve 25611sayılı Resmi Gazetede yayınlanan 5237 Sayılı yeni Türk Ceza Kanununda, "Bilişim Alanında Suçlar" ve "Özel Hayatın Gizli Alanına Karşı Suçlar" olarak iki bölüm halinde ele alınmıştır. Burada suç olarak düzenlenen fiiller özellikle bilgi teknolojileri sistemleri ile yani işlemci bir bilgisayar ve internet erişim ağı aracılığıyla işlenebilir ve bakıldığında bilişim sistemleri olmadan işlenme imkânları çok kısıtlıdır. Bu nedenle kanunda klasik suçların yanında yalnızca bilişim suçu olarak nitelendirilen suç tanımlamaları da ortaya konulmuştur (Karagülmez 2005). Bu belirtilen suçlara ilaveten, TCK'nın değişik bölümlerinde bilişim sistemleri aracılığıyla işlenmesi mümkün olan değişik suç tipleri de yer almaktadır. Ancak suç işlemede gelişen teknolojiyle yeni yöntemlerin keşfedilmesi dolayısıyla bu tür suçlar arasında kesin ve net bir ayrım yoktur (Dülger 2004).

Kanunda ele alınan bilişim alanındaki suçlar şunlardır: Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma (Tck-m.243), bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi (Tck- m.244/1-2), bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama (Tck-m.244/4), banka veya kredi kartlarının kötüye kullanımı (Tck-m.245), tüzel kişiler hakkında güvenlik tedbiri uygulanması (Tck-m.246) başlıkları altında düzenlenmiştir (5237 sylı TCK).

2.4.2 Özel Hayata ve Hayatın Gizliliğine Yönelik Bilişim Suçları

Özel hayata ve hayatın gizli alanına karşı işlenen bilişim suçları üç alt başlık halinde düzenlenmiş olup bunlar; Kişisel verilerin kaydedilmesi suçu (Tck-m.135), kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (Tck-m.136), verilerin yok edilmemesi suçlarıdır (5237 sylı TCK).

2.4.3 Bilişim Sistemleri İle İşlenebilen Diğer Suçlar

Türk Ceza Kanununda suç olarak sayılan ancak bilişim sistemleri aracılığıyla da işlenebilen farklı suçlar da bulunmaktadır. Bu fiiller bilişim sistemleri aracı kılınarak işlendiğinde ceza artırıcı unsur olarak değerlendirilmektedir. Bu suçlar; organ ticareti, cinsel taciz, tehdit, şantaj, haberleşmenin engellenmesi, hakaret, haberleşmenin gizliliğinin ihlal edilmesi, bilişim sisteminin kullanılması yoluyla işlenen hırsızlık, bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık, uyuşturucu veya uyarıcı madde kullanılmasını alenen özendirme veya bu nitelikte yayın yapma, halk arasında korku ve panik yaratmak amacıyla tehdit, suçu ve suçluyu övme, halkı kin ve düşmanlığa tahrik veya aşağılama, yasalara uymamaya tahrik, örgütün veya amacının propagandasını yapma eylemi, müstehcenlik, göreve ilişkin sırrın açıklanması, iftira, gizliliğin ihlali suçu, cumhurbaşkanına hakaret, devletin egemenlik alametlerini aşağılama, Türklüğü, cumhuriyeti, devletin kurum ve organlarını aşağılama, halkı askerlikten soğutma, devletin güvenliğine ilişkin bilgileri temin etme, devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama, gizli kalması gereken bilgileri açıklama, devlet sırlarından yararlanma, devlet hizmetlerinde sadakatsizlik, yasaklanan bilgileri temin, yasaklanan bilgilerin casusluk maksadıyla temini,

yasaklanan bilgileri açıklama, yasaklanan bilgileri siyasal veya askerî casusluk maksadıyla açıklama olarak sayılabilir (5237 sylı TCK).

Ayrıca 5187 sayılı basın kanununa aykırılık suçları, 5846 sayılı fikir ve sanat eserleri kanununa aykırılık suçları, 551 sayılı patent haklarının korunması hakkında kanun hükmünde kararnameye aykırılık suçları, 554 sayılı endüstriyel tasarımların korunması hakkında kanun hükmünde kararnameye aykırılık teşkil eden suçlar, 556 sayılı markaların korunması hakkında kanuna aykırılık suçları ve elektronik imza kanununa aykırılık suçları diğer kanunlarda düzenlenen bilişim sistemleri aracılığıyla işlenebilen suçlardır.

2.5 5651 Sayılı Kanun ile Getirilen Tanımlar Ve Sorumluluklar

5651 sayılı İnternet Ortamındaki Yayınların Düzenlenmesiyle ilgili Kanunla hukuk sistemimize daha önceden mevzuatımızda hiç yer almayan pek çok yeni ve özgün kavramlar kazandırılmıştır. Kanunda başlıca yer sağlayıcı, içerik sağlayıcı ve erişim sağlayıcı kavramlarına yer verilmiş, bu kavramlarla tanımlanan yükümlülük ve sorumluluklar düzenlenmiştir.

2.5.1 Yer Sağlayıcı

Kanunun 2. maddesi (m) bendinde düzenlenen yer sağlayıcı; Sistemleri sağlayan, hizmet ve içerikleri barındıran veya işleten tüzel veya gerçek kişileri ifade etmektedir. Burada kastedilen hosting hizmeti veren firmalardır. Kanunun 5. maddesinde yer sağlayıcıların, sunulmasına veya yayınlanmasına yer sağladıkları içeriği kontrol etme veya hukuka aykırı bir eylemin var olup olmadığını araştırmakla yükümlü tutulmadıkları belirtilmiştir. Ancak 8 inci ve 9 uncu maddelerde belirtilen durumlarda hukuka aykırı olarak nitelenen içerikleri yayından çıkarmakla yükümlü tutulmuşlardır. Hosting hizmeti verdikleri kişi veya işletmelerin bilgilerini tutmakla görevlidirler ancak içerik konusunda muafiyet getirilmiştir. (5651 sylı Kanun Md.8-9)

Yer sağlayıcılar yer sağladıkları hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklama ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla da yükümlü tutulmuşlar, ayrıca tutulan bilgileri sınıflama, hak ve yükümlülükleri itibarıyla farklılaştırabileceklerdir. Ayrıca TİB Başkanlığınca talep edilen bilgileri talep edilen şekil doğrultusunda teslim etmek ve alınması bildirilen tedbirleri almakla da yükümlü tutulmuşlar, aksi davranışlar durumunda TİB tarafından on bin ila yüz bin Türk lirası arasında idari para cezası ile cezalandırılma ile karşı karşıya kalacaklardır (5651 sylı Kanun).

2.5.2 Erişim Sağlayıcı

Aynı kanun 2/e maddesinde düzenlenen erişim sağlayıcı; "İnternet ortamına erişim imkânı sağlayan her türlü gerçek veya tüzel kişiler" şeklinde tanımlanmış olup bu ifade de kanundaki diğer bazı tanımlar gibi, muğlak bir ifade olup açıklığa ihtiyacı vardır. Erişim sağlayıcı kavramıyla kanun koyucu: kullanıcıları internete bağlayan Türk Telekom, Superonline, Türksat, Millenicom, Turknet, Metronet, vb. yapıları kastetmiştir. WAP açısından bakıldığında bunlar, Avea, Turkcell, Vodafone, Bimcell, Pttcell, Pocell vb. olarak genişletmek mümkün olacaktır. Erişim sağlayıcılara getirilen yükümlülükler 6. maddede açıklanmıştır (5651 sylı Kanun Md.2/e).

2.5.3 İçerik Sağlayıcı

Aynı Kanun 2. (f) bendinde tanımlanırken, "İnternet ortamında kullanıcıların eriştiği her türlü bilgi veya veriyi sağlayan, üreten ve değiştiren tüzel veya gerçek kişiler" olarak belirtilmiştir. Burada kastedilen, internet site sahipleri veya yöneticileridir. İçerik sağlayıcılara getirilen sorumluluklar madde 4'de 3 fıkra halinde açıklanmış ve internet ortamında sundukları bütün içeriklerden sorumlu tutulmuşlardır. Burdaki ifadesiyle, site sahip veya yöneticileri sitelerinde blog, paylaşım, ilan, forum, yorum yazma gibi hizmetler sunmaları durumunda bunları da denetleme ve kontrol etmeleri bir zorunluluk olmaktadır. (5651 sylı Kanun Md.2/f)

Hiç şüphesiz ki, bu ortamlarda içerik üreten kullanıcılar gerçek kimliklerini çoğunlukla bırakmazlar. Bu nedenle; kullanıcı tarafından üretilen içerikler aktif olmadan önce site sahibi/yönetici veya admin kontrolünden geçirilmesi çözüm gibi gözükse de: TCK madde 20'de yer bulan cezalarda şahsilik genel kaidesine aykırılık oluşturduğu tartışılan bir konudur. Özellikle, kullanımı yaygın olan sosyal paylaşım ağları, blog, forum ve haber sitelerinde, okuyucu ve kullanıcının ürettiği her içeriği denetlemekle içerik sağlayıcıyı sorumlu tutmak, site yöneticilerinin ekran başına bağlanmasını gerektirir. Ayrıca sosyal paylaşım sitelerindeki beğenme veya haber sitelerindeki köşe yazarlarına ait makaleler ve haberlere yapılan yorumları denetime tabi tutma bir anlamda sansür, engelleme de fikir ve düşünce özgürlüğü önüne konan bir engel olarak tartışılan konulardandır.

Ancak yine içerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu olmayıp, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumlu olacağının belirtilmesi kötü niyetli kişiler açısından kullanılmaya açık bir boşluk alandır. Fason siteler oluşturarak, benimsediği içeriği ve kullanıcının ulaşmasını istediği söz konusu içeriklere sahip yasa dışı sitelere link vererek sorumlu tutulmamak mümkündür. Kanunda, benimseme ve amaçlamanın kriterleri belirtilmemiştir. Benimseme ve amaç açıkça belli ise genel hükümlere göre sorumluluk olacaktır. Ancak bir açıklama yapmadan ya da yorum katmadan amaçlanan sitelere link vermek kötüye kullanım için bir boşluk alan olarak karşımıza çıkmaktadır.

İçerik sağlayıcılarda Başkanlığın taleplerini istenen şekil ve doğrultuda yapmak, istenen bilgileri vermek ve istenen tedbirleri almakla sorumlu kılınmışlardır (5651 sylı Kanun Md.4/3).

2.5.4 Toplu Kullanım Sağlayıcılar

Aynı kanun 2. maddesi (i) bendinde, "Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım imkânı sağlayanları" toplu kullanım sağlayıcılar olarak tanımlanmıştır.

Toplu kullanım sağlayıcıların sorumlulukları, kanunun 7. maddesinde belirtilmiş olup bu faaliyet ticari amaçla yapılacaksa, mahallî mülkî amirden "Faaliyet İzin Belgesi" alınacaktır. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından TİB Kurumuna bildirilir. Denetimler mahallî mülkî amirlerce yaptırılacak olup, İzin belgesinin verilmesi ve denetime ilişkin esas ve usuller, yönetmelikle düzenlenmiştir (5651 sylı Kanun Md.7/1).

Ticari amaçla olup olmadığına bakılmaksızın internet kafeler, okul, eğitim kurumları, oteller, eğlence merkezleri, alış veriş merkezleri, hava alanları, terminaller, ulaşım araçları gibi bütün toplu internet kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlü olup ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür. Ticari amaçla toplu kullanım sağlayıcılarına, belirtilen yükümlülüklerin ihlalinden dolayı ihlalin ağırlığına göre yönetmelikle belirlenen çerçevede uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir (İnt. Kyn.16)

2.5.5 Erişimin Engellenmesi ve Yerine Getirilmesi

Yeterli şüphe sebebiyle hâkim kararıyla yayınlara erişimin engellenmesini gerektiren durumlar 8. maddede belirtilmiştir. Bu suçlar 5237 sayılı YTCK da yer alan; (Md. 228) Kumar oynanması için yer ve imkân sağlama, (Md. 227) Fuhuş, (Md. 226) Müstehcenlik, (Md. 194) Sağlık için tehlikeli madde temini, (Md. 190) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, (Md. 103, 1. fıkra) Çocukların cinsel istismarı ve (Md. 84) İntihara yönlendirme suçlarıyla 1951 tarihli 5816 sayılı Atatürk Aleyhine İşlenen Suçlar olarak sayılmıştır (5651 sylı Kanun Md.8/1).

Erişime engelleme kararı, soruşturma aşamasında sulh ceza hâkimi, kovuşturma aşamasında ise mahkemece verilecektir. Cumhuriyet savcıları ise gecikmesinde sakınca

bulunan hal durumu varsa erişime engelleme kararı verebilecekler ancak bu kararı yirmi dört saat içinde hâkimin onayına sunacak, Hâkim de en geç yirmi dört saat içinde karara bağlayıp eğer karar onaylanmamışsa tedbir, cumhuriyet savcısı tarafından derhal kaldırılacaktır. Eğer amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da erişimin engellenmesi kararı, verilebilir. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin kararlara itiraz yolu açıktır (5651 sylı Kanun Md.8/2).

Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararlarının birer örneği, gereği yapılmak üzere Başkanlığa gönderilecektir.

Birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği Çocukların cinsel istismarı (madde 103, birinci fıkra), Müstehcenlik (madde 226), Fuhuş (madde 227) suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re ’sen Başkanlık tarafından verilebilecektir. Bu karar için TİB Kurumu veya Başkanlık müracaat etme şartına bakmaksızın ve adli süreci tamamlamaksızın kendisi inisiyatif kullanacaktır. Bu karar, erişim sağlayıcısına bildirildiği andan itibaren kararın gereği, derhal ve en geç yirmi dört saat içinde yerine getirilecektir (5651 sylı Kanun Md.8/4).

Başkanlık tarafından erişimin engellenmesi kararına konu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulacaktır (5651 sylı Kanun Md.8/6).

Eğer Cumhuriyet Savcılığınca yapılacak soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilirse, erişimin engellenmesi kararı kendiliğinden hükümsüz kalacaktır. Bu durumda Cumhuriyet savcısı, kararın bir örneğini Başkanlığa gönderecektir. Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalacak, mahkemece beraat kararının bir örneği Başkanlığa gönderilecektir (5651 sylı Kanun Md.8/7).

Konusu birinci fıkrada sayılan suçları oluşturması nedeniyle başkanlıkça erişimi engellenen yayınlarda zararlı içerikler yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılacaktır. Başkanlığın idari tasarrufu ile içeriği engellenen bir yayın engellenme sonrası ancak yayıncının adli makamlara müracaat ederek engelleme kararını kaldırtmasıyla tekrar yayınlanabilecektir. Başkanlığın bu tasarrufunu adli süreçle tamamlama zorunluluğu getirilmemesi en büyük eksiklik olarak dikkat çekmektedir.

Koruma tedbiri olarak Başkanlıkça ve adli makamlarca verilen erişimin engellenmesi kararlarının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılacaktır (5651 sylı Kanun Md.10). Bu miktar 2014 yılı için 15.000 ila 100.000 lira gibi rakamlara tekabül etmektedir.

İdarî tedbir olarak Başkanlık veya TİB Kurumunca verilen erişimin engellenmesi kararının derhal veya 24 saate kadar yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilebileceği, İdarî para cezasının verildiği andan itibaren yirmi dört saat içinde kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilmesi (5651 sylı Kanun Md.11) Başkanlığın elinde yer sağlayıcılar ve içerik sağlayıcılar üzerinde Demokles'in kılıcı gibi kontrolsüz, denetimsiz ağır yaptırımlara sahip mutlak bir güç olarak konumlanmıştır.

14.3.2007 tarihli ve 5602 sayılı Şans Oyunları Hasılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3 üncü maddesinin birinci fıkrasının (ç) bendinde tanımlanan kurum ve kuruluşlar, kendi görev alanına giren suçların internet ortamında işlendiğini tespit etmeleri hâlinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilir ve bu kararları uygulanmak üzere TİB Başkanlığına gönderebilirler (5602 sylı Kanun Md.3).

5651'e göre zararlı içeriğin yayından çıkarılması, içeriğe erişimin engellenmesi kararları ve yapılan işlemlere itirazlar ile Cumhuriyet savcılarınca yapılacak trafik bilgisi taleplerine birden fazla sulh ceza mahkemesinin bulunduğu yerlerde Hâkimler ve Savcılar Yüksek Kurulu tarafından belirlenen ve görevlendirilen sulh ceza mahkemeleri yerine getirecektir (5651 sylı Kanun Md.15).

2.5.6 İçeriğin Yayından Çıkarılması ve Cevap Hakkı

5651'in 9. maddesin de; herhangi bir web sitesindeki içerikle hak ihlâline uğradığını iddia eden kişi, içerik sağlayıcıya yani site sahibi veya yöneticisine, buna ulaşamadığı takdirde hosting firmasına müracaat ederek: kendisiyle ilgili uygunsuz içeriğin yayından kaldırılmasını ve hazırlanan tekzip cevabını yayınlanan içerik süresi kadar veya bir hafta süre ile aynı ortamda yayınlanmasını isteyebilir. Yer sağlayıcıya ulaştırılan düzeltme metni en geç 24 saat içinde yerine getirilmelidir, yayınlanmazsa reddedilmiş sayılır (5651 sylı Kanun Md.9/1-2).

Yer sağlayıcının talebi reddetmesi halinde hak ihlali iddiasında bulunan kişi sulh ceza mahkemesine on beş günlük bir süre içinde başvurabilir, içeriğin yayından kaldırılmasını ve hazırladığı düzeltme metninin internet ortamında yayımlanmasını talep eder. Bu talep 24 saat içerisinde hâkim tarafından karara bağlanır. Hâkim kararına karşı itiraz hakkı genel hükümlere göredir (5651 sylı Kanun Md.6).

2.5.7 Yer Sağlayıcının Trafik Bilgilerini Saklama Yükümlülüğü

5651 sayılı Kanunun 5 inci maddesinde yer sağlayıcının yükümlülükleri düzenlenmiş, yer sağlayıcısı haberdar edildiği hukuka aykırı veya tedbire konu içerikleri yayından çıkarmakla yükümlü tutularak bu hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenen süre kadar saklayıp, bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuştur (5651 sylı kanun Md.5/3).

Yer sağlayıcılar ayrıca TİB Başkanlığınca talep edilen idari nitelikteki bilgileri talep edilen şekilde Başkanlığa teslim etmek ve Başkanlıkça bildirilen tedbirleri de almakla yükümlü tutulmuşlar aksi durumlarda ise Başkanlıkça on bin Türk Lirasından yüz bin Türk Lirasına kadar para cezasına muhatap olma ile karşı karşıya bırakılmışlardır. Tüm bu işlemler için gerekli donanım ve yazılımlar ile teknik altyapı da yer sağlayıcılar tarafından sağlanacaktır (5651 sylı kanun Md.5/5-6).

2.5.8 Yer Sağlayıcının DNS Değiştirerek İçeriklere Ulaşılmasını Engellemesi

5651 sayılı Kanunun 6 ncı maddesi birinci fıkrasında erişim sağlayıcı, içerik sağlayıcı ve yer sağlayıcılarına engelleme ve kısıtlama tedbirleriyle ilgili "Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla" hükmü getirilmiş (5651 sylı kanun Md.6/1-ç) bu kararla yasaklanan, erişimi kısıtlanması istenen tedbire konu içeriklerin her türlü yani sadece Türkiye'den değil yurtdışı sunucular üzerinden erişiminin de engellenmesi getirildiği, doğrudan içeriğin bulunduğu adrese URL' sinden veya dolaylı yollardan DNS değiştirerek erişim imkânlarının önlenmesi uygulanmaktadır.

2.5.9 Toplu Kullanım Sağlayıcıların Tedbir Alma Yükümlülüğü

5651 sayılı Kanunun 7.nci maddesinde düzenlenen Toplu Kullanım sağlayıcılar halk dilinde İnternet kafelerin ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında belirlenen tedbirleri almakla yükümlü tutulmuşlardır (5651 sylı kanun Md.7/2-3).

Bu düzenleme toplu kullanım hizmeti veren internet kafe, okul, yurtlar, alış veriş merkezleri, dinlenme tesisleri, oteller gibi kamu kurumu veya işletmelere ticari amaçlı olup olmadığına bakmaksızın ailenin ve çocukların korunması kapsamında yönetmelikle belirlenen tedbirleri almakla ve erişimle ilgili kayıtları tutmakla yükümlü kılmıştır. Denetim görevini Mülki amirlere vererek ihlallere bin ila on beş bin Türk

Lirası idari para cezası ile faaliyetten 3 güne kadar men cezaları uygulama tasarrufu vermiştir (İnt. Kyn.17).

2.5.10 Yayının Tümünün Engellenmemesi

5651 sayılı Kanunun 9 uncu maddesinde içeriğin yayından çıkarılması ve erişimin engellenmesi konusu düzenlenmiştir. Yayın içeriği nedeniyle kişilik hak ihlali iddiasında bulunan gerçek ve tüzel kişiler ile kurum ve kuruluşlar, yer sağlayıcısına veya içerik sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından kaldırılmasını isteyebilir veya doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilmektedirler (5651 sylı kanun Md.9/1).

İnternet ortamındaki yayın içeriğine bağlı kişilik haklarının ihlal edilmesini içeren talepler içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılması gerekmektedir. Aksi durumlar reddedildiği anlamını taşımaktadır. Yayın içeriği nedeniyle kişilik haklarının ihlal edilme talepleri doğrultusunda sulh ceza hâkimleri de erişimin engellenmesine karar verebilmektedir. Hâkim, vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik haklarının ihlalini içeren yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilecektir (5651 sylı kanun Md.9/4).

2.5.11 Özel Hayat İhlalinde TİB'e Başvurulması

5651 sayılı Kanunun 9/A maddesinde özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi amacıyla kişilere doğrudan TİB'e müracaat etme hakkı tanınmış olup, bu müracaatın içeriğinde yayının URL adresi, ihlale ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilerin olması gerekmektedir (5651 sylı kanun Md.9/1-2). Bu müracaat

TİB resmi web sitesi üzerinde oluşturulan ihbar formu aracılığıyla yapılacaktır (İnt. Kyn.18).

Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Başkanlık tarafından yapılacaktır. Burada belirtilen gecikmesinde sakınca bulunan haller ve kimlerin özel hayat gizliliğinin ihlali acil hallerden sayılacağı ve bireysel müracaat beklemeden doğrudan TİB Başkanı tasarrufu kullanılacağı belirlenmiş değildir. Bu nedenle TİB Başkanı tasarrufuna bırakılan geniş bir kavram karşımıza çıkmaktadır. Bu konu özellikle you tube ve twitter gibi uygulamaların kapatılmasıyla pek çok eleştirilere neden olmuştur (İnt. Kyn.19).

2.5.12 Trafik Bilgisi Talepleri

5651 sayılı Kanunun 2.nci maddesindeki (j) bendi 1 Mart 2014 Tarihli ve 28928 Sayılı Resmî Gazete 6527 Bazı Kanunlarda Değişiklik Yapılması Hakkındaki Kanunla yeniden değiştirilmiş, Trafik bilgisi tanımı detaylı olarak açıklanmış ve "*Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri"* olarak belirlenmiştir**.** Yine aynı Kanunun 3 üncü maddesine yeni bir fıkra daha eklenerek *Trafik bilgisi taleplerinin ancak bir suç soruşturması ve/veya kovuşturması kapsamında mahkemelerce talep edileceğini ve Başkanlık tarafından içerik sağlayıcı, yer sağlayıcı ve/veya erişim sağlayıcıdan alınarak verileceği* hükme bağlanmıştır (5651 sylı Kanun MD.2/j).

Engellemelerin Erişim Sağlayıcılar Birliğince uygulanması ancak bir suç soruşturması veya kavuşturması kapsamındaki talepleri ise ki bu adli birimlerin Cumhuriyet savcılıkları, kolluk ve mahkemelerin taleplerini TİB kontrolünde servis sağlayıcılardan alarak verilmesi esası getirilmesi bir anlamda adli birimlerin 5651 kapsamındaki bütün işlemlerini idari bir kurumun denetim ve bilgisine sunulması demektir. Oluşturulan yeni Birlik tüzel kişilik olarak 5.11.2008 tarih ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetki alan tüm internet servis sağlayıcılarıyla internet erişim hizmeti veren diğer işletmecilerin katılımıyla oluşuyor ve koordinasyonu sağlıyor, o zaman bu

kuruluşun tüm engelleme tedbirlerini uygulamakla görevlendirilmesi ancak trafik bilgisi taleplerinde tüm servis sağlayıcılar üyesi iken devre dışı bırakılması ve trafik bilgilerinin TİB'e aktarılması ve taleplerin TİB'e yapılması tezat olarak ortaya çıkmaktadır. Kanun yapıcının amaçları konusunda kamu yararı ve objektiflik ilkelerinden ziyade idari kurumlar aracılığıyla ben bileyim, benim haberim olsun, benim kontrolümde olsun refleksinin öne çıktığı görülmektedir. TİB tarafından doğrudan idari tasarrufla alınan verilerin soruşturma birimlerine verilme konusunda uzun yol ve prosedürlere bağlanması adli süreçlerin uzamasına neden olacağı açıktır.

2.5.13 Ulusal Siber Güvenlik Faaliyetleri

5651 sayılı Kanunun 10 uncu maddesinde TİB'e verilen idari görevlerin düzenlenmesinde dördüncü fıkranın (a) bendinde yer alan *"yayınları önlemeye"* ibaresinden sonra *" internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye"* ibaresi eklenmiştir.

Başkanlık, Bakanlık bünyesinde 26/9/2011 tarih ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümleri uyarınca oluşturulan İnternet Geliştirme Kurulunca internetin yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli kullanılması gibi konulara ilişkin yapılacak öneriler doğrultusunda gerekli her türlü tedbir veya kararları alma görevi verilmiştir (5651 sylı Kanun Md.10/5).

Ulusal siber tehditler gerekçe gösterilerek TİB'e ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesine yönelik içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlama, gerekli tedbirleri aldırma, bu doğrultuda faaliyet yürütme ve ihtiyaç duyulan çalışmaları yapma yetkisi ve tasarrufu verilmiştir (5651 sylı Kanun Md.10/6).

"Siber güvenlik" gerekçesini göstererek Başkanlık Redhack, Anonimous gibi hacker gruplar dışında tehdit listesine ekleyeceği istediği kişiler hakkında içerik sağlayıcısı, yer sağlayıcısı veya erişim sağlayıcısından istediği trafik bilgilerini elde etme ve tedbir

anlamında istediklerini de yaptırma imkanına sahip olması, bir anlamda idari tasarruflar için gösterilen adli süreçle işlemin tamamlanması prosedürünü anlamsızlaştırdığına dair pek çok eleştiriler yapılmıştır (İnt. Kyn.20).

2.6 Siber Suçlar Açısından Avrupa Konseyi Siber Suç Sözleşmesi

Teknolojik ve ekonomik dönüşüm içerisinde bilgi teknolojileri sistemlerinin kullanımının ceza hukukuna etkisi sadece ülkesel düzeyde düzenlemelerin konusu olmakla kalmamış aynı zamanda *Avrupa Konseyi Sibersuç Sözleşmesi'*nin de konusunu oluşturmuştur. Macaristan'ın başkenti Budapeşte'de 23. 11. 2001 tarihinde imzaya açılan 48 maddeden oluşan Sözleşme, 01.07. 2004 tarihinde yürürlüğe girmiş olup, Türkiye tarafından 10 Kasım 2010'da imzalanmıştır (Avrupa Konseyi Siber Suçlar Sözleşmesi 2001).

Sözleşmede, bir bilişim sistemi olarak bilgisayar ve internet sistemlerinin ceza hukukuna etkisi ve ortaya çıkardığı sorunlar, hem maddi ceza hukuku açısından hem de ceza yargılaması açısından ele alınmış ve bu alanlarda bilgisayar sistemlerinin kullanılması merkezinde ortaya çıkan sorunlara ilişkin çözümler getirilmek istenmiştir. Sözleşmenin ikinci kısmını oluşturan maddi ceza hukukuna ve ceza yargılamasına ilişkin sorunlar iki ana bölüme ayrılmış ve birinci bölümde maddi ceza hukukuna ilişkin düzenlemelere yer verilmiştir (Akıncı 2001).

İkinci bölümde ise, ceza yargılamasına ilişkin sorunlar ele alınarak özellikle delillerin elde edilmesi, korunması ve saklanmasına ilişkin olarak ortaya çıkan sorunlara çözüm getirilmek istenmiştir (Keskin 2002).

Bunun yanında, siber suçlar olarak adlandırılan suçların özellikle internet ve network ağları ile işlenmesinin yaygın bir hal alması ve internet kullanımının hızla yaygınlaşması, bu suçlara ilişkin sorunların ülkesel bir sorun olmaktan çok uluslararası bir sorun haline dönüşmesi gerçeğinden hareketle üçüncü bir bölüme yer verilmiştir. Bu bölümün konusu ise, Sözleşmeye taraf devletlerin suçla mücadelede adli birimleri arasında birbirleri ile yardımlaşmaları ve suçluların iadesidir. Sözleşmenin amaçları; 1.Siber suçlar alanında taraf ülkelerin ceza hukuku düzenlemelerini uyumlu hale

getirmek, 2. Bu suçların ve bilgisayar sistemi kullanılarak işlenen ya da delilleri elektronik formda olan başka suçların soruşturulması ve koğuşturulması için gerekli olan ulusal ceza muhakemesi hukuku yetkilerini belirlemek, 3. Hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmak" şeklinde sıralanmaktadır (Keskin 2002).

"İnternet Ortamında Ceza Sorumluluğunun Avrupa Ana İlkeleri" olarak adlandırdığı ilkeleri şu şekilde sıralamaktadır (Koca 2001):

a) Siber suçlarla ilgili ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce özgürlüğü olmak üzere tüm temel hak ve özgürlüklerin gereklerine uyulması;
b) Bilgisayarlarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde ortak minimum standarda uyulması;
c) Eylemin hukuka aykırı olması;
d) Eylemin kasten işlenmesi.

Sözleşmede belirtilen suçlarda ortak amaç, bu tür suçlara ilişkin olarak üye devletlerin ceza mevzuatlarında uyum sağlamadır. Sözleşmede yer alan suçlar, daha önceki dönemlerde çeşitli ülkelerin ceza mevzuatları içerisinde düzenlenmiş olan suçların uluslararası düzeyde ele alınması şeklinde olmuştur. Aşağıda bu suçlara genel olarak değinilecektir. Sözleşmenin ikinci kısmında *" Bilgisayar Veri ve Sistemlerinin Gizliliğine, bütünlüğüne ve Erişilebilirliğine karsı suçlar"* başlığı altında yetkisiz erişim (madde 2), yetkisiz müdahale (madde 3), verilere müdahale (madde 4), sisteme müdahale (madde 5) ve aygıtların kötüye kullanılması (madde 6) suçlarına yer verilmiştir (Avrupa Konseyi Siber Suçlar Sözleşmesi 2001).

Yetkisiz erişim (2. Madde), kasten ve hukuka aykırı bir şekilde bir bilgisayar sisteminin tamamına veya bir kısmına girme şeklinde tanımlanmıştır. Aynı maddede, yetkisiz erişim suçunun taraf devletlerin ceza mevzuatlarında düzenlenirken, güvenlik önlemlerinin ihlal edilmesi suretiyle işlenebileceğine, verinin elde edilmesi ya da diğer kötü bir niyetle sisteme girilmesi ya da bilgisayar ağları vasıtasıyla birbirine bağlı bilgisayar sistemleri aracılığıyla işlenebileceğine ilişkin ek unsurları getirebilecekleri belirtilmiştir (Koca 2001).

Yetkisiz müdahale 3. maddede düzenlenmiş olup buna göre, bilgisayar sisteminden elektromanyetik dalgalar yayılması da dâhil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, bunlara teknik yöntemler kullanılmak suretiyle müdahale edilmesinin suç haline getirilmesi öngörülmüştür. Bu maddeye göre, taraf devletlerin bu suçun oluşmasını kötü niyet ya da bilgisayar ağları aracılığıyla işlenmesi şartına bağlayabilmeleri mümkündür (Koca 2001).

Veriye müdahale (4. Madde) veriye zarar verilmesi, verinin bozulması, değiştirilmesi veya ortadan kaldırılmasının suç olarak düzenlenmesi gerekmektedir. Madde incelendiğinde, verinin bilgisayar içinde bulunması ya da herhangi bir saklama aygıtı içerisinde olması arasında fark yaratılmadığı görülmektedir. Aynı maddenin ikinci fıkrasında, taraf devletlerin söz konusu suçun gerçekleşmesi için ciddi zararın varlığı şartına yer verebilecekleri ifade edilmiştir (Koca 2001).

Sisteme müdahale (5. madde) sistemin işleyişinin ciddi olarak engellenmesinin suç haline getirilmesi gerektiği belirtilmiştir. Sistemin işleyişinin engellenmesine ilişkin müdahaleler ise sisteme veri yoluyla müdahale edilmesi ya da sistem içerisindeki verilere müdahale edilmesi esas alınarak düzenlenmiştir. Bu açıdan fiziki müdahaleler sözleşmede sistemin işleyişine müdahale kapsamında değerlendirilmemiştir (Koca 2001).

Sözleşmenin 6. maddesinde ise birtakım hazırlık hareketlerinin suç olarak düzenlenmesi yoluna gidildiği görülmektedir. Nitekim 6. maddenin 1. fıkrasına göre Sözleşmenin 2-5. maddelerinde düzenlenen suçların işlenmesi için öncelikli amacının söz konusu suçların işlenmesine yönelik tasarlanmış ya da uyarlanmış olan program da dâhil cihazların söz konusu suçların işlenmesi amacıyla, bir bilgisayarın tamamına ya da bir kısmına erişimi sağlayabilecek bir bilgisayar şifresinin, erişim kodunun ya da benzer verinin, üretiminin, satışının, kullanılmak için tedarikinin, ithal edilmesinin, dağıtılmasının ya da diğer şekilde erişilebilir kılınmasının taraf devletlerce suç olarak düzenlenmesi hükmüne yer verilmiştir. Aynı maddenin "b" bendinde, Sözleşmenin 2 ila 5. maddeleri arasında düzenlenen suçların işlenmesi amacıyla, "a" bendinde sayılan hususların elde bulundurulmasının suç olarak düzenlenmesi gerektiği ifade edilmiştir. Elde

bulundurmanın suç sayılabilmesi için taraf devletlerin yukarıda sayılanların belirli bir sayıda olmasına ilişkin ek şart getirebilecekleri hükmüne yer verilmiştir (Koca 2001).

Maddenin 2. fıkrasına göre yukarıda sayılan hükümler, bu tür aygıt ya da programların, bir bilgisayarın korunması ya da test amacı gibi Sözleşmenin 2 ila 5. maddelerinde belirtilen suçların işlenmesi amacını gütmeyen yasal amaçlar için üretimi, satışı, kullanılmak için tedariki, ithal edilmesi, dağıtılması ya da diğer şekilde erişilebilir kılınmasını cezalandıracak şekilde yorumlanamaz. Aynı maddenin son fıkrasında ise, bilgisayar şifreleri, erişim kodlarının ya da benzer verilerin satışının, dağıtımının ya da diğer şekillerde erişilebilir kılınmasının cezalandırılabilmesine ilişkin hükümler saklı tutulmak kaydıyla, taraf devletlerin ceza mevzuatları içerisinde birinci fıkrada düzenlenen hususları kapsam dışı bırakabileceği belirtilmiştir (Sokullu, Akıncı 2001).

Bilgisayar aracılığıyla sahtekârlık (madde 7), "verilerin açıkça okunabilir ya da anlaşılabilir olup olmadığına bakılmaksızın bilgisayar verilerinin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi ya da hareket edilmesi amacıyla verilerin orijinalliğinin bozulması sonucunu doğuran, bilgisayar verilerine yeni verilerin ilave edilmesi ve bilgisayar verilerinin değiştirilmesi, silinmesi veya erişilemez kılınması ve böylece orijinalinden farklı veriler meydana getirilerek, fiillerin hukuka aykırı olarak kasten işlenmesi" şeklinde tanımlanmıştır (Koca 2001).

Bilgisayar aracılığıyla dolandırıcılık (8. Madde), sistemin işleyişine ekonomik bir yarar sağlanması amacıyla müdahale edilmesi ve yarar sağlanması şeklinde tanımlanmış ve maddede sisteme yeni veri yerleştirilmesi, verinin değiştirilmesi, silinmesi veya erişilmez kılınması, bunların yanında sistemin işleyişine diğer herhangi bir müdahale seçimlik hareketler olarak düzenlenmiştir (Keskin 2002).

İçerikle ilgili suçlar (9.madde) başlığı altında çocuk pornografisinin yasaklanmasına ilişkin hükümler getirilmiştir. Bu kapsamda yasaklanan fiiller, bilgisayar sistemleri aracılığıyla dağıtmak amacıyla çocuk pornografisinin üretilmesi (m. 9/1.a), sunulması veya temin edilebilir hale getirilmesi (m. 9/1.b) ; dağıtılması ya da iletilmesi (m. 9/1.c); kendisi ya da başkası için bilgisayar sistemi aracılığıyla elde edilmesi (m.9/1.d); son

olarak, bilgisayar sistemi içerisinde ya da bilgisayar veri depolama ortamında çocuk pornografisi bulundurulmasıdır (m. 9/1.e). Maddede çocuk pornografisi, bir küçüğün cinsel içerikli bir eylemde kullanılması, küçük gibi görünen bir kişinin cinsel içerikli bir eylemde kullanılması ya da bir küçüğün cinsel içerikli bir eylemde yer aldığını temsil eden gerçekçi imaj olarak tanımlanmıştır. Maddeye göre, küçük 18 yasından küçükleri ifade etmekte, taraf devletlerin 16 yaşına kadar indirilebilmelerine imkân tanınmaktadır (Sokullu-Akıncı 2001).

10. maddede ise, telif hakları ve bağlantılı hakların korunmasına ilişkin uluslararası düzenlemelerde yer alan hükümlerin etkin bir şekilde uygulanabilmesi ve de ihlallerin cezalandırılabilmesine ilişkin cezai hükümlerin getirilmesi düzenlenmiştir. Sözleşme incelendiğinde, siber suçların kapsamının sadece bilgisayar ve veriye yönelik fiilleri esas almadığı bilgi teknolojileri sistemlerinin kullanılmasıyla ve özellikle internet kullanımının yaygınlaşması ile birlikte ortaya çıkan sorunları da kapsadığı görülmektedir. Bu açıdan çocuk pornografisi, telif haklarına ilişkin ihlaller ve son olarak Sözleşmeye yapılan ek protokolle kapsama alınan, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler de bu grubu oluşturmaktadır. Sözleşmede bu suçların minimum bir uzlaşmayı temsil ettiği ve taraf devletlerin kendi mevzuatlarında başka suçları da öngörebilecekleri belirtilmiştir (Sokullu-Akıncı 2001).

2.7 Siber Suçların Sınıflandırılması

Siber suçlar tanımına uyan suçların ve konuların sınıflandırılmasının ve tanımlamasının yapılması siber suçların daha rahat anlaşılmasını sağlayacaktır. Bur da suç türleri arasındaki ayrımda suçun işleniş amacı ana unsur olarak ele alınmalıdır. Bu tür suçlar hangi yöntemle işlenmiş olurlarsa olsunlar, hangi amaca hizmet ettiklerine bakmak gerekir. Siber suçlar kavramının tanımlanmasında görülen görüş ayrılıkları, siber suçların sınıflandırılmasında da görülmektedir.

Bu ayrılıkların temelinde yatan nedenler ise, siber suçların yeni bir suç tipi olması, bilgi teknolojilerinde yaşanan yeniliklerin yeni suç isleme yöntemlerini ortaya çıkarması ve bu yöntemlerin sürekli olarak nitelik ve şekil değiştirmesi nedeniyle ülke

mevzuatlarında yer almamış bir suç şekli olmasıdır. Kanunsuz suç ve ceza olmaz prensibinden hareketle vasıf değiştiren her yeni suç fiilinin hukuki metinlerde yer alması zaman almaktadır.

Siber/Bilişim alanındaki suç tiplerini incelerken Türk Ceza kanununda yer alan ve adli birimlerce en yoğun olarak karşılaşılan suçlar dikkate alınarak aşağıdaki belirtilen suç tipleri temel siber/bilişim suçları olarak açıklanmıştır.

2.7.1 Nitelikli Hırsızlık (YTCK. 142/1-E)

Hırsızlık suçunu, bilişim sistemlerini kullanmak suretiyle işlenmesidir. Suç işleyenin kastı, mağdurun banka hesabında bulunan para veya sair malvarlığı değerlerine sahip olabilmektir. Başka bir ifadeyle elde edilen veriden ziyade, bu verinin taşıdığı parayı alarak kazanç edinme amacındadır. Bunun içinde interneti aracı kılarak bankacılık hesaplarına ulaşması gereklidir.

2.7.2 Nitelikli Dolandırıcılık (YTCK. 158/1-F)

Dolandırıcılık suçunun; bilişim sistemlerini, banka veya kredi kurumlarını araç olarak kullanmak suretiyle işlenmesi (TCK 158/1-f), gerçek kişiye yönelik hileli davranışlarla, gerçek kişi olan mağdurun hataya düşürülmesi, kendisi veya bir başkası aleyhine, şüpheli veya üçüncü bir taraf lehine işlem yapmaya yöneltilerek sonucunda şüphelinin kendisine veya başkaları yararına haksız bir kazanç sağlaması eylemidir. Örneğin, sahibinden.com isimli internet sitesine araç satış ilanı veren ve kendisini arayan müştekiden, ön ödeme, cayma bedeli, aracın nakli için benzin parası isteyip aracı teslim etmeyen, satışı gerçekleştirmeyen failin eylemi bu suçu oluştur. Bir başka sık rastlanan örnek olarak internet üzerinden cep telefonu satın alan bir kişiye hiç cevabi ürün gelmemesi veya daha kıymetsiz farklı bir ürün gelmesi verilebilir.

2.7.3 Bilişim Sistemlerine Yönelik Suçlar

Bilişim sistemlerine yönelik suçlar iki başlık altında incelenmektedir.

2.7.3.1 Bilişim Sistemine Girme

Türk Ceza Kanunu 243. Maddesinde 1, 2 ve 3. fıkralarda düzenlenen bu suç, kişilerin kullandığı kişisel veya ticari e-postaların, üyelik hesaplarının bulunduğu bilişim sistemlerine girerek bir süre orada kalıp, bilgileri öğrenmek, veri trafiğini izlemek veya ele geçirmek suretiyle işlenir.

Burada, sistemde bir süre kalınmakta, ancak, herhangi bir veri kaybına, değişikliğine neden olma kastı bulunmamaktadır. Amaç bazen hedef güvenliği aşma, bazen göz atma, bazen veri trafiğini izleme, bazen de kıymetli görülen verilen alınması şeklinde olmaktadır.

2.7.3.2 Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

Bu suçta bir bilişim sisteminin işleyişinin engellenilmesi, bozulması, sistemdeki verilerin değiştirilmesi, erişilmez kılınması, bozulması, yok edilmesi, var olan verilerin başka yere transfer edilmesi, sisteme harici veri yerleştirilmesi gibi fiillerin işlenmesi suretiyle kendisine veya başkası yararına haksız maddi çıkar sağlanmasıdır (TCK 244/1-2-3-4).

2.7.4 Çocuk İstismarı/ Pornografi

Çocuğun cinsel yönden istismar edilmesi suretiyle elde edilen yazı, görüntü veya resimleri içeren ürünlerin bilişim sistemlerinin kullanılmak suretiyle depolanması, bulundurulması, ülkeye sokulması, satışa veya kiraya arz edilmesi, satılması veya bedelsiz olarak verilmesi, nakledilmesi, dağıtılması ile başkalarının kullanımına sunulmasıdır. Genel olarak çocuk pornografisi, 15 yaşını doldurmamış erkek ve kız çocukların cinsel istismarını amaçlayan müstehcen içerikli karton (çizgi) veya gerçek film sahneleri ile müstehcen resimlerden oluşan, hem Birleşmiş Milletler hem de Avrupa Konseyi Siber Suçlar Sözleşmesince yasaklanmış bulunan zararlı bir pornografi çeşididir. (TCK 103/1, 226/3)

Çocuk pornografisi bu Sözleşmede "cinsel olarak müstehcen kabul edilen bir eyleme reşit görünmeyen ya da reşit olmayan bir kişinin katılım görüntülerini gösterme" olarak tanımlamıştır (Avrupa Konseyi Siber Suçlar Sözleşmesi 2001).

Özellikle internet ortamının kontrolsüzlüğü ve her yerden erişilebilir olması bu alanı hızla pornografik yayınların yaygınlaşması için bir araç yapmış, bu kirli işlerle uğraşanlar için çocukları daha çok uygunsuz cinsel ilişkiye ve şiddete maruz bırakmalarına fırsat olmuştur. Yine siber suçlar veya internet suçları ile ilgili henüz düzenleme yapmayan veya yetersiz olan ülkelerdeki yayınlar bu alandaki mücadeleyi zorlaştırmaktadır.

2.7.5 Banka veya Kredi Kartlarının Kötüye Kullanılması (YTCK. 245/1-2-3)

Kendisine ait olmayan kredi veya banka kartını, hangi usul ve yöntemle olursa olsun elde eden veya bulunduran kimse, gerçek kart hamilinin veya kartın kendisine ulaştırılması gereken sahibinin bilgisi ve onayı olmadan bunu kullanması veya kullandırtarak kendine veya başkalarına yarar sağlaması (TCK. 245/1), bir kimsenin kendisine ait olmayan hesaplarla ilişkilendirilmiş banka veya kredi kartlarını sahte olarak üretmesi, satması, devretmesi, satın alması, satması veya kabul etmesidir (TCK. 245/2). Bir kimsenin, üzerinde sahtecilik yapılmış veya sahte oluşturulmuş kredi kartı veya banka kartları kullanma suretiyle şahsına veya başkasına kazanç sağlaması, bu suç kapsamındadır (TCK. 245/3).

Polis ve adli birimler tarafından tespit edilerek ortaya çıkarılmış ve adli işleme dönüşerek kayıtlara girmiş Banka veya Kredi Kartını Kötüye Kullanma Yöntemleri 'ne bakıldığında (Boğa 2011):

a) Alışveriş ya da ATM (Automatic Transfer Machine, nakit para çekim) cihazlarıyla işlemler esnasında manyetik kart kopyalama cihazları aracılığıyla bilgilerin toplanması,

b) Alışveriş ya da ATM cihazlarıyla yapılan işlemler sırasında kart bilgilerinin fiziki takiple elde edilmesi,

c) İnternet üzerinden online alışveriş sitelerinin kayıtlarını elde ederek, satın alma işlemi yapan kart hamillerinin spam mailler yoluyla kandırılması,

d) İnternet üzerindeki sohbet uygulamaları (Facebook, Messenger gibi) aracılığıyla kart bilgilerinin alınması,

e) ATM makinalarına harici düzenekler monte edilerek kullanıcının kart bilgisi ve şifresinin kopyalanması, alınması,

f) Kredi kartı ile ödeme yapma sırasında özel cihazlar kullanılmasıyla kopyalama yapılması,

g) Şube yapılanmasına sahip büyük mağazaların üyelik kartlarıyla daimi müşterilerine kolaylık ve avantaj sağlamak için depoladıkları müşteri kart bilgilerinin, hackleme veya çalışan suiistimali yoluyla üçüncü kişilerin eline geçmesi,

h) Art niyetli olarak kurulan internet satış sistemlerinde verilen hizmetler karşılığında yapılan ödemeler sırasında kart bilgilerinin elde edilmesi,

ı) Online satış hizmeti veren veya siteler üzerinden mal alış/satışı yapılan alışverişlerde, kullanıcılara ait kart bilgilerinin kaydedilmesi veya güvenlik önlemleri yetersizliği nedeniyle bilgilerin çalınması,

i) Akrabalık, arkadaşlık veya herhangi bir yakınlık sebebi ile kart bilgilerinin ele geçirilerek internet üzerinden mal siparişi verilmesi,

j) Aynı yakınlık ilişkileri sebebi ile pin numarası ele geçirilen banka veya kredi kartının fiziki olarak hırsızlanması ve sonrasında fiziken veya sanal olarak ATM makinelerinde veya internet sitelerinde kullanılması,

k) Sahte olarak oluşturulan web sayfalarına yönlendirme yapılarak, kredi kartı bilgilerinin elde edilmesi,

l) Pornografik içerikli sitelerden cüzi ücretler karşılığı hukuka aykırı içerik sunularak, kredi kartlarının ödeme vasıtası olarak kullanılması sırasında kart bilgilerinin ele geçirilmesi,

m) Bağış amaçlı sitelere cüzi ücretler bağışlanabilmesi için banka veya kredi kartı bilgisinin istenmesi sırasında, kart bilgilerinin ele geçirilmesi,

n) Müşteki tarafından unutulan banka kartının, bir sonraki ATM kullanıcısı tarafından kullanılarak menfaat temin edilmesi,

o) Özellikle yabancı turistlere yardım etme bahanesi ile yanaşıp, şifre bilgilerinin ele geçirilmesinden sonra, kartın el çabukluğu ile hırsızlanıp, makinede kaldığından bahisle müştekinin kandırılması ve sonrasında kartın aynı veya başka bir ATM makinesinde, üye işyerlerinde ya da sanal alışveriş siteleri ile sanal pos işlemlerinde kullanılması,

ö) ATM makinelerine kartın sıkışmasını sağlayan aparatlar takıp, şifre bilgilerini yanaşarak veya kamera vasıtasıyla takip edip, müştekinin ayrılmasından sonra kartı alıp, kullanmak suretiyle yarar sağlanması,

p) Arkadaşlık duygularının sömürülerek, müştekinin rızası ile belirli miktarda harcama yapılması amacıyla verilen kartların, müştekinin bilgisi ve rızası olmaksızın değişik miktarlarda alışveriş veya nakit çekim işlemleri yapılması suretiyle yarar sağlanması,

r) Müştekinin kimlik bilgileri kullanılarak, bankalardan sahte banka veya kredi kartı çıkartılıp, kullanılması,

s) Hack (korsan) yazılımları aracılığıyla, bankaların veya ticaret şirketlerinin kayıtlı tuttuğu kart bilgilerinin ele geçirilmesi,

ş) Bot Net yöntemiyle, yani, köleleştirilmiş bilgisayar ağı oluşturmak suretiyle, kart bilgilerinin öğrenilerek kullanılması olarak sayılabilir.

2.7.6 Sanal Kumar

TCK 228,de yerini bulan Örgütlü olarak, sanal ortam üzerinden, kredi kartı veya para yerine geçen elektronik ödeme sistemleri ile kumar onatma veya oynanmasına imkân sağlama suçudur. İnternet kullanımının yaygınlaşması oyun, eğlence amaçlı pek çok uygulamanın üretilmesiyle beraber şans ve beceriye dayanan bir makineye karşı veya sanal odalarda online kişiler birbirlerine karşı para veya benzeri maddi değerler karşılığı oyunlarda buluşmasını mümkün kılmıştır. "Online casino, online kumar, e-kumar" gibi kavramlarla ifade edilen bu tür oyunların bilişim ortamlarında gerçekleştirilmesidir (Boğa 2011).

2.7.7 Elektronik İmza İhlali

2004 yılında 5070 sayılı kanunla Elektronik İmza kullanımı başlatılarak hukukî yapısı, hizmet sağlayıcıların faaliyetleri ve hangi alanlarda elektronik imzanın kullanılacağı düzenlenmiş, bu düzenlenme sonrası elektronik imza kullanımı başlamış ve bütün kamu kurumları ile e-devlet kullanıcıları tarafından kullanımı yaygınlaşmaktadır (İnt. Kyn.21).

Elektronik imzanın oluşturulma amacına aykırı olarak imza sahibinin rızası dışında elektronik imza verisi oluşturma veya imza oluşturan cihazları elde etme, verme, kopyalama, bu cihazları yeniden oluşturma ile imza sahibinin bilgisi dışında elde edilen imza oluşturma cihazlarını kullanarak izinsiz elektronik imza oluşturulması (EİK md.16),Elektronik sertifikaları tamamen veya kısmen sahte oluşturarak veya geçerli olarak oluşturulan elektronik sertifikaları tahrif etme veya taklit ile bu elektronik sertifikaların bilerek kullanılmasıdır (EİK md.17),

2.7.8 Bilgi Güvenliği Yükümlülüğüne Muhalefet

Bir meslek veya ticari faaliyet nedeniyle elde edilen mesleki ya da ticari sırların, kişiye özel verilerin veya değer taşıyan diğer bilgilerin şahsına veya başkalarına çıkar sağlama ya da zarar oluşturmak saikiyle üye işyerlerinin kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan amaç dışı kullanımı, satılması veya gizliliğin deşifre edilmesidir. (BKK md. 23,39)

Müşteri bilgileri, üyelik bilgileri, hasta bilgileri gibi alışveriş merkezleri, elektrik, su, doğalgaz abonelik servisleri, sağlık merkezleri, banka, devlet kurumları gibi kuruluşlarda tutulan her türlü kimlik, sürücü belgesi, araç tescil, adres, telefon, gayrimenkul kayıtları gibi kişiye özel bilgilerin kendisine veya başkalarına menfaat sağlamak veya zarar oluşturmak amacıyla kişilerin bilgileri dışında izinsiz kullanımıdır (Tulum 2006).

En basitinden son zamanlarda insanların en çok şikâyet ettiği reklam, kampanya, bilgilendirme, tanıtım ve dolandırıcılık amaçlı cep telefonlarına gönderilen mesajlar için kişilerin cep telefon numaralarının belirtilen yerlerden elde edilmesi gibi. Yine en çok adli vakaya dönüşen GSM şirket bayi ve şubelerince abone alımlarında kişilerin kimlik belgelerinin dijital kopyaları alınarak bir üst bayiye gönderme işleminden sonra imha edilmesi gerekirken biriktirilmesi, oluşturulan dijital arşivlerin bedeller karşılığı dolandırıcılık yapan şahıs veya firmalara verilmesidir. Bu yolla kişilerin adına pek çok hat açılmasından kredi kartı çıkartılmasına, hayali şirketler kurulmasına, krediler alınmasına kadar kişilerin özel verileri rızaları dışında kullanılmak suretiyle hem haksız kazançlar elde edilmiş hem de kimlik bilgileri kullanılan kişiler adına çok büyük mağduriyetler yaşandığı kayıtlara geçmiştir (İnt. Kyn.22).

2.7.9 Haberleşmenin Engellenmesi

Bilişim sistemlerini kullanmak suretiyle kişiler (TCK 124/1), kamu kurumları arasındaki haberleşmeyi (TCK 124/2) her türlü basın ve yayın organı yayınlarını hukuken suç sayılan yollarla engelleme fiilleridir (TCK 124/3).

2.7.10 Ekonomi Sanayi ve Ticarete Karşı İşlenen Suçlar

Bilişim sistemlerini kullanmak suretiyle yapmakta olduğu meslek, sıfat, konum veya görev gereği öğrendiği veya erişebildiği ticari sır, müşteri sırrı veya bankacılık sırrı niteliğindeki özel bilgi, belge, fenni keşif ve buluşlar veya sınai uygulamalarla ilgili bilgileri, yetkisiz ve ilgisiz taraflara verme, ifşa etme, bu belge veya bilgileri, hukuka aykırı yollarla elde etme fiilleridir (TCK 239 /1-2).

Bu kapsamda 556 sayılı Markaların Korunması Hakkında Kanun ve 551 sayılı Patent Haklarının Korunması Hakkında Kanun Hükmünde Kararnameye aykırılık teşkil eden suçlar ile 554 Sayılı Endüstriyel Tasarımların Korunması Hakkında Kanun Hükmünde Kararnameye aykırılık teşkil eden suçları içermektedir.

Kanuni olmayan bir maddi kazanç sağlamak ya da ekonomik kayıp vermek amacıyla yetkisi ya da herhangi bir kanuni dayanağı olmaksızın bilişim sistemlerini aracı kullanarak ticari bir sırrın elde edilmesi, transferi, ifşa edilmesi ya da kullanımıdır.
Ticari sırların çalınması, endüstriyel casusluk olarak da tanımlanmaktadır (EGM Bilişim Suçları Çalışma Raporu 2006).

2.7.11 Özel Hayata ve Gizliliğine Karşı İşlenen Suçlar

Kişiler arasındaki haberleşme, haberleşme içeriğinin kaydı, tarafların rızası dışında ifşası, kişilerin kullandığı bilişim sistemlerine izinsiz giriş yapılarak kişiye özel iletişimlerin tespiti, kaydı, aleni olmayan bir ortamdaki söyleşiyi diğer konuşanlardan habersiz ve onay almadan kayda alınması, bu bilgileri kullanarak kişisel yarar sağlama veya başkalarına yayma, yine bilişim teknolojileri kullanarak kişinin özel hayatına

ilişkin resim, görüntü veya seslerin kayda alınarak gizliliğin ihlal edilmesi, yine bu verilerin bilişim sistemleri aracılığıyla ifşası, teşhiri veya dağıtılarak farklı amaçlar için kullanılması bu kapsamda değerlendirilen eylemlerdir (TCK 132-137).

2.7.12 Devlet Sırlarına Karşı Suçlar (Siber Casusluk)

Yetkili makam ve kanunlarca devlet sırrı sayılan, bu kapsamda değerlendirilen, görev gereğiyle öğrenilmiş olsa bile görev bitimi dahil, açıklanması, kendisi veya başka amaçlar doğrultusunda paylaşılması, devletin siyasal ve askeri güvenliği bakımından sakınca oluşturacak her türlü bilgi, belge, teknik buluş, sınai üretim gibi verilerin bulunduğu yerlere bilişim sistemleri aracılığıyla izinsiz girilmesi, verilerin elde edilmesi, kopyalanması, yeni veri yüklenmesi, paylaşılması, başka yerlere transfer edilmesi gibi eylemlerdir. Bu faaliyetler bireysel çıkarlar için olabileceği gibi siyasal veya askeri casusluk amacıyla da yapılabilmektedir (TCK 326-337).

2.7.13 Fikir ve Sanat Eserleri Kanununa Aykırılık Teşkil Eden Suçlar

5846 sayılı Fikir ve Sanat Eserleri Kanununa aykırılık teşkil eden suçları iki başlık altında incelemek uygun olacaktır.

2.7.13.1 Manevi, Mali veya Bağlantılı Haklara Tecavüz

Bu kapsamda bir eserin, icranın, fonogramın veya yapımı hak sahibi kişinin yazılı izni olmaksızın bilişim sistemleri kullanılarak çoğaltılması, değiştirilmesi, dağıtılması, depolanması, yayınlanması, satışa arz edilmesi, ayrıca kaynak göstermeksizin bir eserden iktibasta bulunulması veya yetersiz yanlış aldatıcı kaynak gösterilmesi, başkasına ait eserlere kendi adının koyulması, alenileşmeyen bir eser muhteviyatı ile ilgili açıklamalar yapılması ve bu işlemleri ünlü kişilerin isimlerini kullanarak yapılmasıdır (Boğa 2011).

2.7.13.2 Koruyucu Programları Etkisiz Kılmaya Yönelik Hareketler

Bilgisayar veya türevi işlemcili cihazlarda kullanılmak üzere üretici firma veya kişiler tarafından üretilen, telif hakları ulusal ve uluslararası sözleşmeler ve yasalarla koruma altında olan yazılım ürünlerinin izinsiz ve yetkisiz kullanımı, çoğaltılması, kopyalanması, yayılması ve ticari amaçlı olarak kullanımı suç sayılmıştır (FSEK md.72).

Hacking, Cracking ve Warez Amaçlı Sitelerin Oluşturulması, bilgisayar yazılımlarının ve bu tür programların erişime açık bulundurulması sayılabilir (Canbek 2005).

2.7.14 Propaganda, Kanundışı Yayınlar ve Terörist Faaliyetler

Ucuz ve etkili olan propaganda en kolay ve en çabuk ulaşılabilir olan web aracılığıyla içeriğinin ne olduğu, gerçekliği, doğruluğu yürürlükteki hukuki mevzuata aykırılığı, yasaklanmış veya erişimi engellenmiş yayınlardan olup olmadığına bakılmadan dünyaya veya özel hedeflere saniyelerle metin, resim, elektronik posta gibi dijital veriler şeklinde dağıtılması, yayınlanması veya saklanması veya erişime açılmasıdır (Geers 2008).

Ulusal veya uluslararası hukuk tarafından terör örgütü olarak kabul edilmiş grupların örgütsel propagandalarını, örgüt içi haberleşmelerini, sempatizan kazanma, toplumda korku ve infial oluşturma gayretlerini, eylem amaçlarını başkalarına duyurma çabalarını ve benzeri örgütsel faaliyetlerini yaymak için kullandıkları elektronik postalar ve dokümanlar ile yönettikleri web siteleri terör faaliyeti kapsamında değerlendirilmektedir (Tulum 2006).

Terör örgütlerinin internet öncesi dergi, broşür, kitap, gazete, doküman ve el ilanları ile yaptıkları, gelir elde etme, örgüte yardım toplama, örgütün aldığı kararları ve izleyeceği stratejileri yayınlama, sempatizan toplama, topluma nifak sokarak bölücülük yapma ve bunun propagandalarını gerçekleştirme, meşru devlet faaliyetlerini kötüleme, aşağılama, örgütsel eylemleri yönlendirme, örgüt amaçları için toplumsal olayları manipüle etme,

şiddet ve sokak hareketlerini tahrik ve teşvik etme, sempatizan tabanını genişletmeye çalışma gibi eylemlerini internet ortamlarına taşımışlardır (Boğa 2011).

Terör örgütleri bilişim sistemlerinin yıkıcı gücünü de kullanarak özellikle devletin güvenlik kurumlarının veya endüstriyel şirketlerin bilişim sistemlerine sızma çalışmaları yapmaya çalışmakta ve bu şekilde sistemleri işlemez hale getirerek ulusal eyleme dönüştürmeye çalışmaktadırlar (Tulum 2006).

2.8 Siber Suç Tehdit ve İşleme Yöntemleri

Siber suçları klasik suç tiplerinden ayıran ve farklı bir kategori altında incelenmesine neden olan en belirgin özellik suçun işlenme şekillerindeki farklılıklardır. Klasik suç olarak tanımlanan adam öldürme, yaralama, dolandırıcılık, sahtecilik, hırsızlık, tehdit, hakaret v.b. gibi suçlarda suçun maddi unsurunu oluşturan eylemler faillerin bedeni hareketleri sonucu oluşmaktadır. Siber suçlarda ise fail bir bilgisayar ve internet ağı kullanarak herhangi bir mekânda suçu işleyebilmekte ve suçun neticesinde çok büyük zararlar oluşabilmektedir (Dülger 2004).

Siber suçları diğer suçlardan ayıran bir diğer özellik ise ileri bilgi teknolojileri ürünlerin kullanılması ve bu teknoloji sistemlerini kullanırken de bilgi birikimi ve beceri gerektirmesidir. Bu unsur, siber suçları işleyen kişilerin teknoloji bilgisine ya da eğitim seviyesine sahip olması gerekliliğini zorunlu kılmaktadır.

Siber suçların önemli bir başka özelliği de işlenme şekillerinin yapısı itibariyle genellikle çok kısa bir zaman dilimi içinde oluşmaları ve arkalarında bulunması çok zor, silik ipuçları bırakmalarıdır. Bu nedenle bu suçları ortaya çıkaracak izlerin tespit edilmesi zor olmakta, suçun işlendiği tespit edildikten sonra fail ya da faillere ulaşmak ise daha da zor olmakta, ya da mümkün olmamaktadır. Siber suçların işlenmesinde klasik suçlardaki gibi fiziksel bir eylem olmasa da bilişim sistemlerinin soyut unsuru olan veriler üzerinde suç oluşturan işlemlerin gerçekleştirilebilmesi için özel yazılımların kullanılması ya da özel tekniklerin kullanılması gerekmektedir (Dülger 2004).

2.8.1 Truva Atı

Tarihteki Truva atı bir hediye görüntüsüyle Troya kentini ele geçiren Yunanlı askerleri taşıdığı gibi; bugünde Truva atı olarak nitelenen faydalı yazılımlar gibi görünen bilgisayar programlarıdır, ancak habersizce güvenliğimizi riske atar ve birçok zarara yol açarlar. Truva atları, kullanıcıların güvenilir bir kaynaktan geldiği düşüncesiyle bir programı açması yoluyla yayılır (İnt. Kyn.23).

Sisteme kendini yerleştiren bir Truva atı kendisini sisteme yükleyip sistemdeki ağların aralarındaki açıkları kullanarak, yazılımı üreten tarafa bilgi sızdırır veya onun istekleri doğrultusunda hareket eder. Truva atlarını iki kısma ayırmak uygundur. Birinci kısım bulaştığı sistemde çalışan sunucu, ikinci kısım ise yazılım üreticinin bilgisayarında çalışan istemcidir. Hedefteki bilgisayara yerleşen sunucu programın boyutu küçük olup, başka programlara yama şeklinde de eklenebilir. Tespit edilmesi güçtür. Sistemin çalışmasıyla aktif olur ve fırsat buldukça ağ üzerinden gerekli bilgileri gönderir (Boğa 2011).

Truva atları, virüsler gibi bir taşıyıcı program ile sisteme gelirler; ancak virüsler ile farkları, herhangi bir programa kendilerini eklemek gibi bir yetenekleri olmamasıdır. Taşıyıcıları özel olarak tasarlanmıştır. Truva atı içeren programlar genellikle internet üzerinden dağıtılan shareware ve freeware lisanslı programlardır. Yine e-posta aracılığı ile insanların birbirlerine gönderdiği animasyonlar ve şakalar da taşıyıcı olabilirler. Bu programlardan herhangi biri kullanıcı tarafından çalıştırıldığı anda, truva atı, geri planda çalışıp yöneticisinin bağlanmasını bekleyecek (ya da yöneticisine bağlanacak), programı sisteme yükleyecek, her yeniden açılışta çalıştırılmasını sağlayacaktır. Bu arada bir şüphe çekmemesi için taşıyıcı program da çalışacak, yapması gerekeni (animasyon gösterme, vaat edilen işi yapan bir program gibi çalışma, vb.) yapacaktır. Truva atları sistem dosyalarına benzer isimler kullanacak, eğer işletim sistemi izin veriyorsa çalışan süreçler listesinde görünmeyecek, böyle bir şansı yoksa da bir sistem servisi ismi ile çalışarak fark edilmemeye çalışacaktır (Alaca 2008).

Üretilen Truva atı programlarının istemci bilgisayar komutlarıyla farklı işlemler yapması mümkündür.

2.8.2 Bilgisayar Virüsleri

Bir bilgisayar kodu parçası olan Virüsler, kendini bir dosyaya veya bir programa iliştirerek bilgisayardan bilgisayara atlayabilme özelliğindedir. Bulaşma yeni bilgisayarlara atladıkça yayılır. Virüsler bulaştıkları bilişim sistemlerinde sistemdeki dosyalara en fazla zarar oluşturacak, donanımları ve yazılımları çökertecek şekilde tasarlanmış kodlardır (Boğa 2011).

Bilgisayar virüslerinin yerleşmesi bir dosyaya ya da yazılıma fark edilmeyecek şekilde başlar ve sonrasında kendilerini çoğaltarak kopyalarlar. Sonuç olarak da veri depolama birimleri başta olmak üzere sistemleri çalışamaz hale getirir.

2.8.2.1 Boot Virüsleri

Sabit disklerin veya işlemcilerin "boot" sektörlerine yerleşerek sistemin açılışı ile ilk olarak RAM bellekte bulunan komutları çalıştırırlar. Boot sektöründen yüklenen programın komut akışını değiştiren Boot virüsleri kendisini de yüklemeye devam etmektedir. Ping Pong, Crazy Boot, Brain gibi virüsler örnekler arasında sayılabilir (Taş 2010).

2.8.2.2 Makro Virüsleri

Makro özelliği, bazı işlerin otomatik yapılmasını sağlayan yardımcı programlama dilidir. Makro Virüsleri Microsoft Office uygulamalarında başta Excel, Word gibi makro çalıştırma özelliği bulunan dosyalara bulaşmaktadırlar. Bu virüslerin bozduğu dosyalar sadece makro dili ile yazılmış dosyalar olmaktadır (Taş 2010).

Makro virüsler, yerleştiği excel ya da word dokümanları kullanılırken aktifleşirler. W97M/Ethan, W97M/Class virüsleri örnek olarak söylenebilir.

2.8.2.3 Dosya Virüsleri

Dosya virüsleri com, bat, exe, sys, drv, bin, ovl, ovy uzantılı olup çalıştırılabilir dosyalara bulaşmakta, kendilerini işlemcilerin RAM belleğine yerleştirerek dosya çalıştırılınca da devreye girmektedirler. Virüs işlemci faal olduğu müddetçe hafızada kalır ve çalıştırılan her uygulamaya, programa kendisini bulaştırır. Walker, Disk Killer, Joker, Randex, Meve ve MrKlunky gibi virüsler örnek dosya virüslerindendir (Taş 2010).

2.8.3 Ağ Solucanları

Solucanlar da, virüsler gibi kendilerini bir işlemciden diğer işlemciye kopyalamak için tasarlanmış olan ve kendiliğinden bunu gerçekleştiren yazılımlardır. Sisteme girdikten sonra kendi başına ilerleyen Solucanlar öncelikle bilgisayarda bilgi veya dosya ileten özelliklerin denetimini ele geçirirler. Kendilerini büyük sayılarda çoğaltma becerileri Solucanların en büyük tehlikelerindendir. Oluşan yoğun ağ trafiği domino etkisi göstererek işyeri ağ akışını ve internet bağlantı hızını yavaşlatabilir, işlemci belleğini ve ağ bant genişliğini tüketerek bilgisayarın çökmesine veya sistemin kilitlenmesine yol açabilir (İnt. Kyn.24).

Ortaya ilk çıktıklarında solucanların yayılımı çok hızlıdır. Genellikle internetteki web sayfaları görüntülenirken uzun süre donmalara ve ağların kilitlenmesine yol açarlar. Bir alt sınıf virüs olan Solucan, kendisinin tam kopyalarını ağlardan başka ağlara dağıtarak kullanıcı eylemi olmaksızın yayılır. Yayılmak dosyaya veya taşıyıcı bir programa gereksinim duymayan Solucanlar kullanıcı hareketlerine ihtiyaç duymadan sistemde bir kapı açıp, bilgisayarın denetimini başka birinin uzaktan eline geçirmesini sağlayabilir (İnt. Kyn.25)

2.8.4 Salam Tekniği (Salami Techniques)

Bu yöntem, bankalarda genellikle yaygın olarak işlenen bir metodudur. Bu yöntemin işleyişinde hesaplardaki nakit varlıkların virgülden sonrası küsuratlar fail tarafından

farklı bir hesaba aktarılarak biriktirilmektedir. Hesaplardaki bu küçük miktar hareketler banka çalışanları ve hesap sahipleri tarafından fark edilmesi güçtür ancak biriken bu küçük miktarlar faillere büyük kazançlar sağlamaktadır (Dülger 2004).

Bu yöntemle işlenen suçlarda genellikle kullanılan programlar Truva atı veya benzeri işleve sahip yazılımlar olmaktadır.

2.8.5 Sistem Güvenliğinin Kırılıp İçeri Girilmesi (Hacking)

Siber korsanlar bugünün en yaygın bilgi iletim ağı olan internet üzerinden eylem gerçekleştirecekleri bilişim sistemine girmektedirler. Bu girişi genellikle bilişim sisteminin işletim yazılımını yazan kişilerin gerektiğinde yazılımı ve dolayısıyla sistemi korumak amacıyla bıraktıkları açık kapıları bularak buradan sızmak yoluyla gerçekleştirirler. Bir kere giriş sağlandıktan sonra siber korsan fark edilene kadar sistem içinde dilediği bilgiye ulaşabilmekte ve sistemin işleyişine ait her türlü etkide bulunabilmektedir (Alaca 2008).

Bilişim sisteminin güvenliğinin kırılıp girilmesi eylemini diğer suç işleme şekillerinden ayıran en önemli özellik ise genellikle sisteme giriş sırasında yardımcı yazılımlar kullanılmaması ve eylemin bizzat siber korsan tarafından gerçekleştirilmesidir. Kimi hallerde güvenlik kodlarının çözülmesi için olasılık ve birleşim hesaplarını hızla yapan yardımcı yazılımlar kullanılsa da sistem içinde gezinme ve verileri ele geçirme eylemleri bilişim korsanının kendisi tarafından yapılmaktadır. Hacking ihlalinde aktif rolü oynayan baş aktör siber korsandır (İnt. Kyn.26).

2.8.6 Mantık Bombaları

Mantık bombaları olarak adlandırılan yazılımlar sisteme giriş yaptıktan sonra istenen şartlar hazır oluşuncaya kadar uykuda kalan, yararlı bir program gibi davranarak zararlı bir davranış sergilemeyen ancak şartlar oluştuğunda harekete geçerek aktifleşen ve sistem için yıkıcı etki yapan programlardır. 26 Nisan 1999'a tarih ayarlı olarak ortaya çıkan Çernobil virüsü örnek verilebilir (İnt. Kyn.27).

2.8.7 Hukuka Aykırı İçerik Sunulması

Burada ulusal ve uluslararası hukuk tarafından suç kabul edilen; şiddeti teşvik etme, nefreti körükleme, ayrımcılık, ırkçılık, kişilik haklarına tecavüz, çocuk pornografisi ve insan ticareti gibi konularda içeriğe sahip sitelerin veya veri arşivlerinin internet kullanıcılarının erişimine açık bulundurulmasıdır (İnt. Kyn.28).

Hukuka aykırı içerik sunumu, dosya paylaşımı, elektronik postalar, forumlar, web sayfaları ve link yönlendirmeleri aracılığı ile gerçekleştirilmektedir.

2.8.8 Veri Aldatmacası (Data Diddling)

Bu yöntemde veri arşivleyen sistemlere veri girişleri yapılırken girilen verilerin yanlış olması ya da girilmiş verilerin sonradan değiştirilmesi şeklinde uygulanan yaygın, güvenli ve basit bir siber suç tekniğidir.

Veri aldatmacası yönteminde kullanılan usullere bakarsak; dijital ortamda saklanan verilere özel araçlar aracılığıyla yeni eklemelerin yapılması, mevcut verilerin bir kısmının veya tamamının silinmesi, mevcut dokümanların tahrif edilmesi ile kontrol sistemlerinin bypass edilmesi sayılabilir. Bu suçu işleyenler genelde verilerin kayıt aşamasından, nakil, kontrol ve şifreleme sürecinde görev alan kişiler olmaktadır ancak ağ üzerinden erişime açık sistemlere güvenlik sistemleri aşılarak erişme ve harici müdahalelerle aynı fiillerin yapılması mümkündür (Beyhan 2002, Değirmenci 2002).

2.8.9 İstem Dışı Alınan E- Postalar (Spam)

SPAM maili en yalın haliyle istek dışında gönderilen reklam içerikli mailler olarak tanımlayabiliriz. İnternet üzerinde bir mesajın aynı anda yüzbinlerce e-posta hesabına istem dışı olarak gönderilmesidir.

İnternet kullanıcıları açısından iki tip SPAM vardır. E-mail aracılığıyla gönderilen SPAM ticari reklam amaçlı olup, yarı yasal servislerin duyurularak güvenilirliği tescil edilmemiş ürünlerin bu tür reklamlarla pazarlanması amacına yöneliktir.

İkinci tür SPAM da ise, ticari amacı ön planda olmayan içerikteki talep edilmeyen kitlesel e-postaların (Unsolicited Bulk e-mail), aynı anda milyonlarca e-posta hesabına gönderilen iletileridir. Bu iletiler bir konu hakkında kamuoyu oluşturmak amaçlı olabileceği gibi, politik bir görüşün propagandası içerikli ya da ticari amaçla gönderilen iletiler de olabilir. SPAM la ilgili önemli olan nokta, bir mailin SPAM olarak nitelendirilmesinde kullanılan ölçütte ileti içeriğinin hiç önemli olmamasıdır. Üzerinde fikir birliği oluşan bir nokta da, toplumsal duyarlılık içeren bir konuyla ilgili görüş toplamak için kitlesel olarak gönderilen iletilerde SPAM olarak nitelendirilmektedir (İnt. Kyn.29).

Spam olarak nitelendirilen elektronik postaları gönderenlere "spammer" denilmektedir. Elektronik postaları toplamak için kullanılan pek çok yöntem vardır, E-mail SPAM listeleri genellikle Google sayfalarının taranması, tartışma gruplarının üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur. Bunların ortak noktası web üzerindeki açık kaynakların taranmasıdır (İnt. Kyn.30)

2.8.10 Çöpe Dalma (Scavenging)

"Atık toplama" veya "Çöplenme" olarak da adlandırılan bu yöntemde, bilişim sistemlerinde gerçekleştirilen işlemler sonrasında artakalan bilgilerin toplanmasıdır. Bu bilgilerin toplanması bilişim sistemlerinin parçalarını oluşturan birimler üzerinde bellekteki var olan veya silinmiş verilerin dönüştürülmesi, yazıcı (printer) gibi çıktı alınan birimlerin belleklerinde kalan verilerin alınması, veya eski tip şeritler üzerindeki izler veya atık çıktı ürünleri kağıt gibi üzerindeki bilgilerin derlenmesi gibi yöntemlerle yapılabilmektedir (Yazıcıoğlu 1997).

Çıktı ürünleri üzerinden bilgi elde etme yöntemi fazla bir bilgiye ve teknolojiye ihtiyaç duyulmadan uygulanabilir olmasına rağmen, silinmiş verilerin geri getirilmesi bilişim sistemleri hakkında teknik ve programlama bilgisine ihtiyaç duyar (Değirmenci 2002).

Bilgisayarlar üzerinde çalışılmış bir dosyayı silmek aslında gerçekten o dosyayı tamamen yok etmek anlamına gelmemektedir. Yapılan sadece bellekte adres tablosundan (File Directory Table) arşivdeki ulaşım yolunun silinmesidir. Gerçekte işlemciler üzerindeki dosyaların silinmesi ancak aynı dosya üzerine en az eski veri büyüklüğünde yeni verilerin yazılmasıyla mümkün olacaktır. Bu yanlış bilinme nedeniyle silindiği düşünülen pek çok veri manyetik hasara uğramamış diskler için N-case, FTK, Winhex gibi özel yazılım programları aracılığı ile yeniden geri dönüştürülmesi mümkündür (Değirmenci 2002).

2.8.11 Gizli Dinleme (Eavesdropping-Sniffing)

Gizli dinleme, bilgi teknolojileri ürünlerinin veri taşıma aracı internet ağlarına doğrudan girilerek veya fiber akıştaki manyetik dalgaların vakumlanması şeklinde verilerin elde edilmesidir. İstihbarat örgütlerince sıkça kullanıldığı iddia edilir ve varsayılır. Özellikle NSA faaliyetleri nedeniyle ABD bu konuda sıkça eleştirilmektedir (İnt. Kyn.31).

Bu yöntemle veri elde etmeler arasında; ağ üzerinde akan verilerin fiziksel bağlantı ile elde edilmesi, bilişim sistem merkezlerine elektromanyetik dalgaları yakalayabilen radyo vericileri yerleştirilmesi, monitörlerce yayılan elektromanyetik dalgalar yakalanarak tekrar ekran görüntüsüne dönüştürülebilmesi, araya konulan yükselticiler vasıtasıyla elektromanyetik dalgaların çok uzaklardan yakalanması, fiber ağlardan akan verilerin vakumlanarak tasnif edilmesi gibi yöntemler sayılabilir (Değirmenci 2002).

Sniffer (yakalama) yazılımları vasıtasıyla ağda oluşan datalar gizlice toplanarak gerekli yerlere iletilirler. Snifferler ağ üzerinde iletilen dataları yakalamak suretiyle çalışırlar.
Sniffing işlemi için iki yöntem bulunur:
a) Pasif Gözetleme: Ağda geçen dataların kendisine gelmesini bekleyen ve yalnızca gelen verileri gözetleyen sistemdir.

b) Aktif Gözetleme: Yalnızca kendisine gelen veriyi değil ağ üzerinde dolaşan tüm verileri alabilmek için çaba gösteren sistemlerdir.

2.8.12 Tarama (Scanning)

Bu yöntemle siber ihlal yapacak kişilerin ileri seviye teknik bilgisayar yazılım ve donanım bilgisine sahip olması gereklidir. Oluşturulan yazılımlarla sistem otomatik olarak tanımlanan IP bilgisi, port bilgisi, şifre bilgisi gibi bilgileri art arda denemelerle tarayarak elde etmeye çalışır. Denemeler her seferinde artan numaralarla tekrar edilir başarıya ulaştığında raporlanır. IP adresi sanal veri yolları denilen portlara bölünmüştür. İnternete bağlı bir sisteme ait port bilgilerinin elde edilmesi sistemle veri alış verişi için açık kapıların bulunması demektir. Hackerların en çok kullandıkları yöntem port taramasıdır. Ürettikleri özel yazılımlar ile internete bağlı sistemleri otomatik taramaya tabi tutmaktadırlar ve tarama sonunda açık portlar tespit edilmekte ve istenilen eylem gerçekleştirilmektedir (Aydın 1992).

Şifre taramalarında da yine oluşturulan özel programlar aracılığıyla harf, rakam, simge gibi karakter taramalarıyla başarıyla çözülebilmektedir. Bu tür programları web ortamında bulmak mümkündür.

2.8.13 Süper Darbe (Super Zapping)

Bilgisayardaki sistemler kilitlenerek bir nedenle işlemez hale gelirse, sistemi tekrar çalışır hale getirmek güvenlik kontrollerini bypass ederek sistemde değişiklik yapmaya yarayan programlardır. İlk olarak "kopya koruma" yazılımlarını atlatma amaçlı bir program olarak ortaya çıkan süper darbe programları, bilgisayar sistemlerine ağır zararlar vermek isteyen siber ihlalcilere, bütün güvenlik duvarlarına takılmadan geçebilmesinden dolayı geniş bir imkânlar sağlar (Aydın 1992).

2.8.14 Gizli Kapılar (Trap Doors)

Adından da anlaşılacağı üzere uygulamaya üreten kişi veya firma tarafından daha sonra ortaya çıkacak hatalara kod çözümü üretme veya ürünü geliştirme amaçlı bilinçli olarak açık bırakılan kapılar olarak tanımlanır. Bu aslında sadece üreticinin bildiği bir virüs yazılımdır ancak bu açıkları tespit edecek başkaları için farklı amaçlara kullanılabilecek bir boşluk oluşturur. Güncel bir örnek olarak en çok oynanan android uygulamalarından "Angry Birds" adlı oyun içerisine ABD istihbarat birimlerince güncelleme olarak casus yazılım gönderildiğinin ve bu sayede kullanıcılara ait özel bilgilerin toplandığının yine bir istihbarat elemanının itirafıyla ortaya dökülmesi (İnt. Kyn.32).

2.8.15 Eş zamansız Saldırılar (Asynchronous Attacks)

Bilgisayarlar verilen işlem komutlarına göre çalışırlar, işlemcinin özelliğine göre birden fazla komut aynı anda yerine getirilir bu durum eş zamanlı çalışma olarak adlandırılır. Bazen de iş durumuna göre işlemciler komutları sıraya koyar bir işlemin bitimiyle diğer işleme başlar bu duruma da eş zamansız çalışma denilmektedir. Eşzamanız çalışma olarak nitelenen işlemlerin sıra beklemesi esnasında, bellekte bekleyen verilere müdahale edilerek değişiklik yapılması şeklinde gerçekleşen saldırı tipine eşzamanız saldırı denilmektedir. Örnek olarak printerda çıktı sırası bekleyen verilere silme, ekleme gibi değişiklik yapılması verilebilir. Ancak bu tür işlemleri yapabilmek için ileri seviye programlama bilgisi gereklidir (Değirmenci 2002).

2.8.16 Sırtlama (Piggybacking)

Sırtlama, fiziksel ve elektronik olmak üzere iki şekilde yapılır. Fiziksel türde sistemlere giriş yetkisi olan bir kişinin kullanıcı adı ve şifreleri kullanılarak giriş yapılır. Elektronik türde ise internet veya intranet ağları üzerinden erişim yapılarak sistemlere izinsiz giriş yapılır (Boğa 2011).

Örnek bir olay; 28.10.2013 te Adliye UYAP sistemine giren kimliği belirsiz kişilerce Kocaeli İnfaz Savcılığı'nda hakkında 5 yıllık kesinleşmiş hapis cezası bulunan Oktay D.'nin yakalama kaydının sistemden silinmesi (İnt Kyn.33).

2.8.17 Bukalemun (Chameleon)

Bukalemunlar, çalışırken virüs gibi algılanmayan birtakım hile ve aldatmalarla sistemlerde zarar oluşturan programlardır. Amaçları gizli dosyalara erişip kullanıcıya ait şifre ve kullanıcı kodlarını toplar ve bilgileri bu programı kontrol edene ulaştırır (Değirmenci 2002).

2.8.18 Yerine Geçme (Masquerading)

Kurumsal ve şirketsel anlamda intranet, internet veya özel network yapılanmasıyla ağ bağlantısına sahip sistemlerde her kullanıcıya seviyesine göre erişim ve işlem yetkisi verilir. Bu erişim yetkisi sadece okuma, sorgulama, veri girme, ekleme/düzeltme yapma veya silme olabileceği gibi pozisyona göre tamamı da olabilir.

Bu yöntemde yetkilendirme yapılan kişinin bilgileriyle sisteme giriş yapma ve onun adına işlemde bulunma ifade edilir. Verilerin önemine göre sistemlere giriş için kullanıcı ismi, sayısal şifreler yanında ileri teknoloji destekli parmak izi, retina göz taraması gibi araçlarda kullanılabilir (Değirmenci 2002).

2.8.19 Web Sayfası Hırsızlığı ve Yönlendirme

İnternette bir web sitesine ulaşım DNS veri tabanında tescil edilen alan adları yoluyla olur. DNS sunucuları bütün dünya genelinde alan adlarını IP (İnternet Protocol) sayısal adresleri ile kayıt edildiği ve ilan edildiği veri tabanlarıdır. Bir kullanıcı ulaşmak için bir web tarayıcısına bir web adresi yazdığında önce alan adı DNS sunucusunda IP sorgulamasıyla karşılaştırılır, adres öğrenilerek istenen sayfa ekrana getirilir.

Bu nedenle alan adı denilen web adresi almak isteyenler ISS olarak adlandırılan servis sağlayıcılara başvurarak istedikleri web adının uygunluğunu ve tescil işlemlerini yaptırırlar. Kaydedilmiş bir isim kapatılmadan başkalarınca kullanılamaz ancak tescil kaydını yapan ISS tarafından yada harici erişimciler (hacker) tarafından değiştirilirse mümkün olur.

Web sayfası hırsızlığında bu alan adı tescil bilgilerinin değiştirilmesi söz konusudur, web sayfası yönlendirme de ise alan adının birlikte tescil edildiği IP (İnternet Protocol) adresin değiştirilmesi söz konusudur. Bu yöntem genelde banka web siteleri için sıkça uygulanan bir yöntemdir. Tarayıcıda yazılan adresle ulaşılan web sitesi birbirine benzer farklı bir sayfa olur.

Web sayfası hırsızları özellikle marka veya popüler web sayfaları alan adlarını çalarak tescil sahiplerine para karşılığı tekrar satma amacındadırlar. Web sayfası yönlendiren siber ihlalciler ise kullanıcılara ait alış veriş, banka ve kredi kart bilgileri ile şifrelerini elde etmeyi amaçlarlar (Değirmenci 2002).

2.8.20 Yanlış Yazanları Yakalama (Typing Error Hijacking)

Bu yöntem de web sayfası yönlendirmeden farklı olarak site IP adresi değiştirmek yerine popüler sitelerin isimsel benzeri yeni siteler oluşturur. DNS kayıtları ile servis sağlayıcıların kayıtlarına ulaşıp değiştirmek ileri seviye teknik bilgi ve zorluk gerektiği için daha amatörlerin kullandığı teknik olarak çok bilinen yazım yanlışlarından kullanıcıları yakalayarak kendi sayfalarına yönlendirmedir. Genelde Google gibi tarayıcılardan üst sıralardaki ilk görünen adres çubuklarına dikkatsizce basmalar en çok kişileri bu hatalara yönlendirir (Alaca 2008).

Örneğin, Garanti bankasının http://www.garantibank.com olan asıl internet adresinin birçok kullanıcı tarafından "www.garanti-bank.com" gibi adreslerden ulaşmaya çalışmasını değerlendiren Fail, kendi adına kaydettirdiği alan adını kendi sitesine yönlendirerek bilgileri alır.

2.8.21 Oltaya Gelme (Phishing)

Kısaca online dolandırıcılık olarak tanımlanan Phishing yönteminde temel amaç internet kullanıcısını kandırarak, kullanıcıya ilişkin kredi kartı bilgileri, banka hesap numaralarından bu hesaba ait online internet şifresine kadar birçok özel bilgileri ele geçirmektir.

Bu yöntemle internet kullanıcılarını tuzağa düşüren korsanlar Debit/ATM, kredi kart numaraları, şifreler ve parolalar/ CVV2 internet bankacılığına girişte kullanılan kullanıcı adı ve şifreleri ile hesap numaraları elde etmeye çalışırlar.

Bu yöntemde dolandırıcılar sahte e-posta mesajı göndererek sanki bu ileti, ticari bir kurumdan (alışveriş siteleri, bankalar vb.) gönderiliyormuş izlenimi oluşturup, kullanıcıların kendilerine ait bilgileri girmesi için bağlantıyı (link) tıklamasını isteyen bir ileti olabilir. Mesaj içeriğinde bilgi güncellemesi ve sistemde girilen verilerin hesapta aktifleşmesi için şifre girilmesi gibi içerikler olmaktadır (Boğa 2011).

Eğer kullanıcı iletideki linke tıklarsa kurumun web sitesinin birebir benzeri olan başka bir sayfaya yönlendirilir. Burada girilecek her türlü bilgi başkasının eline geçecektir.
Korunmak için kullanıcıların bazı hususlara riayet etmesi gereklidir bunlar;

a) Tanınmayan kişilerden gelen mesajları cevaplamayarak doğrudan silmek,
b) Online alış veriş yaparken, işlem yaptığınız web sayfasının güvenli olduğuna işaret eden "https://" olup olmadığını kontrol etmek,
c) Alan adı olarak sayısal rakamlar içeren adresler ile karşılaşınca dikkat etmek, web sitelerinin alan adları isimle ve com, gov, org gibi uzantılarla biteceğinden sahte olma ihtimali yüksektir.
d) Güvenli olduğu değerlendirilmeyen ağlarda elektronik işlem yapmamak,
e) Bankalardan gelen kart ekstrelerini, hesapları düzenli olarak kontrol etmek,
f) İşletim sistemi güvenlik yamalarını yükleyerek, anti virüs yazılımını güncel tutmak,
g) e-posta hesap şifreleri ile kurumsal hesap şifrelerini farklı belirlemek ve düzenli aralıklarla değiştirmek (İnt. Kyn.34)

2.9 Alınması Gereken Güvenlik Tedbirleri

Son yıllarda, bilişim sistemleri ile ilgili işlenen suçlarda büyük ölçüde artış meydana gelmiştir. İnternet kullanımının yoğunlaşması, elektronik ticaretin gelişmesi, sosyal ağ uygulamalarının akıllı telefonlarla hayatımızın her anına girmesi gibi nedenler internet üzerinde işlenen suçların artışında büyük ölçüde etkili olmuştur.

Son 2013 Tüik verilerine göre 76.667.864 (TÜİK 2013) (İnt. Kyn.35) olan ülkemiz nüfusunun 10-74 yaş grubunu oluşturan 61.851.647 (TÜİK 2013) (İnt. Kyn.36) kişilik kesimi bilgisayar ve interneti kullanan kesimdir. Bilgisayar ve internet kullanım oranlarının en yüksek olduğu yaş grubu 16-24'tür (TÜİK 2013), internet ve bilgisayar kullanımı tüm yaş grupları içerisinde erkeklerin yüksekliği dikkat çekmektedir (İnt. Kyn.37).

16-74 yaş grubundaki bireylerde bilgisayar ve internet kullanım oranları 2004 yılında sırasıyla %23,6 ve %18,8 iken 2013 yılında sırasıyla %49,9 ve %48,9'a ulaşmıştır. Bu oranlara bakıldığında 2014 yılında hem bilgisayar hem de internet kullanan sayısı artışla ve düşen başlama yaşıyla 30 milyon üzerinde artmaya devam edecektir.

Yine Tüik verilerinde 2013 yılı ilk üççeyreğinde (Ocak-Mart 2013) 16-74 yaş grubu tüm bireylerin %39,5'i İnterneti düzenli olarak (günlük olarak veya en az haftada bir defa) kullandığı tespit edilmiştir (TÜİK 2004-2013) (İnt. Kyn.38).

İnternet üzerinden yapılan işlemlerin fazlalığı, cazipliği, erişim kolaylığı, güvenlik zafiyetleri suç faillerini siber suçlara yöneltmiştir. İstenilen bilgiye çabuk ve ucuz ulaşma imkânı, bilgi teknolojilerindeki hızlı gelişimle bilgisayar ve internetin akıllı telefon ve tablet cihazlarında birleşerek mobil hale dönüşmesi, 3G, 4G ve 5G teknolojilerinin gelişimiyle internet servisinin tamamen mobil cihazlar üzerinden ve Wi-fi bağlantılarıyla da her ortamdan ve günün her saatinde yaşamın bir parçası olarak kullanılır hale gelmesi ve buna paralel olarak ortaya çıkan güvenlik zafiyetlerini fırsat

görerek bulunan yeni suç teknikleri bu artıştaki nedenlerdir. Bu sebeple siber güvenlik teknolojisi, bilgi teknolojilerindeki gelişim hızına yetişememektedir (Alaca 2008).

Bilişim sistemleri aracılığıyla işlenen suçların ve suçluların tespitinde yaşanan zorluklar, soruşturmaya konu suçlar ile ilgili hukuken caydırıcı cezaların ve yaptırımların oluşmaması, yetersiz delil üretimiyle takipsizlikle sonuçlanması, suç faillerindeki hızlı bir artış nedeniyle, siber suçların önlenmesi için çalışmaların hızlandırılmasına neden oldu. Bu çalışmalar sadece suç ve ceza tanımlamaları olan hukuki düzenlemeler değil, suçun soruşturulması evresinde suçu haber alma, tespit etme ve suça ait unsurları delillendirerek ortaya koyma işlemini yürüten adli kolluk (polis) biriminin uzmanlaşması ama daha önemlisi olarak kullanıcıların mağdur olmadan önce, bireysel ve kurumsal olarak bilinç seviyelerini artırma, alınabilecek basit ama etkili tedbirleri güvenlik anlamında uygulayarak zarar görmeden önce teknik tedbirlerle önlem alma yönünde önem kazandı (Değirmenci 2002).

2.9.1 İdari ve Kurumsal Güvenlik

Bilgi teknolojileri sistemlerini kullanan ve işleten kurumların alacağı güvenlik tedbirlerini kapsamaktadır. Burada amaç, kurumsal bilgi güvenlik politikaları ile bilgi güvenliği konusunda idarenin, işletmenin ve kurumsal yönetimin bakış açısı, politikası, prosedürleri ortaya koyması ve çalışanlara ileterek uygulanmasını sağlamasıdır. Bu kurallar doküman olarak yönetim tarafından onaylanmalı, yayınlanmalı ve tüm çalışanlara bildirilmelidir (Doğantimur 2009).

Kurumsal hassasiyetler doğrultusunda güvenlik politikaları farklılıklar gösterebilir. Kurumlara özgü ve kurumların ihtiyaçlarına yönelik olarak bilgi güvenliğinin ana unsurlarından hangileri daha önemli görülüyorsa o unsurları öne çıkaran politikalar hazırlanabilir.

Gizlilik politikası: Elde olan bilgilere tasnif getirerek erişime izin verme anlamında bir grup veya kişilerin erişimine uyarlama, bilginin bu erişim dışındakiler için gizlilik

içermesidir. Burada amaç erişim yetkisi olmayanlar açısından bilgiye erişme durumunda sızmanın varlığının tespitidir (Bishop 2002).

Bütünlük politikası: Bilginin hangi durumlarda kimler tarafından ne şekilde değiştirileceğinin tanımlanmasıdır. Bu sayede erişenler açısından kaynak güvenliği sağlanmış olur.

Kullanılabilirlik politikası: Güvenlik politikası gereği hangi servislerin hangi zaman ve şartlar altında erişim yetkisi olanlarca kullanılabileceğini tanımlar.

Askeri-yönetimsel güvenlik politikası: Gizlilik bu çeşit politikalarda erişilebilirlik ve güvenilirlikten daha önemlidir ve önceliklidir. Diğer ikisi bir şekilde telafi edilebilir ancak gizliliğin delinmesinin sonuçları çok ağır olur (Doğantimur 2009).

Ticari güvenlik politikası: Bu politika çeşidinde amaç verilerin korunmasını sağlayarak değiştirilmesini önlemek ve güvenilirliği muhafaza etmektir.

2.9.2 İnsan Kaynakları Güvenliği

Bilişim sistemleriyle çalışacak tüm personelin işe alım aşamasından başlamak üzere bir takım yeterliliklere tabi tutulmasını, yapılan arşiv araştırmalarını, çeşitli zamanlarda görev değişikliğini, belirli zamanlarda zorunlu eğitime tabi tutulmalarını ve zorunlu izne ayrılmalarına varıncaya kadar alınan tedbirleri kapsar. Dikkatli ve iyi eğitimli personel olası ihlalleri engellenmede ve çözümlemede etkili olmaktadır (Alaca 2008).

İşe alma öncesi, çalışma süresi ve çalışmanın sonlandırılması veya yer değiştirilme aşamalarında önlemler planlanmalıdır. İşe alma öncesi belirlenen güvenlik kriterleriyle çalışan, işveren ve üçüncü taraf kullanıcıların sorumluluk alanlarının belirlenmesi ve düşünülen pozisyonlar için doğru kişilerin seçilmesi, olası bilgi hırsızlıkları ya da imkânların amaç dışı kullanım riskini minimize etmektir.

İşe alınanın çalışması süresinde kurumsal güvenlik politikasını bilerek desteklemesi, bilgi güvenliğine ilişkin tehditler, kaygılar, endişe ve sorumluluklarının farkında olarak, insan kaynaklı hata risklerini azaltacak donanımda olmasını sağlamaktır. Çalışanın işine son verilme veya değiştirilme durumunda güvenliğin amacı, kurumsal bilgilerin korunması ve edinilmiş bilgilerin kurum dışına taşınmamasını sağlamaktır (Doğantimur 2009).

2.9.3 Fiziksel Güvenlik

Bilişim sisteminin bulunduğu alana bir takım fiziki giriş kontrolleri ile birlikte yangından doğal afetlere, güç kaynaklarından kablo güvenliğine kadar alınan önlemlerle girişin kontrolü sağlanmakta, yetkisiz erişimler engellenerek suç faillerinin bilgiye ulaşması önlenmekte ve veri depolama birimleri çalınmaya, hasara ve kesintiye uğramamaya karşı korunmasıdır (Alaca 2008).

Bilgi teknolojilerindeki gelişmelerle cihazlarda kullanılan uygulama ve yazılımların çeşitlenmesi fiziki güvenliğin yanında uygulama ve yazılımların güven(ilir)liğini öne çıkarmıştır.

2.9.4 Haberleşme – Elektronik Güvenliği

Bilişim sistemleri, merkezi işlem biriminin veri işlem hızını kontrol eden sinyaller üretir. Bu sinyaller monitörde bulunan görüntünün yaydığı sinyaller de olabilir. Yakın mesafeye yerleştirilen duyarlı alıcı cihazlar ile sinyaller yeniden görüntüye dönüştürülerek, monitörde bulunan istenilen bilgiye ulaşılabilir. Muhabere elektronik güvenliği, bilgi işlem ağlarının devamlı kontrol altında tutulması, radyasyonu sızdırmayan tempest korumalı odalarda olması, çalışan sistem ekranlarının pencere camına dönük olmaması, metal boruların elektronik sinyalleri iletmeleri ihtimaline karşılık, plastik vb. maddelerde yapılmış boruların tesis edilmesi gibi önlemleri kapsar (Alaca 2008).

2.9.5 Donanım Güvenliği

Bilişim sistemlerinde bulunan fiziksel donanımların zarar görmesini engellemek amacıyla alınan güvenlik tedbirleridir. Bu başlık altında donanım içindeki fiziksel parçalara gelebilecek her türlü zarar donanım güvenliği kapsamındadır (Alaca 2008).

2.9.6 Yazılım Güvenliği

Yazılım güvenliği bilişim sistemlerinin en önemli kısmını oluşturur, sisteme gelen birçok tehdit unsuru uygun güvenlik yazılımları kullanılarak etkisiz hale getirilir. Bilişim sistemlerinde virüsler veya virüs türevi zararlı yazılımların sisteme bulaşması, sistem içine yerleşmesi veya bir şekilde sızmışsa temizlenip sisteme zarar vermeden tespit edilerek etkisizleştirilmesi bu güvenlik sistemleriyle mümkündür. Enfekte olmuş bir sistem uygun bir güvenlik yazılımı ile temizlenip tekrar aktif hale getirilebilir (Alaca 2008).

Yerel ağlara kurulan firewall (güvenlik duvarı) programı ile istenilen sistemin korunması sağlanabilir. Firewall uygulaması ağ güvenlik sistemlerinin vazgeçilmez bir parçası olmuştur. Firewall programı bilgisayar ile internet bağlantı ağı üzerindeki veri akış trafiğini gözetler. Firewall uygulaması bilişim sistemlerinin kapısında duran bir koruma görevlisine benzer. Ağ üzerinden bilgisayara giriş yapan yazılımları denetler ancak harici veri taşıyıcı (flash disk, sd kart, micro sd kart vb.) cihazlarla işlemciye giren ve içerden yapılacak saldırılardan koruyamaz (Boğa 2011).

Bu nedenle internet veya intranet ağlarından gelme ve ağdaki sistemlere zarar verme ihtimali bulunan çeşitli veri veya paket programlardan oluşabilen saldırıları fark etmek üzere tasarlanmış saldırı tespit sistemleri aktif olarak güvenlik duvarı yanında kullanılmalıdır. Bu STS sistemleri her nereden saldırı gelirse önlem almak üzere üretilmiş çözümler olarak, kurum içi ya da dışından bir erişimci sisteme giriş yaptığı anda bu durumu fark ederek giriş yapan kişinin nereden eriştiği ve nereye bağlandığı ve ne tür işlemler yaptığına ilişkin raporlamalar yapmaktadır. Ayrıca belirlenen ayarlara göre atak saldırıları tespit ederek e-posta, mesaj (SMS), sistem kaydı ve veri tabanı gibi

uyarı ve kayıt çıktıları sağlayarak ve gerekirse Güvenlik Duvarı'na saldırı olduğuna dair sinyaller yollayarak erişimleri engelletebilir (Türkiye Bilişim Derneği 2006).

Saldırı Tespit Sistemleri, orta ve küçük boy ağlarda güvenlik duvarının ön veya arkasına olmak üzere iki şekilde konumlandırılabilmektedir. Büyük ağlarda ise, sistem yapısına bağlı olarak gerekli görülen noktalara, STS sensörleri konulabilmektedir. Firewall önüne konumlandırılan sistem tüm paketleri inceleyerek internet ortamında sunucu ağına gelen tüm saldırı ve saldırgan profilleri kolayca tespit edebilmektedir. Saldırıların hedeflerine ve saldırı tiplerine bakarak önlemler almayı kolaylaştırmaktadır.

STS sistemlerinin kullanılırken bazı olumsuzluklarla da karşılaşmak mümkündür. Bazen saldırı aktivitelerini saldırı olarak algılamaması (false-positive), bazen de saldırı olmayan aktiviteleri saldırı olarak algılaması (false-negative) olayıdır. Bu nedenle STS sistemlerinin uygulamasında bilgi ve insan faktörü çok önemlidir. Bazı STS'ler otomatik müdahale etmeye ayarlanabilmektedir. Yani, saldırı alarmı sistemde algılandığında insan unsuru müdahale olmadan tepki verme veya cihazlarda gerekli yapılandırma değişiklikleri yapmaya imkân sağlar (İnt. Kyn.39).

Bu nedenle, STS sistemleri çalışanların eğitilmesi ve arşivlenen verilerin kriptolaması gibi güvenlik önlemleri ile birlikte kullanılmalıdır (Doğantimur 2009).

2.9.7 İşlem Güvenliği

İşlem güvenliği ile bilgi sistemleri üzerinde farklı yetkilendirme seviyeleriyle kullanıcıların erişim, sorgulama, veri girme, verileri değiştirme veya verileri silme gibi yetkilendirmeye tabii tutulmasıdır. Kullanıcılara tanımlanan kodlamalarla yaptıkları işlem hareketlerinin belirli olması sağlanabilir. İşlem güvenliği kullanıcı kontrolü (user controls) ve sistemlere erişim kontrolünü kapsamaktadır. Bilgi sistemlerine erişimde bir takım kullanıcıya özgü taklit edilmesi zor özelliklerin veya şifrelerin kullanılmasıyla, kullanıcının kimliğinin belirlenmesi sağlanabilir (Alaca 2008).

Siber suçların tespiti zaman alan kapsamlı bir suç tipidir. Özel yazılımlar kullanılarak işlenen suç ve suça ilişkin izlerin elde edilmesi oldukça zor olmaktadır. Personel güvenliği ve fiziksel güvenlik tedbirleri işlem güvenliği ile desteklenmedikçe failler sistem güvenliğini aşarak istedikleri hedeflere ulaşacaklardır. Bu nedenle bilgisayar güvenlik stratejileri asgari şu hedefleri sağlamalıdır; yetkisiz her hareketin denenmesi engellenmeli, olası tehditlerin başarıya ulaşması engellenmeli, olası tehdit tespit edilmeli ve bu sonlandırılmalı, zarar potansiyeli minimuma indirilerek, oluşmuşsa düzeltme ve tedavi başlatılmalıdır (Değirmenci 2002).

2.10 Bilgi İletişim Teknolojilerinin Suç Kolaylaştırıcı Yapısı

Bilgi teknolojilerindeki gelişmeler, bu sistemlerin üretim maliyetini düşürdü, azalan üretim maliyetleri satış fiyatlarını da düşürdü ve bunun doğal neticesi olarak bilgi iletişim teknolojileri orta ve alt gelir seviyesine sahip kişiler tarafından da elde edilebilir ve kullanılabilir oldu. Bilgi teknolojilerindeki kullanım artışıyla toplum hayatına giren olumsuzluklardan birisi de "siber suçlar" olmaktadır. Siber suçlardaki artışın temel nedenlerinden biride, bilişim sistemlerinin içerisinde suç işleme kolaylığını barındırmasıdır. Diğer bir ifadeyle bu sistemlerin teknik yapıları gereği taşıdığı bazı özellikler, bu suçların gerçekleşmesine zemin hazırlamaktadır (Alaca 2008).

Bilgi iletişim teknolojileri sistemlerinin yapısı gereği barındırdığı bu suç işlemeyi kolaylaştırıcı imkânlar çok önemsenmediği gibi, aksine bilişim sistemleri aracılığıyla işlenebilen suçların yine bu teknolojik sistemler aracılığıyla önlenebileceği yönünde de yaygın bir görüş eğilimi vardır. Bu görüşü taşıyanlara göre, bilgi teknolojileri kullanmadan ve geleneksel usullerle elle gerçekleştirilen işlemlerde de dolandırıcılık ve hırsızlık zimmete geçirme, irtikâp, sahtecilik olaylarının meydana geldiği dikkate alınırsa, bu elle gerçekleştirilen işlemlerin sayısının azaltılıp, bütün işlemlerin bilgi teknolojileri sistemleri aracılığıyla gerçekleşmesiyle suçlar önlenebilecektir (Aydın 1992).

Bilgi iletişim teknolojisi sistemleri yapısı gereği ve bu sistemlerde bir avantajı olarak görülen bazı özellikler, suç işleme eğiliminde olan kişiler için bir fırsat olarak

değerlendirilip, suç işleme aracı olarak kullanılabilir. Bu özellikleri Aydın; bilgi yoğunlaştırma, kontrol mekanizmasındaki eksiklikler, anonimlik olarak belirtir (Aydın 1992).

Yücel ise bunları bilgisayarların zayıflıkları olarak nitelendirerek dört madde halinde sıralar (Yücel 1992);

a) Bilgisayarın verilen komutları hiçbir sorgulamaya tabi tutmadan uygulamasından dolayı, mantık dışı ve dolandırıcılık içeren komutları fark edememesi,
b) Komutların insan yerine bilgisayardan geldiğinde, bilgisayarın hata yapmayacağına olan inanç yüzünden daha fazla güvenilmesi,
c) Para transferini (EFT) çok uzak mesafelerde, çok kısa sürelerde ve çok büyük miktarlarda yapabilmesi,
d) Suçların anonim şekilde işlenmesine imkân tanıması.

Bilişim sistemlerinde veri depolama ortamlarının, veri kapasitelerinin ve saklanılan veriye erişim hızının çok yüksek, buna karşılık söz konusu verilerin muhafaza etme maliyetlerinin çok düşük olması, barındırdığı veriler üzerinde hiçbir iz, silinti ve kazıntı bırakmadan değişiklik yapılabilme olanaklarının varlığı, bu verilerin yeniden derlenme imkânlarının bulunması ve verilerin elektronik ortamda transferi gibi özellikler aynı zamanda bilgi yoğunlaştırmasının suç yaratıcı faktörleridir. Bu sayede, kâğıtsal bazda sayfalarca tutabilen bilgiler kısa sürede uzak mesafelere aktarılabilmekte veya bu veriler hiçbir iz bırakmadan değiştirilebilmektedir (Alaca 2008).

Terabaytlarla ifade edilen bilgilerin bilişim sistemlerinde toplanması ve günlük olarak çok sayıda yeni verilerin girilmesi, bu verilerin kontrolünde sorunlarla karşılaşılmasına ve bu verilerin işlenmesinde hatalar yapılmasına sebep olabilmektedir.

Büyük miktarlarda bilgiyi içeren veri havuzları kullanıcı işlemleri sırasında eksik bırakılan güvenlik açıkları, bu bilgilere ulaşmak ve bu açıklardan istifade etmek siber ihlalciler ve siber korsanlar tarafından kaçırılmaz bir fırsat olmaktadır. Veriler data depolama birimlerinde manyetik ortamlarda saklanmaktadır. Bu veriler üzerinde geride

tespiti zor izler bırakılmadan değişiklikler gerçekleştirilebilmektedir. Ayrıca terabaytlarla ifade edilen bilgiler çok küçük data taşıyıcı (micro sd, sd kart, flash bellek, Harici disk, vb.) disklerde kopyalanarak, bilişim ağı dışına taşınabilmekte hatta ağ üzerinden erişimle kopyalanabilmektedir. Bu özellikler, bilişim sistemlerinde suç nitelikli eylemlerin işlenmesini kolaylaştırmaktadır (Aydın 1992).

Bilgi teknolojisi ürünlerin günlük ev ve iş hayatında artan kullanımı ile beraber, bu sistemlerin getirmiş olduğu kolaylıklar nedeniyle birçok kontrol tedbiri uygulamadan kaldırılmış ya da göz ardı edilmeye başlanmıştır. İnternet erişimli cihazlarda ağa bağlanıldıktan sonra hata yapılmasını önleyici veya kötü niyetli girişimleri ve erişimleri engelleyici tedbirler kullanıcı tarafından aktif edilmedikçe kendiliğinden devreye girmeyecektir. Güvenlik tedbirleri de kullanıcı bilinç seviyesi ile doğru orantılı olarak kullanılacağına göre, yeterli bilinç düzeyinin oluşmaması suç nitelikli girişimlere kapı aralamaya devam edecektir.

Bilişim sistemlerinin diğer bir suç yaratıcı unsuru ise, bu sistemlerde işlenen suçlarda mağdurun belli olmaması, suçun sisteme karşı işlenmesidir. İhlalci kimin malını aldığını bilmemekte, mağdur sistem olarak gözükmektedir. Bu durum ise müştekisiz başlanılmayan adli bir soruşturmada takibi şikâyete bağlı suçlar açısından failin tespitinde zorluklara neden olmaktadır (Aydın 1992).

Siber suçlarının işlenme şekilleri incelenecek olursa, "çöpe dalma", "göz atma" gibi basit işlenme şekilleri hariç, diğer yöntemlerin icra edilebilmesi için bilgi teknolojileri, web, ağ yapısı ve işleyişi, güvenlik duvarları, şifre kırma gibi bilgilere sahibi olunması gerekliliği görülecektir. Bilgili olma şartı, bir yandan bu nitelikte kişilerin az olması nedeniyle uç etki gösterirken, diğer yandan suç yaratıcı unsur olarak karşımıza çıkmaktadır. Bu bilgi altyapısına sahip kişi/ler, bu alanda suç olarak belirlenen eylemleri planlarken, tüm deneyimini kullanacak ve kendini ele verecek tüm izleri yok etmeye çalışacaktır. Böylece bulunabilme riskini minimuma indirecektir. Bundan dolayıdır ki, bilişim/siber suçu faillerinin büyük kısmı bilgi teknolojileri ile uğrasan kişilerdir (Aydın 1992).

Günümüzde internet erişimli işlemcili kişisel elektronik cihazların kullanımının artması, internet hizmetlerinin yaygınlaşması ile her türlü bilgiye web ortamında kolayca erişebilme imkânı, bilgisayar ve internet bilgisinin artması, siber suçların suç fırsat unsurunu etkileyen bir başka faktördür. Artık meraklı bir kimsenin elindeki akıllı telefondan, tabletten veya ev/ işyerindeki bilgisayardan internet ağına bağlanıp, ağa bağlı diğer kullanıcıların zayıflıklarından faydalanacak çeşitli yazılımlar veya saldırı da kullanılan özel programlar elde etmesi veya başka bir kullanıcının sabit diskindeki özel verilere ulaşması, kişiye özel pek çok bilgiyi elde etmesi çok güç değildir. Bu durum siber ihlalciler açısından artış anlamına gelirken bireylerin özel verilerinin korunması açısından artan bir tehdit olmaya devam edecektir.

2.11 Siber Suç Faillerinin Genel Özellikleri

Siber suçlara ilişkin araştırmalar başta ABD ve Avrupa Birliği ülkelerinde daha yoğun olarak yapılmaktadır. Bu araştırmalar neticesinde oldukça ilginç sonuçlara ulaşılmakta ve suçların boyutu ve işleyenler hakkında detaylı bilgiler elde edilmektedir (Shaw 1998).

Siber suçları işlediği tespit edilen kişiler genelde 20 ila 30 yaş aralığında bulunmakta ve büyük çoğunluğu da erkeklerden oluşmakta olup, teknik bilgi düzeyi yüksek kişiler olarak ortaya çıkmaktadır. Bu kişilere genel olarak bakıldığında duygusal ve psikolojik sorunlarının varlığı ve suç işlemelerinde ana etken olduğu sonucuna ulaşılmaktadır (Demirbaş 2005).

Amerika'daki siber suç failleri hakkında araştırma yapan uzmanlardan; Parker ve Bequai yukarıdaki belirlemelerin yanında, siber failleri daha cüretkâr, maceraperest, sabırsız, uyanık, teknolojik iddialaşma içinde ve çabuk motive olan kimseler olarak tarif eder (Bequai 1998).

Yine Almanya ve Amerika'da faillerin çalışma hayatlarında sıkça iş değiştiren kişiler olduğu tespit edilmiştir. Yine Alman faillerin herhangi bir sabıkası bulunmazken Amerikalı faillerin cüzi bir kısmının sabıkalı olduğu da tespitler arasında. Ayrıca, siber

suç işleyenlerin büyük bir çoğunluğunun toplumda ve çevrede itibarlı, sorumlu ve iyi birer birey olarak ortaya çıktıkları gözlemlenmektedir (Demetriou 2003).

Parker fail davranışlarının, içinde yer aldığı grup hareketlerinden fazla sapma teşkil ettiğini belirtmektedir. Amerika'da bilgisayar kullanımından doğan yaygın hareketler üzerinde yapılan bir araştırmada yönetici ve programcıların rakip şirkette çalışan arkadaşına kendi şirketinden temin ettiği bir programı verip kullanmasını sağlamak, başka bir programcı ile program değiş tokuşu yapmak, izinsiz olarak bir programı bir diğeri ile değiştirmek gibi bazı hukuka aykırı davranışların yazılımcılar veya programcılar tarafından normal kabul edildiği ortaya çıkmıştır (Bequai 1998).

İleri bir "cracker" (lisanslı program çözücüsü) olan Bili Landreth siber suçluları inceleyen ilk teorisyenlerden birisi olup bir çatı altında kategorize etmiştir. Deneyimlerine göre Landreth siber suçluları beş kategoriye ayırmıştır (Landreth 1995): Bunlar;

a) Birinci grupta "çaylaklar" olarak tanımladığı siber suçluları, bilgisayar ve ağlar konusunda becerisi ve bilgisi fazla olmayan ekseriyetle fazla zarar vermeyen suçları işleyen kişiler oluşturur. Bu gruptakiler genelde basit hileleri kullanır ve ufak tefek yaramazlıklar yaparlar (Alaca 2008). Çaylakların faaliyetleri arasında çeşitli sohbet odalarındaki kullanıcıları rahatsız etme, bağlantılarını koparma gibi eylemler sayılabilir.

b) İkinci grubu "öğrenciler" olarak tanımlar ve bu gruptakileri biraz daha deneyimli ve elektronik sapıklar olarak nitelendirir. Bu kişiler, internette surf yaparak zamanlarının çoğunluğunu yetkisiz giriş yapılabilecek bilgisayarları arayarak geçirirler.

c) Üçüncü grubu "turistler" olarak adlandırır ve faaliyetlerini sistemlere izinsiz girmek için çeşitli saldırılar planlamak ve bu maksatla kendilerini güdülemek olarak tanımlar. Turistler işledikleri suçlardan heyecan duyan kişiler olup "arabayı gezmek maksadı ile çalan kişiler" kavramıyla açıklanmaktadır (Landreth 1995).

d) Dördüncü grupta "Çökerticiler" yer alır ve bu kişiler kötü niyetli ve kindar suçlular grubunu oluşturur. Bu grup siber suçluların karanlık yüzünü yansıtmaktadır. Bilgisayar ağlarına sızar sistemleri çökertir ve kasten dosyalara zarar verirler.

e) Beşinci grubu ise "Hırsızlar" oluşturur. Hırsızlar illegal yollardan para kazanmayı amaçlayan kişilerdir. Bu kategoridekiler dışarıdan sisteme sızan kişi olabileceği gibi sistem ya da organizasyon içerisinden biriside olabilir. Hırsızlar bireysel çalışabileceği gibi, farklı şirketler ya da ülkeler için de çalışabilir (Alaca 2008).

Hollinger (1998) ise siber suçlular hakkındaki çalışmasını bir üniversite topluluğu üzerinde uygulamıştır. Çalışma, siber suçluların az ustalık isteyen basit suç ile çok fazla teknik bilgi gerektiren suçlar arasında değişiklik gösterdiğini ortaya koymuştur.

Hollinger (1998) siber suçluların korsanlar (pirates), tarayıcılar (browsers) ve kırıcılar (crackers) olmak üzere üç grupta toplamıştır. "Korsanlar" telif hakkı ihlali yapan ve teknik bilgisi en az düzeyde olan siber suçlularına denilmektedir. "Tarayıcılar" orta seviyede bilgiye sahip olan ve başka insanların dosyalarına yetki dışı ulaşım sağlayan kişilerdir. "Kırıcılar" ise çok fazla teknik bilgiye sahip en tehlikeli grubu oluşturmaktadır.

"Hacker"ların yeraltı dünyası ile ilgili en geniş etnografik çalışmalardan birisi Chantler tarafından yapılmıştır. "Hacker"ların çeşitli özelliklerine göre onları çeşitli kategorilere ayırmıştır. Bu özellikler, "hacker'ların sahip olduğu ustalık, bilgi, motivasyon ve ne kadar süredir "hacking" ile uğraştıklarıdır.

Chantler (1996) bu özelliklerden hareketle, hackerları elit grup, çaylaklar ve lamerler olmak üzere üç kategoriye ayırmıştır.

a) Elit gruplar, üst seviye bilgi, başarma arzusu ve motivasyonu, büyük heyecan ve cesaret taşımaktadırlar.

b) Çaylaklar ise iyi bir bilgiye sahip olmasına rağmen hala öğrenme safhasındadırlar. Müritler genellikle elit gruptakilerin izinden giderler ve onların arasına katılmaya çalışırlar.
c) Lamer'ler ise daha az bilgi sahibi olmakla beraber küçük amaçları gerçekleştirmek; intikam almak, hırsızlık ve casusluk yapmak maksadıyla motive olurlar.

"Hackerların %30'u elit grup, %60'ı çaylak,%10'u ise "lamer" sınıfından oluşmaktadır (Chantler 1996).

Parker'ın (1998) yapmış olduğu başka bir araştırmada siber suçlular, eşek sakası yapanlar (planksters), bilgisayar uzmanları (hackters), kötü niyetli hackerlar (malicious hackers), kişisel problem çözücüler (personel problem solvers), kariyer suçluları (career criminals), aşırı uçtakiler (extreme advocates), memnun olmayanlar malcontents), tiryakiler (addicts), akılsız ve mantıksız olan insanlar (irrational and incompetent people) olmak üzere yedi ayrı grupta değerlendirmiştir.

a) Eşek sakası yapanlar başkalarını kandırmaya yönelik eylemlerde bulunanlardır. Bu eylemleri yapanların niyeti uzun süreli zararlara neden olmamaktır.
b) Bilgisayar uzmanları (hackters) ise Parker (1998)'in ilk nesil "hacker'lar olarak tanımladığı, başkalarının bilgisayar sistemlerine eğitim, merak ve rekabet maksadıyla giren kişilerdir.
c) Kötü niyetli "hackerlar (malicious hackers) daha çok "cracker" tanımına uymaktadır. Bu kişiler genellikle kötü amaçları ve zarar verme düşüncesi olanlardır. Örnek vermek gerekirse, bilgisayar virüsü yazan kişileri kötü niyetli "hacker" olarak nitelendirebiliriz. Kişisel problem çözücüler (personel problem solvers) geleneksel problem çözme yöntemlerinin yetersiz kaldığı durumlarda kendi yöntemleriyle suç isleyen kişilerdir. Bu kişiler genellikle suç işlemeyi en kolay ve hızlı çözüm olarak görmektedir. Bu çalışmada Parker sayıca en fazla olan grubun kişisel problem çözücüler olduğunu belirtmektedir (Parker 1998).
d) Kariyer suçluları (career criminals), hayatının bir bölümünü ya da tamamını suç işleyerek kazanan kişilerdir. Bazılarının başka meslekleri de vardır, bazıları ise organize suç içerisindedir.

e) Aşırı uçtakiler (extreme advocates) teröristlerle eşdeğer özelliktedirler. Bu kişilerin genellikle güçlü, sosyal, politik ve dini görüşleri bulunmaktadır. Bu kişiler durumları suç isleyerek değiştirebileceğini düşünmektedirler.
f) Parker'ın son kategorisi olan, memnun olmayanlar (malcontents), tiryakiler (addicts), akılsız ve mantıksız olan insanlar (irrational and incompetent people), tanımlaması ve korunması en zor olanlardır. Bunlar akli yönden hasta, kimyasal olarak bağımlı ve suçluluk yönünden ise ihmalcidirler.

Siber suçlular hakkında son zamanlarda yapılan ve büyük kabul görmüş araştırmalar neticesinde, suçlular özelliklerine ve davranışlarına göre yedi kategoriye ayrılarak incelenmiştir. Bunlar (Rogers 1999);

a) Newbie/tool kit (NT) (Acemiler/Hazırcılar),
b) Cyber-punks (CP) (Siber punkçular),
c) Internals (IT) (İçeridekiler),
d) Coders (CD) (Kod yazanlar),
e) Old guard hackers (OG) (Koruyucu hackerlar),
f) Professional criminals (PC) (Profesyonel suçlular),
g) Cyber-terrorists (CT) (Siber teröristler).

Rogers (1999) olası sekizinci kategori olarak political aktivistlerinde sayılabileceğini ancak aktivistlerin faaliyetletleri hakkındaki tartışmalar ve spekülasyonlar nedeniyle dikkate alınmadığını belirtir.

Bu kategoriler içerisinde en düşük bilgi seviyesi NT, en yüksek bilgi seviyesi ise OG ve CT'de bulunmaktadır.

NT kategorisindekiler, sınırlı bilgisayar ve programlama bilgisine sahip kişilerden oluşmaktadır. Bu kişiler "hacking" konusunda çok yeni olmalarından dolayı düzenleyecekleri saldırıları alet takımı adı verilen ve internetten kolayca bulunan küçük programcıkları kullanarak yapmaktadırlar (Rogers 1999).

CP kategorisindeki kişilerin bilgisayar bilgisi ve program yazma yeteneği daha iyidir. Bu kişiler kullandığı yazılımların bir kısmını kendileri yazan ve saldıracakları sistem

hakkında yeterli bilgiye sahip kişilerden oluşmaktadır. Ayrıca bu kişiler web sayfalarını tahrip etmek ve rahatsız edici "e-posta" ları göndermek gibi zararlı eylemleri de gerçekleştirmektedir. Bu kişilerin çoğunluğu kredi kartı numaralarını çalma ve web dolandırıcılığı yapmaktadırlar (Rogers 1999)

IT grubundaki kişiler, bilgisayar ve bilgi teknolojileri konusunda uzman, bir kurum ya da organizasyonun eski çalışanı ya da bulunduğu durumdan memnun olmayan çalışanlardan oluşmaktadır. Bu kişiler eylemlerini gerçekleştirirken bulundukları mevkiinin sunduğu imkân ve kabiliyetler ile kişisel bilgi ve becerilerinden faydalanmaktadırlar. Bilgisayarla işlenen suçların yaklaşık olarak %70'ini bu grup suçlular oluşturmaktadır (Power 1998).

OG grubundaki kişiler ise kendi kuyruğuna basılmadığı sürece suçlu davranışı içerisine girmemektedirler. Bu gruptaki kişiler, ilk nesil "hacker'ların ideolojisini taşımakla beraber, bilgi teknolojileri konusunda kendini geliştirmeye adamış kişilerden oluşmaktadır (Parker 1998; Chantler 1996).

PC ve CT grupları siber suçlular arasındaki en tehlikeli grubu oluşturmaktadır. Bu kişiler eski istihbaratçılardan olup her an kiralanabilecek profesyonel suçlulardır (Post 1996). Bu kişiler ortaklaşa casusluk yapmak konusunda son derece uzman olup, modern teknik bilgi ve becerilere sahiptirler. Bu alandaki teorilerden anlaşıldığı üzere, profesyonel suçlular, özellikle doğu bloğu ülkelerinin istihbarat servislerinin dağılmasından sonra ortaya çıkmış ve yaygınlaşmıştır (Denning 1998).

Günümüzde siber suçlar kavramı popüler bir kavram olmasına rağmen bu suçları işleyenler hakkında yeterince bilgiye sahip değiliz. Zira siber suçlar ve suçluları hakkında günümüzde yeterli sayıda araştırma bulunmamaktadır. Var olan araştırmalar da genellikle CP grubundaki suç işleyenlere yönelik yapılan araştırmalardır (Rogers 1999).

Dolayısı ile yapılan araştırmalar çoğunlukla CP grubundakiler hakkında olduğu için, diğer kategorilere genelleştirmek isabetli değildir. Bu araştırmada sonuçlarına göre CP

grubundaki suçlular; beyaz tenli, 12-30 yaşları arasında ve orta gelirli ailelere mensupturlar. Bu kişiler, yalnızlığı seven, sosyal yönleri zayıf, okuldaki performansları düşük kişilerden oluşmaktadır (Chantler 1996). Bu kişiler okuldan iyi bir derece ile mezun olup kariyer yapmak yerine, bilgisayar ve elektronik cihazlarla zamanını değerlendirmektedir (Chantler 1996).

"Hacking" eylemi, kişinin bilgisayarının tek hâkimi olduğu ve tek başına yaptığı bir aktivitedir. Bilgisayar ve internet bu suçu işleyen kişilerin kimliğini gizleyen bir örtü görevini üstlenmektedir. Dolayısıyla suçu işleyen ile kurban arasında yüz yüze bir etkileşim olmaz, suçlular kurbanların karşısına sanal bir kimlik ile çıkarlar. Sanal kimlik güç ve prestij sahibi biri gibi görünmek için kaçırılmaz bir fırsattır. Güç ve prestiji yansıtmak için çeşitli bilim-kurgu kitaplarındaki kahramanların isimlerini rumuz olarak kullanırlar. Bu kişiler gerçekte hayatla barışık olamadıklarından, bilgisayarı gerçeklerden kaçış için bir araç olarak görmektedirler (Hafner and Markoff 1995).

Siber suçlular, topluma önemli bir katkıda bulundukları kanısındadırlar, Onlara göre, kendileri olmasaydı, bilgi teknolojileri güvenliği önemli bir konu haline gelmeyecek ve bu konu üzerinde hiçbir ilerleme sağlanmayacaktı. Bu nedenle kendilerini, zalimlikle ve haksızlıkla savaşan bir bekçi köpeği (watch dog), hükümetleri ve bilişim sistemlerine yeterince önem vermeyen satıcıları gözlem altında tutan bir göz olarak görmektedirler (Rogers 1999).

Bilgisayarın hayatımıza girdiği yıllarda, siber suç failleri bu sistemlerle yakından ilgilenen ya da bu sistemleri kullanan kişilerden oluşurken, zamanla teknolojinin gelişmesi, bilgisayar kullanımının kolaylaşıp yaygınlaşması ve toplumlarda bilişim kültürünün oluşmaya başlamasıyla siber suçları işleyen kişilerin sayısında ve toplumdaki dağılımında artışlar yaşanmıştır (Değirmenci 2002).

Bu nedenle siber suç işleyenleri suç islemeye yönelten ve onları motive eden unsurları Shinder (2002) beş başlık altında gruplamıştır. Bunlar;

a) Oyun amaçlı (just for fun): Genç meraklılar ve/ya hackerlar eğlence için interneti bir oyun alanı, bilgisayarları da bir oyuncak gibi görmektedirler. Onlar için önemli olan oyuncakları kullanarak oyun oynamak ve eğlenmektir. Bu sebeple eğlenmek maksadıyla film indirmek, müzik indirmek, başkasının ağına girmek, web sayfasını kopyalamak, kabiliyet ve yeteneklerini ispat için virüs yollamak veya küçük parasal kazanımlar elde etmeye çalışırlar ve bunu meraklarını giderme ve başarma amacıyla bir eğlence unsuru olarak yaparlar. Asıl niyetleri zarar vermek değildir ancak bu faaliyetleriyle başkalarına maddi zararlar da verebilirler.

b) Para (money): İnsanları suç işlemeye iten en önemli sebeplerden birisi de paradır. Para insanlar için önemli bir değer olduğundan, pek çok kişi iyi para kazanmak maksadıyla bu suçları işlemektedir. Bazen bir banka çalışanı, bazen bir hacker tarafından başkalarının hesaplarından veya kredi kartlarından para çalınması bazen de bir şirketin ticari sırları gibi maddi değer ifade eden veya alıcı bulabilen enstrümanların çalınmasıdır. Bu kategoride genç, yaşlı, kadın, erkek, profesyonel veya farklı sosyo-ekonomik düzeydeki insanlar olabilir beyaz yakalı suçlar olarak da ifade edilir.

c) Duygu/ öfke/ intikam (emotion): Fakat bazen paradan da ön plana çıkan faktörler vardır. Bu faktörler, öfke, intikam ve aşk gibi duygusal faktörlerden oluşmaktadır. Eski arkadaş, eski sevgili, eski eş, eski işveren, hoşnut olunmayan komşu, arkadaş, memnuniyetsizlikle yapılan alış verişler, kötü not alınan ders öğretmenleri gibi pek çok insan bu faktörlerin etkisinde kalarak e-maille taciz, e-maille hakaret, e-maille tehdit, hesaplara izinsiz giriş, gizli sırları veya fotoğrafları deşifre etme, şirket bilgilerini çalma, silinmesini sağlama, şirket web sayfasının kopyasını yapma, ddos saldırıları yapma gibi suçları işlemekte ya da işlenmesine neden olmaktadır.

d) Cinsel amaçlar (sexual impulses): Her ne kadar biraz duygu içerse de bu kategori siber suçlar içerisinde şiddet içermesi yönüyle ayrı ve önemlidir. Seri tecavüzcüler, sadist cinsel ilişki arayışındakiler, çocuk pornosu sapkınları ve istismarcıları (pedophiles) ve hatta seri cinayet işleyenleri bu grupta sayabiliriz. Çocuk pornografisi başkalarını tahrik ve teşvik anlamında ticari amaçlıda olabilir. Bu

gruptakiler genelde erkektir, psikopatik ve depresif bozukluğu olan kişiler olup genç ve üstü yaş gruplarından çeşitlilik gösterirler.

e) Politik ve dini amaçlı (Politics/religion): Politik ve dini amaçlar için suç işleyenler ise interneti bir propaganda aracı olarak kullanmakta ve kendi politik hedeflerine karşı çeşitli saldırılar düzenlemektedirler. Dinsel inanışlar ve siyasi bağlılıklar nedeniyle insanlar çok vahim ve iğrenç tabir edilen suçlar işleyebilmektedirler. Siber terör saldırıları bu kategoride sayılabilir.

Sonuç olarak siber suç işleyen bir kişinin profili gerçek kimliği bilinmeyen bir kişinin karakteristiksel olarak değerlendirilmesidir. Bu değerlendirme kişisel, duygusal karakterle fiziksel yapıyı içermektedir. Karakteristiksel tanımlamaya uyan bir profil fiziksel anlamda uymayabilir, veya fiziksel olarak uyumlu bir profil karakteristiksel uyumsuzlukla olağan şüpheliler isabetli olmayabilir. Sadece soruşturmacılara ek bilgi sağlayan araçlar olarak fayda sağlar.

2.12 Siber Suç Mağdurlarının Genel Özellikleri

Bilgisayar ve internet aracılığıyla işlenen suçlarda bilinmeyen alan oldukça yüksek olup, %80'ler seviyesinin üzerinde olduğu değerlendirilmektedir. Bunun nedeni, mağdurların bu suçları ailelerinden, çevrelerinden, yakınlarından, kamuoyundan ve kolluk kuvvetlerinden saklamak istemelerinden kaynaklanmaktadır. Hatta bazen zarar görenler mağdur olduğunun farkında olmayıp sonradan haberdar olabilmekte, hatta hiç farkında olmadığı da olabilmektedir (Demirbaş 2005).

Kimler mağdur olabiliyor cevabına bakıldığında; hangi amaçla olursa olsun eğitimden eğlenceye, ticarete kadar bilgisayar ve interneti kullanan kişiler, gruplar, şirketler, kamu kurum ve kuruluşları ile yazılım ve güvenlik sistemleri siber ihlalciler açısından hedef olabilmekte ve mağdurlar tarafında yer alabilmektedirler.

Özellikle genç kız kullanıcılar sosyal medya kullanımında mağduriyetle karşılaştığında; (en çok da facebook) sahte hesap oluşturulması, fotoğrafının kullanılması, kimlik

bilgilerinin kullanılması gibi, sinir krizlerine büründüğü, mantıklı düşünemediği, kendi çabaları ve imkânları ile çözmeye çalıştığı, içinden çıkamayacağı veya daha büyük zarar ve kayıplarla yüz yüze kalacağını anladığında öncelikle bilgisi olduğuna inandığı güvenilir kaynaklardan sonrasında ise kolluk birimlerinden yardım istedikleri görülmektedir (İnt. Kyn.40).

Özellikle kişisel verilerin fotoğraf, video, ekran görüntüsü, gibi sosyal medya uygulamaları üzerinden cinsel istismar, şantaj ve tehdit amaçlı kullanıldığında mağdurların panikleyip, bu yolları izledikleri kolluk birimleri ifadelerinden öğrenilmektedir.

Şirketler seviyesinde gerçekleşen suçlar, genellikle kimseye duyurulmadan çözümlenmeye çalışılmaktadır. Bunun nedeni, şirket yöneticilerinin siber/bilişim suçları nedeniyle, kolluğun şirketin iç işlerine karışarak, mali konularda detaylı bilgi sahibi olma, şirket sırlarını öğrenme, yasal olmayan kayıt dışı faaliyetlerin ifşa olması korkularından kaynaklanmaktadır. Ayrıca, bu tür bir araştırmanın şirketin prestij yitirmesine neden olacağı inancı da yaygındır. Gerçekleşen ihlaller, yetkili makamlara bildirilmediğinden iş dünyası içinde gizli kalmakta ve bu nedenle bazı faillerin işlemiş oldukları suçlar gizli kalmaktadır. Özellikle şirket muhasebe kayıtlarını ele geçiren hackerlar kayıtları şifreleyip bir-kaç bin dolar karşılığında firmalara geri satmakta ve çoğunlukla firmaların bu paraları ödedikleri ve polise şikâyetçi olmayıp böyle yapanlar var bilginiz olsun anlamında bilgilendirme yaptıkları öğrenilmektedir.

Bilişim suçlarında mağdur durumunda olan bazı şirketlerin ticari yaklaşımları da belirleyici olmaktadır. Örneğin bazı şirketler, yıllık %5'e kadar olan zararları (parasal kayıpları) araştırma yapmaksızın olağan kabul etmektedirler (Demirbaş 2005). Bu anlamda finansal hizmet veren banka veya finans şirketlerinden "Truva atı" veya benzeri işleve sahip yazılımlar aracılığıyla siber ihlalciler müşterilerin hesaplarından küçük miktar hareketlerle aşırmalar yapmakta, banka çalışanları ve hesap sahipleri tarafından fark edilemeyen veya sonrasında telafi edilen bu küçük miktarlar faillere büyük kazançlar sağlamaktadır (Dülger 2004).

Siber suçlar konusunda uzmanlarca yapılan araştırmalarda, toplumda hangi kesimin daha yoğun olarak mağdur olduğu da incelenmektedir. Parker, bilgisayar ihlalleri (computer abuse) konusunda yaptığı çeşitli araştırmalarda, bu eylemlere bankacılık ve sigortacılık alanında daha çok rastlanıldığını ve bu sebeple de ABD'de bankalar ile sigorta şirketlerinin diğer alanlardaki kurumlara oranla daha yoğun olarak bu eylemlere maruz kaldıklarını açıklamaktadır. Buna karşılık, General Accounting Office ise ABD'de federal kamu kurumlarının bu suçlarda öncelikle mağdur olduğunu iddia etmektedir (Bequai 1998).

Avustralya'da Cit-Carb Chilsolm İnstitute of Technology'nin 2003 yılında gerçekleştirdiği bir araştırmada ise, kamu kurumları ile finans çevrelerinin toplumda en çok zarar gören kesimi oluşturduğu belirtilmektedir (Granville 2003).

Japonya'da 1971-1985 yıllarına ilişkin olarak 1985 yılında yayınlanan bir araştırmada bankalardan sonra en çok finans kuruluşlarının suç mağduru olduğu ortaya koyulmaktadır. Yine 1987 yılındaki AET toplantısında Japon heyeti ülkesindeki duruma ilişkin hazırladığı bir raporda suç mağduru olarak tarımsal kuruluşların birinci sırada yer aldığını bunları bankalar ile kamu kurumlarının izlediğini ifade etmişlerdir (Nir 2005).

İsveç'te National Swedish Council for Crime Prevention hesabına SOLARZ tarafından gerçekleştirilip 2002 yılı Mart ayında yayınlanan bir araştırmaya göreyse, bu ülkede bankalar ve onu takiben kamu sektöründe yer alan kurumlar suç mağdurları arasında birinci sırada yer almaktadır (Taşkın 2009).

National Center of Computer Crime Data'nın iki yıl süreyle Kaliforniya'da gerçekleştirdiği bir başka araştırmaya göre ise, bu suçlara ilişkin mağdurların büyük bir çoğunluğunu sıra ile ticari kuruluşlar, bankalar, telekomünikasyon firmaları, kamu kurumları ve bilgisayar üreten firmalar oluşturmaktadır. Bilgisayar suçu mağdurlarının belirlenmesi açısından genel olarak bu suçlardaki rakamların yüksekliğinden ve çeşitli kurum ve kuruluşların değişik emniyet tedbirleri ile sonuca gitmek istemelerinden dolayı bu konuda da diğer hususlarda olduğu gibi çok sağlıklı sonuçlar elde edebilmek pek mümkün olmamaktadır. Ancak suç mağdurları arasında bankaların ticari ve finans

kuruluşlarının ve kamu sektörünün diğer kesimlere oranla daha yoğun olarak çeşitli ihlallere maruz kaldığı ifade edilebilir (Yazıcıoğlu 1997).

Siber suçlar konusunda yapılan çeşitli araştırmalarda, toplumda hangi sektörün daha çok etkilendiği ve zarara uğradığı tespit edilmeye çalışılmaktadır. Bu çalışmaların ortak amacı, siber suçların yol açtığı zararları ortaya koyarak ekonomi ve finans sektörüne karşı bir tehdit olduğunu vurgulamaktır (Yazıcıoğlu 1997).

Ticaretle uğraşan ve pek çok şubesi olan şirketler birbirleri arasındaki bilgi paylaşımını bilgisayar ağları ile yapmaktadır. Stok, ciro, sipariş takibi gibi işlemler bu ağlar sayesinde şirketlerin bilgi işlem merkezlerine aktarılarak depolanmaktadır. Şirketler için hayati öneme sahip bu depolanmış bilgilere içeriden ulaşılabildiği gibi şirkete ait bilgisayar ağları kullanılarak dışarıdan da ulaşılmaktadır. Bu durum, günümüz teknolojisinin büyük bir miktardaki bilgiyi çok kısa bir sürede kopyalamaya izin vermesinden dolayı endüstriyel casusluk suçunun işlenmesine imkân sağlamaktadır. Özellikle hacker'ların bu ağlara sızıp bilgileri çalması ya da sabotaj etmesi şirketler için çok büyük zararlara neden olmaktadır. Özellikle CIA, FBI, Pentagon ve NATO gibi kuruluşların bilgisayar sistemlerine saldırılar yapılması ve çeşitli bilgilerin ele geçirilmesi, bilgisayar sistemleri ile depolanan bilgilerin her ne kadar güvenlik tedbiri alınsa da yeterince güvende olmadığını göstermektedir (Council of Europe, Organized Crime situation report September 2004).

Bilgisayar ağları sadece ekonomi ve finans sektörü için değil, aynı zamanda kamu ve toplum için de büyük bir önem taşımaktadır. Günümüzde kara, deniz, hava, demiryolu ve metro ulaşım trafikleri, hastane yönetimleri, elektrik, doğalgaz, su ve kanalizasyon işleri ile nükleer, hidro ve termik elektrik santrallerinde, haberleşme ve iletişim sistemleri, web yayıncılığı ve haberciliği, e-devlet hizmetlerinin yürütülmesinde tamamen bilişim sistemleri kullanılmaktadır.

Bunlara ilave olarak askeri birliklerin muhabere ve haberleşmesinde, çeşitli silah sistemlerinde, hava, deniz ve kara savaş araçlarının sevk, komuta ve kontrolünde, dost-düşman tanıma, erken uyarı sistemlerinde, askeri komuta ve kontrol merkezlerinde

bilgisayar ve ağları yaygın olarak kullanılmaktadır. A.B.D. ve Kanada'da 2003 yılında siber teröristler tarafından elektrik dağıtım şebekelerine saldırılar yapılmış ve neticede büyük zararlar ortaya çıkmıştır. Oluşan zararlar göstermiştir ki, bir ülke için hayati öneme sahip olan bu sistemler gerekli güvenlik tedbirleri alınmadığı sürece siber teröristler tarafından tehdit altında olacaktır. Özellikle askeri bilişim sistemlerine karşı yapılacak saldırılar, diğer sektörlere oranla çok daha büyük zararlara yol açacaktır (Council of Europe, Organized Crime situation report September 2004).

Soğuk savaş sonrası devletlerarası mücadeleler kurulan veya yönetilen ”siber ordu”larla siber alanda çok yoğun olarak yaşanmaktadır. Devletlerin sunmakta olduğu hizmetlerin ve bireysel yaşamın web üzerine taşınmasıyla kişisel özel yaşam ve kamusal verilerin ağ üzerinden erişilebilir olması bu alana ilgiyi artırmıştır. Özellikle web üzerinde sunulan çekici veya hayatımızı kolaylaştırıcı ücretsiz uygulama ve hizmetler bu amaçlar için kullanılan araçların başında gelmeye başlamıştır.

Benzer birkaç güncel örneğe bakılırsa;

Angry Birds casus yazılım mı: ABD’nin Ulusal Güvenlik Dairesi NSA’e ait Amerikalı eski istihbaratçı Edward Snowden’ın basına sızdırdığı bir belgede İngiltere ve ABD’nin gizli servislerinin akıllı telefonlar ve bilgisayarlarda oynanan Angry Birds’e sızarak kullanıcıların ziyaret edilen siteler ve telefon rehberi bilgileri ile konum bilgilerine ulaştığı iddiası. (İnt. Kyn.32).

Skype sosyal medya kanallarının Syrian Electronic Army isimli hacker grubunca hacklenmesi: Skype'ın sosyal medya kanallarını ele geçiren Syrian Electronic Army, bu kanallar üzerinden NSA ve Microsoft karşıtı mesajlarını yayınlayıp "Microsoft'un e-maillerini kullanmayın. Hesaplarınızı denetliyor ve verileri hükümete satıyorlar." mesajı verildi (İnt. Kyn.41).

CNN hacklenmesi: CNN'in sosyal medya hesaplarının Suriye Elektronik Ordusunca hacklenmesi. Bilgisayar korsanları bir tweet'le açıklama yaparak saldırının nedeninin "CNN'in yalan haberciliği" olduğunu belirtti (İnt. Kyn.42).

New York Times haber sitesi hacklenmesi: Suriye elektronik ordusu, New York Times ve Twitter internet sitelerini hack'ledi (İnt. Kyn.43).

Başbakanlığ'ın sitesinin Anonymous'ca hacklenmesi: Anonymous isimli Küresel hacker grubu, #OpTurkey (Gezi Parkı eylemleri) kapsamında Suriye Elektronik Ordusu desteğiyle, Türkiye Cumhuriyeti Başbakanlık internet sitesini çökerttiğini duyurdu (İnt. Kyn.44).

Harvard Üniversitesi'ne saldırı: Suriyeli protestocular tarafından İngiltere'nin ve dünyanın en iyi okulları arasında gösterilen Harvard Üniversitesi'nin resmi internet sitesi "www.harvard.edu" hacklenmesi (İnt. Kyn.45).

Güney Kore'nin birçok sitesinin Anonymous hacker grubunca siber saldırıya uğraması: Güney Kore'de Başta başkanlık sarayı Mavi Köşk, başbakanlık gibi önemli devlet kurumları sitelere giriş engellenerek, internet sitelerinin ana sayfasında yaklaşık 10 dakika boyunca "Birleştirici Başkan Kim Jong-un çok yaşa!" gibi ifadelerin yer alması. (İnt. Kyn.46).

İngiltere Siber Ordu Kurulması: İngiltere siber saldırılarla mücadele kapsamında aralarında hackerların da bulunduğu yüzlerce kişinin yer aldığı bir siber ordu kurdu (İnt. Kyn.47).

Türkiye Siber Ordu Kuruyor: Türkiye'nin 200 kişiden oluşturulacak ilk sivil siber güvenlik ordusu hackerlar arasından seçileceği, Bilim Kurulu'nun akademisyenler, Danışma Kurulunun ise kamu kurumları, STK'lar ve özel sektörün üst düzey yöneticilerince oluşturulacağını Bilim Teknoloji Bakanı açıkladı (İnt. Kyn.48).

3.MATERYAL METOT

Bu bölümde araştırmanın türü, evren ve örneklemi, araştırmada kullanılan veri toplama araçları ve veri analizleri hakkında bilgiler yer almaktadır.

3.1 Araştırmanın Modeli

Bu çalışmada TÜİK (2013) istatistiklerine göre en yaygın internet ve bilişim cihazları kullanıcı grubunun 16-24 yaş kategorisinde bulunan kişiler olması, yüksekokul, fakülte ve lisansüstü mezun olanların bilgisayar kullanım oranlarının daha yüksek olması ve e-okul ile liseler ve e-devlet kapsamında tüm kamu kurumlarında internet üzerinden bilgisayar aracılığıyla hizmet verilmesi düşünülerek Afyonkarahisar örnekleminde lise, üniversite ve kamu kurum çalışanlarına yönelik internet kullanım alışkanlıkları, siber (bilişim) suça ilişkin görüşleri ve suç farkındalıklarının ve suça karşı duyarlılıklarının eğitim seviyesi ve cinsiyet bağlamında ortaya konması amacıyla bir anket çalışması uygulanmıştır.

Betimsel çalışmalarda genellikle tarama yöntemi (survey) kullanılır. Genel tarama modelleri, çok sayıda elemandan oluşan bir evrende, evren hakkında genel bir yargıya varmak amacıyla, evrenin tümü ya da ondan alınacak bir grup, örnek ya da örneklem üzerinde yapılan tarama düzenlemeleridir Survey araştırmaları olayları olduğu gibi inceler ve tespitlere varmaya çalışır. Özellikle anket ve mülakat tekniklerinin araştırmalarda önemli bir yeri vardır (Aslantürk 1999, Karasar 2004). Anket çalışmaları, nicel yaklaşımın bir ürünü oldukları için genelde istatistik yöntemler kullanılır. Veriler sayısal rakamlara veya formüllere dayandırılır (Çepni 2001).

3.2 Evren ve Örneklem

Araştırmanın evrenini Afyonkarahisar ili, 2013/2014 eğitim öğretim döneminde Afyonkarahisar Milli Eğitim Müdürlüğüne bağlı lise öğrencileri ile yine aynı dönem Afyon Kocatepe Üniversitesi öğrenci ve öğretim görevlileri ve valiliğe bağlı kamu

kurumları çalışanları oluşturmaktadır. Araştırmanın örneklemi olarak uygun örnekleme yöntemi kullanılmıştır.

Örneklem grupları için tesadüfi olarak liseler arasından Afyonkarahisar Milli Eğitim Müdürlüğüne bağlı Ali Çağlar Anadolu Lisesi ve Zübeyde Hanım Kız Meslek Lisesi, lisans fakülteleri arasından Afyon Kocatepe Üniversitesi Eğitim Fakültesi lisans son sınıf öğrencileri ve kamu kurumlarından Afyonkarahisar'da Valiliğe bağlı Emniyet Müdürlüğü, Defterdarlık, Tapu Müdürlüğü çalışanları ile Ali Çağlar Anadolu Lisesi, Afyon Lisesi, Selçuklu Ortaokulunda çalışan öğretmenler ve Afyon Kocatepe Üniversitesi Öğretim Görevlileri seçilmiştir.

2014 yılı Mayıs ayında Afyonkarahisar il merkezinde gerçekleştirilen Anket uygulaması 2013/2014 eğitim-öğretim dönemi öğrencileri ve bu dönemde adı geçen kurumlarda çalışanların görüşlerini yansıtmaktadır.

3.3 Veri Toplama Aracı

Araştırmada veri toplama aracı olarak anket kullanılmıştır (EK-1). Ölçme Aracı demografik özellikler, internet kullanım alışkanlıkları ve siber suça yönelik görüşleri içeren beş bölümden oluşmakta ve 17 soru içermektedir.

Ölçme aracının ilk bölümünde katılımcıların cinsiyet ve eğitim seviye bilgileri toplanmıştır.

Anketin ikinci bölümünde katılımcıların siber suç işleme, internet kullanım, bağlanma aracı, süre, sıklık, amaç ve sosyal ağ kullanım bilgilerine ulaşılmaya (madde 1.2.3.4.5.6),

Üçüncü bölümde ise bildikleri siber/bilişim suç çeşitleri, suçla karşılaşma, suça karışma veya yakınlarının siber suçla karşılaşma tecrübelerini tespite çalışmaya (madde 7.8.9.10.11.12),

Dördüncü bölümde ise siber/bilişim suçla ilgili kolluk birimlerinin çalışmaları ve kanuni düzenlemeler hakkındaki düşüncelerini tespit etmeye (13.14.15),

Beşinci bölümde ise siber suçların önlenmesi için internette sınırlama getirilmesi ve gözetleme yapılmasına bireysel özgürlüklerin korunması bağlamında yaklaşımları (madde 16, 17) tespit edilmeye çalışılmıştır.

Ölçme aracında kullanılan anket maddeleri İlbaş'ın (2009) tarafından "Bilişim Suçları' nın Sosyo-Kültürel Seviyelere Göre Algı Analizi" adlı anket çalışması ve Dijle'nin (2006) "Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı" isimli anketi kullanılarak geliştirilmiştir. İlbaş'ın (2009) geliştirdiği anketin açık uçlu internet kullanımına ilişkin sorularından 4 maddesi kullanılmış, Dijle'nin (2006) anketindeki sorulardan 7 tanesi kullanılmış ve diğer 6 soru siber suçlara yönelik olarak güncellenerek geliştirilmiştir. Yapılan analizlerde örnekleme yöntemi, numune sayısı ve güven aralığı seviyesi %95 olarak tespit edilmiştir.

3.4 Verilerin Toplanması

Hazırlanmış olan anket formu ve tez önerisi Fen Bilimler Enstitüsü vasıtasıyla araştırma izni için Afyon Kocatepe Üniversitesi Rektörlüğü ve Afyonkarahisar Valiliğine gönderilmiş ve anketlerin uygulanması konusunda Afyonkarahisar Valiliğinden ve AKÜ Rektörlüğünden 2013–2014 eğitim öğretim yılında Afyonkarahisar ilinde lise ve lisans eğitimi alan öğrenciler ile kamu kurumlarında çalışanlara uygulama yapmak üzere izin alınmıştır (EK-2). Afyonkarahisar Milli Eğitim Müdürlüğü'ne bağlı 2 lise okulundaki son sınıf öğrencilere, Afyon Kocatepe Üniversitesi çeşitli bölümlerdeki lisans son sınıf öğrencilerine ve Afyon Kocatepe Üniversitesi Rektörlüğü ile Afyonkarahisar Valiliği kamu çalışanlarına anketleri doldurması rica edilmiştir. Dağıtılan anketlerden 777 tanesi geri dönmüş, eksiklik ve hatalar elden geçirilmiş olup 776 adet katılımcı anketi dikkate alınmış ve çalışmada kullanılmıştır.

3.5 Verilerin Çözümlenmesi

Anketlerin uygulanması sonucu elde edilen veriler SPSS programına aktarılmıştır. Öncelikle uygulamaya katılanların kişisel bilgilerini algı ve yorumlarını betimlemek amacıyla frekans (f) ve yüzde (%) hesaplaması yapılmıştır. Ankette yer verilen açık uçlu sorulara içerik analizi yapılarak niteliksel olarak gözlenen frekanslar arasındaki farkın anlamlı olup olmadığını tespit etmek amacıyla Ki-kare testi (Chi Square test) ile test edilmiştir.

Yapılan tüm istatistiksel çalışmalarda anlamlılık düzeyi 0,05 olarak kabul edilmiştir. Anketten elde edilen sonuçlar, tablolar üzerinde düzenlenerek yorumlanmıştır.

4. BULGULAR

Bu bölümde örneklemin bazı betimsel istatistikleri ile uygulanan anket sorularının değerlendirme sonucu bulgular ve yorumları bulunmaktadır.

4.1 Betimsel İstatistikler

Çizelge 4.1, 4.2, 4.3'de katılımcıların anketteki ilk bölüm olan kişisel bilgi formu kısmında verdikleri cevapların frekans ve yüzdeleri verilmiştir.

Çizelge 4.1 Katılımcıların Kurumsal Dağılımı

Kurum			f	%
Kamu personeli	Emniyet Md.	70	253	32,6
	Tapu Md.	18		
	Maliye	47		
	A.Ç.A.L.	21		
	Afyon Lise	40		
	Selçuklu İ.Ö.O	10		
	A.K.Ü (Öğrt. Görev.)	47		
Öğrenci (Lisans)	Afyon Kocatepe Üniversitesi		257	33,1
Öğrenci (Lise)	Ali Çağlar Anad. Lisesi	134	266	34,3
	Zübeyde H. Kız. Lisesi	132		
Toplam			776	100,0

Çizelge 4.1'de görüldüğü gibi örnekleme alınan 776 katılımcının kurumsal dağılımına bakıldığında kamu çalışanları %32,6 lık oranla 253, Afyon Kocatepe Üniversitesi çeşitli bölümlerden lisans son sınıf öğrencileri %33,1 lik oranla 257, lise son sınıf öğrencileri %34,3 lük oranla 266 kişiden oluşmaktadır.

Çizelge 4.2'de katılımcıların cinsiyet oranlarına bakıldığında %68 lik oranla Kadın katılımcılar 528, %32 lik oranla erkek katılımcılar 248 kişiden oluşmaktadır.

Çizelge 4.2 Katılımcıların Cinsiyet Dağılımı

Cinsiyet	f	%
Kadın	528	68,0
Erkek	248	32,0
Toplam	776	100,0

Katılımcıların Çizelge 4.3'te kurumsal akademik eğitim seviyelerine bakıldığında Lise düzeyi eğitime sahip olanlar %37 ile 287 kişi, Ön lisans eğitime sahip olanların % 8.6 ile 67 kişi olduğu, Lisans eğitime sahip olanların % 50.9 ile 395 kişi olduğu, Lisansüstü eğitime sahip olanların % 3.5 ile 27 kişi olduğu görülmüştür.

Çizelge 4.3 Katılımcılar Akademik Eğitim Seviyesi Dağılımı

Kurumlar	Eğitim seviyesi				Toplam
	Lise	Önlisans	Lisans	L.üstü	
Kamu	21	61	144	27	253
Akü	0	6	251	0	257
Lise	266	0	0	0	266
Toplam	(%37) 287	(%8.6) 67	(%50.9) 395	(%3.5) 27	(%100) 776

4.2 Araştırmaya İlişkin Bulgular

Bu bölümde araştırmanın amaçlarına uygun bir biçimde 2013/2014 yılında Afyonkarahisar ilinde yaşayan ve eğitim gören katılımcıların internet ve sosyal medya kullanım alışkanlıkları, kullanım amaçları, siber/bilişim suçu algıları ve suçla karşılaşma tecrübeleri ve suça duyarlılıkları tespit edilerek, internette denetlenme ve bireysel özgürlüklerin korunmasına yaklaşımları çıkarılarak eğitim düzeyi ve cinsiyet ile suç algısı üzerine değerlendirmeler ortaya konulmuştur. Bu değerlendirmede cinsiyet ve eğitim düzeyi esas alınarak kullanım, bilinç, algı ve hassasiyet düzeyi ile ilgili tespit ve değerlendirmeler için frekans ve yüzde verileri içeren tablolar oluşturulmuş ve içerik analizleri yapılmıştır.

Katılımcıların cinsiyet ve eğitim seviyesi dağılımları Çizelge 4.4 de verilmiş olup bakıldığında örnekleme toplamda 528 kadın katılımcının %2'si (9 kişi) lisansüstü, %45.4'ü (240 kişi) lisans, %2'si (11 kişi) ön lisans, %50'si (268 kişi) lise eğitimli, toplamda 248 erkek katılımcı %7.2'si (18 kişi) lisansüstü, %62.9'u (156 kişi) lisans, %22.5'i (56 kişi) ön lisans ve %7'si (18 kişi) lise eğitimli olarak 776 kişi katılmıştır.

Çizelge 4.4 Katılımcılar Cinsiyet ve Eğitim Seviyesi Dağılımı

Cinsiyeti	Eğitim seviyesi								Toplam
	Lise		Önlisans		Lisans		Lisansüstü		
	f	*%*	f	*%*	f	*%*	f	*%*	
Kadın	268	*50*	11	*02*	240	*45.4*	9	*02*	528
Erkek	18	*07*	56	*22.5*	156	*62.9*	18	*7.2*	248
Toplam	287	*37*	67	*9*	395	*51*	27	*3*	776

Katılımcıların siber suç farkındalığı ve suç işleyip işlemediklerine yönelik yapılan araştırma ve analizde (Çizelge 4.5) genel olarak %4.4 (34 kişi) evet, %83 (646 kişi) hayır, %8.5 (66 kişi) emin değilim, %3 (24 kişi) cevap vermek istemiyorum olarak ortaya çıktığı görülmüştür. Cinsiyet açısından bakıldığında kadınların %3'ü (17 kişi) evet, %84,2'si (445 kişi) hayır, %8'i (42 kişi) emin değilim, %3,5 (19 kişi) cevaplamak istemiyorum dediği, erkeklerin % 6,8'i (17 kişi) evet, %81 (201 kişi) hayır, %9,6 (24 kişi) emin değilim, %2 (5 kişi) cevaplamak istemiyorum dediği görülmüştür. Erkeklerde suç işleme oranının yüksek olduğu, kadınlarda cevap vermeme oranının yüksek olduğu dikkat çekmiştir. Ki kare testinde ($\chi 2$=7,901, df:4, p=0,095) olduğundan cinsiyet ve suç işleme durumu arasında anlamlı bir ilişki tespit edilememiştir.

Çizelge 4.5 Cinsiyete Göre Katılımcılar Siber Suç İşleme Dağılımı

Cinsiyeti	Hiç siber / bilişim suçu işlediniz mi								Toplam	
	Evet		Hayır		Emin değilim		Cevaplamak istemiyorum			
	f	*%*	f	*%*	f	*%*	f	*%*	f	%
Kadın	17	*3*	445	*84,2*	42	*8*	19	*3,5*	528	100
Erkek	17	*6,8*	201	*81*	24	*9,6*	5	*2*	248	100
Toplam	34	*4,4*	646	*83,2*	66	*8,5*	24	*3,1*	776	100

Katılımcıların siber suç işleme dağılımına eğitim seviyelerine göre bakıldığında (Çizelge 4.6) evet cevabının en yüksek %4.7 ile lisans seviyesinde, en düşük %2 ile ön lisans seviyesinde olduğu, hayır cevaplarının %86 ile en yüksek ön lisans seviyesinde, lisans seviyesinde %84 ve lise ve yüksek lisans seviyesinde ise %81 olduğu, emin değilim cevaplarıyla kararsızlığın en yüksek olduğu grup %14'le lisansüstü seviyesi olduğu diğer seviyelerde %8'lerde olduğu görülmüş, cevap vermek istemeyenlerin

sayısı en yüksek lise seviyesinde %5 olup lisans seviyesinde %2, ön lisans seviyesinde %1 olduğu, lisansüstü seviyesinde ise tüm katılımcıların cevap verdiği görülmüştür.

Çizelge 4.6 Eğitim Seviyesine Göre Katılımcılar Siber Suç İşleme Dağılımı

Hiç siber/bilişim suçu işlediniz mi	Eğitim seviyesi								Toplam
	Lise		Önlisans		Lisans		Lisansüstü		
	f	*%*	f	*%*	f	*%*	f	*%*	
Evet	12	*4*	2	*2*	19	*4,7*	1	*3,7*	34
Hayır	233	*81*	58	*86*	333	*84*	22	*81*	646
Emin değilim	23	*8*	6	*8,9*	33	*8,3*	4	*14*	66
Cevaplamak istemiyorum	15	*5*	1	*1*	8	*2*	0	*0*	24
Cevap Vermeyen	3	*1*	0	*0*	3	*0.7*	0	*0*	6
Toplam	287	100	67	100	395	100	27	100	776

Sonuç olarak suç işlemiş olduğundan emin olmama kararsızlığının (%14) lisansüstü eğitim seviyesinde en yüksek olduğu, cevap vermeme eğiliminin en yüksek lise seviyesinde (%5) görüldüğü, bilerek suç işleme eğiliminin en yüksek lisans (%4,7) seviyesinde olduğu görülmüştür.

Katılımcıların genel olarak internet kullanım süreleri dağılımına bakıldığında (Çizelge 4.7) 776 katılımcıdan %32,6'sının 10 yıl ve uzun süreli kullanıcı olduğu, %25,5'nin 6-9 yıl süreli kullanıcı olduğu, %28,9'unun 2-5 yıldır kullandığı, %5,8'inin 1 yıl ve kısa süreli kullanıcı olduğu yine %5 kişinin ise hiç internet kullanmadığı görülmüştür. Tablo incelendiğinde lisansüstü grubunun en az 6 ve daha uzun süreli ve tamamı internet kullanan grup olduğu, lisans seviyesinde 6 ve daha uzun süreli internet kullanımı %60 larda olduğu, ön lisans seviyesinde (tamamı kamu çalışanı) aynı durum %66 seviyelerinde olduğu, lise grubunun ise kullanım sürelerinin en düşük ve internet kullanmama sayısının en yüksek (%7) olduğu görülmüştür. Ki kare bağımsızlık testinde eğitim seviyesi ile internet kullanım süreleri arasında (χ^2=85,597, df:15, p=0,000) anlamlı bir ilişki tespit edilmiştir. Sonuç olarak eğitim seviyesi yükseldikçe internet kullanımının arttığı görülmüştür.

Çizelge 4.7 Eğitim Seviyesine Göre Katılımcılar İnternet Kullanım Dağılımı

Ne Kadar Süredir İnternet Kullanıyorsunuz	Eğitim seviyesi								Toplam	
	Lise		Önlisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
Cevap Vermeyen	11	*3,8*	2	*2,9*	2	*0,5*	0	*0*	15	*1,9*
Kullanmıyorum	21	*7*	5	*7,4*	15	*1,5*	0	*0*	41	*5,3*
1 yıldan Az Süre	29	*10*	2	*2,9*	14	*1,5*	0	*0*	45	*5,8*
2-5 yıldır	86	*30*	13	*19,4*	125	*31,5*	0	*0*	224	*28,9*
6-9 yıldır	73	*25,5*	21	*31*	102	*25,7*	2	*7,4*	198	*25,5*
10 yıl ve Uzun süreli	66	*23*	24	*35,8*	138	*34,8*	25	*92,5*	253	*32,6*
Toplam	287	100	67	100	395	100	27	100	776	100

Çizelge 4.8'de katılımcıların internete hangi ortamlardan bağlandıklarına dair yapılan analizlerde kullanıcılara cep telefonu, mobil modem(vınn, jet vb.), wi-fi ortak erişim ve kablolu ağ üzerinden olmak üzere sunulan seçeneklerde birden fazla erişim kaynağı kullanıldığı görülmüş, en çok kullanılan erişim kaynağının %62,6 ile wi-fi ortak erişim alanları olduğu, daha sonra %60 kullanıcı ile cep telefonları üzerinden internete bağlanıldığı, kablolu erişim ağı kullanımının %47,7, en az tercih edilen yöntemin ise %32 ile mobil modemler olduğu görülmüştür.

Çizelge 4.8 Eğitim Seviyesine Göre Katılımcılar İnternete Bağlanma Ortamları Dağılımı

İnternete Hangi Ortamlardan Bağlanıyorsunuz	Eğitim seviyesi								Toplam	
	Lise		Önlisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
Wi-fi ile Ortak Erişim	171	*59,5*	36	*53,7*	257	*65*	22	*81,4*	486	*62,6*
Cep Telefonu	189	*65,8*	37	*55,2*	225	*56,9*	16	*59,2*	467	*60,2*
Mobil Modem ile	85	*29,6*	29	*43,2*	124	*31,3*	11	*40,7*	249	*32*
Kablolu Ağ Üzerinden	127	*44,2*	44	*65,6*	182	*46*	17	*62,9*	370	*47,7*
Toplam	287	100	67	100	395	100	27	*100*	776	*100*

Lise öğrencilerinin en çok cep telefonu ile (%65,8) ve wi-fi erişim (59,5) bağlanma yöntemini kullandıkları, ön lisans grubunun en çok kablolu ağ ile (%65,6) bağlandığı,

lisans seviyesinde en çok wi-fi (%65)ve cep telefonu (%56,9), yüksek lisans seviyesinde wi-fi erişimlerinin en çok (%81,4) ve kablolu (%62,9) kullanıldığı görülmüştür. Sonuç olarak Wi-fi ortak erişim ortamlarının en yaygın kullanılan bağlanma aracı olması kullanıcılar için ekonomik olmakla birlikte saldırıya açık olma ve en güvensiz yöntemle bağlanma olarak öne çıktığı görülmüştür.

Çizelge 4.9'da katılımcıların interneti hangi amaçlar için kullandıklarına dair yapılan analizde genel olarak en çok kullanım amacının %74 ile iş ve derslerle ilgili konularda araştırma, %68,4 ile haber güncel gelişmeleri takip, % 63,7 ile özel ilgi duyulan alanlar, %61,5 ile iletişim, %42 ile oyun ve eğlence olduğu ve en az belirtilen %2,4 ile diğer gerekçeler olduğu görülmüştür.

Lise öğrencilerinin interneti en çok derslerle ilgili araştırma (%72), iletişim (sosyal medya) (%61,3), kişisel ilgi duyulan alanlar (%58,8), haber ve güncel gelişmeler (%51,5), oyun eğlence amaçlı (%49,8) kullandığı,

Ön Lisans grubunun ise en çok haberler ve güncel gelişmeleri takip (%71,6), iş ile ilgili konularla araştırma (%59,7), özel ilgi alanları (%58,2) ve iletişim (%56,7) (sosyal medya) amaçlı kullandığı,

Lisans grubunda en çok haber ve güncel gelişmeler (%78,7), iş dersle ilgili konular (%77,9), özel ilgili konular (%67), iletişim (%61), oyun eğlence (%37,7) ve sosyal çevre edinmek için (%28) amaçlı kullanıldığı,

Lisansüstü grubunda ise internet en çok iş ve dersle ilgili araştırma (%96), haberler ve güncel konuları takip (%88,8), özel ilgi alanları (%77), iletişim (%70), sosyal çevre (%22) amaçlı kullanıldığı görülmüştür.

Sonuç olarak en çok internet kullanımı lisansüstü seviyede, ders ve işle ilgili konularda araştırma en çok lisansüstü ve lisede, ön lisans ve lisans gruplarında haberler ve güncel konuları takip önde, oyun ve sosyal çevre edinme amaçlı en çok lise seviyesinde

kullanım dikkat çekmektedir. Yine iletişim amaçlı internetin en yüksek kullanımı lisansüstü seviyede olduğu görülmüştür.

Çizelge 4.9 Eğitim Seviyesine Göre Katılımcılar İnternete Bağlanma Amaçları Dağılımı

İnterneti Hangi Amaçlar İçin Kullanıyorsunuz	Eğitim seviyesi								Toplam	
	Lise		Önlisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
İş/Dersle İlgili Araştırma	207	*72*	40	*59,7*	308	*77,9*	26	*96*	581	*74,9*
Kişisel Olarak İlgi Duyduğum	169	*58,8*	39	*58,2*	265	*67*	21	*77,7*	494	*63,7*
Haber ve Güncel Gelişmeleri Takip	148	*51,5*	48	*71,6*	311	*78,7*	24	*88,8*	531	*68,4*
İletişim	176	*61,3*	38	*56,7*	244	*61,7*	19	*70*	477	*61,5*
Sosyal Çevre Edinme	96	*33,4*	19	*28,3*	98	*24,8*	6	*22,2*	219	*28,2*
Oyun ve Eğlence	143	*49,8*	25	*37,3*	149	*37,7*	11	*40,7*	328	*42,3*
Diğer	9	*3*	4	*5,9*	6	*1,5*	0	*0*	19	*2,4*
Toplam	287	*100*	67	100	395	100	27	*100*	776	*100*

Katılımcıların interneti kullanım sıklığına yönelik yapılan analizlerde (Çizelge 4.10) toplamda %57,6'lık bir bölümün hemen hemen her gün, %20,5'in haftada birkaç gün, % 8,6'nın iş ve okul saatleri dışında, %7'nin haftada bir günden az internet kullandığı görülmüştür. Hemen hemen her gün internet kullanımı %77.7 ile en yüksek Lisansüstü grubunda, %64,3 ile lisans, %55,2 ile ön lisans ve %47 ile en düşük lise grubunda olduğu görülmüştür.

Ki kare bağımsızlık testinde eğitim seviyesi ile internet kullanım sıklığı arasında ($\chi 2$=454,394, df:15, p=0,000) anlamlı bir ilişki tespit edilmiştir. Sonuç olarak eğitim seviyesi arttıkça internet kullanım sıklığının arttığı görülmektedir.

Katılımcıların sosyal paylaşım sitelerindeki hesapları (Çizelge 4.11) ile ilgili analizde genel olarak en çok kullanılan sosyal paylaşım sitesinin facebook %79,8 olduğu, bunu twitter 41.1, instagram (fotoğraf, video paylaşım sitesi) %18.3, foursquare (yer bildirim) %12.8 ve linkedin %3.5 uygulamalarının takip ettiği görülmüştür.

Lise grubu öğrenciler arasında en popüler uygulamanın %76.3 ile facebook, %34'le twitter, %16.7 instagram ve %13.9 ile foursquare uygulamasının kullanıldığı görülmüştür.

Çizelge 4.10 Eğitim Seviyesine Göre Katılımcılar İnternet Kullanım Sıklığı Dağılımı

İnternet Ortalama Kullanım Sıklığı	Eğitim seviyesi								Toplam	
	Lise		Önlisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
İş/Okul Saatleri Dışında	19	*6,6*	11	16,4	36	*9*	1	*3,7*	67	*8,6*
Haftada 1 Günden Daha Az	27	*9,4*	5	7,4	21	*5,3*	2	*7,4*	55	*7,1*
Haftada Bir Gün	17	*5,9*	2	2,9	9	*2,2*	1	*3,7*	29	*3,7*
Haftada Bir Kaç Gün	75	*26*	10	14,9	72	*18,2*	2	*7,4*	159	*20,5*
Hemen Hemen Her Gün	135	*47*	37	55,2	254	*64,3*	21	*77,7*	447	*57,6*
Cevap Vermeyen	13	*4,5*	2	2,9	4	*1*	0	*0*	19	*2,4*
Toplam	287	*100*	67	100	395	100	27	*100*	776	*100*

Çizelge 4.11 Eğitim Seviyesine Göre Katılımcılar Sosyal Paylaşım Siteleri Kullanım Dağılımı

Hangi Sosyal Paylaşım Sitelerde Hesabınız Var	Eğitim seviyesi								Toplam	
	Lise		Önlisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
Facebook	219	*76,3*	55	82	326	*82,5*	19	*70*	619	*79,8*
Twitter	98	*34,1*	20	29,8	187	*47,3*	14	*51,8*	319	*41,1*
İnstagram	48	*16,7*	8	11,9	84	*21,2*	2	*7,4*	142	*18,3*
Foursquare	40	*13,9*	6	8,9	52	*13,1*	1	*3,7*	99	*12,8*
Linkedin	2	*0,6*	2	2,9	15	*3,7*	8	*29,6*	27	*3,5*
Myspace	6	*2*	0	0	13	*3,2*	1	*3,7*	20	*2,6*
Hi5	3	*1*	1	1,4	6	*1,5*	0	*0*	10	*1,3*
Pinterest	2	*0,6*	0	0	2	*0,5*	0	*0*	4	*0,5*
Badoo	2	*0,6*	3	4,4	5	*1,4*	0	*0*	10	*1,3*
Friendfeed	1	*0,3*	0	0	1	*0,2*	0	*0*	2	*0,3*
Toplam	287	*100*	67	100	395	100	27	*100*	776	*100*

Önlisans grubunda sosyal paylaşım uygulamalarından %82 ile facebook, %20.8 ile twitter, %11,9'la instagram, %8,9 ile foursquare ve %4,4 ile badoo (arkadaşlık sitesi) kullanıldığı görülmüştür.

Lisans grubunda ise %82.5'le facebook, %47,3 ile twitter, %21 ile instagram, %13'le foursquare, %3.7 ile linkedin (iş cv oluşturma sitesi), %3'le myspace uygulamalarının kullanıldığı görülmüştür.

Lisansüstü grubunda %70'le facebook, %51.8'le twitter, %29.6 ile linkedin uygulamalarının kullanıldığı görülmüştür.

Sosyal paylaşım siteleri kullanımı cinsiyet yönüyle incelendiğinde (Çizelge 4.12) kadınlarla erkeklerde facebook ve twitter kullanımı birbirine yakın iken instgram kullanımında kadınların %21,4 ile erkeklere %11,6 göre daha çok kullandıkları, foursquare kullanımında kadınların %14,9 ile erkeklere %8 göre daha çok kullandıkları, Linkedin uygulamasını erkeklerin %6,4 ile kadınlara %2 göre daha çok kullandığı görülmüştür.

Sonuç olarak en yaygın sosyal paylaşım uygulamasının Facebook olduğu tüm kullanıcı gruplarında %80 ortalama ile kullanıldığı, Twitter kullanımının lise ve ön lisans grubunda daha az popüler iken lisans ve lisansüstü gruplarında ise her iki katılımcıdan birinin kullandığı, instagram (fotoğraf, video paylaşım sitesi) uygulamasının en çok lisans grubunca ve kadınlar tarafından kullanıldığı, foursquare (yer bildirim) uygulamasının ise lise grubunda ve kadınlar tarfından en çok kullanıldığı, iş müracaat ve cv oluşturma sitesi Linkedin uygulamasının ise lisansüstü grubunca ve erkekler tarafından en çok kullanıldığı görülmüştür.

Çizelge 4.12 Cinsiyete Göre Katılımcılar Sosyal Paylaşım Siteleri Kullanım Dağılımı

Cinsiyet	Hangi Sosyal Paylaşım Sitelerinde Hesabınız Var										Toplam
	facebook		twitter		instagram		foursquare		linkedin		
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*	
Kadın	425	*80,4*	248	*41,8*	113	*21,4*	79	*14,9*	11	*2*	528
Erkek	194	*78,2*	776	*39,5*	29	*11,6*	20	*8*	16	*6,4*	248

Katılımcıların siber/ bilişim suç çeşitleri ile ilgili bilgilerini (Çizelge 4.13) ölçmek için yapılan analizde tüm gruplarda en yaygın bilinen siber suçu olarak hacking (sanal korsanlık) olduğu en az bilinen suç türünün bot-net/ d-dos saldırıları olduğu görülmüştür.

Lise seviyesinde en çok bilinen siber suç sıralamasına bakıldığında %55,4'le hacking, %44'le banka ve kredi kartları hakkında işlenen suçlar, %42,5'le çocukların cinsel istismarı ve pornografi, %40'la verileri kanunsuz ele geçirme ve %40'la hakaret suçunun izlediği ve en az bilinen %10'la bot-net/ d-dos saldırıları suç türü olduğu görülmüştür.

Ön lisans grubunda en çok bilinen suç türleri sıralamasında %62.6 ile banka ve kredi kartları hakkında işlenen suçlar, %61ile hacking, %46 ile verileri kanunsuz ele geçirme, %44,7 ile nitelikli interaktif dolandırıcılık, %43 ile hakaret, %41 ile çocukların cinsel istismarı/ pornografi olarak devam ettiği en az bilinen suç türünün ise%5 ile bot-net/ d-dos saldırıları olduğu görülmüştür.

Lisans seviyesinde en çok bilinen siber suç sıralamasında %72,6 ile hacking, %58,9 ile banka ve kredi kartları hakkında işlenen suçlar, %50 ile çocukların cinsel istismarı/ pornografi olarak devam ettiği ve %9 ile en az bilinen suç türünün bot-net/ d-dos saldırıları olduğu görülmüştür.

Lisansüstü seviyesinde en çok bilinen siber suç sıralamasında %92,5 ile hacking, %74 ile banka ve kredi kartları hakkında işlenen suçlar ve verileri kanunsuz ele geçirme, %55 ile çocukların cinsel istismarı/ pornografi ve müstehcenlik olarak devam ettiği en az bilinen suç türünün %22 ile bot-net/ d-dos saldırıları olduğu görülmüştür.

Sonuç olarak siber suç bilgisinin eğitim seviyesi arttıkça oransal yükseldiği görülmüş, tüm eğitim seviyelerinde hacking (sanal korsanlık) suçunun en üst seviyede bilindiği, ön lisans seviyesinde mal varlığına ve ekonomik kazanımlara karşı suçların öne çıktığı, sanal kumarın lisansüstü seviyede en çok bilindiği, müstehcenlik / pornografi ve çocukların cinsel istismarı suçlarının lisans ve lisansüstü düzeyinde daha çok bilindiği,

tüm eğitim seviyelerinde crackli yazılım kullanma, örgütlü kumar ve d-dos siber saldırı suçlarının en az bilindiği görülmüştür.

Çizelge 4.13 Eğitim Seviyesine Göre Katılımcılar Siber Suç Bilgileri Dağılımı

Bildiğiniz Siber Suç Çeşitleri Nelerdir	Eğitim seviyesi								Toplam	
	Lise		Önlisans		Lisans		L.üstü			
	f	%	f	%	f	%	f	%	f	%
Hacking (Sanal Korsanlık)	159	*55,4*	41	*61*	287	*72,6*	25	*92,5*	512	*65,9*
Banka ve Kredi Kartı Hakkında İşlenen Suçlar	127	*44,2*	42	*62,6*	233	*58,9*	20	*74*	422	*56,9*
Verileri Kanunsuz Ele Geçirme	117	*40,7*	31	*46,2*	199	*50,3*	20	*74*	367	*47,2*
Çocukların Cinsel İstismarı Ve Pornoğrafi	122	*42,5*	28	*41,7*	201	*50,8*	15	*55,5*	366	*47,1*
Hakaret	115	*40*	29	*43,2*	163	*41,2*	10	*37*	317	*40,8*
Nitelikli İnteraktif Dolandırıcılık/ Hırsızlık	100	*34,8*	30	*44,7*	169	*42,7*	12	*44,4*	311	*40*
Terör veya Yasa Dışı Örgütsel Faliyetler	81	*28,2*	22	*32,8*	151	*38,2*	10	*37*	264	*34*
Müstehcenlik	61	*21,2*	19	*28,3*	116	*29,3*	15	*55,5*	211	*27,1*
Online Örgütlü Kumar	66	*22,9*	17	*25,3*	110	*27,8*	11	*40,7*	204	*26,2*
Cracklı Yazılım Kullanma	45	*15,6*	12	*17,9*	62	*15,6*	9	*33,3*	128	*16,4*
Bot-net / d-Dos Saldırıları	30	*10,4*	4	*5,9*	39	*9,8*	6	*22,2*	79	*10*
Toplam	287	*100*	67	100	395	100	27	*100*	776	*100*

Çizelge 4.14' de Toplumda tehlikeli olarak bilinen siber suç türlerinin tespitine yönelik yapılan analizde genel olarak %58 ile interaktif dolandırıcılık (ATM, kredi kartı) suçu öne çıkarken, %30'la yasa dışı yayınlar ikinci sırada, %25'le siber casusluğu takiben %11.5 ile bilgisayar korsanlığı, %7,7 ile lisans hakları ve %3.4 ile diğer suçların takip ettiği görülmüştür.

Çizelge 4.14'de Eğitim seviyelerine göre ekonomik kazanımlara karşı işlenen suçlar tüm seviyelerde en yüksek tehlikeli algılanırken lisansüstü seviyede %70 ile en yüksek, ön lisans seviyesinde %52 ile en düşük görülmüş, yasadışı yayınlar %40 ile lisansüstü seviyede en yüksek, %28,9 ile lise seviyesinde en düşük, lisans hakları lisans ve lisansüstü seviyede %11 olurken lise seviyesinde %2,7 olmuştur.

Çizelge 4.14 Eğitim Seviyesine Göre Toplumda En Tehlikeli Bilinen Siber Suç Türleri Dağılımı

En Tehlikeli Bilinen Siber Suçlar	Eğitim seviyesi								Toplam	
	Lise		Önlisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
İnterak. Dolandırıcılık (Atm, Kredi Kartı)	165	57,4	35	*52,2*	231	*58,4*	19	*70,3*	450	58,0
Yasa Dışı Yayın. (Pornografi, Hakaret)	83	28,9	22	*32,8*	122	*30,8*	11	*40,7*	236	30,4
Siber Casusluk	59	20,5	16	*23,8*	110	*27,8*	10	*37*	194	25,0
Bilgisayar Korsanlığı	32	11,1	10	*14,9*	39	*9,8*	8	*29,6*	89	11,5
Lisans hakları	8	2,7	5	*7,4*	44	*11,1*	3	11,1	60	7,7
Diğer	5	*1,7*	3	*4,4*	16	*4*	2	*7,4*	26	3,4
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.15'de Cinsiyete göre bakıldığında kadınlar tarafından en tehlikeli görülen siber suçların %58,3 ile interaktif dolandırıcılık, %30 ile yasadışı yayınlar (pornografi, müstehcenlik, hakaret), %19,5 il e siber casusluk, %10 ile siber korsanlık, %6,4 lisans hakları olduğu, erkekler tarafından en tehlikeli görülen %57,2 ile interaktif dolandırıcılık, %36,6 ile siber casusluk, %30,6 ile yasadışı yayınlar (pornografi, müstehcenlik, hakaret), %13,7 ile siber korsanlık, %10,4 ile lisans hakları olduğu görülmektedir. Her iki cinsiyette de ekonomik kazanımlara karşı işlenen dolandırıcılık suçları ve yasa dışı yayınların aynı oranda tehlikeli görüldüğü, siber casusluk ve lisans hakları ile bilgisayar korsanlığı erkeklerde daha çok bilindiği görülmüştür.

Çizelge 4.15 Cinsiyete GöreToplumda En Tehlikeli Bilinen Siber Suç Türleri Dağılımı

Size Göre Aşağıdaki Siber/Bilişim Suçlarından En Tehlikelisi Hangisidir	Cinsiyeti				Toplam
	Kadın		Erkek		
	f	%	f	%	
Siber Casusluk	103	*19,5*	91	*36,6*	194
Lisans Hakları	34	*6,4*	26	*10,4*	60
Yasa Dışı Yayınlar (Pornoğrafi, Hakaret)	160	*30*	76	*30,6*	236
Bilgisayar Korsanlığı	55	*10,4*	34	*13,7*	89
İnteraktif Dolandırıcılık (Atm, Kredi kartı vb)	308	*58,3*	142	*57,2*	450
Toplam	528	*100*	248	*100*	776

Toplumda en çok işlendiği düşünülen siber suçların tespitine yönelik (Çizelge 4.16) birden fazla şık işaretlemeleri istenen katılımcı cevaplarının analizinde genel olarak en yüksek %59,6 ile dolandırıcılık/hırsızlık suçlarının, %52,8 ile e- posta ve sosyal medya hesaplarının çalınması, %46,1 ile pornografi/müstehcenlik, %45 ile sosyal medyada taciz, tehdit, hakaret suçları, %34,2 ile bilgisayar ve network ağlarına izinsiz erişim ve %31,7 ile siber terör (casusluk, hizmeti durdurma) belirtildiği görülmüştür.

Eğitim seviyelerine göre (Çizelge 4.16) bakıldığında dolandırıcılık ve müstehcenlik suçlarının lise seviyesinde en yüksek, siber terör ve bilgisayar ağlarına izinsiz erişim lisansüstü seviyede daha yüksek, sosyal medya da taciz tehdit lise seviyesinde en yüksek olduğu görülmüştür.

Çizelge 4.16 Eğitim Seviyesine Göre En Çok İşlendiği Düşünülen Siber Suçlar Dağılımı

Size Göre En Çok İşlenen Siber/ Bilişim Suçu Hangisidir	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
Dolandırıcılık /Hırsızlık Suçları	172	*59,9*	39	*58,2*	238	*52,6*	14	*51,8*	463	59,6
E-Posta ve Sosyal Medya Hesaplarının Çalınması	150	52,2	29	*43,2*	219	*55,4*	12	44,4	410	52,8
Pornografi/ Müstehcenlik	158	*55*	35	*52,2*	183	*46,3*	12	*44,4*	358	46,1
Sosyal Medyada Taciz, Hakaret, Tehdit	138	*48*	29	*43,2*	171	*43,2*	11	*40,7*	349	44,9
Bilgisayar ve Network Ağlarına İzinsiz Erişim	112	*39*	16	*23,8*	127	*32,1*	11	*40,7*	266	34,2
Siber Terör, Propaganda Casusluk, Hizmeti Durdurma	84	*29,2*	21	*31,3*	131	*33,1*	10	*37*	246	31,7
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.17'de toplumda en çok işlendiği düşünülen siber suçlara cinsiyet açısından bakıldığında dolandırıcılık suçlarının kadın ve erkeklerde aynı oranda (%59) bilindiği, e-posta ve sosyal ağ hesap çalınması yine %52,8 ile aynı bilinirlikte olduğu, pornografi ve müstehcenlik erkeklerde %50 ile daha yüksek olduğu, yine erkeklerde siber terör konusunun %37 ile daha çok bilindiği dikkat çekmiştir.

En çok işlendiği yaygın olarak bilinen siber suçlardan "Sizin veya Arkadaşlarınızın Kullandığı Mail/Sosyal Ağ Hesabı veya Şifreleri Çalındı mı" (Çizelge 4.18) sorusu ile ilgili katılımcı cevaplarının analizinde katılımcıların %39,3 ile hayır, %26 ile evet, %20 ile evet birden çok, %12,8 ile bilgim yok cevaplarının verildiği görülmüştür.

Çizelge 4.17 Cinsiyete Göre Toplumda En Çok İşlendiği Düşünülen Siber Suçlar Dağılımı

Size Göre En Çok İşlenen Siber/Bilişim Suçları Hangisidir	Cinsiyeti				Toplam
	Kadın		Erkek		
	f	%	f	%	
Dolandırıcılık/Hırsızlık	316	*59,8*	147	*59,2*	463
E- Posta Ve Sosyal Medya Hesaplarının Çalınması	279	*52,8*	131	*52,8*	410
Pornografi/Müstehcenlik	232	*43,9*	126	*50,8*	358
Sosyal Medyada Taciz, Hakaret, Tehdit	234	*44,3*	115	*46,3*	349
Bilgisayar Ve Network Ağlarına İzinsiz Erişim	183	*34,6*	83	*33,4*	266
Siber Terör (Propaganda, Casusluk, Hizmeti Durdurma	154	*29,1*	92	*37*	246
Toplam	528	*100*	248	*100*	776

Yine Çizelge 4.18'e eğitim seviyelerine göre bakıldığında evet cevapları en yüksek ön lisans seviyesinde %34,3, lisansüstü seviyesinde %33, lisans seviyesinde %25,8 olurken en düşük lise seviyesinde %23,6 olduğu görülmüştür. Hayır, cevapları olarak bakıldığında en yüksek lisans seviyesinde %42,5, ön lisans %40, lise %36 ve en düşük lisansüstü seviyesinde %22 olduğu görülmüştür. Evet birden çok cevaplarına bakıldığında en yüksek %23.6 ile lise seviyesi, %20 ile lisans, %18.5 ile lisansüstü ve en düşük %9 ile ön lisans seviyesinde olduğu görülmüştür. Bilgisi olmayanlara bakıldığında en yüksek %22 ile lisansüstü, %15 ile ön lisans, %13,5 ile lise, en düşük %11 ile lisans grubunda olduğu görülmüştür.

Çizelge 4.19'da mail/sosyal ağ hesabı veya şifreleri çalınma dağılımı cinsiyet açısından incelendiğinde kadınların %40,5 ile hayır, %22,7 ile evet, %22,3 ile evet birden çok dediği, erkeklerin %36,6 ile hayır, %33 ile evet, %16,1 ile evet birden çok dediği, bilgisi olmayanların %12'lerde olduğu görülmüştür. Ki kare bağımsızlık testinde hesap şifrelerinin çalınması ve cinsiyet arasında ($\chi 2$=11,038, df:4, p=0,026) anlamlı bir ilişki

tespit edilmiştir. Sonuç olarak erkeklerin şifre çalınma olaylarını daha çok yaşadığı anlaşılmıştır.

Çizelge 4.18 Eğitim Seviyesine Göre Mail/Sosyal Ağ Hesabı veya Şifreleri Çalınma Dağılımı

E-Mail veya Sosyal Ağ Şifrelerin Çalınması	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
Evet	68	*23,6*	23	*34,3*	102	*25,8*	9	*33,3*	202	*26,0*
Hayır	104	*36,2*	27	*40,2*	168	*42.5*	6	*22,2*	305	*39,3*
Evet, birden çok	68	*23,6*	6	*8,9*	79	*20*	5	*18,5*	158	*20,4*
Bilgim yok	39	*13,5*	10	*14,9*	44	*11,1*	6	*22,2*	99	*12,8*
Cevap Vermeyen	7	*2,4*	1	*1,4*	3	*0,7*	1	*3,4*	12	*1,5*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.19 Cinsiyete Göre Kullanılan Mail/Sosyal Ağ Hesabı veya Şifreleri Çalınma Dağılımı

Cinsiyet	Sizin veya Arkadaşlarınızın Kullandığı Mail/ Sosyal Ağ Hesabı veya Şifreleri Çalındı mı								Toplam	
	Evet		Hayır		Evet, Birden Çok		Bilgim Yok			
	f	%	f	%	f	%	f	%	f	%
Kadın	120	*22.7*	214	*40,5*	118	*22,3*	67	*12,6*	528	*100*
Erkek	82	*33*	91	*36,6*	40	*16,1*	32	*12,9*	248	*100*

Çizelge 4.20'de ileri seviye bilginiz olsa hackerlik yapar mısınız sorusuyla ilgili herhangi bir amaç belirtilmeyen analizde genel olarak bakıldığında hayır diyenler %44,1, kesinlikle hayır diyenler %28,8, evet diyenler %17,3 olduğu görülmüştür.

Çizelge 4.20'ye eğitim seviyelerine göre bakıldığında evet cevapları en yüksek %23'le lise seviyesinde, en düşük %11'le lisansüstü seviyesinde olduğu, hayır cevaplarının en yüksek %53,7 ile ön lisans ve en düşük %23'le lise seviyesinde olduğu, kesinlikle hayır cevaplarının en yüksek %34' le lise seviyesinde ve en düşük %23'le ön lisans seviyesinde olduğu, fikir beyan etmeyenlerin ise en yüksek %9.5 ile lisans seviyesinde en düşük %6 ile ön lisans seviyesinde olduğu görülmüştür. Eğitim seviyesi ile hackerlik yapma konusunda Ki kare bağımsızlık testinde ($\chi 2$=37,258, df:12, p=0,000)

anlamlı bir ilişki tespit edilmiştir. Sonuç olarak eğitim seviyesi düştükçe hackerlik yapma eğilimi artmaktadır.

Çizelge 4.20 Eğitim Seviyesine Göre İleri Seviye Bilgisi Olma Durumunda Hackerlik Yapma Dağılımı

Hackerlik Yapma	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Evet	67	*23,3*	9	*13,4*	55	*13,9*	3	*11,1*	134	*17,3*
Hayır	92	*32*	36	*53,7*	202	*51,1*	12	*44,4*	342	*44,1*
Kes. Hayır	100	*34,8*	16	*23,8*	97	*24,5*	9	*33,3*	222	*28,8*
Fikrim Yok	22	*7,6*	4	*5,9*	38	*9,6*	2	*7,4*	66	*8,5*
Cev.Vermeyen	6	*2*	2	*2,8*	3	*0,7*	1	*3,4*	12	*1,5*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.21'de cinsiyet açısından hackerlik yapma konusuna bakıldığında hayır cevapları erkeklerde %50 iken kadınlarda %41.2, kesinlikle hayır diyenler kadınlarda %32, erkeklerde %21,3, fikir beyan etmeyenler erkeklerde %10,4 ve evet cevapları yaklaşık %17 ler ile yakın oranlarda olduğu görülmüştür. Ki kare bağımsızlık testinde ($\chi 2$=11,548, df:4, p=0,021) Cinsiyet ile hackerlik yapma konusunda anlamlı ilişki tespit edilmiştir. Sonuç olarak kadınlarda bu eğilimin yüksekliği dikkat çekmiştir.

Çizelge 4.21 Cinsiyete Göre İleri Seviye Bilgisi Olma Durumunda Hackerlik Yapma Dağılımı

Cinsiyet	İleri Seviyede Bilginiz Olsa Hackerlik/ Korsanlık Yapar mısınız								Toplam	
	Evet		Hayır		Kesinlikle hayır		Fikrim yok			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Kadın	92	*17,4*	218	41,2	169	*32*	40	*7,5*	528	*100*
Erkek	42	*16,9*	124	50	53	*21,3*	26	*10,4*	248	*100*

Çizelge 4.22'de Katılımcılara siber suçla karşılaştıklarında bunu önemli görüp ihbar etmeleri ile ilgili cevapların analizinde genel olarak %67.9 oranla evet cevabının

verildiği, önemsemeyenlerin %17.8 olduğu, hayır diyenlerin %9 olduğu, kesinlikle hayır diyenlerin %1.2 olduğu görülmüştür.

Çizelge 4.22 eğitim seviyesine göre incelendiğinde evet diyenlerin en yüksek %81,4 ile lisansüstü, %74,6 ile önlisans, %71,3 ile lisans ve %60 ile en düşük lise seviyesinde olduğu, hayır diyenlerin en yüksek %9,8 ile lisans seviyesi, %9 ile ön lisans, %8,3 ile lise ve %7,4 ile lisansüstü seviyesi olduğu, kesinlikle hayır cevabı ön lisans ve lisansüstü seviyesinde olmazken lise seviyesinde %2 ve lisans seviyesinde %1 civarında olduğu, önemsemeyenlere bakıldığında en yüksek %23,6 ile lise seviyesi, %15 ile lisans, %11.9 ile ön lisans olurken en düşük %7.4 ile lisansüstü seviyesinde olduğu görülmüştür. Suçu önemli görüp ihbar etme ile eğitim seviyesi arasında Ki kare bağımsızlık testinde ($\chi 2$=21,975, df:12, p=0,038) anlamlı bir ilişki olduğu, eğitim seviyesi yükseldikçe suçu önemseme ve ihbar etme eğiliminin arttığı tespit edilmiştir.

Çizelge 4.22 Eğitim Seviyesine Göre Siber/Bilişim Suçla Karşılaşmada İhbar Etme Dağılımı

Suçla Karşılaşmada İhbar Etme	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Evet	173	*60,2*	50	*74,6*	282	*71,3*	22	*81,4*	527	67,9
Hayır	24	*8,3*	6	*8,9*	39	*9,8*	2	*7,4*	71	9,1
Kesinlikle Hayır	6	*2*	0	*0*	3	*0,7*	0	*0*	9	1,2
Önemsemem	68	*23,6*	8	*11,9*	60	*15,1*	2	*7,4*	138	17,8
Cevap Vermeyen	16	*5,5*	3	*4,4*	11	*2,7*	1	*3,7*	31	*4*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.23'e cinsiyet açısından bakıldığında evet diyen erkekler %75,4, kadınlar %64,3, hayır diyen erkekler %10,8, kadınlar %8,3, önemsemem diyen kadınlar %21,5 iken erkeklerin %9,6 olduğu görülmüştür. Cinsiyet ve suçu ihbar etme konusunda Ki kare bağımsızlık testinde ($\chi 2$=18,943, df:4, p. p=0,001) olduğu ve anlamlı bir ilişki bulunduğu, kadınların suçu önemseme ve ihbar etme konusunda daha duyarsız olduğu görülmüştür.

Çizelge 4.24'de Siber/Bilişim suç mağduru olanların şikâyetçi olduklarında hak arayışında sonuç elde ettiğine inanma konusunda genel olarak yapılan analizde

katılımcıların %38,7 ile hayır, %17,1 ile kesinlikle hayır, %9,9 ile evet , %31,3 ile fikir beyan etmeyen olduğu görülmüştür.

Çizelge 4.23 Cinsiyete Göre Siber/Bilişim Suçla Karşılaşmada İhbar Etme Dağılımı

Cinsiyet	Bir Siber/Bilişim Suçuna Şahit Olursanız Bunu İhbar Eder misiniz								Toplam	
	Evet		Hayır		Kesinlikle hayır		Önemsemem			
	f	%	f	%	f	%	f	%	f	%
Kadın	340	64,3	44	*8,3*	6	*1,1*	114	*21,5*	528	*100*
Erkek	187	75,4	27	*10,8*	3	*1,2*	24	*9,6*	248	*100*

Çizelge 4.24 eğitim seviyelerine göre incelendiğinde evet cevaplarının en yüksek ön lisans %19,4, lisansüstü %18,5, lisans %9 ve en düşük %8 ile lise seviyesinde olduğu görülmüştür. Hayır, cevaplarının ön lisans ve lisans seviyesinde %41,7, lise seviyesinde % 35 ve en düşük lisansüstü seviyesinde %25,9 olmuştur. Kesinlikle hayır cevapları en yüksek %22,2 lisansüstü, %18,4 lise, %16,4 ile lisans ve %13,4 ile önlisans seviyesinde olduğu görülmüştür. Hak arayışında sonuç elde etmeye inanç konusunda olumsuz düşünceye sahiplik açısından lise, lisans ve ön lisans seviyelerinde %50 üzerinde bir görüşün hâkim olduğu görülmüştür. Fikir sahibi olmama konusunda ise en yüksek % 33 ile lise ve %31,8 ile lisans seviyesi olduğu görülmüştür. Öğrenime devam eden öğrenci gruplarında bu konuda bilgilendirmeye ihtiyaç olduğu görülmektedir. Ki kare bağımsızlık testinde ($\chi 2$=29,095, df:12, p=0,004) olduğu ve mağdurların hak arayışında sonuç elde etme konusunda eğitim seviyesi ile anlamlı bir ilişki olduğu, eğitim seviyesi azaldıkça hak arayışında sonuç elde etmeye olan inançın da azaldığı tespit edilmiştir.

Çizelge 4.25'de hak arayışında sonuç elde etmeye olan inanç dağılımı cinsiyet yönüyle incelendiğinde evet cevapları kadınlarda %6,8 iken erkeklerde %16,5 olduğu, hayır cevapları kadınlarda %38,6 iken erkeklerde %39,1 olduğu, kesinlikle hayır cevapları kadınlarda %18,1 iken erkeklerde 14,9 olduğu, fikir beyan etmeyenlerin kadınlarda %32,7 ve erkeklerde %28,2 olduğu görülmüştür. Ki kare bağımsızlık testinde ($\chi 2$=21,612, df:4, p=0,000) olduğu dolayısıyla cinsiyet ile hak arayışı arasında sonuç elde etmeye inanç konusunda anlamlı bir ilişki bulunduğu erkeklerde bu eğilimin yüksekliği tespit edilmiştir.

Çizelge 4.24 Eğitim Seviyesine Göre Mağdurların Şikâyetçi Olduklarında Sonuç Elde Etmesine İnanç Dağılımı

Şikayette Sonuç Elde Etmeye inanç	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Evet	23	*8*	13	*19,4*	36	*9,1*	5	*18,5*	77	*9,9*
Hayır	101	*35,1*	28	*41,7*	165	*41,7*	7	*25,9*	301	*38,7*
Kesinlikle Hayır	53	*18,4*	9	*13,4*	65	*16,4*	6	*22,2*	133	*17,1*
Fikrim Yok	95	*33,1*	14	*20,8*	126	*31,8*	8	*29,6*	243	*31,3*
Cevap Vermeyen	15	*5,2*	3	*4,4*	3	*0,7*	1	*3,7*	22	*2,8*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.25 Cinsiyete Göre Mağdurların Şikâyetçi Olduklarında Sonuç Elde Etmesine İnanç Dağılımı

Cinsiyet	Mağdurların Şikâyetçi Olduklarında Sonuç Elde Etmesine İnanç								Toplam	
	Evet		Hayır		Kesinlikle hayır		Fikrim Yok			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Kadın	36	6,8	204	38,6	96	*18,1*	173	*32,7*	528	*100*
Erkek	41	16,5	97	*39,1*	37	*14,9*	70	*28,2*	248	*100*

Siber suçlarla mücadelede emniyet teşkilatının çalışmalarını yeterli bulma konusunda (Çizelge 4.26) genel olarak katılımcı cevaplarının analizinde yeterli diyenler %15.9, kesinlikle yeterli 2.4, yetersiz diyen %59,4 ve kesinlikle yetersiz diyenlerin %18 olduğu görülmüştür. Yetersiz görenler %77 oranında olması dikkat çekmiştir.

Çizelge 4.26'ya eğitim seviyesi yönüyle bakıldığında yetersiz görenler en yüksek %64,8 ile lisans, %56,7 ile ön lisans öne çıkarken kesinlikle yetersiz diyenler en yüksek %20,2 ile lise ve %18,5 ile lisansüstü olduğu görülmüş, yeterli görenler ise en yüksek %20 ile ön lisans olurken en düşük %7,4 ile lisansüstü seviyesi olmuştur. Yeterlilik konusunda genel olarak lise seviyesinde %20, ön lisansda %21, lisansda %16 ve lisansüstü seviyede %11 kanaatin olduğu görülmüş, eğitim seviyesi arttıkça yeterli bulma düzeyinin azaldığı dikkat çekmiştir. Eğitim seviyesi ile Emniyet Teşkilatı çalışmalarını yeterli bulma konusunda Ki kare bağımsızlık testine göre ($\chi 2$=24,255, df:12, p=0,019)

olduğundan anlamlı bir ilişki olduğu, eğitim seviyesi yükseldikçe yeterli bulma oranı azaldığı saptanmıştır.

Çizelge 4.26 Eğitim Seviyesine Göre Siber Suçlarla Mücadelede Emniyet Çalışmalarını Yeterli Bulma Dağılımı

Emniyet Çalışmalarını Yeterli Bulma	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Kes. Yeterli	8	*2,7*	1	*1,4*	9	*2,2*	1	*3,7*	19	*2,4*
Yeterli	52	*18,1*	14	*20,8*	55	*13,9*	2	*7,4*	123	*15,9*
Yetersiz	152	*52,9*	38	*56,7*	256	*64,8*	15	*55,5*	461	*59,4*
Kes. Yetersiz	58	*20,2*	10	*14,9*	67	*16,9*	5	*18,5*	140	*18*
Cev. Vermeyen	17	*4,3*	4	*5,9*	8	*2*	4	*14,8*	33	*4,3*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.27'ye cinsiyet açısından bakıldığında kadınlar %59,8 yetersiz, %18,9 kesinlikle yetersiz ve yeterli olarak %6,5 olduğu, erkeklerin %58,4' ü yetersiz, %16,1'i kesinlikle yetersiz gördüğü yeterli olarak görenlerin %6,8 de kaldığı görülmüştür. Ki kare bağımsızlık testine göre cinsiyetle Emniyet çalışmalarını yeterli bulma arasında anlamlı bir ilişki bulunamamıştır.

Çizelge 4.27 Cinsiyete Göre Emniyet Çalışmalarını Yeterli Bulma Dağılımı

Cinsiyet	Siber Suçlarla Mücadelede Emniyet Teşkilatının Çalışmalarını Yeterli Buluyor musunuz								Toplam	
	Kesinlikle Yeterli		Yeterli		Yetersiz		Kesinlikle Yetersiz			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Kadın	24	*4,5*	11	*2*	316	*59,8*	100	*18,9*	528	*100*
Erkek	9	*3,6*	8	*3,2*	145	*58,4*	40	*16,1*	248	*100*

Siber/bilişim suçlarıyla ilgili mevcut yasaları yeterli bulma konusunda Çizelge 4.28'de ilgili katılımcıların cevapları analizinde genel olarak %62.4 ile yetersiz, %17.7 ile kesinlikle yetersiz, %14.4 ile yeterli, %2.4 ile kesinlikle yeterli olduğu görülmüştür. Olumsuz düşünce hâkimiyeti %80'ler civarında olduğu, olumlu düşünenlerin %17'ler

seviyesinde kaldığı görülmüştür. Bu anlamda ekseriyetle mevcut yasaların yetersizliği düşüncesinin yaygın olduğu ortaya çıkmıştır.

Çizelge 4.28'de mevcut yasaları yeterli bulma düşüncesine eğitim seviyelerine göre bakıldığında kesin yeterli diyen en yüksek %3,4 ile lise, %2 ile lisans, %1,4 ile ön lisans olurken lisansüstü seviyede sıfır olduğu, yeterli görenlerin en yüksek %20,9 ile lise, %11,3 ile lisans ve %11,1 ile lisansüstü olduğu, en düşük %5,9 ile ön lisans seviyesinin olduğu görülmüş, yeterli olarak olumlu değerlendirenler genel olarak %23 ile en yüksek lise seviyesinde olduğu, en düşük %11 ile lisansüstü seviyede olduğu anlaşılmıştır. Yetersiz olarak görenler en yüksek %68 ile lisans, %64 ile ön lisans, %62,9 ile lisansüstü ve en düşük %54 ile lise seviyesi olduğu, kesinlikle yetersiz kanaati en yüksek ön lisans seviyesinde %25,3, lisans seviyesinde %17,2, lisede %16,7 ve en düşük lisansüstü de %14,8 olduğu görülmüştür. Olumsuz görüşler en yüksek %89 ile ön lisans, %85 ile lisans, %78 ile lisansüstü ve en düşük %60 ile lise seviyesinde olduğu görülmüştür. Ki kare bağımsızlık testinde ($\chi 2$=37,590, df:12, p=0,000) olduğu dolayısıyla mevcut yasaları yetersiz bulma ile eğitim seviyesi arasında anlamlı bir ilişki olduğu, eğitim seviyesi arttıkça yetersiz bulma eğiliminin arttığı tespit edilmiştir. Bu kanaatin oluşmasında yaş ve deneyimlerinde etkilediği olduğu değerlendirilmiştir.

Çizelge 4.28 Eğitim Seviyesine Göre Mevcut Yasaları Yeterli Bulma Dağılımı

Mevcut Yasaları Yeterli Bulma	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Kes. Yeterli	10	*3,4*	1	*1,4*	8	*2*	0	*0*	19	2,4
Yeterli	60	*20,9*	4	*5,9*	45	*11,3*	3	*11,1*	112	14,4
Yetersiz	155	*54*	43	*64,1*	269	*68,1*	17	*62,9*	484	62,4
Kes. Yetersiz	48	*16,7*	17	*25,3*	68	*17,2*	4	*14,8*	137	17,7
Cev. Vermeyen	14	*4,8*	2	*2,9*	5	*1,2*	3	*11,1*	24	*3,1*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.29'daki veriler cinsiyet açısından analiz edildiğinde kadınlarda kesinlikle yeterli diyenler %2,2, yeterli %14,7, yetersiz %63, kesinlikle yetersiz %16,4 olduğu, erkeklerde kesinlikle yeterli %2,8, yeterli %13,7, yetersiz %60,8, kesinlikle yetersiz

%20,1 olduğu görülmüştür. Erkeklerde yetersizlik oranının kadınlardan daha yüksek olduğu anlaşılmıştır. Siber suçlarla mücadelede mevcut yasaları yeterli bulma ile cinsiyet arasında anlamlı bir ilişki tespit edilememiştir.

Çizelge 4.29 Cinsiyete Göre Siber Suçlarla Mücadelede Mevcut Yasaları Yeterli Bulma Dağılımı

Cinsiyet	Siber Suçlarla Mücadelede Mevcut Yasaları Yeterli Bulma								Toplam	
	Kesinlikle Yeterli		Yeterli		Yetersiz		Kesinlikle Yetersiz			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Kadın	12	*2,2*	78	*14,7*	333	*63*	87	*16,4*	528	*100*
Erkek	7	*2,8*	34	*13,7*	151	*60,8*	50	*20,1*	248	*100*

Çizelge 4.30'da Siber/bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesini olumlu karşılama konusu ile ilgili yapılan analizde genel olarak evet diyeneler %44,3, hayır diyenler %28, kesinlikle hayır diyenler %20, önemsemem diyenlerin %5 olduğu görülmüştür. Olumsuz düşünenlerin %48 ile olumlu düşünen %44'den fazla olduğu ve hemen hemen her iki kişiden birinin bu konuda kısıtlama veya sınırlama düşüncesine karşı olduğu görülmüştür.

Çizelge 4.30'da internet kullanımına sınırlama getirilmesine eğitim seviyelerine göre bakıldığında evet diyenler en yüksek %49 ile lisans seviyesi, %43 ile ön lisans, %38 ile lise ve en düşük %33 ile lisansüstü olduğu görülmüş, hayır diyenler lise, ön lisans ve lisans seviyelerinde %28 olduğu, lisansüstü seviyesinde %26 olduğu görülmüş, kesinlikle hayır diyenlere bakıldığında en yüksek %37 ile lisansüstü, %25 ile ön lisans, %23 ile lise ve %16 ile lisans olduğu görülmüştür. Kısıtlama konusuna olumsuz bakanların en yüksek %63 ile lisansüstü , %53 ile ön lisans, %51 ile lise ve %44 ile en düşük lisans seviyesi olmuştur. Kısıtlamaya olumsuz bakan en çok iki gurubun kamu çalışanları ve yaşça daha olgun kesim olduğu anlaşılmıştır. Bu durumu önemsemeyenlere bakıldığında %6 ile lise ve %5 ile lisans, %1 ile ön lisans olduğu lisansüstü seviyesinde önemsiz gören kimsenin olmadığı görülmüş, öğrenci olan katılımcıların bu konuya daha az duyarlılık gösterdikleri dikkat çekmiştir. Ki kare bağımsızlık testinde ($\chi 2$=31,330, df:12, p=0,002) olduğu dolayısıyla internet

kullanımına sınırlama getirilmesini olumlu karşılama ile eğitim seviyesi arasında anlamlı bir ilişki olduğu, eğitim seviyesi yükseldikçe olumlu karşılamanın azaldığı tespit edilmiştir. Ancak çalışanların verilerine göre yaş ve deneyiminde önemli olduğu değerlendirilmiştir.

Çizelge 4.30 Eğitim Seviyesine Göre İnternet Kullanımına Sınırlama Getirilmesi Dağılımı

İnternet Kullanımının Sınırlanması	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	%	f	%	f	%	f	%	f	%
Evet	109	*37,9*	29	*43,2*	197	*49,8*	9	*33,3*	344	44,3
Hayır	80	*27,8*	19	*28,3*	112	*28,3*	7	*25,9*	218	28,1
Kes. Hayır	67	*23,3*	17	*25,3*	63	*15,9*	10	*37*	157	20,2
Önemsemem	19	*6,6*	1	*1,4*	21	*5,3*	0	*0*	41	5,3
Cev.Vermeyen	12	*4,1*	1	*1,4*	2	*0,5*	1	*3,7*	16	*2*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

Çizelge 4.31'e cinsiyet yönüyle bakıldığında evet diyen kadınların %45,8 erkeklerden %41,1 fazla olduğu, hayır ve kesinlikle hayır diyen erkeklerin %29,4/ %24,1 kadınlardan %27,4/ %18,3 fazla olduğu, önemsemeyenlerin %5,8 ve %4 olduğu görülmüştür. Sonuç olarak erkeklerin %53,5 le olumsuz baktığı, kadınlarda ise %45,7'lerde olduğu görülmüştür. Cinsiyetle internet kullanımına sınırlama getirilmesini olumlu karşılama arasında ki kare bağımsızlık testinde anlamlı bir ilişki tespit edilememiştir.

Çizelge 4.31 Cinsiyete Göre İnternet Kullanımına Sınırlama Getirilmesi Dağılımı

Cinsiyet	Siber/bilişim Suçlarını Önlemek Amacıyla İnternet Kullanımına Sınırlama Getirilmesini Olumlu Karşılama								Toplam	
	Evet		Hayır		Kesinlikle Hayır		Önemsemem			
	f	%	f	%	f	%	f	%	f	%
Kadın	242	*45,8*	145	*27,4*	97	*18,3*	31	*5,8*	528	*100*
Erkek	102	*41,1*	73	*29,4*	60	*24,1*	10	*4*	248	*100*

Çizelge 4.32'de Siber suçları önlemek amacıyla internette gözetlenme konusuna olumlu bakmaya katılımcı cevaplarının genel olarak analizinde en yüksek %37,4 ile hayır, %31,7 ile kesinlikle hayır, sadece %21,6 ile evet denilirken önemsemeyenler % 7,3 olmuştur. Katılımcılardan internette gözetlenmeyi istemeyenlerin siber suçları önlemek amacıyla da olsa toplamda %69,1 olduğu dikkat çekmiştir.

İnternette gözetlenmeye olumlu bakışın eğitim seviyelerine göre analizinde evet diyenler en yüksek %31,3 ile ön lisans, %25 ile lisans, %22 ile lisansüstü ve en düşük %14,6 ile lise seviyesi olduğu görülmüştür. Hayır diyenler en yüksek % 40 ile lisans, %37 ile lisansüstü, %35 ile lise, en düşük %31 ile ön lisans seviyesi olduğu görülmüştür. Kesinlikle hayır diyenler en yüksek %39,7 ile lise olurken %33 ile lisansüstü, %28 ile ön lisans ve en düşük %26,5 ile lisans seviyesi olmuştur. Hayır olarak olumsuz görüşlere genel bakıldığında en yüksek %74.5 ile lise seviyesinde olduğu, sonra lisansüstü seviyede %70 lerde olduğu, lisans seviyesinde %66 olurken en düşük önlisans %59 seviyesinde olduğu görülmüştür. En genç ve en alt eğitim seviye katılımcıları (lise) ile en yüksek eğitim seviyesine sahip (lisansüstü) kesimin internette gözetlenmeye en çok karşı olan grup olduğu görülmüştür.

Çizelge 4.32 Eğitim Seviyesine Göre İnternette Gözetlenmeyi Olumlu Karşılama Dağılımı

Gözetlenmeyi Olumlu Karşılama	Eğitim seviyesi								Toplam	
	Lise		Ön lisans		Lisans		Lisansüstü			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Evet	42	*14,6*	21	*31,3*	99	*25*	6	*22,2*	168	*21,6*
Hayır	101	*35,1*	21	*31,3*	158	*40*	10	*37*	290	*37,4*
Kes. Hayır	114	*39,7*	19	*28,3*	104	*26,3*	9	*33,3*	246	*31,7*
Önemsemem	20	*6,9*	5	*7,4*	31	*7,8*	1	*3,4*	57	*7,3*
Cev. Vermeyen	10	*3,4*	1	*1,4*	3	*0,7*	1	*3,7*	15	*1,9*
Toplam	287	*100*	67	*100*	395	*100*	27	*100*	776	*100*

İnternet ortamında siber suçları önlemek amacıyla da olsa gözetlenmeye olumlu bakış hakkında Ki kare bağımsızlık testinde (χ^2=30,561, df:12, p=0,002) olduğu anlamlı bir ilişkinin varlığı tespit edilmiştir. Sonuç olarak lise seviyesindeki internet kullanıcılarının bireysel özgürlük ve özel hayatın gizliliğine önem verme konusunda daha hassas olduğu

ve gerekçesi ne olursa olsun hayatın gizli alanına karşı gözetlenme konusuna olumlu bakmadığı anlaşılmıştır.

Çizelge 4.33'de internette gözetlenmeyi olumlu karşılama konusu cinsiyet açısından incelendiğinde evet diyen erkeklerin %24,1 ile kadınlardan %20,4 yüksek olduğu, hayır cevaplarının %37 lerde aynı olduğu, kesinlikle hayır cevapları kadınlarda %32,7 ile erkeklerden %29,4 daha yüksek olduğu, önemsemeyenlerin %7'lerde olduğu, olumsuz düşüncenin kadınlarda %70,2 ile erkeklerden %66,4 daha yüksek olduğu görülmüştür. Cinsiyet ile gözetlenmeye olumlu bakış arasında anlamlı bir ilişki tespit edilememiştir.

Çizelge 4.33 Cinsiyete Göre İnternette Gözetlenmeyi Olumlu Karşılama Dağılımı

Cinsiyet	İnternette Gözetlenmeye Bakış								Toplam	
	Evet		Hayır		Kesinlikle Hayır		Önemsemem			
	f	*%*	f	*%*	f	*%*	f	*%*	f	*%*
Kadın	108	*20,4*	198	*37,5*	173	*32,7*	38	*7,1*	528	*100*
Erkek	60	*24,1*	92	*37*	73	*29,4*	19	*7,6*	248	*100*

5. TARTIŞMA, SONUÇ VE ÖNERİLER

Bu bölümde çalışma kapsamında frekans ve yüzde ile edilen bulgular ile ki kare bağımsızlık test sonuçları yorumlanmış olup benzer olduğu tespit edilen çalışmalar ile karşılaştırma ve kıyaslamalar yapılmıştır.

TÜİK istatistiklerine göre en yaygın internet ve bilişim cihazları kullanıcı grubu olan 16-24 yaş kategorisi lise ve lisans eğitim seviye grubunda öğrenim gören kesimi kapsadığından çalışmada ana hedef grubu olmuştur. Afyonkarahisar örnekleminde 2013/2014 dönemi öğrenci ve kamu çalışanları üzerinde gerçekleştirilen çalışmada ankete cevap veren geçerli 776 katılımcının 623 kişisi bu yaş aralığındadır. Bu katılımcılardan 528'i kadın ve 248'i de erkektir. Katılımcılardan 287 kişi lise eğitimli, 67 kişi ön lisans, 395 kişi lisans ve 27 kişi lisansüstü eğitimlidir.

Taş'ın (2010) çalışmasında bilişim suçu işlediği tespit edilen 1727 kişinin cinsiyetlerine göre dağılımında erkeklerin 1533 kişi ile (%89), kadınların 194 kişi ile (%11) olduğunu tespit etmiştir. Çalışmada katılımcıların siber suç farkındalığı ve suç işleyip işlemediklerine yönelik yapılan analizde (Çizelge 4.2) Ki kare testinde cinsiyet ve suç işleme durumu arasında anlamlı bir ilişki tespit edilememiş ancak suç işlediğini bilen erkekler (%6,8) bayanlardan (%3) iki kat daha fazla olmuş, erkeklerde suç işleme oranı kadınlara göre daha yüksek olduğu dikkat çekmiştir.

Slovenya'da Maja ve Bojan'nın (2010) çalışmasında 20 ila 48 yaş arası genel katılımcılar arasında "hiç siber suç işlediniz mi" sorusu için bulduğu sonuçlar katılımcıların %54'ü evet, %42'si hayır ve %4'ü ise bilmiyorum olmuştur. Eğitim seviyesi olarak yükseköğretim (tüm lisans grupları) %47 evet, %47 hayır ve %8 bilmiyorum olmuştur. Alt eğitim seviyelerinde %67 evet ve %33 hayır cevaplarını bulmuştur.

Katılımcıların siber suç işleme durumlarının incelenmesinde (Çizelge 4.6) evet cevabının en yüksek %4.7 ile lisans öğrencilerinde, hayır cevaplarının genel olarak

%83,2 olduğu, kararsızlığın en yüksek %14'le lisansüstü seviyeli akademik personelde olduğu görülmüştür.

İlbaş'ın (2009) çalışmasında bulduğu internet kullanım sürelerine bakıldığında 10 yıl ve üzeri %27,7, 6-9 yıl %46,1, 2-5 yıl %23,2, 1 yıl ve üzeri %7 ve kullanmayan %1,2 olduğu, Afyonkarahisar örneklemindeki aynı kriterlere bakıldığında (lisans ve lisansüstü birlikte) 10 yıl ve üzeri %63,6, 6-9 yıl %16,5, 2-5 yıl %15,75, 1 yıldan az süre 0,75, kullanmayan %0,75 olduğu görülmüştür.

Afyonkarahisar örnekleminde internet kullanım sürelerinin yüksekliği ve kullanmayan sayısındaki düşüklük dikkat çekmekte olup 2009'dan bu yana internet kullanımının yaygınlaştığıda anlaşılmaktadır.

İnternet kullanımıyla ilgili çalışma kapsamında 776 katılımcının %32,6 ile çoğunluğunun 10 yıl ve üzeri kullanıcı olduğu anlaşılmıştır. Eğitim seviyelerine göre lisansüstü eğitim kapsamındaki akademik personelin en az 6 yıl ve daha uzun süreli ve tamamı %100 internet kullanan kesim olduğu ve lise seviyesinde kullanım sürelerinin düşüklüğü ve internet kullanmama sayısının yüksekliği dikkat çekmiştir.

İlbaş'ın (2009) çalışmasında tespit ettiği değerler İnternet'e evden bağlananlar (kablolu) %93,3, İnternet'e işyeriden veya okuldan bağlananlar % 67,8, İnternet'e İnternet kafelerden bağlananlar %18,7, İnternet'e ortak kullanım alanlarından bağlananlar (wi-fi) % 31,9 olarak tespit etmiştir. Afyonkarahisar örnekleminde wi-fi kullanımı aynı kriterde (lisans %65 + lisansüstü %81,4) %73,2 olduğu, kablolu bağlanımın (lisans öğrencileri %46 + akademik personel %62,9) %54,4 olduğu görülmektedir. 2009 yılından 2014'e bireysel internet kullanımında wi-fi hizmet ve kullanımının büyük artış göstermesi olarak değerlendirilmiştir.

İlbaş'ın (2009) çalışmasında internet kullanım amaçları ile ilgili tespitlerinde İş / ders ile ilgili konularda araştırma yapmak % 93,5, İlgi duyulan kişisel konularda araştırma yapmak % 90,5, Haber ve güncel gelişmeleri takip etmek % 81,8, İletişim amaçlı kullanım % 86,3 Sosyal çevre edinme amaçlı kullanım %24,9 olarak bulmuştur.

Aynı kriterlere göre Afyonkarahisar örnekleminde (lisans öğrencileri ve akademik personel) değerler iş ve dersle ilgili konularda araştırma %86,9, haberler ve güncel gelişmeleri takip %83,7, İlgi duyulan kişisel konularda araştırma yapmak %72, iletişim %65,5, sosyal çevre edinme amaçlı kullanım %25 seviyelerinde olmuştur. Kullanım amaçlarındaki öncelik iş ve dersle ilgili konularda araştırma olurken haberler ve güncel konuları takip konusunda popülerliğin arttığı dikkat çekmiştir. Afyonkarahisar'da yaşayan öğrenciler ve kamu çalışanlarının gündem oluşturan gücel gelişmeleri ve haberleri takip ettiği bunun için sık sık interneti kullandığı anlaşılmıştır.

Yine Dijle'nin (2006) çalışmasında internet kullanım amaçları ile ilgili sonuçları; Araştırma yapmak için %73,9, Arkadaş edinmek için %2,3, Haberleşmek için %23,8 olarak tespit etmiştir.

Toruk'un (2007) çalışmasında internete bağlanma amacı ile cinsiyet arasında anlamlı bir ilişki bulamadığı gibi bu çalışmada da anlamlı bir ilişki gözlenmemiştir.

İnternetin kullanım sıklığına yönelik analizlerde (Çizelge 4.7) genelde %57,6'lık bir bölümün hemen hemen her gün internet kullandığı, hemen hemen her gün internet kullanımın %77,7 ile en yüksek Lisansüstü grubunda, olduğu görülmüş, Ki kare bağımsızlık testinde eğitim seviyesi ile internet kullanım sıklığı arasında (χ^2=454,394, df:15, p=0,000) anlamlı bir ilişki tespit edilmiş ve eğitim seviyesi arttıkça internet kullanım sıklığının arttığı görülmüştür.

İlbaş'ın (2009) çalışmasında internet kullanım sıklığı ile ilgili sonuçlarında Hemen hemen her gün kullanıyorum % 85,5, İş / Okul saatleri dışında kullanmıyorum % 2,5, Haftada 1 günden daha seyrek olarak kullanıyorum %1,0, Haftada bir gün kullanıyorum %1,5, Haftada birkaç gün kullanıyorum % 9,5 olarak bulmuştur.

İnternet kullanımında internete erişim için kullanılan bağlanma ortamları da önem arz etmektedir. Nitekim internete bağlanma ortamlarına dair analizlerde en çok kullanılan

erişim kaynağının %62,6 ile wi-fi ortak erişim alanları, %60 ile cep telefonları olduğu, öncelikli tercihin ücretsiz ortamlar ve sonrasında cep telefonları olduğu anlaşılmıştır.

Cep telefonlarının %60 ile ikinci en çok bağlanma aracı olması, akıllı tabir edilen multi fonksiyonlu telefonların kullanımının yaygınlaştığının ve hayatımızın her anında yakınımızda olduğunun bir göstergesi olarak değerlendirilmiştir.

Cep telefonu ile internete bağlanmayı en yüksek Lise öğrencilerinin (%65,8) kullanması, lise seviyesindeki öğrencilerin internet erişimli cep telefonuna sahip olma ve kullanma oranlarını göstermesi bakımından önemlidir.

Mobil modemlerin (jet, vın vb.) %32 ile en az tercih edilen bağlanma yöntemi olması akıllı telefonlara eklenen mobil wi-fi dağıtım (hot-spot) özellikleri ile doğru orantılı olarak azalması şeklinde değerlendirilmiştir.

Kamu çalışanlarının internete erişimde en çok kablolu ağ kullanması (ön lisans %65,6) çalışanların kamu kurumu imkânlarını kullanması olarak değerlendirilmiştir.

Üniversite öğrencilerinin (%65) ve üniversite akademik personelin (%81,4) wi-fi erişimlerini en çok kullanan kesim olması üniversite kampüs alanlarında ve yurtlarda sunulan ücretsiz wi-fi hizmetiyle orantılı olması olarak değerlendirilmiştir.

Çalışmada en yaygın internete bağlanma yöntemi olarak öne çıkan wi-fi aracılığıyla internet erişimi, güvenli veri transferi ve saldırılara açık olma açısından en az güvenli olan bağlanma yöntemi olmasıyla önemli bir zayıflık olarak değerlendirilmiştir.

Sosyal paylaşım uygulamalarındaki hesaplar ile ilgili çalışmada Ki kare bağımsızlık testinde cinsiyet ve eğitim seviyesi ile sosyal paylaşım site sahipliği arasında anlamlı bir ilişki tespit edilememiştir. Ancak %80 ile en çok kullanılan sosyal paylaşım sitesinin facebook olduğu görülmüş, kullanımın en yüksek üniversite öğrencilerinde ve yine lise öğrencilerinde olması, kullanım amaçları açısından sorgulanması gereken bir konu olarak değerlendilmiştir.

İkinci olarak en çok twitter uygulamasının kullanıldığı, lisansüstü (%51,8) ve lisans (%47) kesimlerinde yaygın olduğu, interneti kullanım amaçlarıyla uyumlu olarak haber ve güncel gelişmeleri takip sonuçlarıyla uyumlu olduğu görülmüştür.

İnstagram (fotoğraf video paylaşım) uygulaması en çok üniversite öğrencilerinde (%21) ve kadınlarda yaygın olduğu, foursquare (yer bildirim) uygulamasının ise lise öğrencilerinde (%13.9) ve kadınlarda yaygın olması, iş müracaat ve özgeçmiş (cv) oluşturma sitesi LinkedIn uygulamasının ise lisansüstü grubunca (%29.6) ve erkeklerde en çok kullanılması yaş seviyeleri ve cinsiyete göre ilgi alanlarını ve öncelikleri göstermesi bakımından önemli görülmüştür.

Maja ve Bojan'nın (2010) çalışmasında siber suç bilgisi ile ilgili bulgularında lisans hakları ihlali %24 ile ilk sırada, %20 ile bilişim sistemleri ve ağlara illegal erişim ikinci, verilere kanunsuz erişim %11 ve çocuk pornografisi %11, kimlik hırsızlığı %10, interaktif dolandırıcılık %8 olarak tespit etmiştir.

Slovenya'da en çok bilinmen lisans hakları ihlali suçunun Afyonkarahisar örnekleminde çok önemli olarak görülmediği, ekonomik kazanımlara karşı yaygın olan interaktif dolandırıcılık suçlarının da Slovenya'da çok bilinmediği anlaşılmıştır. Buradan hareketle toplumda mağdurların en çok karşılaştığı suçların kulaktan kulağa anlatılan hikâyelerle en yaygın bilinen suçlar olduğu değerlendirilmiştir.

Toplumda en tehlikeli olarak bilinen siber suç türlerine bakıldığında %58 ile interaktif dolandırıcılık (ATM, kredi kartı) suçu öne çıkarken, %30'la yasa dışı yayınlar ikinci sırada, %25'le siber casusluğu takiben %11,5 ile bilgisayar korsanlığı, %7,7 ile lisans hakları suçlarının takip ettiği görülmüştür.

Dijle'nin (2006) çalışmasında en tehlikeli siber/bilişim suç türlerinde dolandırıcılık %61, lisans hakları %13,6, bilgisayar sabotajı %14,9 ve yasadışı yayınlar (pornografi, hakaret vb.) %10,6 olarak tespit etmiştir.

Toplumda hala ekonomik kazanımlara karşı işlenen siber suçların en tehlikeli olarak görüldüğü, yasadışı yayınların (pornografi, müstehcenlik, taciz, hakaret vb.) ise tehlikeli görülme algısı artarak 2006 yılına göre üç kat oranda yükseldiği, lisans hakları ile ilgili suçların önem kaybettiği anlaşılmıştır.

Bilişim sistemleri aracılığıyla ekonomik kazanımlara karşı işlenen dolandırıcılık ve hırsızlık suçlarının %59,6 en çok işlendiği düşünülen siber/bilişim suçlarından olduğu, bunu %52,8 ile e-posta ve sosyal medya hesaplarının çalınması, %46,1 ile pornografi/müstehcenlik, %45 ile sosyal medyada taciz, tehdit, hakaret suçları, %34,2 ile bilgisayar ve network ağlarına izinsiz erişim ve %31,7 ile siber terör (casusluk, hizmeti durdurma) suçları takip ettiği görülmüştür.

Dijle'nin (2006) çalışmasında en çok işlenen yasa dışı suçlarda Pornografi %45,6, Siber terör %19,8, Hakaret %9,4 olarak tespit etmiş, bu çalışma ile kıyaslandığında siber terör algısının ve siber uzayda hakaret fiillerinin 2006 yılından bu yana ciddi oranda arttığı görülmüştür

E- posta ve sosyal medya hesaplarının çalınması ile ilgili tespitlerde evet ve evet birden çok cevapları toplamının %46 olması ve hayır cevaplarından yüksek olması katılımcı her iki kişiden birinin bu konuda ya mağdur ya da mağdur olanlarla yakın olduğunu göstermektedir. Özellikle facebook sosyal ağ kullanımının %80'lerde olduğu da dikkate alınınca buradan mail veya sosyal hesaplarda kullanılan şifrelerin güvenli olarak oluşturulması veya kullanılan şifrelerin güvenli olarak saklanması, paylaşılmaması konularında ihmallerin olduğu anlaşılmaktadır. Öğretim görevlileri ve kamu çalışanlarında evet cevaplarının yüksekliği kamu çalışanlarının şifre güvenliğine ve paylaşımına daha az dikkat ettikleri, özellikle lise öğrencilerinin bu konuda daha duyarlı olduğu anlaşılmıştır. Hayır cevaplarının azlığıyla akademik personel arasında şifre paylaşımının yaygın olduğu, birden çok hesap veya şifre çaldırma durumlarının bayan öğrencilerde fazla olduğu dikkat çekmiştir.

Siber suçla karşılaştıklarında bunu önemli görme ve ihbar etme duyarlılığının (Çizelge 4.22) toplumda %67,9, önemsemeyenlerin %17,8 olduğu görülmüş, ihbar etme ile

eğitim seviyesi arasında Ki kare bağımsızlık testinde ($\chi 2$=21,975, df:12, p=0,038) anlamlı bir ilişki olduğu, eğitim seviyesi azaldıkça ihbar etme ve suçu önemseme eğiliminin azaldığı anlaşılmış, cinsiyet açısından bakıldığında cinsiyet ve suçu ihbar etme arasında Ki kare bağımsızlık testinde ($\chi 2$=18,943, df:4, p. p=0,001) anlamlı bir ilişki bulunduğu, erkeklerin suçu daha çok önemsediği ve ihbar etmede daha duyarlı olduğu anlaşılmıştır.

Dijle'nin (2006) çalışmasında suçu ihbar etmeye evet diyenler %69,8 hayır diyenler %30,2 olmuştur.

Maja ve Bojan'ın (2010) çalışmasında aynı soruya bulduğu sonuçlar evet %69, olaya bağlı %19, hayır %8 olmuştur.

Çalışma kapsamındaki sonuçlar ile diğer çalışmalardaki toplumun suçu ihbara hassasiyet oranlarının yakınlığı dikkat çekmiştir.

Çizelge 4.20'de ileri seviye bilgileri olması durumunda hackerlik yapma eğilimi ile ilgili tespitlerde herhangibir bir özel amaç belirtilmediği halde hayır diyenler %44,1, kesinlikle hayır diyenler %28,8, evet diyenler %17,3 olduğu görülmüş, eğitim seviyesi ile hackerlik yapma konusunda Ki kare bağımsızlık testinde ($\chi 2$=37,258, df:12, p=0,000) anlamlı bir ilişkinin olduğu, eğitim seviyesi düştükçe hackerlik yapma eğiliminin arttığı görülmüştür. Yine Cinsiyet ile hackerlik yapma konusunda da anlamlı bir ilişkinin ($\chi 2$=11,548, df:4, p=0,021) olduğu, kadınlarda eğilimin yüksekliği dikkat çekmiştir.

Dijle'nin (2006) çalışmasında aynı soruya bulduğu sonuçlar da evet diyenler %46,1 hayır diyenler %74,5 olmuştur.

Sonuç olarak bilgi ve yeteneklerini hackerlik yapma konusunda kullanma eğilimi olumlu veya olumsuz amaçlar gözetilmeden lise eğitim seviyesinde yüksek düzeyde olduğu, suç bilgisinin ve bilincinin oluşmasıyla üst eğitim düzeylerinde bu düşüncenin azaldığı ancak fikir beyan etmeme ve cevap vermeme oranlarının lisans ve lisansüstü

seviyesinde yüksek olması bu konuda bir kararsızlığın olduğunu ve eğer ulusal veya barışçıl amaçlar belirtilirse fikirlerin daha belirginleşeceğinin anlaşıldığı, ancak kesinlikle hayır cevaplarının üst eğitim seviyelerinde yüksek olmaması yapılacak fiillerin suç oluşturma şüphesinin pek de önemsenmediğini göstermesi olarak değerlendirilmiştir.

Siber suçlarla mücadelede Emniyet Teşkilatı çalışmalarının (Çizelge 4.26) %77 oranında yetersiz bulunduğu, Eğitim seviyesi ile Emniyet Teşkilatı çalışmalarını yeterli bulma konusunda Ki kare bağımsızlık testine göre ($\chi 2$=24,255, df:12, p=0,019) olduğundan anlamlı bir ilişki olduğu, eğitim seviyesi arttıkça yeterli bulma düzeyinin azaldığı saptanmıştır.

Dijle'nin (2006) çalışmasında aynı soruya bulduğu sonuçlar da yeterli diyenler %1,4, yetersiz diyenler %29,2 ve kesinlikle yetersiz diyenler 29,6 ve fikrim yok diyenler %39,7 olmuştur.

Yine Maja ve Bojan'nın (2010) çalışmasında aynı soruya bulduğu sonuçlar evet %19, hayır %39, bazen %15, fikrim yok %27 olmuştur.

Afyonkarahisar örnekleminde Emniyet teşkilatının siber suçlarla mücadelede yaptığı çalışmaları yeterli görme oranı (%18,3) ile Slovenya'daki emniyet birimlerinin çalışma oranlarının (%19) birbirine yakınlığı dikkat çekmiştir. Dijle'nin çalışmasındaki yeterlilik oranının %1,4 ten 2006'dan 2014 yılına % 18,3 lere yükselmesi Emniyet birimlerinin gelişmesi ve kat ettikleri aşamaları göstermesi bakımından olumlu olarak değerlendirilmiştir.

Siber/bilişim suçlarıyla ilgili mevcut yasaları yeterli bulma konusunda Çizelge 4.28'de olumlu düşüncenin, %14,4 olduğu görülmüş Ki kare bağımsızlık testinde ($\chi 2$=37,590, df:12, p=0,000) olduğu dolayısıyla mevcut yasaları yetersiz bulma ile eğitim seviyesi arasında anlamlı bir ilişkinin varlığı tespit edilmiş, eğitim seviyesi yükseldikçe çevresel ve yaşamsal tecrübeler ile yaş olarak edinilen deneyimlerle yasaların yeterli görülme oranının azaldığı tespit edilmiştir**.**

Bu anlamda mevcut yasaların yetersizliği düşüncesinin ekseriyetle yaygın olduğu, kanun yapıcıların mağdurların hak arayışına cevap verecek veya süreci hızlandıracak yasal düzenlemeleri yapmaları gerekliliğine ihtiyaç olduğu anlaşılmıştır.

Dijle (2006) çalışmasında aynı soruya bulduğu sonuçlar da yeterli diyenler %3, yetersiz diyenler %33 ve kesinlikle yetersiz diyenler 24,4 ve fikrim yok diyenler %39,6 olmuştur.

Dijle'nin çalışmasında olumlu düşünenler %3 iken bu çalışmada olumlu düşünenler %17 olmuş, olumsuz düşünenler %57,4 iken %80 lere yükselmiş, 2006'dan bu yana fikir sahibi olmayanlarda (%39,6) bir düşünce netleşmesi olarak değerlendirilmiştir.

Yine Maja ve Bojan (2010) çalışmasında aynı soruya bulduğu sonuçlar evet %27, hayır %58, bazen %15 bulmuştur. Slovenya'daki yasaları yeterli bulma %27 iken bu çalışmada olumlu düşünenlerin %17 de kalması ülkeler arası toplumlarda önemli bir fark olarak değerlendirilmiştir.

Cinsiyet açısından Erkeklerde yetersiz bulma oranının kadınlardan daha yüksek olduğu anlaşılmış, Ki kare bağımsızlık testinde anlamlı bir ilişki tespit edilememiştir.

Siber/bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesini olumlu karşılayanalrın %44,3 ile olumsuz karşılayanlardan %48 daha az olduğu görülmüş, eğitim seviyesi ile internet kullanımına sınırlama getirilmesine olumlu bakış arasında Ki kare bağımsızlık testinde ($\chi 2$=31,330, df:12, p=0,002) anlamlı bir ilişkinin olduğu, eğitim seviyesi yükseldikçe çevresel ve yaşamsal tecrübeler ile yaş olarak edinilen deneyimlerle olumsuz karşılama oranının yükseldiği tespit edilmiştir**.** Cinsiyetle olumlu karşılama arasında anlamlı bir ilişki tespit edilememiş, erkeklerin %53,5' le kadınlardan %45,7 daha olumsuz baktığı görülmüştür.

Dijle'nin anılan çalışmasında hayır diyenler %63,2 iken evet diyenler %36,8 olarak bulunmuştur.

Siber suçları önlemek amacıyla internette gözetlenmeyi (Çizelge 4.32) istemeyenlerin toplamda %69,1 olduğu tespit edilmiş, bu oran Dijle'nin (2006) anılan çalışmasında %70,6 olarak bulunmuştur. İnternet ortamında siber suçları önlemek amacıyla da olsa gözetlenmeye bakış hakkında Ki kare bağımsızlık testinde ($\chi 2$=30,561, df:12, p=0,002) olduğu, anlamlı bir ilişkinin varlığı, eğitim seviyesi arttıkça hayır eğiliminin arttığı tespit edilmiştir. Cinsiyet ile internette gözetlenmeye bakış arasında anlamlı bir ilişkinin olmadığı, olumsuz düşüncenin kadınlarda %70,2 ile erkeklerden %66,4 daha yüksek olduğu görülmüştür.

Çalışma kapsamında tespit edilen sonuçları şöyle sıralayabiliriz;

Geçmiş zamanlarda siber suç işlediğini düşünen katılımcıların oransal düşüklüğü (%4,7) ve erkeklerde yüksek olduğu (%6,8) görülmüştür.

Siber suç fiillerinden herhangi birini işlemiş olma kararsızlığı en net olarak lisansüstü eğitim seviyeli öğretim görevlilerinde (%14) görülmüş, neyin siber suç olduğu veya suç sayıldığı konusunda büyük bir bilgi boşluğu olduğu anlaşılmıştır.

Genel olarak internet kullanım sürelerinin yüksekliği ve kullanmayan sayısındaki düşüklük dikkat çekmiş, en çok (6 yıl ve üzeri) ve uzun süreli internetin üniversite öğretim görevlilerince kullanıldığı anlaşılmıştır. Eğitim seviyesi yükseldikçe internet kullanımının arttığı tespit edilmiştir.

İnternete erişimde en çok wi-fi ortak erişim alanları (%62,6) ile cep telefonlarının (%60) kullanıldığı, öncelikli tercihin ücretsiz ortamlar ve sonrasında cep telefonları olduğu anlaşılmıştır.

Akıllı tabir edilen multi fonksiyonlu cep telefonlarını internete bağlanmada en yaygın şekilde lise öğrencilerinin (%65,8) kullandığı görülmüştür.

Kamu çalışanlarının internete bağlanmada kamu imkânlarını (%65,6) yüksek oranda kullandıkları anlaşılmıştır. Genel olarak kullanıcıların ülkemizdeki internete bağlanma ve abonelik ücretlerinin ucuz olmayışını dikkate alarak kullanım önceliğinde ücretsiz bağlanım kaynaklarını tercih ettikleri tespit edilmiştir.

Öğretim görevlileri ve öğrencilerin internet kullanmaktaki önceliklerinin iş ve dersle ilgili olduğu, kamu çalışanlarının ise öncelikle haber ve gündemdeki gelişmeleri takip etme amaçlı olduğu görülmüştür.

İnterneti oyun eğlence amaçlı (%49,8), sosyal çevre edinme amaçlı (%33,4) en çok lise öğrencilerinin kullandığı anlaşılmıştır.

Katılımcıların en yaygın kullandığı sosyal paylaşım sitesinin facebook (%79,8) olduğu, en yüksek kullanımın üniversite öğrencilerinde (%82,5) ve kamu çalışanlarında (%82) olduğu tespit edilmiştir.

Twitter uygulamasının ikinci olarak en çok kullanıldığı, öğretim görevlileri ve lisansüstü eğitim seviyeli kesimce (%51,8) ve lisans eğitimli kesimce (%47) çoğunlukla kullanıldığı görülmüştür.

İnstagram (fotoğraf video paylaşım) uygulamasının en çok üniversite öğrencilerinde (%21) ve kadınlarda yaygın olduğu, foursquare (yer bildirim) uygulamasının ise lise öğrencilerinde (%13,9) ve kadınlarda yaygın olduğu, iş müracaat ve cv oluşturma sitesi LinkedIn uygulamasının ise lisansüstü eğitimli akademik personel tarafından (%29,6) ve erkeklerde en çok kullanıldığı tespit edilmiştir.

Siber suç bilgisinin eğitim seviyesi ile orantılı olarak arttığı, tüm katılımcılarda en üst seviyede bilinen siber suç türünün hacking (sanal korsanlık) (%65,9) olduğu anlaşılmış, kamu çalışanlarının mal varlığına ve ekonomik kazanımlara karşı işlenen siber suçları daha çok bildiği (%62,6) tespit edilmiştir.

Sanal kumar suçu en çok lisansüstü eğitimlilerce (%40,7) bilindiği, müstehcenlik / pornografi ve çocukların cinsel istismarı suçlarının yine lisansüstü (%55,5) ve lisans eğitimli (%50,8) kişilerce bilindiği görülmüştür.

Afyonkarahisarda en tehlikeli siber suçun nitelikli interaktif dolandırıcılık (%58) (ATM, kredi kartı) olduğu düşünülmektedir.

Katılımcıların en çok işlendiğini düşündüğü siber suçların nitelikli dolandırıcılık ve hırsızlık suçları (%59,6) ile e-posta ve sosyal hesap şifrelerinin çalınması (%52,8) olduğu anlaşılmıştır.

Katılımcıların en çok işlendiğini düşündükleri siber suçlardan pornografi/müstehcenlik (%46,1) ile sosyal medyada taciz, tehdit, hakaret suçlarının (%45) yüksekliği görülmüş, bu yüksek oranların toplumu özellikle de çocuk ve gençlerin ruh ve beden sağlıklarının korunmasını tehdit eden bir faktör olduğu değerlendirilmiştir.

E- posta ve sosyal medya hesaplarının çalınması ile katılımcılar veya yakınlarının (%26) oranında karşılaştığı, katılımcı her dört kişiden birinin bu konuda ya mağdur ya da mağdur olanlarla yakın olduğu, erkek kullanıcı veya yakınlarının şifre veya hesap çalınma olaylarını daha çok yaşadığı anlaşılmıştır. Özellikle facebook sosyal ağ kullanımının %80'lerde olduğu da dikkate alınınca buradan mail veya sosyal hesaplarda kullanılan şifrelerin güvenli olarak oluşturulması veya kullanılan şifrelerin güvenli olarak saklanması, paylaşılmaması konularında zayıflığın, ihmallerin olduğu, bu konuda bilinçlenmeye ihtiyaç olduğu değerlendirilmiştir.

Katılımcıların siber suçla karşılaştıklarında bunu önemli görme ve ihbar etme duyarlılığının (%67,9) yüksek olduğu görülmüş, eğitim seviyesi yükseldikçe ihbar etme ve suçu önemseme eğiliminin arttığı, erkeklerin suçu daha çok önemsediği ve ihbar etmede daha duyarlı olduğu tespit edilmiştir.

Katılımcıların ileri seviye bilgileri olması durumunda hackerlik yapma eğilimlerine özel bir neden belirtilmediği halde genel olarak olumsuz (%73) baktıkları, eğitim seviyesi

düştükçe hackerlik yapma eğiliminin arttığı (lise % 23), kadınlarda eğilimin yüksekliği (%17,4) tespit edilmiştir.

Katılımcılarda siber suç mağduru olma durumunda hak arayışında sonuç elde etme konusuna inançlarının çok düşük (%9,9) seviyelerde olduğu, müracaat edilse bile netice alınamayacağına dair inancın ise (%38,7)'lerde olduğu, bu konuda herhangibir fikir sahibi olmayanların ise (%31,3) gibi yüksek olduğu görülmüştür. Eğitim seviyesi azaldıkça hak arayışında sonuç elde etmeye olan inançın da azaldığı, , erkeklerde bu eğilimin kadınlardan yüksekliği (%16,5) tespit edilmiştir. Mağdurlar ve kamuoyunda şikâyet mekanizması, müracaat birimleri ve usulleri, adli işlemler, süreçler ile kolluk birimlerinin yaptığı iş ve işlemlerin bilinmediği, bu alanda büyük bir bilgi boşluğunun olduğu, bilgilendirilme ve güven tesisine ihtiyaç olduğu anlaşılmıştır.

Çalışmada siber suçlarla mücadelede Emniyet Teşkilatı çalışmalarının yetersiz (%77) olduğu düşünülmektedir. Eğitim seviyesi arttıkça yeterli bulma düzeyinin azaldığı (%11) tespit edilmiştir.

Siber/bilişim suçlarıyla ilgili mevcut yasaları yeterli bulma konusunda katılımcılarda olumlu düşüncenin düşük (%14,4) olduğu, eğitim seviyesi yükseldikçe çevresel ve yaşamsal tecrübeler ile yaş olarak edinilen deneyimlerle yasaların yeterli görülme oranının azaldığı (%11), erkeklerde yetersiz bulma düşüncesinin (%80,9) kadınlardan yüksek olduğu tespit edilmiştir.

Siber suçları önlemek amacıyla da olsa katılımcıların internette gözetlenmeye yaklaşımlarının olumsuz olduğu (%69,1), kullanıcıların bireysel özgürlük ve özel hayatın gizliliğine önem verme konusunda hassas olduğu ve gerekçesi ne olursa olsun hayatın gizli alanına karşı gözetlenme konusunu olumlu karşılamadığı anlaşılmıştır. Kadınlarda olumsuz düşüncenin (%70,2) erkeklerden (%66,4) daha fazla olduğu görülmüştür. İnternette gözetlenmeye en çok karşı olan katılımcıların lise öğrencileri ile yükseköğretim görevlileri olduğu tespit edilmiştir.

Araştırmadan elde edilen sonuçlara göre şu önerilerde bulunabiliriz;

Analizlerde internete en yaygın bağlanma yöntemi olarak öne çıkan wi-fi aracılığıyla internet erişimi bu anlamda önemli bir zayıflık olarak değerlendirilmektedir. Wi-fi ortamı bağlanma, güvenli veri transferi ve saldırılara açık olma açısından en az güvenli olan bağlanma yöntemidir. Bu yöntemle bağlananların veri şifreleme konusuna dikkat etmeleri, kullanıcı log kayıtları için verilen T.C kimlik ve telefon numaralarının hizmet sağlayıcı tarafından kaydedildiğini bilmeleri, mümkün olduğunca banka veya kredi kartları ile alışveriş için kullanmamaları gereklidir.

Toplumda en çok işlendiği düşünülen siber/bilişim suçlarında en yüksek (%59,6) dolandırıcılık/hırsızlık suçlarının olması e-ticaret alanında ve internet bankacılığı kullanımında ciddi güvenlik ihmallerinin olduğunu göstermektedir. Bu anlamda hem e-ticaret kapsamında satış yapan firma ve şirketler "https" ile doğrulanmış ve güvenilir sunucu sertifikaları ile hizmet sunarak bankalarla 3D secure sistemi üzerinden satış yapmaları, hem de kullanıcıların bu yeterlilikleri taşıyan firmaları tercih etmeleri gereklidir.

Yine en çok işlendiği anlaşılan e-posta ve sosyal medya hesaplarının çalınmasının %52,8 oranında olması, güvenli şifre oluşturulması ve hesap şifrelerinin paylaşılmaması ile gizliliğin korunması için kullanıcıların bireysel olarak bilinçlenmeli, uygulama geliştiriciler şifre formatları için farklı karakter girme zorunluluğu oluşturmalıdırlar.

Pornografi/müstehcenlik, ile sosyal medyada taciz, tehdit ve hakaret suçlarının toplumda en çok işlendiği düşünülen siber suçların içerisinde ve oranlarının yüksek olması çocuk ve gençlerin ruh ve beden sağlıklarının korunması, özellikle düşen internet kullanım yaşları ve gelişmiş cihazların kullanımı dikkate alınarak çocuk istismarları için en savunmasız ve zayıf olunan bir ortamda istismarcıların tehdit ve şantajlarına karşı küçükler özellikle genç kızlar korunmalıdır.

Sosyal paylaşım siteleri içerisinde %80 lere varan kullanımıyla facebook uygulaması hem öğrenciler hem de kamu çalışanlarında aynı oranlarda kullanıcı bulması bu sitenin

ne kadar yaygın olduğu, pek çok kesime hitap edebilen bir içeriğe sahip olduğu, çok farklı kullanıcıları aynı ortamda buluşturduğu ve katılımcıların günlük hayatında hem ziyaret hem de zaman geçirme olarak önemli bir yer tuttuğunu göstermesi bakımından önemli görülmektedir. Bu çalışma kapsamında olmayan ortaokul ve ilkokul seviyelerindeki facebook kullanıcılığı oranları ayrı bir çalışmayla tespit edilmelidir. Platform olarak pek çok farklı kullanıcı ve yaş grubunu bir arada buluşturan uygulama özellikle küçük yaştaki kullanıcıların zarar görmemesi ve istismara uğramaması açısından bu sitelerde zaman geçirirken güvenlik adımları ve korunma konularında bilinçli olmaları yaşanabilecek mağduriyetlerin önlenmesi açısından önemli görülmektedir. Bu durum aileler, eğiticiler ve suçla mücadele eden birimler tarafından önemsenmeli ve değerlendirilmelidir. Özellikle tüm okullarda (ilk-orta ve lise) güvenli medya kullanımı ile ilgili bir ders planlaması seçmeli de olsa müfredata alınmalı, eğitsel faaliyetlerde işlenmelidir.

Her yaş ve eğitim seviyesinde siber ortamda güvenliğin sağlanması ve güvenli internet kullanımı, e-posta ve sosyal ağ hesap ve şifre güvenlikleri konularında bilgi ve farkındalık eksikliğinin bireysel ve kurumsal anlamda asgari seviyelere yükseltmek için konferans, seminer, panel, kurs ve hizmeti içi eğitim takviyeleriyle artırılması gerekli görülmektedir. Özellikle eğitim seviyeleri içerisinde siber suç, siber tehdit ve tehlikeler ile güvenli internet kullanımı ve hesap/şifre güvenliği konularında en zayıf olarak ortaya çıkan lise seviyelerinde Fatih Projesi kapsamında tablet kullanımının başlayacağı da dikkate alınınca lise öğrencileri için sosyal medya okuryazarlığı gibi ders olarak düzenlenmesi gerekliliği zaruri görülmektedir.

Gerçekleştirilen ve ilerde düzenlenecek olan siber güvenlik konferans, seminer ve çalıştayları ortaya çıkaracağı faydalar açısından çok önemli görülmekte olup bu etkinliklerin üniversiteler, adli birimler, Aile ve Sosyal Politikalar Bakanlığı, Milli Eğitim Bakanlığı ve Bilgi Teknolojileri Kurumunca ve özel sektör tarafından desteklenmesi ve teşvik edilmesi ile kamu spotları ve afişler hazırlatılarak görsel medyada yayınlatılması önemli görülmektedir.

Temeli bilgi paylaşımı ve bilgiye erişim olan İnternette güvenlik gerekçeleri ile kısıtlama ve gözetleme faaliyetlerinin %70 ler oranında olumsuz karşılanması önemsenerek kanun koyucu veya düzenleyici Telekomünikasyon İletişim Başkanlığınca ulusal güvenlik ile özel hayatın gizliliği ve özgürlükler dengesinin iyi korunması ve İnternetin işlevsiz hale getirilmemesi önemli olarak görülmektedir.

Toplumda siber/bilişim suçları ile mücadelede mevcut yasaların yetersizliği düşüncesinin %80 oranlarında yaygın olması ülkemizdeki yasal düzenlemelerin Siber güvenlik konusundaki gelişmelerin gerisinde kaldığını göstermektedir. Bu nedenle ilgili yasal düzenlemeler siber güvenlik alanındaki gelişmelere paralel ihtiyaçlar doğrultusunda güncellenerek etkin ve caydırıcı hale getirilmelidir.

Siber tehdit ve suçlardan zarar gören mağdurların adli makamlara müracaattan sonra netice elde etme konusuna inancın en yüksek %20'leri aşmaması, özellikle lise ve üniversite öğrencilerindeki olumsuzluğun oransal yüksekliği önemli görülmekte olup, suçla mücadelede suçların ve suç işleyenlerin ortaya çıkarılıp cezalandırılması, maddi ve manevi kayıpların önlenmesi, suçu ve suçluyu ihbar etmenin teşvik edilmesinde önemli rol oynadığı değerlendirilmektedir. Adli birimlerin ve hatta kanun yapıcıların soruşturma ve yargılama süreleri konusunda toplumda güven oluşturucu bir standartta hizmet sunmaları gerekliliği önemli görülmektedir.

Siber/ bilişim suçlarıyla adli mücadelede tek kolluk birimi olan Emniyetin yeterli görülme oranının düşük olduğu, başarılı neticeleri veya sonuca ulaşmada yaşadığı sıkıntıları kamuoyu ile paylaşmayı başaramadığı, bu konuda yeterli bilgilendirme ve paylaşımda bulunmadığı anlaşılmaktadır. Siber suçlarla mücadelede eğer kurumsal kapasitenin kullanımında sıkıntı var ise bu alanda kurumsal uzmanlaşmaya önem verilmesi, eğer kurumsal kapasite kullanımında sorun yok ise toplumda oluşan olumsuz kanaati oluşturan sebepleri aydınlatacak bilgilendirmeler yapılması kurumsal güven ve yeterliliğin oluşmasında önemli görülmektedir.

Siber dünyada güvenli yaşam için siber tehditleri önlemede gerek bireysel olarak kendimizi gerekse kurumsal olarak personelimizi veya tüm internet kullanıcılarını siber güvenlik konusunda eğitmek ve son bilgilerle donatmak artık kaçınılmaz bir zarurettir.

Kurumsal ve/ya bireysel kullanımdaki bilgisayarlar yazılımsal olarak en son teknoloji ve güvenlik yazılımları ile donatılmalı, aile ve çocuk filtreleri kullanılmalı, hem aile hem de çocuklar interneti doğru okuyabilmesi için bilinçlenmeli, siber suçlar ile ilgili tespitler ihbar edilmelidir.

6. KAYNAKLAR

Alaca, B. (2008). Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik Ve Hukuki Boyutları İle). Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Anonim, (2001). Avrupa Konseyi Siber Suçlar Sözleşmesi, Budapeşte, Macaristan

Anonim, (2004). Council of Europe, Organized Crime Situation Report, Focus On The Threat of Cybercrime, Strasbourg, France.

Anonim, (2006). EGM Bilişim Suçları Çalışma Grubu Raporu, Ankara.

Anonim, (2006). Türkiye Bilişim Derneği Bilişim Sistemleri Güvenliği El Kitabı. Sürüm 1.0, Ankara

Aslantürk, Z. (1999). Araştırma Metot ve Teknikleri. Emre Matbaası, İstanbul.

Aydın, E. (1992). Bilişim Suçları ve Hukukuna Giriş. Doruk Yayınları, Ankara.

Bequai, A. (1998). A Guide To Cyber Crime Investigations. *Computer And Security Journal*, **17:7**, 579–582.

Beyhan, C. (Temmuz- Aralık 2002). Türkiye'de Bilişim Suçları ve Mücadele Yöntemleri. *Polis Bilimleri Dergisi*, Ankara, **4:** 3-4.

Bishop, M. (2002). Computer Security-Art and Science. Adison –Wesley Professional Publications, California, USA.

Boğa, U. (2011). Bilişim Suçlarıyla Mücadele Yöntemleri, Uzmanlık Tezi, Radyo Televizyon Üst Kurulu.

Brenner, S. W. and Clarke, L. L. (2005). Distributed Security: Preventing Cybercrime.

The John Marshall Journal of Computer & Information Law, **4:** 659-671.

Canbek, G. (2005). Klavye Dinleme Ve Önleme Sistemleri Analiz, Tasarim ve Geliştirme. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Cavelty, M. D. (2007). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge; 1 edition, ETH Zurich.

Chantler, N. (1996). Profile Of A Computer Hacker. Auerbach Publications, Florida, USA.

Clifford, R. D. (2001). Cybercrime: The Investigation, Prosecution and Defense of A Computer-Related Crime. Carolina Academic Press, North Carolina, USA.

Çepni, S. (2008). Kuramdan Uygulamaya Fen ve Teknoloji Öğretimi, 7.Baskı, Pegem Akademi Yayıncılık.

Değirmenci, O. (2002). Bilişim Suçları. Yayınlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Demetriou, C. And Silke A. (2003). A Criminological Internet 'Sting': Experimental Evidence of Illegal and Deviant Visits to a Web Site Trap. *British Journal of Criminology* **43:1,** 213–222.

Denning, Dorothy E. (1998). Information Warfare and Security. Addison-Wesley Publication; 1st Edition. Georgetown, Washington, USA.

Dijle, H. (2006) . Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Demirbaş T. (2005). Kriminoloji. Seçkin Yayıncılık, Ankara.

Dülger, M. V. (2004). Bilişim Suçları. Seçkin Yayıncılık, Ankara.

Doğantimur, F. (2009). Kurumsal Bilgi Güvenliği. Maliye Bakanlığı Uzmanlık Yeterlik Tezi, Ankara.

Geers, K. (2008). Cyberspace and the Changing Nature of Warfare. *SC Magazine*, *Black Hat*, 2008/7, United Kingdom.

Goodman, M. & Brenner, S. (2002). The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law and Technology*, 3. Retrieved on 12th May.2011from www.lawtechnournal.com/articles/2002/03_020625_goodmanbrenner.pdf.

Grabosky, P. (2007). Electronic Crime. Upper Saddle River Publication, New Jersey: Pearson/Prentice Hall, USA.

Granville, J. (2003). The Dangers of Cyber Crime and a Call for Proactive Solutions. *Clemson University, Australian Journal of Politics and History*. Australia. **49:1**, 102-109.

Hafner K. and Markoff J. (1995). Cyberpunks: Outlaws And Hackers On The Computer Frontier. First Touchstone Edition. New York, USA.

Hollinger, R. (1998). Computer Hackers Follow A Guttman-Like Progression. *Social Sciences Review* **72:** 199-200.

İlbaş, Ç. (2009). Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi. Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Karagülmez, A. (2005). Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri. Seçkin Yayıncılık, Ankara

Karasar, N. (2004). Bilimsel Araştırma Yöntemi. Nobel Yayın Dağıtım, Ankara.

Keskin, S. (2002). Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, **59:1-2**, 155-180.

Koca, M. (2001). Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, **59:*1*-*2***, 62.

Landreth, B. (1995). Out Of The Inner Circle. Redmond: Microsoft Books, USA.

Maja, D and Bojan D. (2010). Perception of Cybercrimes in Slovenia, *Journal of Criminal Justice and Security*. Slovenia. **12:4**, 378-396.

Moitra, S. (2005). Developing Policies for Cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice*,**13:3,** 435-464.

Nir, K. (2005). Pattern of Global Cyber War and Crime: A Conceptual Framework. *Journal of International Management*. Bryan School of Business and Economics, The University of North Carolina at Greensboro. NC, USA. **11**(2005)**:** 541-562.

Parker, B. Donn. (1998). Fighting Computer Crime: A New Framework For Protecting Information. Published by Jhon Viley & Sons İnc. New York, USA.

Post, J. (1996). The Dangerous Information System Insider: Psychological Perspectives. htttp\\www.infowar.com

Power.R. (1998). Current and Future Danger, A CSI Primer on Computer Crime and Information Warfare. *Computer Security Institute*, 3rd ed., San Fransisco, USA.

Rogers, M. (1999). A New Hacker Taxonomy, Graduate Studies, Dept.of Psychology, University of Manitoba, Manitoba, Kanada. www.criminologia.org International

Crime Analysis Association.

Shaw, Ruby E. 1998. The Insider Threat to Information Systems: The Psychology of the Dangerous Insider", *Security Awareness Bulletin*, **2:**1-10**.**

Shinder, D. L. (2002). Scene of the Cybercrimes. Syngress Publishing Inc, Rockland, USA.

Sokullu-Akıncı, F. (2001). Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, **59:1-2** 11-38.

Taş, K. (2010). Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi. Yüksek Lisans Tezi, Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü, Adana.

Taşkın, Ş. C. (2009). Bilişim Hukuku Uluslararası Uyuşmazlıklar. *Türkiye Barolar Birliği Dergisi.* Ankara, **85**: 332.

Toruk, İ. (2008). Üniversite Gençliğinin Medya Kullanma Alışkanlıkları Üzerine Bir Analiz. *Selcuk Universitesi Sosyal Bilimler Enstitüsü Dergisi*, **19**.

Turhan, O. (2006). Bilgisayar Ağları İle İlgili Suçlar. Uzmanlık Tezi, Devlet Planlama Teşkilatı, Ankara.

Tulum, İ. (2006). Bilişim Suçları ile Mücadele. Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta.

Wall, D. S. (2001). Cybercrimes and the Internet. Routledge publish, New York, USA.

Whittekar, J. (2004). The Cyberspace Handbook. Routledge publish, London, GB.

Yar, M. (2006). Cybercrime and Society. Thousand Oaks and New Delhi: SAGE Publications, London, England.

Yayla, M. (2013). Bu makale, TUBİTAK tarafından sağlanan destek kapsamında 2012-2013 Döneminde ABD The City University of New York John Jay College'da yürütülen çalışmalar kapsamında hazırlanmıştır. http://portal.ubap.org.tr/App_Themes/Dergi/2013-104-1247.pdf.

Yazıcıoğlu, Y,. (1997). Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile. Alfa Yayınevi, İstanbul

Yücel M. (1992). Bilişim Suçları. *Ankara Barosu Dergisi*, **49:4,** 505.

İnternet kaynakları:

1. http://www.internetworldstats.com/top20.htm, 30.06.2012
2. http://www.tdk.gov.tr/index.php?option=com_gts&view=gts, 04.02.2014
3. http://siber.nedir.com/, 04.02.2014
4. http://tr.wikipedia.org/wiki/Siber, 04.02.2014
5. http://unterm.un.org/dgaacs/unterm.nsf/WebView/99B98BDBCBAB096185256E620052EFD3?OpenDocument, 05.02.2014
6. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, 10.02.2014
7. http://sibersuclar.iem.gov.tr/siber_suclari.html, 10.02.2014
8. https://twitter.com/TheRedHack, 20.05.2014
9. http://www.teknolojide.com/ulusal-siber-guvenlik-tatbikati_5179.aspx, 13.1.2014
10. http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/siberguvkurulu.php, 21.05.2014
11. https://www.facebook.com/TskSiberSavunmaMerkeziBaskanligi, 13.01.2014
12. http://www.egm.gov.tr/Sayfalar/SiberSuclarlaMucadeleDaireBaskanligi.aspx, 13.01.2014

13. http://www.resmigazete.gov.tr/eskiler/2013/06/20130620.pdf, 21.05.2014

14. http://www.resmigazete.gov.tr/eskiler/2013/11/20131111.pdf, 21.05.2014

15. www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm, 21.05.2014

16. http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.11694&MevzuatIliski=0&sourceXmlSearch=, 21.05.2014

17. http://www.tib.gov.tr/tr/tr-menu-28-5651_sayili_yasa_hakkinda.html, 21.05.2014

18. http://www.ihbarweb.org.tr/ohg/, 22.05.2014

19. http://internetozgurdur.com/2014/02/21/yeni-internet-yasasi/, 22.05.2014

20. http://www.gazetecileronline.com/newsdetails/12857-/GazetecilerOnline/bir-de-siber-yetki-sansurde-geri-adimdan-uckagit-c, 22.05.2014

21. http://www.mazarsdenge.com.tr/printerFriendly.php?contentId=435, 16.03.2014

22. http://www.hukuki.net/archive/index.php?t-91988.html, 22.05.2014

23. http://www.virusguvenlik.com/trojan-truva-ati-nedir/, 10.02.2014

24. http://www.bilgiservisim.net/virusler-solucanlar-ve-truva-atlari-nedir/, 02.02.2014

25. http://tr.wikipedia.org/wiki/Solucan_%28vir%C3%BCs%29, 22.05.2014

26. http://en.wikipedia.org/wiki/Hacker_%28computer_security%29, 22.05.2014

27. http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/106901-cernobil-virusu-nedir.html, 02.02.2014

28. www.antalya.adalet.gov.tr/duyurular%5Cbasin2013.ppt, 22.05.2014

29. http://web.deu.edu.tr/sss/spam.html, 10.02.2014

30. http://ww2.sdenizhan.net/1051-spamda-son-nokta-ulkeye-gore-spam.html, 22.05.2014

31. http://www.uzmanabi.com/haberler/nsa-herseyi-dinliyor-99139.imo, 22.05.2014

32. http://www.chip.com.tr/haber/angry-birds-bile-abd-casusu-cikti_45082.html, 02.02.2014

33. http://www.aktifhaber.com/iste-uyaptaki-buyuk-skandal-892541h.htm, 07.02.2014

34. http://www.guvenliweb.org.tr/guvenlik/content/phishing, 07.02.2014

35. http://www.tuik.gov.tr/UstMenu.do?metod=temelist, 07.02.2014, Yıllara Göre İl Nüfusları, 2007-2013

36. http://www.tuik.gov.tr/UstMenu.do?metod=temelist, 07.02.2014, Yıllara, Yaş Grubu ve Cinsiyete Göre Nüfus, 1935-2013

37. http://www.tuik.gov.tr/PreTablo.do?alt_id=1028, 10.02.2014 Girişimlerde Bilişim Teknolojileri Kullanımı Araştırması, Hanelerde Bilişim Teknolojileri Kullanımı Araştırması (16-74 yaş arası bireyler), 2004-2013

38. http://www.tuik.gov.tr/PreTablo.do?alt_id=1028/, 07.02.2014, Bilgi toplumu istatistikleri, 2004-2013,

39. http://www.zaferkarakus.com.tr/saldiri-tespit-sistemleri-intrusion-detection-systems/?, 10.02.2014

40. http://cybervictims.blogspot.com.tr/ Beware examinees, 27 02.2014

41. http://www.sondakika.com/haber/haber-skype-suriyeli-hackerlarin-saldirisina-ugradi-5502899/, 07/02/2014

42. http://hurarsiv.hurriyet.com.tr/goster/ShowNew.aspx?id=25640726, 07.02.2014

43. http://www.hurriyet.com.tr/planet/24601641.asp, 07.02.2014

44. http://hurarsiv.hurriyet.com.tr/goster/ShowNew.aspx?id=23438255, 07.02.2014

45. http://hurarsiv.hurriyet.com.tr/goster/ShowNew.aspx?id=18839171, 07-02-2014

46. http://www.trthaber.com/haber/dunya/guney-koreye-siber-saldiri-90829.html, 07.02.2014

47. http://www4.cnnturk.com/2013/bilim.teknoloji/%C4%B1nternet/10/04/ingiltere.siber.ordu.kuruyor/725850.0/index.html, 07.02.2014

48. http://tv.haberturk.com/gundem/video/turkiye-siber-ordu-kuruyor/103935, 07.02.2014

ÖZGEÇMİŞ

Adı Soyadı: Musa SÜRER

Doğum Yeri ve Tarihi: Konya- 1973

Yabancı Dili: İngilizce

İletişim (Telefon/e-posta) : 505 2159300/ musa.surer@egm.gov.tr

Eğitim Durumu (Kurum ve Yıl)

Lise: Polis Koleji – 1991.

Lisans: Polis Akademisi/ Güvenlik Bilimleri Fakültesi – 1995.

Yüksek Lisans: Afyon Kocatepe Üniversitesi Fen Bilimleri Fakültesi İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı. 2012/2014.

Çalıştığı Kurum ve Yıl:

1995-2000 Aydın Polis Meslek Yüksek Okulu.
2000- 2006 Şanlıurfa Emniyet Müdürlüğü.
2006- 2014 Afyonkarahisar Emniyet Müdürlüğü.
2001/2002 Birleşmiş Milletler Barış Koruma Misyonu KOSOVA.
2004/2005 Birleşmiş Milletler Barış Koruma Misyonu LİBERYA.

EKLER

Ek 1. Anket Formu

Sayın Katılımcı, Bu ankette, Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi Ana Bilim Dalı, yüksek lisans tez çalışması için **"Siber Suçlar Üzerine Bir Araştırma (Afyonkarahisar ili Örneği)** konusunun araştırılması amaçlanmıştır. Soru formunda verdiğiniz yanıtlar gizli kalacaktır ve tamamen bilimsel bir amaca yönelik olarak kullanılacaktır.

Katkı ve yardımlarınız için teşekkür ederiz.

Bu Bölüm Herkes Tarafından Doldurulacaktır

Cinsiyetiniz : ☐ Kadın ☐ Erkek

Eğitim seviyeniz: ☐ İlköğretim ☐ Lise ☐ Ön Lisans ☐ Lisans ☐ Lisansüstü

1.Hiç siber/bilişim suçu işlediniz mi?

☐ 1- Evet ☐ 2- Hayır ☐ 3- Emin değilim ☐ 4- Cevap vermek istemiyorum

2. Ne kadar süredir İnternet kullanıyorsunuz?

☐ 1- İnternet kullanmıyorum. (Lütfen 07. Soruya geçiniz) ☐ 2- 1 yıldan az süredir kullanıyorum.

☐ 3- 2–5 yıldır İnternet kullanıcısıyım. ☐ 4- 6 – 9 yıldır internet kullanıcısıyım.

☐ 5- 10 yıl ve uzun süreli İnternet kullanıyorum.

3. İnternete hangi ortamlardan bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

☐ 1- Cep telefonundan ☐ 2- Mobil modem ile

☐ 3- Wi-fi ile ortak erişim alanlarından ☐ 4- Kablolu ağ üzerinden

4. İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

☐ 1- İşimle / derslerimle ilgili konularda araştırma ☐ 2- Kişisel olarak ilgi duyduğum konularda araştırma

☐ 3- Haber ve güncel gelişmeleri takip etme ☐ 4- İletişim

☐ 5- Sosyal çevre edinme ☐ 6- Oyun ve eğlence

☐ 7- Diğer .....

5. İnterneti ortalama olarak kullanım sıklığınız nedir?

☐ 1- İş /okul saatleri dışında kullanmıyorum. ☐ 2- Haftada 1 günden daha az olarak kullanıyorum.

☐ 3- Haftada bir gün kullanıyorum ☐ 4- Haftada birkaç gün kullanıyorum.

☐ 5- Hemen hemen her gün kullanıyorum.

6. Hangi sosyal paylaşım sitelerinde hesabınız var? (Birden fazla seçenek işaretleyebilirsiniz.)

☐ 1- Twitter ☐ 2- Facebook ☐ 3- Foursquare ☐ 4- Linkedin ☐ 5- İnstagram ☐ 6- Badoo

☐ 7- Myspace ☐ 8- Pinterest ☐ 9- Friendfeed ☐ 10- Hi5 ☐ 11- Diğer .....

7. Bildiğiniz "Siber Suç" çeşitleri nelerdir?

☐ 1- Hacking (sanal korsanlık) ☐ 2- Verileri kanunsuz ele geçirme

☐ 3- Bot-Net / D-Dos saldırıları ☐ 4- Çocukların cinsel istismarı ve pornografi

☐ 5- Online örgütlü kumar ☐ 6-Nitelikli interaktif dolandırıcılık/ hırsızlık

☐ 7- Banka ve kredi kartı hakkında işlenen suçlar ☐ 8- Müstehcenlik

☐ 9- Hakaret ☐ 10- Crackli yazılım kullanma

☐ 11- Terör veya yasa dışı örgütsel faaliyetler ☐ 12- Diğer .....

8. Size göre aşağıdaki siber/bilişim suçlarından en tehlikelisi hangisidir?

☐ 1- Lisans hakları ☐ 2- İnteraktif dolandırıcılık (ATM, kredi kartı vb.)

☐ 3- Yasa dışı yayınlar (pornografi, hakaret vb.) ☐ 4- Bilgisayar korsanlığı

☐ 5- Siber casusluk ☐ 6- Diğer

9.Size göre en çok işlenen Siber/Bilişim suçu hangisidir? (Birden fazla işaretleyebilirsiniz)

☐ 1- Elektronik posta ve sosyal medya hesaplarının çalınması ☐ 2- Pornografi/Müstehcenlik

☐ 3- Bilgisayar ve network ağlarına izinsiz erişim ☐ 4- Sosyal medyada taciz, hakaret, tehdit

☐ 5- Siber terör (propaganda, casusluk, hizmeti durdurma) ☐ 6- Dolandırıcılık/ Hırsızlık suçları

☐ 7- Diğer

10.Sizin veya arkadaşlarınızın kullandığı mail/sosyal ağ hesabı veya şifreleri hiç çalındı mı?

☐ 1- Hayır ☐ 2- Evet ☐ 3- Evet, birden çok ☐ 4- Bilgim yok

11. Size göre önemli gördüğünüz bir siber/bilişim suçuna şahit olursanız bunu ihbar eder misiniz?

☐ 1- Evet ☐ 2- Hayır ☐ 3- Kesinlikle hayır ☐ 4- Önemsemem

12.İleri seviye bilginiz olsa "Hackerlik/Korsanlık" yapar mısınız?

☐ 1- Evet ☐ 2- Hayır ☐ 3- Kesinlikle hayır ☐ 4- Fikrim yok

13. Siber/Bilişim suç mağduru olanların şikâyetçi olduklarında hak arayışında sonuç elde ettiğine inanıyor musunuz?

☐ 1- Evet ☐ 2- Hayır ☐ 3- Kesinlikle hayır ☐ 4- Fikrim yok

14. Siber/Bilişim suçlarıyla mücadelede Emniyet Teşkilatının çalışmalarını yeterli buluyor musunuz?

☐ 1- Kesinlikle yeterli ☐ 2- Yeterli ☐ 3- Yetersiz ☐ 4- Kesinlikle yetersiz

15. Siber/Bilişim suçlarıyla ilgili mevcut yasaları yeterli buluyor musunuz?

☐ 1- Kesinlikle yeterli ☐ 2- Yeterli ☐ 3- Yetersiz ☐ 4- Kesinlikle yetersiz

16. Siber/Bilişim suçlarını önlemek amacıyla internet kullanımına sınırlama getirilmesini olumlu karşılar mısınız?

☐ 1- Evet ☐ 2- Hayır ☐ 3- Kesinlikle hayır ☐ 4- Önemsemem

17. Siber suçları önlemek amacıyla internette gözetlenmeyi olumlu karşılar mısınız?

☐ 1- Evet ☐ 2- Hayır ☐ 3- Kesinlikle hayır ☐ 4- Önemsemem

Ek-2 Araştirma İzin Belgesi

T.C.
AFYONKARAHİSAR VALİLİĞİ
İl Yazı İşleri Müdürlüğü

Sayı : 53299009-490-1722
Konu : Anketler

05/03/2014

AFYON KOCATEPE ÜNİVERSİTESİ REKTÖRLÜĞÜNE
(Öğrenci İşleri Daire Başkanlığı)

İlgi : 03.03.2014 tarihli ve 3215 sayılı yazınız,

Üniversiteniz Fen Bilimleri Enstitüsü İnternet ve Bileşim Teknolojileri Anabilim Dalı Yüksek Lisans öğrencisi Musa SÜRER'in "Siber Suç Algısı ve Eğitim Düzeyi ile İlişkisi' konulu anket uygulamasını Valiliğimiz ve Valiliğimize bağlı kurumlarda gerçekleştirmesi uygun görülmüştür.

Bilgilerinize rica ederim.

Adem USLU
Vali a.
Vali Yardımcısı

*Bu belge elektronik imzalıdır. İmzalı suretinin aslını görmek için https://www.e-icisleri.gov.tr/EvrakDogrulama adresine girerek (TUa/8t-xa/Pp4-1Z+7T3-DTq8ZC-ElncLAaV) kodunu yazınız.

Milli Birlik Cad. Hükümet Meydanı 03100 Afyonkarahisar Ayrıntılı bilgi için irtibat:M.Arif ALKAÇ
Telefon: (272)213 44 58 Faks: (272)214 07 59
e-posta: afyonkarahisar@afyonkarahisar.gov.tr Elektronik Ağ. www.icisleri.gov.tr