BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

SİBER SUÇLAR VE MÜCADELE YÖNTEMLERİ: DÜNYA UYGULAMALARI VE TÜRKİYE İÇİN ÇÖZÜM ÖNERİLERİ

Uğur ÖZÜDOĞRU

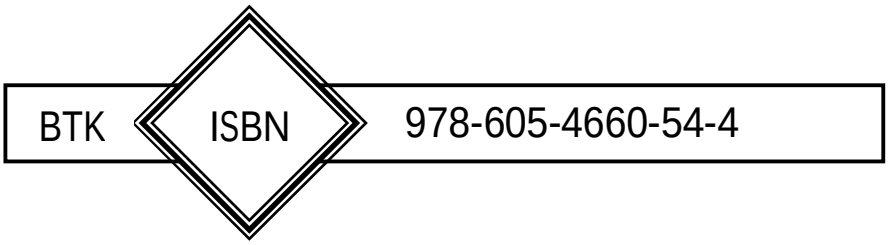
Bilişim Uzmanlığı Tezi

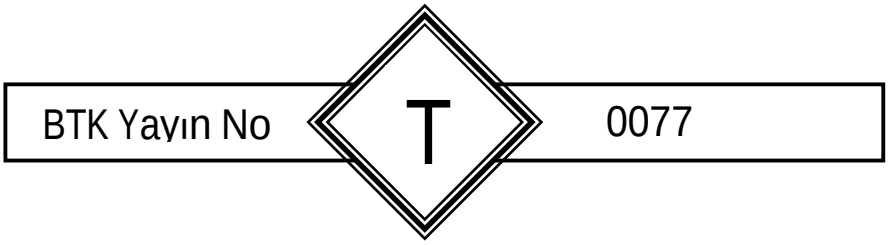
Aralık 2011

Ankara

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.





BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

SİBER SUÇLAR VE MÜCADELE YÖNTEMLERİ: DÜNYA UYGULAMALARI VE TÜRKİYE İÇİN ÇÖZÜM ÖNERİLERİ

Uğur ÖZÜDOĞRU

Bilişim Uzmanlığı Tezi

Aralık 2011

Ankara

Uğur ÖZÜDOĞRU tarafından hazırlanan SİBER SUÇLAR VE MÜCADELE YÖNTEMLERİ: DÜNYA UYGULAMALARI VE TÜRKİYE İÇİN ÇÖZÜM ÖNERİLERİ adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Leyla KESER BERBER
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : Yaşar GÖK

Üye : Dr. Muhterem ÇÖL

Üye : Mustafa ÜNVER

Üye : Cafer CANBAY

Üye : Yasin BAKIRCI

Üye : Yrd. Doç. Dr. Leyla KESER BERBER

Üye : Nihat SÜMER

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Siber Suçlar Ve Mücadele Yöntemleri: Dünya Uygulamaları Ve Türkiye İçin Çözüm Önerileri
Türü	Bilişim Uzmanlığı
Yazar	Uğur ÖZÜDOĞRU
Teslim Tarihi	05.12.2011
Anahtar Kelimeler	Siber Suçlar, Siber Güvenlik, Bilişim Suçları
Tez danışmanı	Yrd. Doç. Dr. Leyla KESER BERBER
Sayfa Adedi	148

Özet

Bu çalışmanın amacı, siber suçlarla mücadele yöntemlerinin ve bu konuda uluslararası alanda ve Avrupa Birliğinde yapılan çalışmaların incelenmesi, konuyla ilgili ülkemizde mevcut olan düzenlemelerin değerlendirilmesi ve çözüm önerilerinin sunulmasıdır.

Yapılan çalışmada siber suçlar, siber suçların işleniş şekilleri ve sınıflandırılması hakkında bilgi verilmiştir. Siber suçlarla mücadele yöntemleri belirlenerek yabancı ülke örnekleri ve uluslararası kuruluşların çalışmaları değerlendirilmiş, Avrupa Konseyi tarafından hazırlanan Siber Suç Sözleşmesi incelenmiş, ülkemizde siber suçlarla mücadeleye yönelik olarak yapılan çalışmalar ve düzenlemeler üzerinde durulmuş ve ülkemiz için çözüm önerileri getirilmiştir.

Yapılan inceleme ve değerlendirmeler neticesinde siber suçlarla etkin bir mücadele için gelişen teknolojinin doğal sonucu olarak ortaya çıkacak yeni suç tiplerine de cevap verebilecek esnek çözümlerin geliştirilmesi, bu alanda uluslararası işbirliğinin sağlanması için milli mevzuatımızın Avrupa Konseyi tarafından hazırlanan ve ülkemizin de imzaladığı Siber Suç Sözleşmesi'ne uygun hale getirilmesi ve her kurum ve kuruluşun ulusal işbirliği için teknik altyapılarını bu yasal düzenlemelere uygun olarak biçimlendirmesi gerektiği sonucuna varılmıştır.

ABSTRACT

INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY	
Thesis	Cybercrimes And Fighting Methods: Global Experiences And Solution Proposals For Turkey
Type	ICT Expert
Author	Uğur ÖZÜDOĞRU
Submission Date	05.12.2011
Key Words	Cyber Crimes, Cyber Security, Computer Related Crimes
Advisor	Yrd. Doç. Dr. Leyla KESER BERBER
Total Page	148

Abstract

The aim of this study is to analyze the existing studies which were made by other countries and especially by the European Union members on the issue of fighting cyber crime; to evaluate the sufficiency of the regulations in our country on this matter and to offer solutions for Turkey.

In this study; cyber crimes, modus operandi and classification of cyber crimes are explained. After fighting methods are defined, experiences of foreign countries and studies of international organizations are assessed. Convention on Cybercrime which is prepared by the Council of Europe is examined. Studies and regulations on fighting cyber crimes in Turkey are focused on and proposals of solutions for Turkey are developed.

As a result of these examinations and evaluations, effectively fighting cybercrime must develop of flexible solutions to meet the new types of crime will emerge as the natural result of developing technology, align national legislation with the Convention on Cybercrime prepared by the Council of Europe and signed by our country to ensure international cooperation in this area and accordingly technical infrastructure of each institution and the organization's in accordance with these regulations for national co-operation.

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Yrd. Doç. Dr. Leyla KESER BERBER'e, değerli eleştirileri ve tavsiyeleri ile çalışmamın son halini almasında büyük katkısı olan Bilgi Teknolojileri Dairesi Başkanı Mustafa ÜNVER'e, tez sürecinde elindeki kaynaklardan yararlanmamı sağlayan çalışma arkadaşım Bilişim Uzmanı Meltem TURHAN'a, desteklerini esirgemeyen arkadaşım Bilişim Uzmanı Yüksel GÜNAYDIN'a, tezimi okuyarak görüşlerini bildiren arkadaşım Bilişim Uzmanı Ayşe Gül MİRZAOĞLU'na ve özellikle bu yoğun süreçte kızlarımız Seher ve Serra'yı ihmal etmeden en büyük yardımcım olan sevgili eşim Çevre Yüksek Mühendisi Arife ÖZÜDOĞRU'ya teşekkürü bir borç bilirim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ACLU	American Civil Liberties Union (Amerikan Sivil Özgürlükler Birliği)
ADSL	Asymmetric Digital Subscriber Line (Bakışımsız Sayısal Abone Hattı)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (Fransa Ağ ve Bilgi Güvenliği Ajansı)
APCERT	Asia Pacific Computer Emergency Response Team (Asya Pasifik Bilgisayar Olaylarına Müdahale Ekibi)
BDDK	Bankacılık Düzenleme ve Denetleme Kurulu
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİLGEM	Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BİT	Bilgi ve İletişim Teknolojileri
BKA	Bundeskriminalamt (Federal Kriminal Dairesi)
BM	Birleşmiş Milletler
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BSI	Bundesamt für Sicherheit in der Informationstechnik (Almanya Bilişim Güvenliği Federal Dairesi)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CDA	Communications Decency Act (İletişim Ahlakı Yasası)
CERT	Computer Emergency Response Team (Bilgisayar Olaylarına Müdahale Ekibi
CERT/CC	CERT/Coordination Centre (CERT/Koordinasyon Merkezi)
CIA	Central Intelligence Agency (Amerikan Merkezi Haber Alma Örgütü)
COPA	Child Online Prevention Act (Çocukların Online Yayınlardan Korunması Yasası)
CoU	The Council of Europe (Avrupa Konseyi)
CPPA	Child Pornography Prevention Act (Çocuk Pornografisinin Önlenmesi Yasası)
DARPA	Defence Advanced Research Projects Agency (Savunma İleri Araştırma Projeleri Ajansı)

DCPJ	Direction Centrale De La Police Judiciaire (İç Güvenlikten Sorumlu Adli Polis)
DoD	Department of Defense (ABD Savunma Bakanlığı)
DOJ	Department of Justice (ABD Adalet Bakanlığı)
DOS	Denial of Service (Hizmetin Engellenmesi)
DDOS	Distributed Denial of Service Attack (Dağıtılmış Hizmetin Engellenmesi)
DHS	Department of Homeland Security (ABD İç Güvenlik Bakanlığı)
DNS	Domain Name System (Alan Adı Sistemi)
ECPA	Electronic Communications Privacy Act (Elektronik Haberleşmenin Gizliliği Yasası)
EGM	Emniyet Genel Müdürlüğü
ENISA	European Network and Information Security Agency (Avrupa Şebeke ve Bilgi Güvenliği Ajansı)
EPCIP	European Programme for Critical Infrastructure Protection (Avrupa Kritik Altyapıların Korunması Programı)
EUROPOL	European Police Office (Avrupa Polis Teşkilatı)
FBI	Federal Bureau of Investigation (Federal Araştırma Bürosu)
FIRST	Forum of Incident Reponse and Security Teams (Olay Müdahale ve Güvenlik Ekipleri Forumu)
FTC	Federal Trade Commission (Federal Ticaret Komisyonu)
FTP	File Transfer Protocol (Dosya Transfer Protokolü)
GAA	Geniş Alan Ağları
GAO	Government Accountability Office (ABD Genel Muhasebe Ofisi)
GCA	Global Cybersecurity Agenda (Küresel Siber Güvenlik Gündemi)
G-8	The Group of Eight (8'ler Topluluğu)
GMT	Greenwich Mean Time (Greenwich Ortalama Saati)
IBM	International Business Machines (Uluslararası İş Makinaları)
ICCP	International Computer and Communications Policy Committee (Uluslararası Bilgisayar ve İletişim Politikaları Komitesi)
ICPO	International Criminal Police Organization (Uluslararası Polis Teşkilatı) (INTERPOL)

IC3	Internet Crime Complaint Center (İnternet Suç Şikâyet Merkezi)
IDS	Intrusion Detection Systems (Saldırı Tespit Sistemleri)
IMPACT	International Multilateral Partnership Against Cyber Threats (Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği)
INTERPOL	International Police (Uluslararası Polis Teşkilatı)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention Systems (Saldırı Önleme Sistemleri)
IRC	Internet Relay Chat (İnternet Aktarmalı Sohbet)
ISPA-UK	The Internet Services Providers' Association UK (İngiltere İnternet Servis Sağlayıcıları Birliği)
ISPC	Information Security Policy Council (Japonya Bilgi Güvenliği Politika Konseyi)
ITU	International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
İSS	İnternet Servis Sağlayıcısı
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center (Japonya BOME Koordinasyon Merkezi)
KBA	Kritik Bilgi Altyapısı
KYMP	Kötücül Yazılımlarla Mücadele Projesi
KOM	Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı
KVKK	Kişisel Verilerin Korunması Kanunu
MAA	Metropol Alan Ağları
MIC	Ministry of Internal Affairs and Communications (Japonya İçişleri ve İletişim Bakanlığı)
NASA	National Aeronautics and Space Administration (Ulusal Havacılık ve Uzay Dairesi)
NIPC	National Infrastructure Protection Center (Ulusal Altyapı Koruma Merkezi)
NIRT	National Incident Response Team (Ulusal Olaylara Müdahale Ekibi)
NISC	National Information Security Center (Japonya Ulusal Bilgi Güvenliği Merkezi)
NPA	National Police Agency (Japonya Ulusal Polis Teşkilatı)

NW3C	National White Collar Crime Center (ABD Ulusal Beyaz Yaka Merkezi)
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (Fransa Siber Suçlarla Mücadele Merkez Ofisi)
OECD	Organization for Economic Cooperation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
PP/BEFTI	Brigade d'enquêtes sur les fraudes aux technologies de l'information (Paris Polis Valiliği/Siber Suçlarla Mücadele Birimi)
PUKÖ	Planla-Uygula-Kontrol Et-Önlem Al
SMS	Short Message Service (Kısa Mesaj Servisi)
SMTP	Simple Mail Transfer Protocol (Basit Posta İletim Protokolü)
STRJD	(Siber Suçlarla Mücadele Birimi)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
TBMM	Türkiye Büyük Millet Meclisi
TCK	Türk Ceza Kanunu
TCP	Transmission Control Protocol (İletim Denetimi Protokolü)
TCP/IP	Transmission Control Protocol/Internet Protocol (İletim Denetimi Protokolü/İnternet Protokolü)
TİB	Telekomünikasyon İletişim Başkanlığı
TR-BOME	Türkiye Bilgisayar Olaylarına Müdahale Ekibi
TSE	Türk Standartları Enstitüsü
TTNET	Türk Telekom İnternet
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
ULAKBİM	Ulusal Akademik Ağ ve Bilgi Merkezi
Ulak-CSIRT	Ulusal Akademik Ağ-Bilgisayar Güvenlik Olaylarına Müdahale Ekibi
UN	United Nations (Birleşmiş Milletler)
URL	Uniform Resource Locator (Birörnek Kaynak Konumlayıcı)
US-CERT	United States Computer Emergency Readiness Team (ABD Bilgisayar Olaylarına Müdahale Ekibi)
USGT	Ulusal Siber Güvenlik Tatbikatı
VOIP	Voice Over Internet Protocol (İnternet Protokolü Üzerinden Ses)

VPN	Virtual Private Network (Sanal Özel Ağ)
WIPO	World Intellectual Property Organization (Uluslararası Telif Hakları Teşkilatı)
WSIS	World Summit on the Information Society (Dünya Bilgi Toplumu Zirvesi)
YAA	Yerel Alan Ağları
ZaRD	Zentralstelle für anlassunabhängige Recherchen in Datennetzen (Veri Ağlarında Olay Bağımsız Araştırma Merkezi Birimi)

GİRİŞ

Bilgi ve iletişim teknolojileri (BİT) geleceğin dünyasını inşa etmektedir. Eski dünyanın yaşantı biçimi giderek yerini yeni bir hayat tarzına bırakmakta, eğitim, üretim, ticaret hatta sosyal hayat artık bilişim ağları üzerinde yaşanmaktadır. Devletler tarafından sunulan kritik hizmetler bilişim altyapılarına, yazılımlara ve donanımlara dayanmakta, insanlar finansal işlemlerini tamamen bilişim ağları üzerinden gerçekleştirmektedir.

Yakın geçmişe kadar geleceğin dünyasını tanımlarken kullanılan "küreselleşen dünya" söylemi artık yerini "bilgi toplumu (information society)" kavramına bırakmaktadır. İnternetin ani bir şekilde insanlığın hayatına girmesi ile fiziksel sınırlar baki kalsa da küreselleşme gerçekleşmiştir. Zaten bilgi toplumu da sınırlarla fazla ilgilenmemektedir. Bilgi toplumu değişen dünyada yeni ihtiyaçlarla ortaya çıkmıştır. Bilgiye bağımlı olan bu yeni nesil bilginin korunmasına muhtaçtır.

Günümüzde kapalı ağlardaki basit ve tek başına işletilen sistemlerin yerini; güçlü kişisel bilgisayarlar, ilerleyen teknolojiler ve internetin geniş kapsamlı kullanımı almıştır. Kullanıcılar giderek artan oranda ağlarla birbirine bağlanmakta ve bu bağlantılar ulusal sınırları aşmaktadır. Ayrıca internet enerji, ulaştırma ve finans gibi önemli altyapıları da desteklemekte olup, şirketlerin işleyişinde, hükümetlerin vatandaşlara ve teşebbüslere sundukları hizmetlerde ve bireylerin iletişim ve bilgi alışverişinde önemli bir rol oynamaktadır.

İletişim ve bilgi altyapısını oluşturan teknolojilerin yapısı ve çeşidi de oldukça değişmiştir. Altyapı erişim araçlarının sayısı ve yapısı sabit, kablosuz ve mobil araçları kapsayacak şekilde çoğalmıştır. Erişim, artık artan bir oranda sürekli çevrimiçi olan bağlantılar aracılığıyla yapılmaktadır. Sonuç olarak bilgi alışverişinin doğası, hacmi ve hassasiyeti büyük ölçüde artmıştır. Bilgi sistemleri ve ağlarının birbirleri ile bağlantısındaki artışın sonucu olarak, bilgi sistemleri ve ağlarının güvenliği artık artan sayıda ve çeşitlilikte siber tehditlere maruzdur (OECD, 2002).

Siber tehdit kavramı, güvenlik açıkları ve altyapısal zayıflıklardan yararlanılmasını ifade etmektedir. Bu tehditlere karşı alınacak önlemler hukukiden ziyade daha çok teknik olmaktadır. Farklı kuruluşlar aktif olarak siber savunma ile uğraşmaktadırlar. Buna karşın siber suçlar ise özellikle özel kuruluşlara yönelik bir yarar sağlama veya zarar verme amacını taşıyan saldırılardır. Siber suçlar internet ağ güvenliği geliştirilerek azaltılabilmesine rağmen, devletler siber suçlularla mücadele amacıyla yargı yetkisine sahip olma ve uygun hukuki araçları oluşturma çabası içindedirler (Keser Berber, 2011).

Bu kapsamda yapılan çalışmanın amacı; siber suçlarla mücadele yöntemlerinin ve bu konuda uluslararası alanda ve Avrupa Birliğinde yapılan çalışmaların incelenmesi, konuyla ilgili ülkemizde mevcut olan düzenlemelerin değerlendirilmesi ve çözüm önerilerinin sunulmasıdır.

Çalışma genel olarak dört bölümden oluşmaktadır. Giriş bölümünü takiben ilk bölümde; bilgisayar ile ilgili temel tanımların yanı sıra hukuki tanımlama da yapılarak günlük yaşama ve hukuksal düzenlemelere konu olan bu tanımların içeriğinin doğru olarak kavranması amaçlanmıştır. Ardından siber suç kavramı anlatıldıktan sonra siber suçların sınıflandırılması ve işleniş şekilleri konularında ayrıntılı bilgi verilmiştir.

İkinci bölümde, siber suçlarla mücadele yöntemleri olarak belirlenen hukuki, polisiye ve teknik yöntemler hakkında teorik bilgi verilmiştir.

Üçüncü bölümde; uluslararası örgütlerden Birleşmiş Milletler (BM), Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Uluslararası Telekomünikasyon Birliği (ITU), Avrupa Birliği, Avrupa Konseyi, Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (IMPACT), Avrupa Şebeke ve Bilgi Güvenliği Ajansı (ENISA), 8'ler Topluluğu (G-8), Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST), Avrupa Polis Teşkilatı (EUROPOL), Uluslararası Polis Teşkilatı (INTERPOL)'ün siber suçlarla mücadele konusundaki çalışmalarının yanı sıra ABD, Almanya, Fransa

ve Japonya gibi ülkelerin siber suçlarla mücadelede hukuki, polisiye ve teknik uygulamaları incelenmiştir.

Dördüncü bölümde siber suçlar ile ilgili olarak Türkiye'deki uygulamalardan hukuki boyutta Türk mevzuatındaki düzenlemeler, polisiye boyutta Emniyet Genel Müdürlüğü'nün (EGM) faaliyetleri ve teknik boyutta Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) çalışmaları incelenip değerlendirilmiştir.

Sonuç ve öneriler bölümünde ise bütün bu incelemeler doğrultusunda yapılması gereken düzenlemeler, alınması gereken tedbirler ve uygulanması gereken programlar hakkında görüş sunulmuştur.

1.SİBER SUÇLAR

Bu çalışmanın ilk bölümünde siber suç ve siber suçla ilişkili kavramlar açıklanmıştır. Öncelikle siber suça konu olan bilişim sistemleri ile ilgili temel tanımlar yapılmış sonrasında siber suç kavramı ve siber suçların sınıflandırılması ve işleniş şekilleri konularında ayrıntılı bilgi verilmiştir.

1.1.Temel Kavramlar

Bu bölümde siber suçlara konu olan bilişim sistemleri ile ilgili temel tanımların yanı sıra hukuki tanımlamalar da yapılarak sonraki bölümlerde sıkça ele alınan bu kavramların içeriğinin doğru olarak anlaşılması amaçlanmıştır. Bilişim ile ilgili kavramların tanımlanmasında hukuki bir perspektif takip edilerek tez kapsamında yer verilen hukuki değerlendirmelere bir dayanak teşkil etmesi planlanmıştır.

1.1.1.Bilgisayar

Bilgisayar, çok sayıda aritmetiksel ya da mantıksal işlemlerden oluşan bir işi, çalışması sırasında bir işletmenin işe karışması gerekmeksizin, önceden verilmiş bir izlenceye göre, otomatik olarak yürüten bir veri işleyicidir. Bir bilgisayar dizgesi elektronik ve mekanik birimlerden oluşan donanım ile bu donanım birimlerini ya da kaynakları istenen işlere yöneltip verimli bir çalışma düzeni içerisinde kullanabilmek için gerekli tüm izlencelerden ve veri yapılarından oluşan yazılım öğelerini kapsar (Köksal, 1981).

Kurt (2005) bilgisayarı, programlara ve verilen komutlara göre sıralı işlem yapan, otomatik olarak çalışan, verileri depolama, işleme tabi tutma, tasnif ve terkip etme, iletme özelliklerine sahip olan elektronik ya da manyetik akımlarla çalışan, mantıklı sonuçlar üreten, programlanabilen, genel amaçlı kullanılabilme özelliklerine sahip elektronik cihazlar olarak tanımlamıştır.

1.1.2.Bilgisayar ağları

Bilgi üretilmesi ve işlenmesinin en verimli olarak gerçekleştirildiği bilgisayar sistemlerinin birbirine bağlanarak bilginin iletildiği ve paylaşıldığı yapılara bilgisayar ağları denilmektedir. İki bilgisayar eğer bilgi alışverişinde bulunabiliyorsa bu iki bilgisayar birbirine bağlıdır denir. Bu bağlantı sadece bakır teller aracılığıyla olmaz; fiber optik kablolar, mikrodalgalar ve iletişim uyduları da kullanılabilir (Soğukpınar, 2006).

Bilgisayar ağları boyutlarına (kapsadıkları alanın büyüklüğüne) göre genellikle, Yerel Alan Ağları (YAA), Metropol Alan Ağları (MAA) ve Geniş Alan Ağları (GAA) olmak üzere üç grup altında toplanmaktadır. YAA'lar bir odayı, binayı ya da kampüsü kapsayabilecek boyutta olup, en fazla birkaç kilometre (km) uzunluğunda ağlardır. MAA'lar bir şehri kapsayacak boyuttadırlar. Bir şehirdeki kablolu TV ağı MAA olarak gösterilebilir. GAA'lar ise coğrafi olarak büyük alanları (bir ülke ya da kıta boyutunda) kapsarlar (Oktuğ, 2010).

1.1.3.Veri

Veri; olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi olarak tanımlanmaktadır (Köksal, 1981). Bir bilgisayarda ya da bilgisayarlar tarafından okunabilen araçlarda saklanabilen ve üzerinde işlem yapılabilen her şey veridir (Yenidünya ve Değirmenci, 2003).

Veri, bilgi işleme sürecinin temel hammaddesi olan ve çeşitli sembol, harf, rakam ve işaretlerle temsil edilen, ham, işlenmeye hazır, işlenmemiş gerçekler ya da kazanımlardır (Bensghir, 1996).

1.1.4.Bilişim

Bilişim kelimesinin kaynağı Fransızca bilgi vermek kökeninden gelen informatique (enformasyon) kelimesidir. Önceleri enformasyon olarak kullanılan kelimenin

yerine zamanla bilgi kökeninden gelen bilişim kullanılmaya başlanmıştır (Dülger, 2004).

Köksal (1981) bilişimi insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve mantıksal biçimde işlenmesi bilimi olarak tanımlamaktadır.

Aydın (1992)' ye göre bilişim; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevresindeki yerinde ve zamanında kullanılan teknolojileri içine alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinliklerdir.

Bilgisayar verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetlerini yani verilerin işlenmesini sağlamakta iken, bilişim hem verilerin işlenmesini hem de verilerin iletişimini kapsaması sebebiyle bilgisayara göre daha üst bir kavramdır (Yenidünya ve Değirmenci, 2003).

1.1.5.İnternet

İngilizce "Interconnected Networks" (kendi aralarında bağlantılı ağlar) kelimelerinden türetilen internet, dünya üzerine yayılmış milyonlarla ifade edilen sayıdaki bilgisayarın birbirine bağlanması ile oluşan ağların yine birbirine bağlanması ile oluşan çok geniş yapıdaki bir ağı tanımlar (Boğaç ve Songür, 1999). Ayıca internet, birden fazla haberleşme ağının birlikte meydana getirdikleri metin, resim, müzik, grafik, yazılı metin vb. dosyalar ile bilgisayar yazılımlarının, kısaca insanlar tarafından oluşturulmuş her türlü bilginin veri halinde paylaşıldığı ve iletildiği bilgisayarlar arasındaki ağ olarak tanımlanabilir (Özdilek, 2002).

Veri trafiğinin kurallarını düzenleyen "TCP/IP Protokolü" ve internet üzerinde veri arama ve aktarmaya yarayan yazılım sistemi "World Wide Web" (Dünyayı saran ağ) internetin teknik unsurlarıdır. İnternetin teknik alt yapısını ise internet üzerideki veri iletişimini sağlayan ana iletişim hatları olan "omurga"lar oluşturmaktadır.

İnternet' in kökeni, hataya dayanıklı, sağlam ve özel bir bilgisayar ağı kurmak isteyen Amerika Birleşik Devletleri (ABD) hükümeti tarafından 1960 yılında başlatılan araştırmalara dayanmaktadır. 1980'lerde Ulusal Bilim Vakfı tarafından yeni bir ABD omurgasının finansmanı için toplanan özel fonlar, dünya çapında katılıma ve birçok özel ağın birleşmesine neden olmuştur. 1990'larda ise bu uluslararası ağın yaygınlaşması ile internet, modern insan hayatının temelinde yer almıştır.

İnternet herhangi bir kişinin buluşu ya da ticari malı değildir. Bu büyük ağ sistemi sisteme giren herkesin katkısıyla oluşmuş anonim bir yapı olduğundan internetin bir sahibi ya da yöneticisi yoktur (Sınar, 2001). İnternetin bir yöneticisinin olmamasının faydalı yönleri olduğu gibi zararlı yönleri de bulunmaktadır. Bu faydalı yönleri arasında internetin bugüne kadar hiç olmadığı kadar demokratik bir yapıya ve sınırsız bir ifade özgürlüğüne sahip olması, çıkar grupları kadar tek tek bireylerin de seslerini duyurabilmeleri, ekonomik açıdan hiçbir yere bağlı olmayışı ve her türlü gelişmeye açık bulunması gösterilebilir. Bu sınırsız özgürlüğün zararlı tarafı ise yine özgürlüğün kendisinden gelmekte, hiçbir kuralın ya da sınırın olmadığı bir ortamda her yeni teknolojik gelişmede karşılaşılan kötüye kullanımların, rahatsız edici davranışların ve suç oluşturan eylemlerin de gerçekleştirilebilmesi internetin zararlı tarafını oluşturmaktadır (Dülger, 2004).

Bilişim hukukuna konu olan internet süjeleri; telefon/telekomünikasyon idareleri, sunucu, servis sağlayıcılar ve kullanıcılardır. Bu süjelerden servis sağlayıcıları da; içerik sağlayıcı, hizmet sağlayıcı ve erişim sağlayıcı olmak üzere üç gruba ayrılmaktadır. Bu ayrım internet suçları söz konusu olduğunda cezai sorumluluğu belirleme açısından önem kazanmaktadır (Yıldız, 2006).

1.1.6.Suç

Suç, tarihin en eski devirlerinden itibaren var olmuş ve ileride de var olmaya devam edecek olan evrensel bir olaydır. İnsanların içinde ihtiraslarla birlikte toplum halinde yaşamanın ortaya çıkardığı çeşitli sosyal çelişkiler, uyumsuzluklar bulundukça suç da var olacaktır. Suç topluma zarar verdiği ya da tehlikeli olduğu kanun koyucu tarafından kabul edilen ve belirtilen eylemdir. Her devirde, bir hareketin topluma zarar vermekte olduğu veya tehlikeli bulunduğu fikir ve kanaatinde olan kanun koyucular sözü geçen fiilleri kanunlarla yasaklar ve ceza müeyyideleriyle karşılarlar (Dönmezer, 1994).

Türk Ceza Kanunu (TCK)' nun, 'Kanunun sarih olarak suç saymadığı bir fiil için kimseye ceza verilemez.' hükmünü koyan birinci maddesinden hareketle ceza kanunu tarafından açıkça cezalandırılan her fiilin suç olduğu söylenebilir (Alacakaptan, 1975). 2004 yılında yayımlanan 5237 sayılı TCK' da bu hüküm 'Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz.' şeklinde değiştirilmiştir.

Suç; kanuni, maddi, manevi unsur ve hukuka aykırılık unsuru olmak üzere dört unsurdan oluşur. Buna göre;

Kanuni unsur; yasanın açıkça suç saymadığı bir eylem için ceza verilemez. Buna göre bir eylemin suç sayılabilmesi için her şeyden evvel yasanın özel hükümleri arasında ya da ceza hükümlü özel bir yasada yer alan belli bir maddedeki tanıma uygun olması gerekir (Alacakaptan, 1975).

Hukuka aykırılık unsuru; fiilin suç teşkil etmesi için kanunda belirtilen harekete uyması gereklidir. Bu unsur kanunilik ilkesinden ortaya çıkar (Alacakaptan, 1975).

Maddi unsur; dış dünyada bir değişikliğe yönelmiş müspet veya menfi bir fiil bulunmadıkça bir suçun varlığı da ileri sürülemez. Maddi unsur bir suçun var olması için kanuni tarife uygun bir fiilin bulunması şartıdır (Dönmezer ve Erman, 1967).

Manevi unsur; failin kusurlu bir şekilde hareket etmesinden yani kusurlu olmasından ibarettir (Gözübüyük, 1989). Manevi unsuru kısaca fiillerin iradiliği olarak da tanımlanmaktadır. Bu iradiliğin yanında bu iradenin isnad kabiliyetine sahip bir kişiye ait de olması gerekir (Alacakaptan, 1975).

Bahsi geçen unsurlar ve koşullar ışığında suç; isnad yeteneğine sahip bir kişinin kusurlu iradesinin yarattığı icraî veya ihmali bir hareketin meydana getirdiği yasada yazılı tipe uygun, hukuka aykırı ve müeyyide (yaptırım) olarak bir cezanın uygulanmasını gerektiren bir eylem olarak tanımlanabilir (Alacakaptan, 1975).

1.2.Siber Suç Kavramı

Teknolojik gelişmeler, gerek suçların işlenmesinde kolaylık, gerekse suçun konusu olabilecek objelerde çeşitlilik ve insanların birçok aktivitelerini elektronik ortam üzerine aktarması ile geniş bir platformda birçok hukuki yararın ihlal edilmesine açık bir ortam yaratılmasını sağlamıştır (Beceni, 2003). Bilişim ortamında işlenen suçları tanımlamak üzere bilgisayar suçu (computer crime), bilgisayarla ilgili suç (computer-related crime), bilgisayarla işlenen suç (computer assisted crime), bilgisayara karşı işlenen suç (crimes against computer) ve bilgisayarın kötüye kullanımı (computer abuse) gibi kavramlar kullanılmakta birlikte son dönemde siber suç (cyber crime) kavramının kullanımı yaygınlık kazanmıştır.

Herhangi bir suçun elektronik ortam içerisinde işlenebilme imkânı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçlar siber suçlar olarak adlandırılır (Beceni, 2003).

Dülger (2004) siber suçu verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suç şeklinde tanımlamıştır.

1.3.Siber Suçların Sınıflandırılması

Siber suçlarla mücadelede hangi yöntemlerin, nasıl kullanılacağı sorusuna cevap aramadan önce ne ile mücadele edileceğini daha iyi anlamak için yapılan siber suç tanımına ek olarak bunların sınıflandırılması üzerinde bir inceleme yapmak gerekmektedir. Zira ceza hukukunun temel ilkelerinden biri olan "kanunsuz suç ve ceza olmaz" ilkesi uyarınca, kanun koyucularının kanunlarda suçları tanımlamaları ve bu suçlar için düzenlemeler yapması gerektiği ifade edilmiştir. Ancak bu konuda farklı zamanlarda yapılan çalışmalar teknolojinin ve suç tiplerinin değişimine paralel olarak farklılık arz etmektedir. Genel olarak siber suçların sınıflandırılması hukuki ve yine hukuki değerlendirmelere zemin teşkil edecek şekilde teknik olarak ikiye ayrılabilir.

Bu çalışmada, siber suçların sınıflandırılmasında hukuki bir yol izleyen BM bildirilerinde ve Avrupa Konseyi Siber Suç Sözleşmesi'nde yer alan sınıflandırmalara kısaca değinilmiş, bunları kapsayan bir yapıda olan ITU sınıflandırması ise detaylı olarak incelenmiştir. Ayrıca teknik bir sınıflandırma örneği olarak kabul edebileceğimiz, McConnell International adlı, Amerikan küresel politika ve teknoloji yönetimi danışmanlık firması tarafından yapılan sınıflandırma incelenmiştir.

1.3.1.Birleşmiş Milletler sınıflandırması

BM'nin yayınladığı "Uluslararası Suç Politikasının Değerlendirilmesi-Bilgisayarla İlişkili Suçlar Kontrol ve Korunma Rehberi"nde yaygın olarak görülen bilgisayarla ilişkili suçlar 5 kategoriye ayrılmıştır (Birleşmiş Milletler, 1994).

- Bilgisayar manipülasyonu ile dolandırıcılık
- Bilgisayar sahteciliği
- Bilgisayar veri ve/veya programlarının değiştirilmesi ya da hasara uğratılması
- Bilgisayar sistem ve servislerine yetkisiz erişim
- Yasal olarak korunan programların izinsiz çoğaltılması

1.3.2.Avrupa Konseyi siber suç sözleşmesi sınıflandırması

Avrupa Konseyi Bakanlar Komitesince 8 Kasım 2001 tarihinde onaylanan ve hedefi ortak bir ceza politikasının oluşturulması ile toplumun siber suça karşı korunması, özellikle gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin gerçekleştirilmesi olan Avrupa Konseyi Siber Suç Sözleşmesi'nde siber suçlar dört ana kategoride incelenmiştir. Bunlar;

- Bilgisayar veri ve sistemlerinin bütünlüğüne, gizliliğine ve erişebilirliğine ilişkin suçlar
- Bilgisayarlarla ilgili suçlar
- İçerikle ilgili suçlar
- Telif Hakları ile ilgili suçlardır.

'Bilgisayar veri ve sistemlerinin bütünlüğüne, gizliliğine ve erişebilirliğine ilişkin suçlar', 'İçerikle ilgili suçlar' ve 'Telif Hakları ile ilgili suçlar' kategorileri nesnenin yasal olarak korunmasına odaklanmıştır. 'Bilgisayarlarla ilgili suçlar' kategorisi ise nesnenin yasal olarak korunmasına değil metoda odaklanmıştır. Bu tutarsızlık bazı kategoriler arasında çakışmaya yol açmaktadır. Ayrıca, suç eylemlerini tanımlamak üzere kullanılan bazı terimler de örneğin siber terörizm ve yemleme (phishing) çeşitli kategorilerde çakışmaktadır. Bununla birlikte, Siber Suç Komitesi tarafından hazırlanan bu kategoriler siber suç kavramının tartışılmasında yararlı bir temel kaynak olarak hizmet etmektedir (ITU, 2009).

1.3.3.Uluslararası Telekomünikasyon Birliği sınıflandırması

ITU'nun BİT Uygulamaları ve Siber Güvenlik Birimi tarafından hazırlanan raporlardan biri olan Siber Suçları Anlamak: Gelişmekte Olan Ülkeler için Rehber (ITU, 2009) de tanımlanan siber suç kategorileri aşağıda incelenmiştir. ITU'nun suç sınıflandırması Avrupa Konseyi Siber Suç Sözleşmesindeki sınıflandırma temel alınıp bunların daha da geliştirilmesiyle oluşturulmuştur.

1.3.3.1.Bilgisayar veri ve sistemlerinin bütünlüğüne, gizliliğine ve erişebilirliğine ilişkin suçlar

Bu kategorideki tüm suçlar gizlilik, bütünlük ve erişilebilirlik ilkelerini bozmaya yöneliktir. Yüzyıllardır ceza hukukunca kapsanan suçlardan (hırsızlık, adam öldürme vs.) farklı olarak bilgisayar sistemlerinin son 60 yılda ortaya çıktığı ve geliştiği düşünülürse suç ve tacizin sayısallaşması göreceli olarak çok yenidir. Bu suçların sağlıklı kovuşturması sadece somut varlıkların ve fiziksel dokümanların korunmasına yönelik olmamalı aynı zamanda yeni yasal prensipleri de içerecek şekilde genişletilmelidir. Bu kategoride yer alan ve en çok gerçekleşen suçlar genel olarak aşağıda açıklanmıştır.

1.3.3.1.1.Yasadışı erişim (Illegal Access- Hacking, Cracking)

Bilgisayarlarla ilgili en eski suç olan ve sistem kırıcılık olarak anılan bu suç bir bilgisayar sistemine yasadışı olarak erişmeye denir. Bilgisayar ağlarının özellikle de İnternetin gelişmesi ile bu suç büyük ölçüde artmıştır. Hacking ataklarının ünlü hedefleri arasında Amerikan Havacılık ve Uzay Dairesi (NASA), ABD Hava Kuvvetleri, Pentagon, Yahoo, Google, Ebay ve Almanya Hükümeti bulunmaktadır.

Sistem kırıcılık saldırılarına örnek olarak şifre korumalı internet sitelerinin şifrelerini kırmak ve bilgisayarların şifre korumasını atlatmak verilebilir. Bu saldırıların hazırlık aşamaları aşağıdaki şekillerde olabilmektedir:

- Bir bilgisayar sistemine girmek için gerekli şifreyi elde etmeye yönelik donanım ve yazılım geliştirmek,
- Kullanıcıların şifrelerini ele geçirmek için yanıltıcı (spoof) İnternet siteleri kurmak,
- Virüs, trojan vb. kötücüller vasıtasıyla hedef bilgisayarlara veya cihazlara her klavye hareketini (şifre girişi vs.) kaydeden donanım ve yazılım yüklemek.

Bilgisayar sistemlerine yasadışı erişimin hızlı bir şekilde artan bir suç şekli olduğu bilinmektedir. Sadece 2007 yılının Ağustos ayı içerisinde dünyada 250 milyon vaka kaydedilmiştir. Sistem kırıcılık ataklarının artmasında üç önemli faktör vardır. Bunlar; bilgisayar sistemlerinin yetersiz ve eksik korunması, saldırıları otomatikleştiren yazılımların geliştirilmesi ve hacker (saldırgan) stratejilerinde özel bilgisayarların artan rolüdür.

Avrupa Konseyi Siber Suç Sözleşmesinin "Yasadışı Erişim" başlıklı 2 nci maddesinde "Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır" (Avrupa Konseyi, 2001) denilmek suretiyle sözleşmeye taraf olanların bu konuda hukuki bir düzenleme getirmesi gerektiği belirtilmiştir.

1.3.3.1.2.Veri casusluğu (Data Espionage)

Günümüzde kişisel bilgiler, ülke sırları, ticari projeler gibi hassas bilgiler genellikle bilgisayar sistemlerinde tutulmaktadır. Eğer bilgisayar sistemi İnternet'e bağlı ise siber saldırganlar dünyanın her yerinden İnternet aracılığıyla bu bilgiye erişme şansına sahiptir. Hassas bilginin değeri ve bu bilgiye uzaktan erişebilirliğin sağlanması veri casusluğunu cazibeli hale getirmiştir.

1980'lerde bir grup Alman sistem kırıcı ABD hükümetinin ve askeriyesinin bilgisayar sistemlerine girmiş, bazı gizli verileri ele geçirmiş ve bunu Sovyetler Birliğine satmıştır. Saldırganlar kurbanların bilgisayarlarına erişmek için korunmasız kapıları tarayan (port scanning) yazılımlar, güvenlik önlemlerini atlatan yazılımlar ile sosyal mühendislik (social engineering) gibi farklı yöntemler kullanmışlardır.

Özellikle sosyal mühendislik ile ilgili son maddede, normal güvenlik aşamalarını geçmek için teknik yollar değil, insanları kandırma yöntemi kullanılmıştır. Sosyal mühendislik teknikleri, iyi korunmuş bilgisayar sistemlerine yapılan saldırılardan

daha az etkili bir yöntem olarak değerlendirilmemelidir. Bu yöntemin temelinde insani duyguların bilgisayar sistemlerine erişmek için istismar edilmesi yatmaktadır. Sosyal mühendislik, bilgisayar güvenliğindeki en zayıf halka insan olduğundan genellikle başarılı bir yöntemdir.

Ancak iyi eğitilmiş kullanıcılar saldırganlar için kolay bir kurban değildir. Kullanıcı eğitimi siber güvenlik stratejisinin önemli bir parçasını oluşturmaktadır. Şifreleme teknikleri güvenliği arttırmada yardımcı olacağından, kullanıcılar için bu teknikleri kullanarak şifreleme yapmanın önemine dikkat çekilmelidir. Hassas bilgiyi saklayan kişi ya da organizasyonun düzgün şifreleme teknikleri kullanması fiziksel güvenlik tedbirlerinden daha önemlidir. Saldırganların hassas bilgileri elde etmede başarılı olma nedenlerinden biri de güvenlik önlemlerinin eksik olmasıdır.

1.3.3.1.3.Yasadışı müdahale (Illegal Interception)

Bu suç tanımıyla veri iletişiminin gizliliği hakkının korunması amaçlanmıştır. Siber Suç Sözleşmesinin açıklayıcı raporunun üçüncü maddesinde teknik yöntemler kullanarak müdahalenin kapsamının, iletişimin içeriğinin dinlenmesi, denetlenmesi ya da izlenmesi ve verilerin içeriğinin bilgisayar sistemine erişim ve sistemin kullanımı yoluyla doğrudan ya da elektronik gizli dinleme cihazlarının yardımı ile dolaylı olarak elde edilmesi ile ilgili olduğu belirtilmiştir (Avrupa Konseyi, 2001).

Saldırganlar kişiler arasındaki e-posta benzeri iletişime ya da herhangi veri iletimine, gönderilip alınan veriyi kaydederek müdahale edebilirler. Saldırganlar bu ihlali yaparken kablolu ya da kablosuz herhangi bir iletişim ortamını kullanabilirler. İnternet servis sağlayıcılar arasındaki iletişim genelde iyi korunmuştur ve ihlal edilmesi zordur. Ancak saldırganlar en zayıf noktayı ararlar. Kablosuz sistemler oldukça yaygın kullanılmakla beraber bunların geçmişten gelen bir savunmasızlığı da vardır. Şimdilerde oteller, restoranlar gibi hizmet sektöründeki birçok unsur İnternet hizmetini kablosuz olarak vermektedir. Bununla birlikte, kablosuz ağların yaydığı sinyalleri bulunulan yere ve erişim noktasının gücüne bağlı olarak uzak sayılabilecek bir mesafeden algılamak saldırganlar için mümkün olabilmektedir.

Bazı saldırganlar hassas bilgilere ulaşmak için popüler yerlerin civarında kendi erişim noktalarını kurarak şifresiz hizmet vermektedirler. İnternete erişmek amacıyla bu erişim noktalarını kullanan kişiler önemli bilgilerini çaldırabilmektedir.

Bu konuda sabit hatların kullanımı da saldırganların ataklarını engelleyememektedir. Öyle ki, veri iletim hattından geçerken yayılan elektromanyetik alanı doğru cihazların kullanılmasıyla algılayarak kaydeden saldırganlar hassas verileri ele geçirebilmektedirler.

Avrupa Konseyi Siber Suç Sözleşmesinin "Yasadışı Müdahale" başlıklı 3 üncü maddesinde "Kamuya açık olmayan bilgisayar verilerinin iletimi sırasında teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verilerin bulunduğu bilgisayar sistemi üzerinden veri iletimine haksız surette dahil olma fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır" denilmiştir (Avrupa Konseyi, 2001).

1.3.3.1.4.Verilere müdahale (Data Interference)

Siber Suç Sözleşmesi Açıklayıcı Raporun dördüncü maddesine göre bu hükmün amacı, bilgisayar verilerini ve bilgisayar programlarını kasıtlı hasar verme girişimlerine karşı koruma altına almaktır.

Bilgisayar verisinin bütünlüğü ve erişilebilirliği kişisel, iş veya yönetim amaçlı kullanım söz konusu olduğunda büyük önem arz etmektedir. Veriye erişimdeki kesintiler önemli ölçüde finansal kayıplara yol açabilmektedir. Saldırganlar verinin bütünlüğünü ve erişilebilirliğini aşağıdaki yollarla ihlal edebilmektedir;

- Verileri silerek,
- Verileri gizleyerek,
- Verileri değiştirerek,
- Veriye erişimi engelleyerek.

Bilgisayar verisinin silinmesinin genel bir örneği olarak virüsler verilebilir. Bilgisayar teknolojisinin ilk var olduğu zamanlardan beri bilgisayar virüsleri yeterli güvenlik önlemi almayan kullanıcılar için daima önemli bir tehdit oluşturmuştur.

Taşınabilir depolama araçlarıyla bulaşan ilk bilgisayar virüslerinden beri e-posta aracılığıyla yayılan ya da İnternetten indirilen yazılımlar aracılığıyla bulaşan bilgisayar virüsleri oldukça yaygın ve hızlıdır. SQL Slammer virüsü İnternet'teki korunmasız bilgisayarların %90'ını tahmini 10 dakika gibi bir sürede etkilemiştir (GAO, 2005).

Avrupa Konseyi Siber Suç Sözleşmesinin "Verilere Müdahale" başlıklı 4 üncü maddesinde "Taraflardan her birinin, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiillerinin kasıtlı olarak yapıldıklarında kendi ulusal mevzuatları kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır" denilmiştir (Avrupa Konseyi, 2001).

1.3.3.1.5.Sistemlere müdahale (System Interference)

Siber Suç Sözleşmesi Açıklayıcı Raporun beşinci maddesinde telekomünikasyon olanakları da dahil olmak üzere bilgisayar sistemlerinin yasalara uygun şekilde kullanımının, bilgisayar verileri kullanılarak ya da bu veriler etkilenerek engellenmesi fiili suç olarak tanımlanmaktadır.

Bilgisayar verilerine karşı yapılan saldırılarla ilgili zafiyetlerden duyulan kaygıların aynıları bilgisayar sistemleri için de geçerlidir. 7/24 esasına göre hizmet veren işletmeler İnternet hizmetlerini üretim süreçleriyle her geçen gün daha çok birleştirmektedir. Saldırganlar bilgisayar sistemlerinin işlemesini az da olsa sekteye uğratsalar, saldırıya uğrayanlar için bu etkiden doğan finansal kayıp azımsanmayacak büyüklükte olacaktır.

Avrupa Konseyi Siber Suç Sözleşmesinin "Sistemlere Müdahale" başlıklı 5 inci maddesinde "Taraflardan her birinin bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır" denilmiştir (Avrupa Konseyi, 2001).

1.3.3.2.Bilgisayarlarla ilişkili suçlar

Bu kategoride gerçekleştirilen suçları iki kategoride değerlendirmek mümkündür.

- Bilgisayar yoluyla sahtekârlık fiilleri
- Bilgisayar yoluyla dolandırıcılık fiilleri

1.3.3.2.1.Bilgisayar yoluyla sahtekârlık fiilleri

Bilgisayarlarla bağlantılı sahtekârlık, verilerin alınması, değiştirilmesi ve silinmesi yollarından biriyle, bir başkasının, hile teşkil edecek bilişim teknikleri kullanarak hataya düşürülmesi ve kendisinin veya bir başkasının lehine, mağdur aleyhine haksız menfaat temin edilmesi olarak tanımlanabilir (Kurt, 2005).

Avrupa Konseyi Siber Suç Sözleşmesinin "Bilgisayarlarla İlişkili Suçlar" başlıklı 7 nci maddesinde "Taraflardan her biri, söz konusu verilerin doğrudan doğruya okunabilir ve anlaşılabilir nitelikte olup olmadığına bakılmaksızın, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme fiillerinin, söz konusu verilerin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi amacıyla, kasıtlı olarak ve haksız şekilde yapıldığında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır" şeklinde belirtilmiştir (Avrupa Konseyi, 2001).

1.3.3.2.2.Bilgisayar yoluyla dolandırıcılık fiilleri

Bilgisayar yoluyla yapılan dolandırıcılık suçları, saldırganın kimliğini gizlemesini sağlayan yazılım araçları kullanılarak kolaylıkla yapılabildiğinden, İnternet üzerinden işlenen en popüler suçlardan biridir. Bu yazılım araçları saldırganın birçok küçük işlemden büyük kazançlar elde etmesini sağlayabilir.

Kişilerin hassas bilgilerinin yetkisiz kişilerce dolandırıcılık fiilinde ya da diğer suçların işlenmesinde kullanılmak üzere ele geçirilmesi, değiştirilmesi, başkasına verilmesi olarak tanımlanabilecek kimlik hırsızlığı suçu da bilgisayar yoluyla yapılan dolandırıcılık fiillerinin arasında gelmektedir.

Bilgisayar yoluyla dolandırıcılık fiillerinden biri olan yemleme yöntemleri ile oluşturulan uydurma e-postalar, kolluk kuvvetleri için önemli bir sorun oluşturmaktadır. Yemleme saldırılarıyla kişisel bilgilerin açığa çıkarılması amaçlanmaktadır. Saldırganlar genellikle, gerçeğinden ayırt edilmesi oldukça zor olan e-postaları yasal bir finansal kuruluştan geliyormuş gibi gönderirler. Bu mesajlarda kişiden bazı kişisel bilgilerini doğrulaması istenebilir. Birçok kişi bu e-postalara inanmakta ve hassas bilgilerini ifşa etmektedir.

Yemleme yöntemi ile yapılan farklı bir saldırı 2006 yılında Nijerya'da meydana gelmiştir. Olayda, saldırgan, kurbanlara gönderdiği bir e-posta ile uçak kazasında ölen karısının 10 milyon dolarlık banka hesabını ABD'de yaşayan ailesinin hesabına aktarmak için başka bir hesaba ihtiyaç duyduğunu belirtmiş bunun için kurbanın kendi hesabını doğrulamak için kendi hesabına 10 dolar yatırmasını istemiştir. Karşılığında ise 10 milyon doların, 1 milyon dolarının kurbanın kendisinde kalabileceğini belirtmiştir (Huffman, 2006).

Avrupa Konseyi Siber Suçlar Sözleşmesinin "Bilgisayarlarla İlişkili Suçlar" başlıklı 8 inci maddesinde "Sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilemez

kılma, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme faaliyetlerinde bulunmak suretiyle bir başkasının mülkiyetinin ziyanına sebep olma fiilinin kasıtlı ve haksız olarak yapıldığında kendi ulusal mevzuatı kapsamında cezai birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır" denilmektedir (Avrupa Konseyi, 2001).

1.3.3.3.İçerikle ilgili suçlar

Bu kategori, çocuk pornografisi, yabancı düşmanlığı içeren materyaller ya da yasadışı olarak kabul edilen içeriği kapsamaktadır. Bu kategori ile ilgili yasal araçların geliştirilmesinde kültürel ve hukuki esasları dikkate alan ulusal yaklaşımlardan yararlanılmaktadır. Yasadışı içerik ile ilgili değer sistemleri ve hukuk sistemleri toplumlar arasında geniş farklılık gösterir. Yabancı düşmanlığının yaygınlaştırılması ile ilgili malzemeler birçok Avrupa ülkesinde yasadışı iken, ABD'de özgürlük ilkesi kapsamında yasal olarak korunmaktadır. Peygamberler ile ilgili olarak aşağılayıcı sözler kullanılması birçok Arap ülkesinde suç olduğu halde bazı Avrupa ülkelerinde suç kapsamına girmemektedir.

1.3.3.3.1.Pornografi

Toplumun ar ve hayâ duygularını incitecek şekilde genel ahlaka aykırı pornografik görüntülerin internette yayınlanmasıdır. Yurtdışında çocuk pornografisine karşı tedbir alınmakla birlikte, ülkemizde çocuk veya yetişkin pornografisi gibi bir ayrım yapılmadığından bütün pornografik yayınlar yasaklanmıştır (Dokurer, 2001).

1.3.3.3.2.Çocuk Pornografisi

Çocuk pornografisi terimi 18 yaşından küçük kimseleri görsel anlamda teşhir eden pornografik malzemeler için kullanılmaktadır. Avrupa Konseyi Siber Suçlar Sözleşmesinde içerikle ilgili suçlardan sadece çocuk pornografisi ana sözleşmeye dahil edilmiş diğer içerik suçlarına ana sözleşmede yer verilmemiştir.

1.3.3.3.3.Siber Propaganda

Bir kişinin ya da örgütün görüşlerini televizyon ya da gazete gibi medya araçlarında yayımlamasının zorluğu ve bu tür yayınların denetime tabi olduğu göz önüne alındığında internette propaganda yapmanın suçlular açısından ne kadar avantajlı olduğu daha iyi anlaşılmaktadır. İnternet, terör örgütleri mensuplarının birbirleri ile iletişim kurmada, şiddet ve nefret içerikli mesajlarını kitlelere, sempatizanlarına ulaştırmada bir vasıta / yol haline gelmiştir (Ergün, 2008).

1.3.3.3.4.Din karşıtı suçlar

Birçok devlet anayasaları ile din ve vicdan hürriyetini koruma altına almıştır. Bununla birlikte İnternet sitelerinde giderek artan sayıda din karşıtı ifadelerin yer aldığı siteler bulunmaktadır. Bu malzemelerin bazıları nesnel olgular ve eğilimler dahi olsa (örneğin Avrupa'da kiliseye katılım oranlarının azalması) bu tür içerikler bazı yerlerde yasadışı olarak kabul edilmektedir. Dinlere hakaret edilmesi ya da karikatürlerin yayınlanması da bu tür suçlara örnek olarak verilebilir.

1.3.3.3.5.Siber kumar

Kumar da her ülkenin kanunlarında suç olarak düzenlemeyen konulardan biridir. Bu yüzden kumarın yasal olduğu ülkelerden yayın yapan İnternet oyunları ve kumar İnternette en hızlı büyüyen alanlardan biridir. TCK'nın 228. maddesinin 1. fıkrası gereğince internet ortamında oynanan kumar da cezalandırılmaktadır.

1.3.3.3.6.Hakaret ve yanlış bilgiler

Genellikle şahsi düşmalıklardan dolayı kişi ve kurumlara karşı hakaret içeren ve yanlış bilgilerin verildiği internet sayfaları oluşturulmaktadır. Bunun yanında e-posta, forum ya da sohbet programları aracılığıyla bu suçun işlenmesi mümkün olmaktadır (Ergün, 2008).

1.3.3.3.7.İstem dışı elektronik posta (Spam)

Spam, istenmeyen toplu mesajlara verilen addır. Çeşitli tipte dolandırıcılık olmakla birlikte en yaygın olanı spam e-postalar aracılığıyla yapılanlardır. Suçlular genellikle ürün ve hizmetleri tanıtan spam reklam e-postalarına kötücül yazılım eklemektedir.

1.3.3.4.Telif hakları ile ilgili suçlar

İnternetin önemli işlevlerinden biri bilginin yayılmasıdır. Şirketler ürünleri ve hizmetleri hakkında bilgi dağıtmak için İnterneti araç olarak kullanmaktadır. Başarılı şirketlerin marka imajı ve kurumsal tasarımı korsanlar tarafından kullanılarak taklit ürünlerin pazarlanması yapılabilmektedir.

İnternet üzerinden doğrudan ürünlerinin dağıtımını yapan şirketler de ürünlerinin kopyalanıp dağıtılıp indirilmesi sonucunda telif hakkı ihlalleri ile ilgili yasal sorunlarla karşı karşıya kalmaktadırlar.

1.3.4.McConnell siber suç sınıflandırması

Uluslararası platformda genel kabul gören McConnell International adlı ABD menşeli küresel politika ve teknoloji yönetimi danışmanlık firması tarafından yapılan sınıflandırmaya göre siber suçlar veri suçları, ağ suçları, erişim suçları ve ilgili suçlar şeklinde dört başlık altında incelenmiştir (McConnell-International, 2000).

1.3.4.1.Veri suçları

Bu başlık altında incelenecek suçların objesi, ham bilginin bilişim teknolojileri alanında kullanılabilecek şekilde işlenmesi sonucu ortaya çıkan veridir. Bilişim teknolojilerinin veri iletimi eksenli işleyişi, öncelikle maddi ceza hukuku normları ile verilere karşı gerçekleştirecek hukuka aykırı fiilleri müeyyide altına almayı gerekli kılmıştır. Verilere karşı gerçekleştirilecek ihlaller şu alt gruplar altında incelenmektedir.

1.3.4.1.1.Verilere müdahale edilmesi (Data Interception)

Bu suçun oluşumu için verilerin, aktarım esnasında üçüncü kişiler tarafından hukuka aykırı müdahaleye maruz kalması gerekmektedir. Bu müdahale verilerin aktarımının engellenmesi, aktarım rotalarının değiştirilmesi, üçüncü kişiler tarafından verilerin aktarım sırasında ele geçirilmesi şeklinde ortaya çıkabilir.

1.3.4.1.2.Verilerin değiştirilmesi (Data Modification)

Verilerin değiştirilmesi, tahrip edilmesi veya silinmesi eylemleri cezai müeyyide altına alınmaktadır. Bu başlık altında incelenen eylemler yukarıda belirtilen verilere müdahale edilmesi suçundan, işlendiği ortamda bir sınırlama olmaması açısından kesin bir çizgiyle ayrılmaktadır. Aktarım sırasında verilere müdahale edilerek bu veriler değiştirilebilir veya tahrip edilebilir veya silinebilirler.

1.3.4.1.3.Veri hırsızlığı (Data Theft)

Veri hırsızlığı başlığında verilerin ele geçirilmesi ve kopyalanması eylemleri cezalandırılmaktadır. Verilerin, verinin sahibine veya başkalarına zarar vermek veya failin kendisine veya başkalarına haksız kazanç sağlamak amacıyla bulunduğu yerden alınması ve kopyalanması veri hırsızlığı suçunun oluşumu için yeterli unsurları oluşturmaktadır.

1.3.4.2.Ağ suçları

İkinci suç grubu ağ suçlarıdır. Yukarıda açıklanan verilerin bir yerden bir yere iletilmesini sağlayan ağ sistemleri, bu suçun objesini oluşturmaktadır. Ağ suçları da iki ana başlık altında incelenmektedir.

1.3.4.2.1.Ağ engellemesi (Network Interference)

Bu suç grubunda ağın tamamına veya bir bölümüne diğer kişilerin erişiminin engellenmesi veya önlenmesi durumu ortaya çıkmaktadır. Bu suç çok değişik modus operandi'ler (suçun işleniş şekli) kullanılarak gerçekleştirilebilir. En çok görülen şekli web siteleri ve İSS üzerine yağdırılan DDOS (distributed denial of service) saldırılarıdır. DDOS saldırıları, failin verdiği komutlara uyması için "hack" edilerek "zombi" haline getirilen birçok bilgisayardan hedef olarak seçilmiş siteye, bilgisayara veya sisteme sürekli veri gönderilmesi ile hedef siteye, bilgisayara veya sisteme diğer kişilerin erişiminin engellenmesi ya da önlenmesi durumudur.

Ağ engellemesi sistemin gayri fiziki bileşenlerine yönelmiş eylemleri gruplandırmaktadır. "Hacking", "cracking", DDOS suçun farklı formlarda işleniş şeklini belirten birer modus operandi'dir. Bu konuda Kıta Avrupası Hukuk Sistemine mensup olan ülkeler arasında anılan suçun işleniş şekillerini müstakil bir kanunla suç olarak yaratan ülkeler de vardır. Örneğin Kasım 2000 tarihinde Belçika Parlamentosu tarafından kabul edilen ve 13 Şubat 2001 tarihinde yürürlülüğe giren Yeni Belçika Ceza Kanununun 4. Babının Başlığı "Computer Hacking" olarak belirlenmiştir. Bu başlık altında yer alan maddelerde "hack" etme suçunun hangi fiillerden meydana geldiği açıklanmaya çalışılmıştır.

1.3.4.2.2.Ağ sabotajı (Network Sabotage)

Ağ sabotajı, ağın veya sistemin tahrip edilmesi yahut değişikliğe uğratılması sonucu ortaya çıkmaktadır. Burada daha çok sistemin fiziki bileşenlerine yönelmiş eylemler vardır.

1.3.4.3.Erişim suçları

Yukarıdaki veri ve ağ suçlarında, suçun objesi olan veri ve ağ belirlenerek bir ayrıma gidilmiştir. Burada ise suçun hareket unsuru ön plana çıkartılarak bir grup

oluşturulma yolu izlenmiştir. Buna göre erişim suçları olarak belirlenen suçlar şu şekilde gruplanabilir:

1.3.4.3.1.Yetkisiz erişim (Unauthorized Access)

Bir sistem içersindeki bilgilere yetkili kişilerin ulaşması esastır. Yetkili kişiler dışında yer alan kişilerin, sistem içersindeki bilgilere ulaşmaya ve bunları 3. kişilerle paylaşmaya yetkili kılınmış kişilerin izni dışında erişim sağlaması birçok ülke mevzuatında suç olarak düzenlenmektedir.

1.3.4.3.2.Virüs yayımı (Virus Dissemination)

Virüs yayımı olarak belirlenen hareket, bilişim ve iletişim sistemlerinin donanımsal veya yazılımsal bileşenlerine zarar vermek amacıyla gerçekleştirilen bir tür suçun işleniş şeklidir. Virüs yayımı, küresel ölçekte büyük zararlara yol açması sebebiyle birçok ülkenin kanununda bu konuyla ilgili ayrı bir başlık altında düzenlemeye gidilmiştir.

1.3.4.4.İlgili suçlar

Bu başlık altında öncelikle düzenlenen husus bilişim teknolojileri alanında işlenen suçlarda iştirak ile yardım ve yataklık etmenin cezalandırılmasıdır. Son olarak bu başlık altında bilişim teknolojilerinin kullanılması yoluyla gerçekleştirilen dolandırıcılık ve sahtekârlık suçlarından bahsedilecektir. Dolandırıcılık ve sahtecilik fiilleri gerek karşılaştırmalı hukukta gerekse ülkemiz mevzuatında suç olarak tanımlanmıştır. Burada düzenlemesi gereken hususlar bilişim teknolojilerinin bu suçların işlenmesinde araç olarak kullanılması ve bu ortamın kendisine has özelliği nedeniyle, yalnızca bu alanda gerçekleştirilen faaliyetler üzerinde, dolandırıcılık ve sahtecilik fiillerinin cezai müeyyide altına alınmasıdır.

1.4.Siber Suçların İşleniş Şekilleri

Siber suçları, diğer suçlardan yani geleneksel anlamdaki suçlardan ayıran en önemli özellikler bu suçların işleniş şekillerinin farklılığı ve tespit edilmelerinin zorluğudur (Dülger, 2004). Siber suçların işlenmesine vasıta olan maddi hareket çok farklı şekillerde ortaya çıkabilir. Söz konusu suçlar, yepyeni ve çok farklı yollarla işlenebilir. İşin içine bilgisayar ve internet girdiğinde bir suç hem çok hızlı ve kolay bir şekilde işlenebilmekte hem de suçun tespit edilmesi zorlaşmaktadır. Yine suç tespit edilse bile suçun failinin yakalanması için zorlu bir uğraş verilmesi gerekmekte, suçluların BİT imkânlarını kullanarak kolaylıkla delilleri karartabilme veya kimliklerini gizleme imkânı olması nedeniyle failin her zaman yakalanması mümkün olamamaktadır (Değirmenci, 2002)

Yukarıda belirtilen nedenlerden ötürü, siber suçların meydana gelmesine sebep olan modus operandilerin tanımlanmasında ve tespit edilmesinde yarar görülmektedir. Bu tanımlama ve tespit işlemi sınırlayıcı değil, örnekleyicidir. Çünkü internet gibi bilgisayar ağlarında her geçen gün kendini yenileyen bu teknolojik gelişme karşısında kesin bir belirlemeye gitmek büyük bir hata olacak ve bu suçlarla mücadelede geri düşülmesine sebep olunacaktır (Yazıcıoğlu, 1997). Bu nedenle her yeni olay yeni bir modus operandi ortaya çıkarabildiğinden aşağıda incelenecek teknikler sadece şu ana kadar görülmüş modus operandilerdir.

1.4.1.Yemleme (Phishing)

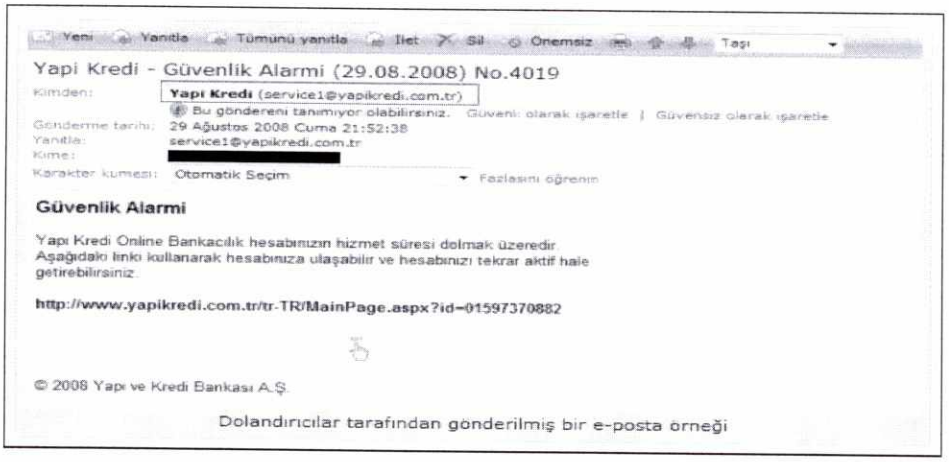
Yemleme; BİT imkânlarını kullanmak suretiyle, hedef alınan kişilerin aldatılarak veya ikna edilerek kişisel ve/veya gizli verilerinin ele geçirilmesi ve söz konusu verilerin kötü niyetle kullanılmasıdır. Bu yönüyle yemleme, bir tür "sosyal mühendislik" saldırısı olarak da nitelendirilmektedir (Ünver ve Mirzaoğlu, 2011). İngilizce "Password (şifre)" kelimesinin baş harfi olan "P" ile "Fishing (Balık tutma)" anlamına gelen sözcüğün birleştirilmesiyle türetilen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenerek oluşturulmuştur.

Yemleme saldırılarında kullanılan iki temel yöntem; aldatma yoluyla yemleme ve teknik yoldan yemlemedir. Aldatma yoluyla yemlemede hedef alınan kişileri aldatmak suretiyle sahte internet sitesine veya telefon numarasına yönlendirme veya kullandıkları sistemlere kötücül yazılım bulaştırma, nihayetinde ise kişisel verilerini ele geçirme ve çıkar amaçlı kullanma vardır. Teknik yoldan yemleme ise çeşitli teknik hileler uygulayarak, hedef alınan kişilerin kullandıkları sistemlerde veya bağlandıkları internet sitelerinde ayar değişiklikleri yaparak kişisel verilerini ele geçirme ve çıkar amaçlı kullanmadır (Ünver ve Mirzaoğlu, 2011).

Yemleme yöntemi ile banka hesap numaraları, kredi kartı numaraları gibi kişisel bilgiler, banka gibi resmi bir kurumdan gönderilen resmi bir mesaj gibi gözüken e-postalarla bireylerden elde edilmektedir. Sosyal mühendisliğin bir uygulama alanı olan bu tür sahte e-postaları alan bireyler, istenilen gizli bilgileri göndererek, bu bilgilerin kötü niyetli üçüncü şahısların eline geçmesine ve akabinde oluşabilecek zararlara maruz kalınmasına neden olmaktadır (Sağıroğlu ve Canbek, 2007).

İnternet kullanıcısının müşterisi olduğu bankanın, e-posta veya bunun gibi bilgi girmeyi gerektiren bir kuruluşun İnternet sayfasının bir kopyasının yapılarak söz konusu kullanıcının hesap bilgilerinin çalınması sık görülen yemleme yöntemlerinden biridir. Sahtekârlığı gerçekleştirecek kişi/kişiler; bir banka, kart şirketi veya bir finans şirketinden geliyormuş gibi hazırladığı sahte e-postayı, elde edebildiği tüm e-posta adreslerine gönderir (Turhan, 2010). Şekil 1.1.'deki e-postanın geldiği adrese bakıldığında, bankanın kendi e-posta alanından geliyormuş gibi görünmektedir. Bu durum birçok kullanıcının e-postanın gerçekten banka tarafından gönderildiğini düşünmesine sebep olmaktadır. Bu postayı atan kişiler muhtemelen kendi müdahale imkânlarının olduğu bir DNS kullanmakta ve böylece e-posta adreslerini bankanın adres alanındanmış gibi gösterebilmektedir. E-postanın içeriğinde ise müşterinin internet bankacılık hesabının süresinin dolmak üzere olduğu ve postaya eklenmiş bir link yardımıyla hesabın tekrardan aktif hale getirilebileceği belirtilmektedir (Pclabs, 2009).

Şekil 1.1 Örnek bir yemleme e-postası



Kaynak: Pclabs, 2009

E-postaya eklenen bağlantı adresinin üzerine gelindiğinde linkte görünen adres ile tarayıcının sağ alt köşesinde görünen linkin kullanılması durumunda yönlendirilen adres Şekil 1.2'de görüldüğü üzere tamamen farklıdır.

Şekil 1.2 Örnek bir yemleme e-postasının yönlendirdiği adres

```
Return-Path: <nobody@srv1.lwhsrv1.com.br>
Received: from srv1.lwhsrv1.com.br (srv1.lwhsrv1.com.br [75.126.72.113])
        by mx.google.com with ESMTP id 24si2220103wrl.2007.03.20.18.43.
        Tue, 20 Mar 2007 18:43:28 -0700 (PDT)
Received-SPF: pass (google.com: best guess record for domain of nobody@
Received: from nobody by srv1.lwhsrv1.com.br with local (Exim 4.63)
        (envelope-from <nobody@srv1.lwhsrv1.com.br>)
        id 1HTprM-0000xr-85
        for ekarademir@gmail.com; Tue, 20 Mar 2007 22:43:28 -0300
```

Kaynak: Pclabs, 2009

Yemleme metodu dünyada gün geçtikçe yaygınlaşmakta olan bir metottur. Bunun nedeni ise bu metotla çok az maliyet karşılığında yüksek miktarlarda kolay ve haksız para kazanma ihtimalinin olmasıdır (Turhan, 2010). İnternet kullanıcılarının daha spesifik sosyal ağlara veya çevrimiçi kaynaklara yönelmesi dolandırıcıların daha da dikkatini çekmektedir. Bu nedenle PayPal, Amazon, Yandex, MasterCard, Facebook

ve MySpace gibi popüler siteler 2010'un en çok saldırıya uğrayan sosyal ağları arasında yer almıştır (Turk.internet.com, 2011).

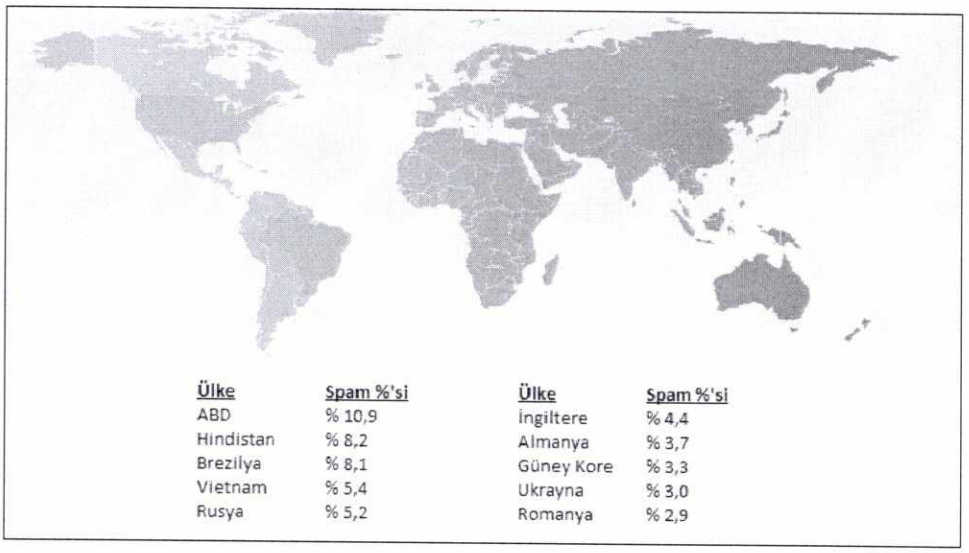
1.4.2.İstem dışı elektronik postalar (Spam)

Spam, Amerikan kökenli bir kelime olup, bir Amerikan firmasının baharatlı domuz eti ve jambon için kullandığı "Spiced Pork And Ham" kelimelerinin baş harflerinin alınması ile oluşturulmuştur (Memiş, 2005). Spam genellikle pazarlama, reklâm veya sosyal içerikli olarak büyük kitlelere ulaştırılmak istenen mesajların kullanıcının isteği dışında kendisine İnternet ya da cep telefonu gibi teknolojiler aracılığı ile yollanmasına dayanmaktadır (İnternet Üst Kurulu, 2005).

Spam ilk başlarda sadece rahatsızlık verici bir durum olarak algılanırken, gün geçtikçe gerek bireyler, gerekse işletmeler için ciddi bir siber güvenlik problemi olarak görülmeye başlanmıştır. Spam bilgisayar yoluyla dolandırıcılık amacıyla araç olarak kullanılabileceği gibi, kötücül yazılım türlerinin yayılmasında ve bilgisayar kullanıcılarının yemleme vb. yollarla kendileri hakkında kötü sonuçlar doğurabilecek önemli bilgilerin verilmesinde de kullanılabilmektedir (OECD, 2006).

Sophos tarafından yapılan bir araştırmaya göre, günümüzde ticari e-posta'ların %97'si istem dışı elektronik postadır (Sophos, 2009). Ayrıca söz konusu tehdit teknolojinin gelişmesiyle birlikte cep telefonları ve anlık mesajlaşma hizmetleri gibi teknolojilere de yayılmaktadır (OECD, 2006). Şekil 1.3'de 2010 yılında dünyada en fazla spam yayan ülkeler görülmektedir. Buna göre ilk üç sırayı ABD, Hindistan ve Brezilya almaktadır (IBM, 2011). IBM tarafından 2009 yılında yayımlanan raporda ise Türkiye %7,8 ile en çok spam yayan ülkeler arasında Rusya ve ABD'den sonra üçüncü sırada yer almaktaydı (IBM, 2009).

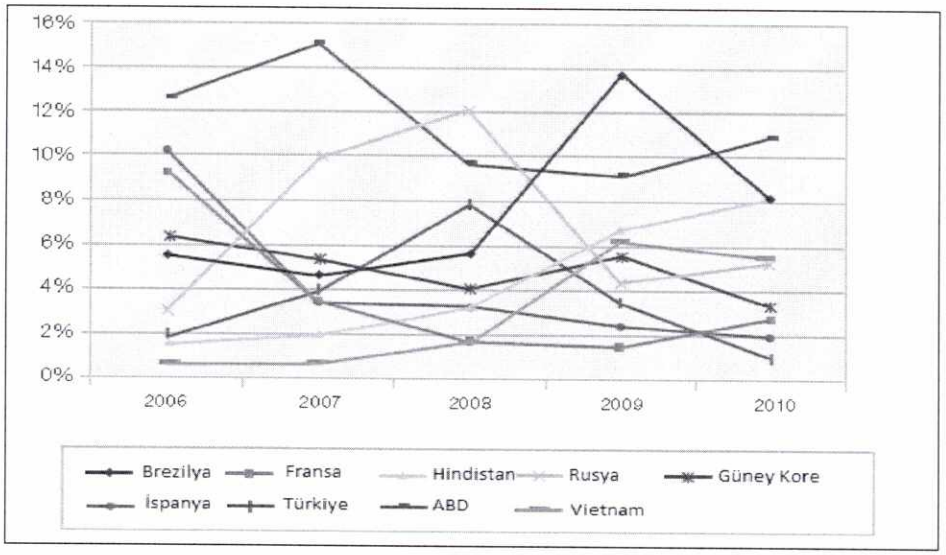
Şekil 1.3 En fazla spam yayan ülkeler



Kaynak: IBM, 2011

IBM tarafından 2011'de yayımlanan İnternet Güvenlik Sistemleri X-Force Tehditler Raporuna göre, Şekil 1.4'de de görüldüğü gibi son beş yıla bakıldığında ülkelerin spam gönderme oranlarındaki bazı uzun dönem eğilimleri görünür hale gelmektedir. Buna göre; Türkiye'nin 2006'dan 2008 yılına kadar olan spam gönderme oranındaki artış bu yıldan sonraki iki yıllık sürede azalma eğilimi göstermiş olup, Türkiye'de 2009 yılında gerçekleştirilen Spam ile Mücadele Projesi sayesinde 2010 yılında 2006'daki %2 oranının da altına düşmüştür. Hindistan sürekli artış gösteren tek ülkedir. İki yıllık belirgin artıştan sonra Brezilya ve Vietnam ilk defa azalma göstermiştir. İki yıl aradan sonra ABD 2010'nun en yüksek spam gönderme oranına sahip olan ülkedir. İspanya ve Fransa 2007 yılındaki, Rusya ise 2009'daki baskın rolünü kaybetmiştir. Güney Kore ilk defa %4'ün altına düşmüştür (IBM, 2011).

Şekil 1.4 Yıllara göre spam gönderilme oranları



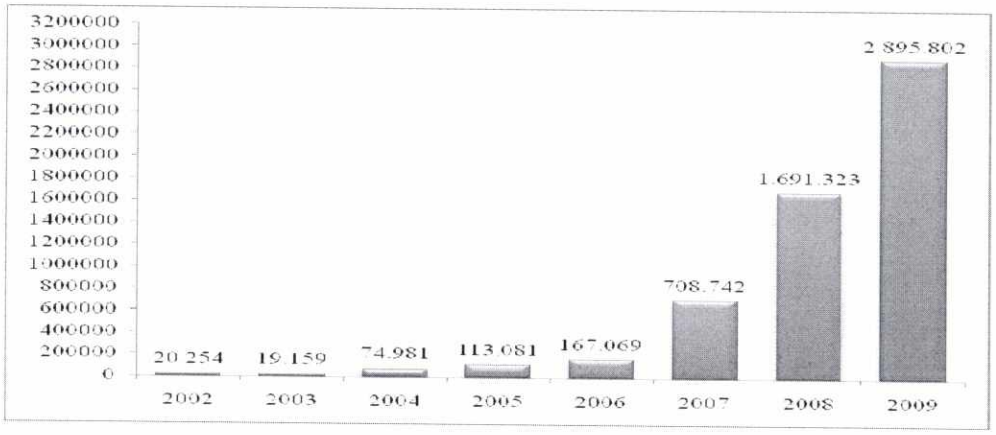
Kaynak: IBM, 2011

1.4.3. Kötücül yazılımlar

Kötücül yazılım; sahibinin bilgisi dışında bilgisayarlara sızmak ya da zarar vermek amacıyla tasarlanmış yazılımların ortak adıdır ve bir bilişim sistemine söz konusu sisteme zarar vermek amacıyla veya kullanıcılarının amaçları dışında kullanılmak üzere yerleştirilir (OECD, 2009). Her geçen gün artan ve çeşitlenen kötücül yazılımların 2002–2009 yılları arasındaki artışı Şekil 1.5'te gösterilmektedir.

Kötücül yazılımın sisteme bulaşmasının çeşitli yolları vardır. Hedef bilgisayardaki açıklıklardan yararlanan bu yöntemlerin etkinliği bilgisiz kullanıcıların varlığıyla artmaktadır. Kötücül yazılımlar; % 65 web tarayıcılarının, % 13 e-posta eklerinin, % 11 işletim sistemlerinin, % 9 indirilen dosyaların ve % 2 diğer yöntemlerin kullanımı ile sistemlere bulaşmaktadır (Barroso, 2007 ve Ünver vd.,2010).

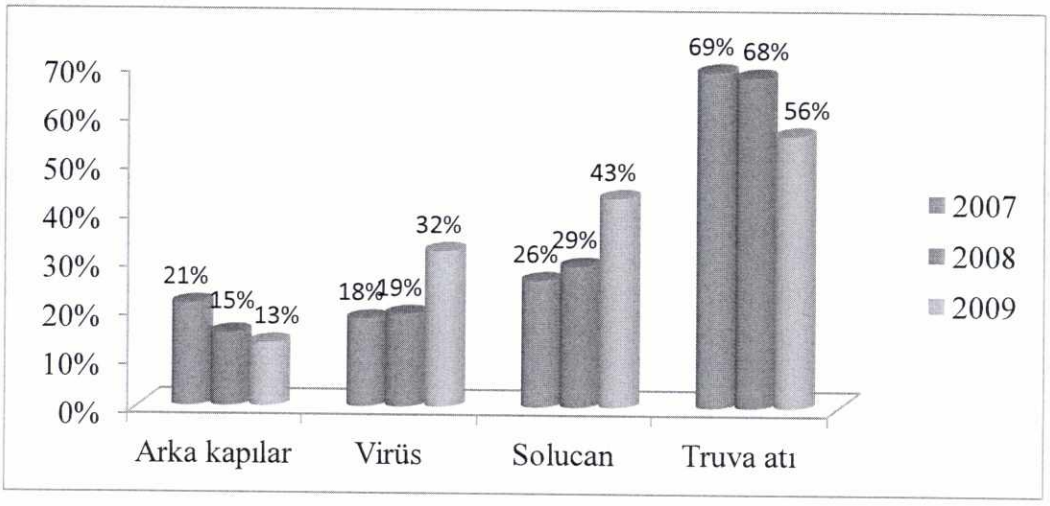
Şekil 1.5 Kötücül yazılımlardaki artış



Kaynak: Symantec, 2011

2009 ve 2011 yılında Symantec tarafından yayımlanan İnternet Güvenlik Tehdit Raporlarına göre, en sık görülen kötücül yazılım türleri truva atları (trojan), solucanlar (worm), virüsler ve arka kapılar (backdoor) dır. Şekil 1.6'da bu yazılım türlerinin 2007-2009 yılları arasındaki yüzdelik dağılımı görülmektedir. Virüs ve solucanların oranı geçen yıllarla artış gösterirken, truva atı ve arka kapıların oranlarında azalma olmuştur.

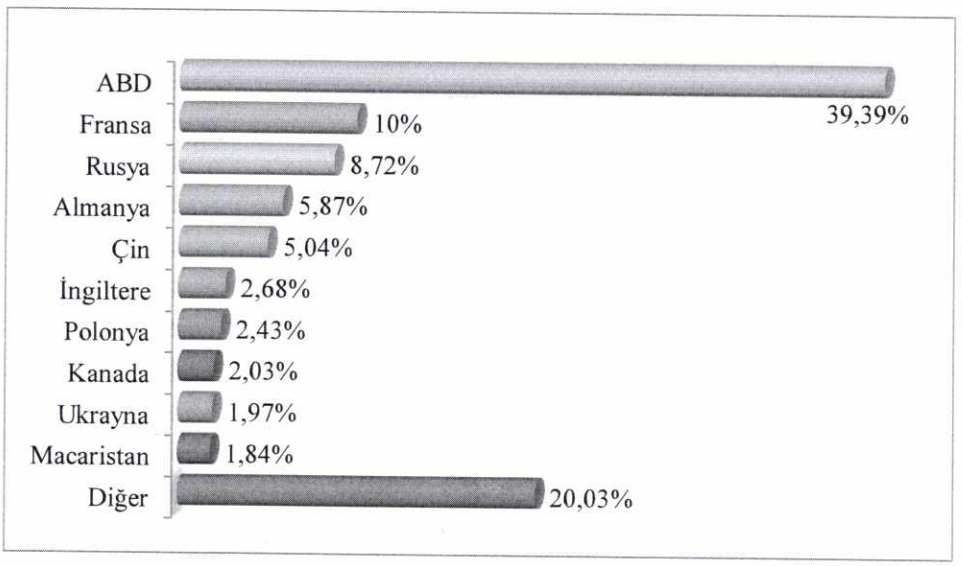
Şekil 1.6 Kötücül yazılım türleri



Kaynak: Symantec, 2009 ve 2011

Ülkemiz Sophos'un 2009 yılı verilerine göre en fazla kötücül yazılım barındıran ülkeler arasında %2,5' lik pay ile dünya sıralamasında 7 nci sırada iken, 2011 verilerine göre (Şekil 1.7) kötücül yazılım barındıran ilk on ülke arasında bulunmamaktadır (Sophos, 2009 ve 2011). Bu durum ülkemizde kötücül yazılımlara karşı alınan güvenlik tedbirlerinin ve halkın farkındalığının arttığının göstergesidir.

Şekil 1.7 2010 yılında kötücül yazılım barındıran ülkeler



Kaynak: Sophos, 2011

1.4.3.1.Truva atı

Truva atı; yararlı gibi görünen fakat arkasında gizli bir kodun da yer alması nedeniyle bilişim güvenliğine zarar veren bir programdır. Yunan mitolojisinde bir armağan gibi görünüp, aslında Truva kentini ele geçirme hedefi olan Yunanlı askerleri taşıyan tahta bir ata verilen isim olan truva atları diğer kötücül yazılımlar olan bilgisayar virüsleri ve bilgisayar solucanları gibi kendi başlarına işlem yapamazlar. Aynen Yunanlıların planlarının işleyebilmesi için atın Truvalılar tarafından içeri alınması gerektiği gibi Truva atlarının zararlılığı da kullanıcının hareketlerine bağlıdır. Truva atları kendilerini kopyalayıp dağıtsalar bile her kurbanın programı (Truvayı) çalıştırması gerekir (Dülger, 2004).

Truva atları bilgisayarları uzaktan yönetmek için arka kapı açan programlardır. Lisanslı programların yasa dışı kopyalarının veya aktivasyon kodlarının dağıtıldığı "warez" olarak adlandırılan siteleri veya bedava mp3, oyun veya porno içerik dağıtan siteleri ziyaret eden kullanıcılar, farkında olmadan yukarıda belirtilen programları bilgisayarlarına indirirken, aynı zamanda kötü niyetli programları da indirmiş olurlar. Bilgisayara kurulan bu programlar arka plandan çalışarak, kullanıcının sistemine uzaktan erişim imkânı sağlar. Truva atlarıyla sisteme arka kapıdan (backdoor) ulaşan bilgisayar korsanları, bilgisayarın sistem yapılanmasını değiştirebilir, kullanıcının şifrelerine ve diğer kişisel bilgilerine ulaşma imkânına sahip olabilirler. Yani truva atı sisteme bulaştıktan sonra, sistemin açılmasıyla beraber kendisini belleğe yükler ve sistem ağlarının açıklarını kullanarak, programı yerleştiren taraf olan bilgisayar korsanının isteklerini yerine getirir (Değirmenci, 2002).

Güvenlik yazılımları üreten bir şirket olan Kaspersky Lab verilerine göre 2009 yılından bu yana kötücül yazılım programlarının, kullanıcıların özel bilgilerini çalma oranı %100'den fazla bir artış göstermiştir. Kaspersky Lab veri tabanına ulaşan Truva atı sayısının 2010'da 25,000'i geçtiği ve bu sayının 2006'ya oranla 5 kat daha fazla olduğu bildirilmiştir (Turk.internet.com, 2011).

1.4.3.2.Arka kapılar (Backdoors)

Bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde, normal kimlik doğrulama süreçlerini atlamayı veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler arka kapı olarak adlandırılmaktadır. Bir sisteme sızmak için oldukça zahmetli bir çaba harcayan bilgisayar korsanları, daha sonra aynı sisteme erişmek için daha kolay bir yolu sisteme eklemek isterler (Turhan, 2010).

En sık karşılaşılan arka kapı yöntemi, hedef sistemde dinleme ajanı iliştirilmiş bir kapıyı (port) açık tutmaktır. Arka kapılar kimi zaman, sistemi geliştiren programcı tarafından test edilen sisteme erişmek amacıyla kullanılan fakat daha sonra unutulan açıklar olarak karşımıza çıkmaktadır. Bu durumun bir şekilde farkına varan kötü

niyetli kişiler, bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir. Arka kapılar çoğunlukla Truva atları ile karıştırılabilmektedirler. Her ikisi de hedef sisteme sızmaya yarayan kötü amaçlı yazılımlardan; truva atları faydalı bir program gibi gözükürken; arka kapılar sadece sisteme erişimi sağlayan gizli yapılardır (Sağıroğlu ve Canbek, 2007).

1.4.3.3.Solucanlar (Worms)

Solucan; bilgisayar ağları arasında herhangi bir donanıma veya yazılıma zarar verme zorunluluğu olmadan dolaşan, kullanıcı müdahalesine gerek kalmadan kendi kendini aktif hale getirebilen ve bir kopyasını ağa bağlı olan diğer bilgisayarlara bulaştırabilen programdır (Nickolov, 2008). Solucanlar genellikle virüslerle karıştırılmaktadır ancak solucanlar, virüsler gibi sisteme zarar verme zorunluluğu olmaksızın da sistemin içinde hareket edebilmektedirler (OECD, 2009).

Solucanları yaymak için hedef sistemdeki korunmasızlıklardan faydalanmak veya sosyal mühendislik gibi yöntemler kullanılmaktadır. Solucanlar başka dosyaları değiştirmez fakat etkin bir şekilde bellekte durur ve kendilerini kopyalarlar. Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında, diğer işlemekte olan görevleri yavaşlattığında veya bu görevlerin sonlanmalarına neden olduğunda farkına varılabilir (Sağıroğlu ve Canbek, 2007).

İlk bilinen solucan, 1988 yılında ortaya çıkan Morris solucanıdır ve dünya üzerinde yaklaşık altı bin bilgisayarı etkilemiştir. Daha sonra NIMDA, The Code Red, Mi2g gibi solucanlar dünya çapında milyarlarca dolar değerinde zarara yol açmışlardır (Nickolov, 2008).

1.4.3.4.Virüsler

Virüsler; bilgisayar belleğine yerleşen, çalıştırılabilen programlara kendini ekleyebilen, yerleştiği programların yapısını değiştirebilen ve kendi kendini çoğaltabilen programlardır (Nickolov, 2008).

Virüsler en tehlikeli ve en eski kötücül yazılım olarak kabul edilmektedirler. Organizmalardaki hücrelere bulaşan küçük parçacıklar olarak tanımlanan biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri, kendi kopyalarını çalıştırılabilir diğer kodlara veya belgelere yerleştirilerek yayılan ve kendi kendine çoğalan programlardır. Ekranda rahatsız edici, çalışmaya kısa süreliğine de olsa mani olan mesajlar göstermek gibi zararsız sayılabilecek türlerinin de bulunmasına karşın, çoğu virüs programlarının, önemli dosyaları silmek veya ev sahibi (host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri bulunmaktadır. Virüsler bir dosyanın açılması, bir e-postanın okunması veya virüs bulaşmış bir programın çalıştırılması gibi yöntemlerle yayılırlar (Sağıroğlu ve Canbek, 2007).

Virüslerin yol açtığı zararlar küçük gibi gözükse de toplamda çok büyük zararlara yol açabilmektedirler. Nitekim 3 Mayıs 2000 günü tüm dünyada yayılan ve e-postaya ekli olarak gelen "I Love You" olarak bilinen bir virüs, çok kısa zamanda 55 milyon bilgisayara ulaşmış ve bunlardan 2,5-3 milyonuna bulaşarak 8,8 milyar dolar zarara sebebiyet vermiştir (Zetter, 2000).

1.4.3.5.Casus yazılımlar ve reklam destekli yazılımlar

Casus yazılımlar; kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılımlardır (OECD, 2009).

Casus yazılımlar virüs ve solucanlardan farklı olarak, sistemlere bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Casus yazılımların amacı, kurban olarak seçilen sistem üzerinde gizli kalarak istenen bilgileri toplamaktır. Bunun dışında şirketler, İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları İnternet üzerinde yayabilmektedirler. Kullanıcıların haberi olmadan sistemlere bulaşabilen casus yazılımlar, kişisel gizliliğe karşı gerçekleştirilen en önemli saldırılardan biridir (Sağıroğlu ve Canbek, 2007).

Reklam destekli yazılımlar ise, yüklenildiği bilgisayara yüklenme işleminden sonra program kullanımdayken otomatik olarak çalışan, reklam gösteren ve indirme yapan yazılımlardır. Amaçları, bilgisayar kullanıcılarına reklâmları göstermektir. Casus yazılımlar gibi, üzerinde bulundukları sistemdeki kişisel veya istatistiksel verileri sahibinin bilgisi ya da izni olmadan üçünü kişilere göndermek suretiyle kişisel verilerin elde edilmesi amacıyla kullanılmaktadırlar (SpamLaws, 2009).

1.4.3.6.Köle bilgisayar ağları (Botnet)

Botnet; "robot" kelimesinin ikinci hecesi ile "network" kelimesinin ilk hecesinin birleştirilmesinden oluşmuş bir kelimedir ve merkezi bir kontrol noktasına bağlanmış tehlikeli bilgisayar ya da diğer adıyla köle (zombi) bilgisayar yığınını ifade etmektedir (OECD, 2009). Köle bilgisayar ağı ile virüs ya da diğer kötücül yazılımların bulaştırılması suretiyle birçok bilgisayar, sahiplerinin izni ve haberi olmaksızın uzaktan ve tek bir noktadan kötü amaçlar doğrultusunda yönetilmekte ve kontrol edilmektedir. Dolayısıyla aynı anda binlerce bilgisayar, bir ağ sistemi ile gizlice yönetilmiş olmaktadır. Bu ağ sistemini yönetmek için özel olarak tasarlanan kötü niyetli programlara ise "bot" adı verilmektedir (ITU, 2008). Bir köle bilgisayar ağı sahibi saldırgan, ağındaki tüm bilgisayarları dünyanın herhangi bir yerinden kolay bir şekilde yönetebilmekte, köle bilgisayar ağındaki masum kullanıcılar da haberleri bile olmadan saldırganların siber suçlarına büyük destek oluşturmaktadırlar.

Köle bilgisayar ağlarının asıl hedefi ev kullanıcılarıdır ve dünya üzerindeki ev bilgisayarlarının %10'luk bir kısmının köle bilgisayar ağlarının bir parçası olduğu bilinmektedir. Nitekim arama motoru Google tarafından, 100 milyondan fazla bilgisayarın köle bilgisayar ağlarında olduğu belirtilmiştir. Birleşmiş Milletler, 2008 yılının başında köle bilgisayar ağı saldırısına uğramıştır. BM resmi internet sitesini ele geçiren bilgisayar korsanları, kurumun sitesine "Hey İsrail ve ABD, çocukları ve diğer insanları öldürmeyin. Barış evrenseldir. Savaşa hayır" mesajını bırakmıştır (Zaman, 2008).

1.4.4.Hizmetin engellenmesi saldırıları (DoS/DDoS)

Hizmetin engellenmesi saldırıları kurumların veya şirketlerin bilgi ve iletişim sistemlerini ve hizmetlerini devre dışı bırakmak için yapılan saldırılardır ve saldırıya uğrayan sistemlerin aşırı şekilde yüklenmesi ile oluşmaktadır. Bilgisayar korsanları bilgisayar kullanıcılarına bir program yüklemekte ve belirlenen günde bütün bilgisayarlar aynı anda, önceden belirlenmiş bir İnternet sitesine giriş talebi göndermeye başlamaktadır. Bu tür talep sayısı on binleri bulduğunda karşı tarafın sunucusu yanıt veremez duruma gelmekte; sonuçta İnternet sitesi çökmekte, işlem yapamaz hale gelmekte ve site sahipleri maddi zarara uğramaktadır (OECD, 2009).

14 Aralık 2007 tarihinde Kırgız Merkez Seçim Komisyonu İnternet sitesi seçim süresince saldırıya uğramış ve "Bu site Estonya Rüyası Örgütü tarafından saldırıya uğratılmıştır" mesajı bırakılmıştır. Seçim kampanyası süresince ve seçimden önce meydana gelen ayaklanmalarda Kırgız internet servis sağlayıcılarına hizmetin engellenmesi saldırıları düzenlenmiştir. Ağustos 2009'da ise dünyaca ünlü paylaşım sitesi Twitter hizmetin engellenmesi saldırıları nedeniyle erişime kapatılmıştır (Cnetnews, 2009).

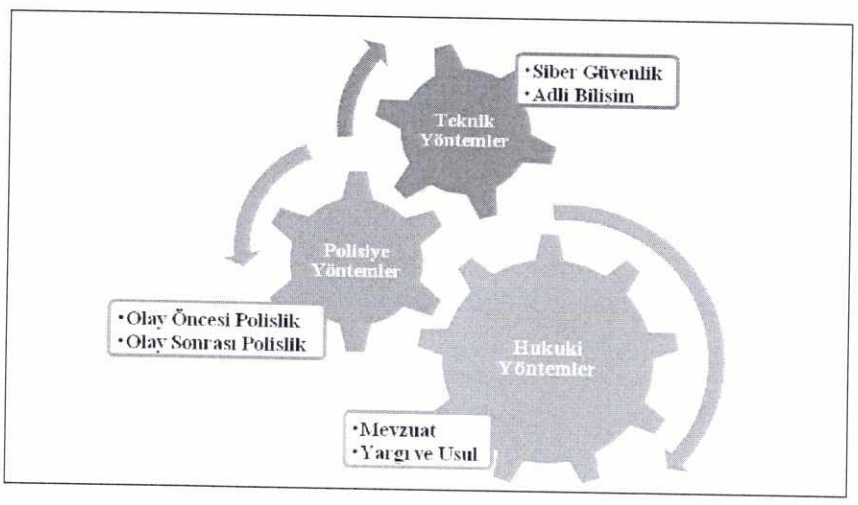
2.SİBER SUÇLARLA MÜCADELE YÖNTEMLERİ

Siber suçlarının çok ciddi bireysel ve toplumsal sonuçları olduğundan bu suçlarla yürütülecek mücadelenin de çok boyutlu olması gerekmektedir. Ancak ceza hukuku normlarıyla sağlanmaya çalışılan koruma, siber suçlarla mücadelenin yalnızca bir boyutudur (Dülger, 2005). Siber suçlarla mücadelenin diğer boyutları polisiye ve teknik yöntemleri içermektedir.

Siber ortamın doğası gereği suçun sınırlarla kayıtlı olmaması ve hemen her türden kullanıcının bilişim ağlarına dâhil olabilmesi nedeniyle siber suçlarla mücadele, oldukça güçtür. Siber suçlarla etkin bir mücadele yürütebilmek için; yasal mevzuatın hazırlanması, uluslararası uyum ve işbirliğinin sağlanması ve eğitimli uzman kişilerin yetiştirilmesinin yanı sıra, yeterli donanım ve teknik altyapı gerekmektedir (Şen, 2007).

Bu çalışma kapsamında siber suçlarla mücadelede kullanılan yöntemler; hukuki, teknik ve polisiye yöntemler olmak üzere üç grupta ele alınmıştır. Şekil 2.1'de de görüldüğü gibi tüm bu yöntemleri birer çark olarak kabul edersek her bir çark kendi içinde tutarlı olmak kaydı ile bir birine uyumlu bir şekilde işlediğinde siber suçlarla etkin biçimde mücadele edilmiş olacaktır.

Şekil 2.1. Siber suçlarla mücadele yöntemleri



2.1.Hukuki Yöntemler

Bu çalışma kapsamında siber suçlarla mücadelede hukuki olarak, ulusal ve uluslararası alanda hazırlanmış olan mevzuatlar, düzenlemeler ve tavsiye kararları incelenmiştir.

Siber suçlarla mücadelede hukuki yöntemler; mevzuat hazırlanması, usul hukuku ve yargılama olarak üç aşamada değerlendirilebilir. Mevzuat hazırlanmasında konu hakkında yapılmış öncül uluslararası düzenlemelere başvurulduğu gibi teknik yöntemlerden destek alınması gerekmektedir. Yargılama ve usul hukukunun işleyişi ise polisiye ve teknik yöntemlere yoğun olarak ihtiyaç duymaktadır. Hukuki yöntemler oldukça zaman gerektiren süreçlere tabi olmasına rağmen diğer yöntemlerin sağlıklı, etkin ve geçerli olabilmelerinde vazgeçilmez bir role sahiptir.

Siber suçlar, sınırları aşan yapısı nedeniyle hemen hemen bütün ülkeler tarafından hukuksal düzenleme konusu olmuştur. Bu düzenlemeler incelendiğinde büyük çoğunluğunda iletişim sistemi aracılığıyla dolandırıcılık, verilere zarar verme, sabotaj, verilerde sahtekârlık, sisteme yetkisiz girme, verilerin hukuka aykırı olarak ele geçirilmesi ve veri hırsızlığı gibi eylemlerin suç olarak düzenlendiği görülmektedir (Akbulut, 1999).

Günümüzde ülkeler, siber suçlar konusunda ya ceza hukuku ile ilgili mevcut kanunlardan ayrı olarak özel düzenlemeler ihdas etmekte, ya da mevcut hükümlerde değişiklikler yaparak mevzuatlarını geliştirmektedirler. Siber suçları özel düzenlemeye tabi tutan ülkeler ceza kanunlarında iki farklı yöntem izlemişlerdir. Birinci yöntem, siber suçları ceza kanunundan ayrı bir kanun çıkarmak suretiyle düzenleme altına alan yöntemdir. Özellikle Anglo-Sakson hukukuna tabi olan İngiltere, İrlanda ve ABD'de bu yöntem izlenmiştir. İkinci yöntem ise Kıta Avrupası ülkelerinde uygulanan yöntemdir ki, bu yöntemde siber suçlar ceza kanunları içerisinde ayrı bir fasılda düzenlenmektedirler. Bu yöntemi uygulayan ülkelere örnek olarak Fransa, Lüksemburg verilebilir. Ülkemiz de bu yöntemi kendi mevzuatında tatbik etmiştir (Yazıcıoğlu, 1997).

2.2.Polisiye Yöntemler

Bilişim sistemlerinin giderek hayatın içinde yer alması ve çalışmamızda sıkça vurgulandığı gibi, siber suçların yaygınlaşması kaçınılmaz olarak kolluk kuvvetlerini de bu alanda çalışma yapmaya yöneltmiştir.

Polis teşkilatları yasalarla kendilerine verilen yetkiler çerçevesinde kendilerine has yöntemlerle suç ve suçlularla mücadele etmektedirler. Genel olarak polisiye yöntemler; olay öncesi ve olay sonrası polislik olmak üzere iki kısımdır. Olay öncesi polislik kısmına bilgi alma ve tarama yapma faaliyetleri girer. Olay sonrası polislik de ise soruşturma ve analiz işlemleri yürütülür (Dokurer, 2005).

Olay öncesi polisiye yöntemler suçun işlenmesinin önlenmesini amaçlaması nedeni ile göreceli olarak olay sonrası polislikten daha değerlidir. Siber suçlarla mücadelede de önleyici polisiye tedbirler almak ve suçluları eylem hazırlığı içinde yakalayabilmek polis teşkilatları için çok önemlidir.

Polisin siber suçların işlenmesini önlemek için alacağı ve üçüncü kişileri de etkileyen yöntemler, "siber suçları kovuşturan birimlerin eğitilmesi", "siber terörizm olgusuna karşı alınan önlemler", "devletlerin siber alanı denetlemesi" ve "uluslararası işbirliği yapılması" şeklinde dört başlık altında toplanabilir.

Siber suçları kovuşturan birimlerin eğitilmesi kavramıyla özellikle polisin ve savcıların bu suçların niteliği ve delillerin elde edilmesi açısından acele ve etkin bir biçimde eğitilmesi kastedilmektedir. Özellikle polisler açısından, bu alanda "ya bir polisi alıp bilişim uzmanı yapacaksınız ya da bir bilişim uzmanını polis yapacaksınız" ifadesi kullanılmaktadır (Dülger, 2004 ve Yenidünya/Değirmenci 2003). Bu alanda polis açısından önemli gelişmelerin olduğu ve bunların somut ürünlerinin uygulamaya geçirildiği söylenebilirse de hakim, savcı ve avukatlar açısından aynı ifadeleri kullanmak mümkün görülmemekte olup, onların da benzer eğitimleri alması gerekmektedir (Dülger, 2004).

Siber terörizm, belirli bir siyasal ve sosyal amaca ulaşabilmek için bilişim sistemleri kullanılarak bireylere, mallara ve toplumsal yasayış düzenine zarar verilerek, toplumu ve yöneticileri yıldırma ve baskı altında tutma çalışmaları olarak tanımlanmaktadır (Özcan, 2004). Terör örgütlerinin siber terörizmle gerçekleştirebilecekleri ve toplum üzerinde çok büyük zararlara neden olabilecek, acil önlem alınması gereken eylemlerine örnek olarak; istenilen kentin bütün trafik ışıklarının durdurulması, telefon hatlarının felç edilmesi, elektriğin ve doğalgazın kapatılması, bilişim sistemlerinin işletim dışı bırakılması, ulaşım ve su sistemlerinin isleyişinin bozulması, bankacılık ve finans sektörünün çökertilmesi, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasının engellenmesi verilmektedir.

Özellikle 11 Eylül 2001'de ABD'nin New York kentinde bulunan ve ikiz kuleler olarak anılan Dünya Ticaret Merkezi'ni yıkan terörist saldırılar için gerekli örgütlenme, destek ve eğitim için internetin çok geniş ve denetlenemeyen olanaklar sunduğu belirtilmektedir (Tanyol, 2002). Bu eylemden ve ABD'li yetkililerin bu eylemin hazırlanması için teröristlerin internet üzerinden iletişime geçtiklerini açıklamasından sonra birçok ülkede siber terörizme karşı önlemler alınması yönünde çalışmalar başlatılmıştır. Ülkemizde ise, uzun yıllar terörizmle mücadele edilmiş ve edilmekte olmasına, bu konuda çok zarar görülmüş ve çok acıya katlanılmış olmasına rağmen ciddi bir tehdit olan siber terörizme ve gerçekleşebilecek terörist eylemlere karşı ceza hukuku açısından hiçbir düzenleme yapılmadığı görülmektedir (Dülger, 2004).

Siber suçlarla mücadelede polisin kullanabileceği etkin yöntemlerden birisi de siber alanın özellikle de internetin denetlenmesi ve bu alan üzerindeki iletişimin kontrol altında tutulmasıdır. Polis teşkilatı diğer suçlarla mücadelede olduğu gibi siber suçlarda da ihbar mekanizması ile çalışabildiği gibi kendi yaptığı tarama ve denetleme faaliyetleri ile de suçluları tespit edebilmektedir. Bu konuda Federal Alman Polis teşkilatı tarafından yürütülen bir proje bu çalışma kapsamında incelenmiştir.

Ancak siber alanın denetlenmesindeki temel sorunun; kişi mahremiyeti ve iletişim özgürlüğü gibi, demokratik toplumların olmazsa olmaz ilkelerinin zedelenmeden, bir denetim mekanizmasının kurulup kurulamayacağı olduğu ifade edilebilir. Bu konuda yaşanan ikilem; özgürlük alanı olarak tanımlanan özellikle internet aracılığıyla gerçekleştirilen siber suçlarla mücadelenin, bireyin evrensel temel hak ve özgürlüklerinin özüne dokunulmadan gerçekleştirilmesindeki güçlüktür. Ancak bu çekincelere rağmen halkın bilgisine açık, bağımsız yargıçların denetiminde olan bir kurumun temel halk ve özgürlükleri kısıtlamaksızın, belli başlı suçlara ve özellikle çocuk pornografisine ilişkin filtreleme yapması ve böylelikle olası suç ve suçluları belirlemesi seklinde bir yöntem geliştirilebilir (Dülger, 2004).

Polisiye yöntemler başlığı altında değinilecek olan son konu devletlerin siber suçlarla mücadelede uluslararası işbirliğine yönelmelerinin kaçınılmazlığıdır. Bu suç tipleri doğaları gereği ve genellikle görüldüğü üzere birçok ülke sınırlarını geçen veri iletim ağları üzerinde gerçekleştirilmektedir. Siber suçlarla mücadelede polisiye yöntemlerin başarılı olabilmesi, bu çalışmada yer verilen diğer yöntemler gibi uluslararası işbirliğinden geçmektedir. Hali hazırda INTERPOL bu görevi yürütmekte ve dünya polis teşkilatları arasında özel bir ağ kurmaktadır.

Siber suçlarla mücadelede olay sonrası polislik yapılan soruşturma ile suçluların tespit edilmesi için elde edilen delillerin adli bilişim teknikleri kullanılarak analiz edilmesidir. Adli bilişim, genelde polis teşkilatında olay sonrası polislik faaliyetleri içinde yer alsa da, sivil teşebbüsler tarafından da bu alanda bilirkişilik yapılabildiği ve adli makamlarca bu bilirkişilik kabul görebildiği için bu çalışma kapsamında teknik yöntemler başlığı altında incelenmiştir.

2.3.Teknik Yöntemler

Siber suçlarla mücadelede bu çalışma kapsamında incelenen teknik yöntemler; siber güvenlik ve adli bilişim süreçleridir.

Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü olarak tanımlanmaktadır. Kurum, kuruluş ve kullanıcıların varlıkları; bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, elektronik haberleşme sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır (Ünver vd., 2009).

Adli bilişim ise olay yerinden alınan elektronik bir delilin mahkemede sunulmasına kadar geçen süre içerisinde yapılan laboratuar çalışmalarını düzenler. Bu anlamda yapılan çalışmalara örnek olarak; geriye dönük kayıt incelenmesi (log), veri kurtarma ve veri analizi verilebilir.

2.3.1.Siber güvenlik

Siber suçlarla mücadelede siber güvenlik yöntemleri genel olarak, siber alan güvenliğinin sağlanmasını amaçlayan kritik bilgi altyapılarının, süreçlerin ve içeriğin korunması için önlemler alınması, bilgisayar olaylarına müdahale merkezlerinin oluşturulması, kötücül yazılımlarla, köle bilgisayar ağlarının oluşturulmasıyla ve istenmeyen e-posta trafiği ile mücadele edilmesi gibi konularını kapsamaktadır.

Bilgi güvenliğinin esasları; gizlilik, kimlik doğrulama, bütünlük ve erişilebilirliktir. Buna göre, bilgi ve bilgi kaynakları; gizlilik dereceli işlemlere tabi olmalı, gerçek kimliklere sahip olunduğu doğrulanmalı, izinsiz kullanım ve değişikliklere karşı bütünlük içerisinde ve yetkili erişimlere sürekli açık olmalıdır. Bunu sağlamak için çoklukla uluslararası standartlarla belirlenmiş ve bilişim alanında genel kabul görmüş siber güvenlik ilkeleri uygulanır.

Türk Standartları Enstitüsü (TSE) tarafından türkçeye çevrilerek yayımlanan TS ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı, bilgi güvenliğinin sağlanması alanında en önde gelen uluslararası standarttır. Bu standart çerçevesinde; iş sürekliliği, log yönetimi ve izlenmesi, çevresel güvenlik, insan kaynakları güvenliği, yasalara uyum gibi önemli konular prosedür ve politikalarla belirlenmiş çalışma biçimleri doğrultusunda yürütülmektedir. Buna göre kurumsal siber güvenliğin sağlanması için alınması gereken başlıca önlemler;

- Sistem yöneticileri tarafından iç ve dış şebeke trafiğinin sürekli izlenmesi
- Sistem güvenlik güncellemelerinin düzenli olarak yapılması
- Son kullanıcıların güvenlik konusunda eğitimlerinin güncel tutulması
- Düzenli olarak güvenlik ve zafiyet testlerinin yapılması şeklinde sıralanabilir.

Bilişim sistemlerinin güvenliği; idari ve kurumsal güvenlik, personel güvenliği, fiziksel güvenlik, iletişim ve elektronik güvenliği, donanım güvenliği, yazılım güvenliği ve işlem güvenliği olmak üzere yedi ana konudan oluşmaktadır (Dülger, 2004 ve Yenidünya/Değirmenci 2003). Bu güvenlik önlemleriyle, hem bilişim sistemleri için öngörülen güvenlik, hem sistemde bulunan verilerin gizliliği ve yetkisiz erişimlerin önlenmesi, hem de sistemin kesintisiz olarak çalışması sağlanmalıdır (Akbulut, 1999).

Bilişim sistemlerinin güvenliğinin sağlanmasında en çok başvurulan ve etkili olan teknik yöntemler;

- **Bilişim sisteminin dış dünyaya yani internete açık bacağında bulundurulan ve yetkisiz erişimleri engelleyen "firewall" adı verilen güvenlik duvarı yazılımları:** Firewall yazılımlarının temel mantığı güvenli bir sistem elde etmek için öncelikle gerekmedikçe erişim noktası tanımlanmamasıdır. Sisteme sadece izin verilen adreslerden yetki verilen kullanıcılara tanımlanmış özel erişim noktaları (port) üzerinden erişim sağlamak gerekmektedir. Farklı coğrafi konumlarda bulunan sistemleri birbirine bağlamak için internet üzerinden VPN (Sanal Özel Ağ) tanımlaması da genelde firewall yazılımı kullanılarak yapılır.

- **Firewall yazılımlarına ek olarak kullanılan IPS/IDS (Intrusion Prevention Systems/Intrusion Detection Systems) denilen saldırı önleme ve izleme sistemleri:** Bu sistemler internetten gelen trafiği üzerlerine alıp denetleyerek güvenli olup olmadığına karar vermekte, ayarlarındaki saldırı tanımına uyan trafik türlerini kurum içi ağa geçirmemektedir. Dolayısı ile bu yazılımların sağlıklı çalışabilmeleri için üzerlerindeki ayarların son derece doğru yapılandırılmış olması gerekmektedir.
- **Anti-virüs yazılımları:** Sistem yöneticileri her ne kadar ağı internetten gelen tehditlerden koruyabilseler de, kullanıcılar taşınabilir ortamlar kullanmak suretiyle farkında olarak veya olmayarak bilişim sistemlerine güvenlik açığı içeren kötücül yazılımlar bulaştırabilirler. Bunlarla mücadele edebilmenin en temel yolu son kullanıcılardan sunuculara kadar ağda bulunan bütün bilgisayarlara anti-virüs programları kurulmasından geçer. Anti-virüs programlarının da verimli çalışabilmeleri için sürekli güncel tutulmalarının sağlanması gerekmektedir.
- **Anti-spam yazılımları:** Kurumsal ağlarda spam sorununa çözüm olarak kullanılan bu yazılımların temel mantığı kurumun e-posta sunucusuna gelen ve giden tüm e-postaların başlık bilgilerinin yazılımın veritabanındaki imzalarla karşılaştırarak spam olup olmadığına karar vermesidir. Bu yazılımlar genelde üreticinin internetteki güncelleme sunucusuna otomatik olarak bağlanarak son çıkan spam türlerine karşı kendini otomatik olarak güncellemektedir. Bununla birlikte her sistemin belli oranda spam kaçırma ihtimali vardır. Bu tarz açıklıklar yazılıma ayrıca tanıtılarak sorun giderilebilmektedir. Spam ile mücadelede anti-spam yazılımlarının yanı sıra port değişikliği vb. değişik teknikler de kullanılabilmektedir.
- **İçerik filtreleme yazılımları:** İş bilgisayarlarının güvensiz internet sitelerine bağlanmalarının ve bunlardan oluşabilecek zararların önüne geçilebilmesi için içerik filtreleme yazılımları kullanılmaktadır. Bu yazılımlar kabiliyetlerine göre URL filtrelemeden, tanımlanan kelimelerin geçtiği internet sitelerine erişimin engellenmesine kadar değişik ayarlarla erişimi

denetleyebilmektedirler. Ayrıca bu yazılımlar kullanıcıların internet erişim kayıtlarını da tutmaktadır.

- **Kayıt takip yazılımları:** Bu sistemler sunucular ve diğer ağ bileşenleri üzerinde tutulan kayıtlara erişip bunları anlamlı hale getirerek sistem yöneticilerinin işlerini oldukça kolaylaştırırlar. Temelde aslında var olan veriyi işleyerek kullanıcıya sunma mantığına dayanırlar. 5651 sayılı kanuna uyumlu çalışmaları için TİB tarafından sağlanan bir yazılıma entegre olarak tutulan kayıtlara zaman bilgisini bu yazılımdaki değerlerle girmeleri gerekmektedir.
- **Kriptolama – şifreleme yazılımları:** Bilgisayarlarda tutulan verileri korumanın en önde gelen yollarından biri de şifreleme yazılımları kullanmaktır. Bu yazılımlar kullanılarak veri iletişiminde güvenlik sağlanabildiği gibi disk şifrelemesi ile diskin çalınması veya kaybolması durumunda hassas bilgilerin başkalarının eline geçmesine engel olunabilmektedir.

Siber güvenliği tehdit eden unsurların başında siber saldırılar gelmektedir. Siber saldırıların dört evresi vardır. Bunlar; bilgi toplamak, tarama yapmak, sisteme giriş sağlamak, sisteme yerleşmek ve izleri temizlemektir.

Öncelikli olarak saldırgan hedefi hakkında aktif ve pasif yöntemlerle bulabildiği kadar bilgi toplar. Aktif bilgi toplamada hedef ile doğrudan irtibat kurarak bilgi alınır. Pasif bilgi toplamada sosyal mühendislik yöntemleriyle açık kaynaklar kullanılarak bilgi toplanır.

Tarama yapma; ağ taraması, port taraması, ağ haritası oluşturma ve zaaf taraması yapmaktır. Ağ taramasında ağ üzerindeki aktif sistemler tespit edilir. Port taramasında sistemde hangi portların aktif ve çalışır durumda olduğu belirlenir. Zaaf taramasında ise sistemin zayıf olduğu noktalar tespit edilir. Ağ haritası oluşturmada, hedef alınan kurumun ağ topolojisi belirlenmeye çalışılır.

Saldırgan sistemin zaaflarından faydalanarak sisteme giriş hakkı elde eder. Zayıf şifre kullanımı saldırganların işini oldukça kolaylaştırır. Hedef sistemin güvenlik açısından tasarımı ve saldırganın beceri seviyesi sisteme girişte önemli faktörlerdir.

Saldırgan sisteme giriş hakkını elde ettikten sonra sistemde kalıcı olmak için çalışır. Sistem tasarımını değiştirir, zararlı yazılımlar yükleyerek sistemi zombi haline getirebilir. Sisteme yerleşmekte kullanılan bazı yazılım türleri Backdoor, RootKit ve Trojanlardır. Saldırı için köle bilgisayar sistemlerini kullanabilir.

Saldırı sonrasında saldırgan yakalanmamak için bıraktığı izleri temizler. Sistemde tutulan kayıt dosyalarını siler.

Yukarıda sayılan siber saldırı evrelerinin her biri için farklı seviyelerde güvenlik önlemleri almak gerekmektedir.

Birinci evrede yer alan bilgi toplamaya karşı alınabilecek en etkili önlem öncelikli olarak bilgi güvenliği konusunda sistem kullanıcılarının farkındalık düzeyinin tam olmasıdır. Tüm kullanıcılar güvenlik açığı olabilecek bilgi sızıntısına karşı tedbirli olmalı, özellikle kullanıcı adı ve parola gibi özel bilgilerini herkesin ulaşabileceği bir şekilde bırakmamalıdır.

Tarama yapılarak sistemdeki açıklıkların bulunmasına karşı alınacak öncelikli önlem ise siber saldırgan bunu yapmadan önce çeşitli zafiyet testleri yaparak sistemde oluşan açıklıkların saldırı öncesi tespit edilerek kapatılmasıdır. Sistem ayarları her değiştiğinde ve bu değişimler işin gereği olarak sık yapıldığından farkında olmadan güvenlik açıklarının meydana gelmesi söz konusu olabilir. Bu yüzden bu zafiyet testlerinin belirli periyotlarla tekrarlanması gerekmektedir. Ayrıca saldırı tespit sistemleri sistemde tarama yapıldığını algılayabilmektedir. Bu durumda taramayı yapan adrese doğru trafik kesilerek bir önlem alınabilir.

Bütün bu önlemlere rağmen saldırgan sisteme giriş sağlamışsa, giriş sağladığı sistemi diğer sistemlerden izole etmekten başka yapacak fazla bir şey yoktur. Bu durumun

öncesinde alınabilecek en etkili önlem birbirine doğrudan ihtiyaç duymayan sistemleri mantıksal olarak farklı katmanlarda barındırmaktır. Yani ağ üzerinde gerekli ayarlamaları yaparak kurumun kullandığı fakat birbiri ile bilgi alışverişinde bulunmayan sistemlerin birbirlerine erişimlerini kesmektir. Bu işlem firewall yazılımları kullanılarak yapılabildiği gibi ağ bileşenleri üzerinde sanal ağlar oluşturularak ta yapılabilmektedir. Bu durumda sistemin birine saldırı olsa bile diğerlerine bulaşması engellenmiş olur.

Saldırganın sistemde kalıcı olmasının engellenmesi için anti-virüs yazılımlarının güncel tutulması ve periyodik taramalar yapılarak sistemlerin daima temiz kalmasının sağlanması gerekmektedir.

Siber güvenlik tatbikatları ile saldırı meydana geldiğinde yapılacak işlemlerin simüle edilebilmesi bu yöntemlerden biridir. Ülkemizde de TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) ve BTK koordinasyonunda 25-28 Ocak 2011 tarihleri arasında bir Ulusal Siber Güvenlik Tatbikatı 2011 gerçekleştirilmiş ve bu tatbikata enerji, finans, telekom, savunma, sağlık ve sosyal güvenlik gibi kritik bilgi-sistem altyapılarını oluşturan 41 kamu ve özel sektör kurum/kuruluşu katılmıştır.

2.3.2.Adli bilişim

Adli bilişim, bir bilgisayarda veya iletişim aygıtındaki silinmiş veya var olan bir elektronik delille ilgili yapılan araştırmadır. Adli bilişim, sonunda yasal veya idari bir süreçte sunulmak üzere bilişim sistemi üzerine yapılan detaylı bir araştırmadır (Karagülmez, 2005)

Dijital/elektronik delil (e-delil), "bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir (Keser Berber, 2004). Dijital deliller, klasik delillerden farklılık arz eder. Klasik deliller, gözle görülebilen, üzerinde el koyma, muhafaza altına alma kararı verilerek kolayca götürülebilen deliller iken; dijital deliller, bu kadar somut bir yapıya sahip değildir.

Bir dijital delilin içerisinde bulunduğu bir donanım aygıtı mutlaka vardır ancak önemli bu donanım aygıtı içerisindeki e-delillere ulaşabilmektir (Tan, 2010).

Adli bilişim safhaları, elektronik bulgunun, hukuki bir delile dönüştürülme sürecinde takip edilen prosedürlerdir ve dört bölümde incelenebilir:

- Toplama (Collection)
- İnceleme (Examination)
- Çözümleme (Analysis)
- Raporlama (Reporting)

Toplama; olay yerinin fotoğraflanması, ortamda bulunan bilgisayar, yazıcı ve diğer donanım aygıtlarının konumları belirtilecek şekilde notlar ve krokiler hazırlanması, elektronik delillerin toplanması, bilgisayarların muhafaza altına alınarak incelenmek üzere laboratuarlara götürülmesi ve aygıtlardaki verilerin sağlıklı kopyalarının (imaj) alınması işlemidir.

İnceleme; imajı alınmış verilerin gözle görünür biçime getirilme sürecidir. İnceleme aşaması sonucunda her türlü veri ortaya konmuş olacaktır. Örneğin; fotoğraflar, grafik dosyaları, videolar, çeşitli yazı dökümanları (word, excel, openoffice vb.), konuşma kayıtları (chat, MSN, GTalk vb.), e-postalar, ziyaret edilmiş ve sık kullanılan web siteleri, sıkıştırılmış dosya ve klasörler, şifreli dizinler, silinmiş dosya ve klasörler, dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları ilk başta akla gelen ve de en sık rastlanan hususlar olarak sayılabilir. Bu aşamada da birtakım yazılımlar kullanılmaktadır. Bu yazılımlara da, ülkemizde de kolluk kuvvetleri tarafından kullanılan EnCase ve FTK örnek olarak verilebilir.

Çözümleme; elde edilen verilerin hangilerinin ve ne ölçüde adli makamlara sunulmak üzere raporlanacağının tespiti yapılmaktadır. Tüm ilgisiz dosyalar bu değerlendirme aşamasında elenecek, raporlama aşamasına geçilmeyecektir. Ancak işe yarayabileceği düşünülen bulgular, elde ediliş metotlarını da ayrıntılarıyla anlatan tutanaklarla teslim edilecektir.

Raporlama; hangi bulguların o soruşturma açısından kullanılabilir olduğunun belirlenerek adli makamlara sunulmasıdır. Bu yönüyle raporlama safhası, hukuki bir değerlendirmeyi içermektedir. Adli bilişim uzman(lar)ının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilecek ve adli makamlara sunulacaktır. Bu sunum ile birlikte ayrıca ayrıntılı olarak dijital delillerin nasıl elde edildiğine ilişkin teknik boyutu ve adli bilişimin hangi metotlarının kullanıldığı da anlaşılır bir dille belirtilecek, açıklayıcı bir rapor hazırlanacaktır. Hazırlanacak bu raporda ayrıca, olayla ilgili bilgiler, araştırmanın yapıldığı zaman dilimi, incelenen elektronik deliller, inceleme esnasında kullanılan yazılım ve donanımlar hakkında bilgiler, inceleme sırasında kullanılan metotlar, araştırma sonunda ele geçen bulgulara ilişkin bilgiler yer almalıdır (Tan, 2010).

3.ULUSLARARASI UYGULAMALAR

3.1.Uluslararası Örgütlerin Çalışmaları

İnternetin ülke sınırlarını aşan uluslararası yapısı, veri iletiminin sınırsız olması ve bunun denetlenmesinin çok güç olması, bilişim suçlarıyla mücadeleyi de kaçılmaz olarak ülke sınırlarının dışına taşımaktadır.

Siber suçlarla etkin bir şekilde mücadele edebilmek için devletlerin ortak hareket etmeleri gerekmekte ise de, bu durum bazen klasik bir takım sebeplerden bazen de siber suç kavramına farklı yaklaşımlar olmasından dolayı gerçekleşememektedir. Devletlerin siber suçlar konusunda ortak hareket edememelerinin sebepleri genel olarak;

- Siber suçlarla ilgili hangi tipte yapısal düzenlemenin yapılması gerektiği konusunda uzlaşma sağlanamaması,
- Suç oluşturan fiillerin hukuki tanımlamalarının yapılmasında bir bütünlük sağlanamaması,
- Genel anlamda kovuşturma makamlarının ve kolluk kuvvetlerinin bu alandaki tecrübe eksikliği,
- Ulusal düzeydeki usul yasalarındaki kovuşturma hükümlerinin farklılığı sebebiyle siber suçların kovuşturulmasında uyumun sağlanamaması,
- Siber suçların birçoğunun uluslararası karakter arz etmesi,
- Suçluların iadesi ve karşılıklı yardım anlaşmalarındaki eksiklikler nedeniyle uluslararası işbirliğine izin veren kovuşturma mekanizmalarının uyumlu bir şekilde çalıştırılamaması,
- Devletlerin, egemenlik haklarında uluslararası organizasyonlar lehine tavizde bulunmak istememeleri olarak gösterilebilir (Beceni, 2003).

Uluslararası organizasyonlar, siber güvenliğin sağlanması hususunda erken dönemlerden itibaren bir farkındalık kazanmışlar ve siber suçlarla mücadele için uluslararası işbirliğine gidilmesine ve bu alanda yüksek seviyede bir hukuk

düzenlemesi yapılmasına katkı sağlamak için çalışmalar yapmışlardır. Dünyada siber güvenlik konusunda çalışmalar yapan birçok uluslararası ve ulusal kuruluş bulunmaktadır. Tablo 3.1'de bu kuruluşlardan bazılarının isimleri ve siber güvenlik konusunda hangi tür çalışmalar yaptıkları verilmiştir.

Tablo 3.1 Siber güvenlik konusunda çalışan kurumlar (Alfabetik sırayla)

KURUMLAR	**SİBER GÜVENLİKTEKİ ROLLERİ**
Uluslararası Kuruluşlar	
Avrupa Konseyi	Uluslararası mevzuat.
Avrupa Birliği	Çalışma grupları için sponsorluk, eylem planları, yönergeler.
ENISA	Farkındalık artırımı, kamu ve özel sektör arası işbirliğinin sağlanması, AB'ye siber güvenlik konularında tavsiyeler, veri toplama.
EUROPOL	Avrupa Birliği'nin kolluk ajansı olarak çalışmak.
G8 İleri Teknoloji Suç Alt Grubu	INTERPOL'ün 7/24 hattına sponsorluk, çeşitli politika yönergeleri.
IMPACT	Küresel tehdide tepki merkezi, veri analizi, gerçek zamanlı erken uyarı sistemi.
INTERPOL	7/24 hattını yönetmek, kanun uygulayıcısı teşkilatları eğitmek, soruşturmalarda bulunmak.
ITU	IMPACT'a sponsorluk, konferanslar organize etmek, yönergeler yayımlamak.
NATO	NATO üyesi ülkelerdeki askeri saldırılara tepki vermek.

NATO CCDCOE (NATO Siber Savunma Mükemmeliyet Merkezi)	NATO'nun siber savunma kapasitesini geliştirmek.
OECD	Politika geliştirmek, konferanslar organize etmek, yönergeler ve iyi uygulamaları yayımlamak.
UNODC (Birleşmiş Milletler Uyuşturucu ve Suç Ofisi)	Yasal mevzuatı desteklemek, farkındalık ve uygulama eğitimleri düzenlemek.
WSIS (Birleşmiş Milletler Dünya Bilgi Toplumu Zirvesi)	Bilgi güvenliğinde küresel zirve, envanter çalışmaları için uygulama izleme ve çözüm önerileri yayımlamak.
BOME'ler (CERTs)	
AP-CERT (Asya Pasifik Bilgisayar Olaylarına Müdahale Ekibi)	Asya bölgesel koordinasyonu.
CERT-CC (Bilgisayar Olaylarına Müdahale Ekibi Koordinasyon Merkezi)	Küresel BOME'lerin koordinasyonu, özellikle ulusal BOME'lerin.
FIRST (Olay Müdahale ve Güvenlik Ekipleri Forumu)	BOME'ler için forum ve bilgi paylaşımı.
TF-CSIRT (Terena Görev Gücü-Bilgisayar Olaylarına Müdahale Ekibi)	Avrupa'da bölgesel koordinasyon.
Ulusal BOME'ler	Ulusal koordinasyon, ulusal savunma ve tepki.

Kaynak: Keser Berber, 2011

Bu konuda çalışmalar yapan uluslararası kuruluşlardan; Birleşmiş Milletler, ITU), IMPACT), Avrupa Birliği, EUROPOL, ENISA, G-8, OECD, Avrupa Konseyi, FIRST ve INTERPOL bünyesinde yapılan çalışmalar aşağıda incelenmiştir.

3.1.1.Birleşmiş Milletler

Birleşmiş Milletler, 1945 yılında, İkinci Dünya Savaşı sonrası oluşan küresel buhran ortamında bozulan milletlerarası barış ve güvenliği yeniden tesis etmek amacıyla oluşturulmuş bir birliktir. Birleşmiş Milletler, insan haklarının korunması ve geliştirilmesinden yoksullukla mücadele ve ekonomik kalkınmaya kadar geniş bir yelpaze içinde çalışmalarına devam etmektedir.

Birleşmiş Milletler bünyesinde 1985 yılında düzenlenen " 7. Suçtan Korunma ve Suçluların Rehabilitasyonu" kongresinin ardından hazırlanan Milan Eylem Planının 42'nci ve 44'üncü paragrafları arasında Bilgisayar Suçları ele alınmıştır. "8. Suçtan Korunma ve Suçluların Rehabilitasyonu" kongresinin hazırlık çalışmaları sırasında düzenlenen "Asya Pasifik Bölgesel Katılımcılar Toplantısında" teknolojik gelişimin etkileri ve bilgisayar suçlarının giderek arttığı belirtilmiştir (Birleşmiş Milletler, 1994).

"8. Suçtan Korunma ve Suçluların Rehabilitasyonu" kongresinin 13. toplantısında üye ülkeler tarafından, içerisinde bilgisayar suçlarıyla ilgili çözüm önerilerinin de bulunduğu bir taslak kabul edilmiştir. Bu taslak ile bilgisayar suçlarıyla mücadele konusunda önemli çalışmalar yapılması kararlaştırılmış olup, bu çalışmalar sırasında bazı konuların dikkate alınması tavsiye edilmiştir. Bu konular:

- Kolluk kuvvetlerine ve yargı organlarına ve vatandaşlara bilgisayar suçlarından korunmanın öneminin anlatılması,
- Kolluk kuvvetlerinin ve yargı organlarının bu suçlarla mücadele konusunda eğitilmesi,
- İlgili organizasyonlarla işbirliğine gidilerek bilgisayar kullanımı ile ilgili etik kurallarının tespit edilmesi ve bu kuralların bilişim eğitiminin bir parçası olarak öğretilmesinin sağlanmasıdır.

2000 yılında İtalya'da düzenlenen "Sınırlar Ötesi Organize Suçlarla Mücadelenin Önemine İşaret Edilmesi" sempozyumunda siber suçlar tartışılmış ve üye ülkelerin

aşağıda belirtilen eylemleri cezai müeyyide ile karşılamaları önerilmiştir. BM'nin panelinde önerilen hususlar ceza kanunumuzda da suç olarak düzenlenmiştir. Bahsi geçen eylemler;

- Bilgisayar sistemlerine yetkisiz giriş,
- Bilgisayar veya bilgisayar sistemlerinin hukuka uygun olarak kullanılmasına engel olunması,
- Bilgisayar sistemleri içerisindeki verilerin yok edilmesi veya değiştirilmesi
- Gayri fiziki ekonomik değer taşıyan objelerin çalınması,
- Aldatma yoluyla değer elde edilmesidir (Beceni, 2003).

3.1.2. Uluslararası Telekomünikasyon Birliği (ITU)

Bir Birleşmiş Milletler ajansı olan Uluslararası Telekomünikasyon Birliği (ITU), bilgi ve iletişim teknolojileri hakkında çalışmalar yürütmekte ve kamu ve özel sektör kuruluşlarına gelişmekte olan bilgi ve iletişim şebekeleri ve hizmetleri alanında küresel çapta bir merkez sunmaktadır. Merkezi İsviçre'nin Cenevre kentinde bulunan ITU'nun ülkemizin de aralarında bulunduğu 191 devlet bazında üyesi ve 700'den fazla sektör üyesi bulunmaktadır. Farklı görevleri olmakla birlikte, ITU, siber güvenliğin sağlanması alanında da çalışmalar yürütmektedir.

ITU, Birleşmiş Milletlerin onayı ile geleceğin bilgi toplumu için ortak bir vizyon belirlemek amacıyla ilk aşaması 2003 yılında Cenevre'de, ikinci aşaması 2005 yılında Tunus'ta yapılan, Dünya Bilgi Toplumu Zirvesi (WSIS) adıyla uluslar arası toplantılar düzenlemiştir. Bu toplantılar neticesinde yayınlanan sonuç dokümanlarında ITU, "Bilgi ve İletişim Teknolojilerinin Kullanımında Güven ve Güvenliğin Tesis Edilmesi" konusunda görevlendirilmiştir.

Bu kapsamda çeşitliği faaliyetler yürüten ITU Genel Sekreterliği, 2007 yılında, bilgi toplumunda güven ve güvenliğin sağlanmasına yönelik uluslar arası işbirliği ve koordinasyon kurulması yönelik bir çerçeve model belirleyen Küresel Siber Güvenlik Gündemi'ni (GCA) yayımlamıştır.

Bu gündem ile küresel düzeyde, uygulanabilir ortak bir politika ve siber güvenlik mevzuatı geliştirilmesi, siber güvenlikle ilgili çalışan ulusal ve bölgesel kuruluşların kurulması, siber güvenlik ölçütlerinin ve teknik sistemlerin akreditasyon planlarının oluşturulması, siber güvenlik olaylarının izlenmesi, uyarı sistemlerinin kurulması ve müdahale ekiplerinin koordinasyonunu sağlayan bir yapılanmanın oluşturulması, siber güvenlik konusunda bilgi alışverişi için kapasitenin artırılması ve anılan konularda uluslar arası işbirliği hedeflenmiştir (Ünver vd., 2009).

3.1.3.Siber tehditlere karşı uluslararası çok taraflı işbirliği (IMPACT)

Küresel Siber Güvenlik Gündemi'nin fiziksel yerleşkesi olarak kabul edilen, Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (IMPACT), küresel toplumun siber tehditlere ilişkin önleme, savunma ve karşı koyma kapasitesini geliştirmeyi hedefleyen uluslararası bir kamu-özel sektör girişimidir.

IMPACT bünyesinde;

- Siber tehditlerle ilgili küresel bilginin gerçek zamanlı olarak toplanması, analiz edilmesi ve dağıtılması,
- Küresel siber tehditlere karşı erken uyarı ve acil durum müdahale sistemi oluşturulması,
- Siber güvenliğin teknik, yasal ve politik yönleri ile ilgili kapasitenin geliştirilmesine katkı sağlanması alanlarında çalışmalar yürütülmektedir. (BTK,2009)

3.1.4.Avrupa Birliği

Avrupa Birliği (AB) ekonomik, politik, sosyal ve kültürel alanlarda faaliyetler yürüten ve 27 üyesi bulunan bölgesel bir kuruluştur. Ülkemizin de AB'ye tam üyelik müzakere süreci devam etmektedir.

Avrupa Birliği, siber güvenliği, bilgi toplumunun önemli bir bileşeni olarak ele almakta ve şebeke güvenliği, internet, elektronik ticaret, kişisel verilerin korunması, fikri haklar gibi konulara ilişkin araştırma, geliştirme ve düzenleme faaliyetleri yürütmektedir. AB, bir yandan BİT gelişimini destekleyici araştırma ve geliştirme projeleri yürüterek, bir yandan da AB vatandaşlarının söz konusu teknolojilerden mümkün olduğunca yararlanmalarını sağlamak amacıyla kişisel verilerin korunması ve şebeke güvenliği gibi hususlarda tavsiye kararları ve direktifler oluşturmak suretiyle bilgi toplumuna dönüşüme katkıda bulunmaktadır.

3.1.4.1.Avrupa Birliği'ndeki hukuki uygulamalar

AB tarafından hazırlanan ve kısmen veya tamamen siber güvenliğin sağlanmasına yönelik hükümler içeren temel direktifler şunlardır:

- 1995/46/EC sayılı Kişisel Verilerin Korunması Direktifi
- 1999/93/EC sayılı Elektronik İmza Direktifi
- 2000/31/EC sayılı Elektronik Ticaret Direktifi
- 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Gizliliğin Korunması Direktifi
- 2006/24/EC sayılı Kamusal Elektronik Haberleşme Hizmetlerinin Sunumu Sırasında veya Kamusal Haberleşme Şebekeleri Üzerinden Elde Edilen Verilerin Muhafazasına İlişkin Direktif

Direktiflerin yanı sıra, AB'nin siber güvenliğin sağlanması ile ilgili almış olduğu bazı tavsiye kararları da bulunmaktadır. Bunlar;

- Avrupa Birliği Konseyi ve üye ülke temsilcileri tarafından alınan 17 Şubat 1997 tarihli İnternet üzerindeki yasadışı içerik ile ilgili tavsiye kararı,
- Avrupa Komisyonu tarafından alınan 25 Ocak 1999 tarihli küresel şebekelerde yasadışı ve zararlı içerik ile mücadele etmek suretiyle İnternetin daha güvenli kullanımını sağlamaya yönelik bir kamusal eylem planı oluşturulmasına dair tavsiye kararı,

- Avrupa Birliği Konseyi tarafından alınan 18 Şubat 2003 tarihli şebeke ve bilgi güvenliği kültürüne ilişkin Avrupa Birliği yaklaşımı ile ilgili tavsiye kararı,
- Avrupa Birliği Konseyi tarafından alınan 24 Şubat 2005 tarihli bilgi sistemlerine yönelik saldırılara ilişkin çerçeve kararı, (Üye ülkeleri, bilgi sistemlerine ve bilgiye yetkisiz erişim ve müdahale fiillerini suç olarak düzenlemeye, söz konusu fiilleri etkin, makul ve caydırıcı şekilde cezalandırmaya ve işbirliğini güçlendirmek amacıyla 7 gün 24 saat ulaşılabilir temas noktaları oluşturmaya çağırmaktadır.)
- Avrupa Birliği Konseyi tarafından alınan 22 Mart 2007 tarihli Avrupa'da güvenli bir bilgi toplumu oluşturma stratejisine ilişkin tavsiye kararı,
- Avrupa Parlamentosu ve Konseyi tarafından alınan 16 Aralık 2008 tarihli İnterneti ve diğer iletişim teknolojilerini kullanan çocukları korumaya yönelik bir kamusal program oluşturulmasına dair tavsiye kararıdır (Ünver vd., 2009).

3.1.4.2.Avrupa Birliği'ndeki polisiye uygulamalar

Avrupa Birliği üyesi ülkeler arasında ulusal sınırların büyük ölçüde kaldırılmasından doğan sorunlarla (organize suç örgütleri gibi) mücadele etmek üzere daha ileri düzeyde bir polis işbirliğine gereksinim duyulmuştur ve sonuçta Avrupa Polis Ofisi (EUROPOL) kurulmuştur.

EUROPOL'ün mevcut görev ve yetki alanına giren konular, yasadışı uyuşturucu ticareti, radyoaktif ve nükleer maddelerin yasadışı ticareti, gizli göç ağlarını içeren suçlar, yasadışı araç ticareti, seks amaçlı çocuk ticareti de dâhil insan ticareti, terörizm, para ve diğer ödeme araçlarına ilişkin sahtekârlık, bütün bu suç türleri ile bağlantılı olan yasa dışı para aklama faaliyetleridir (Sözen vd., 2003).

Europol'ün siber suçlara karşı mücadelede rolü;

- AB Siber Suç Görev Gücü; siber suçlara karşı AB ve aday ülkelerde mücadeleyi kolaylaştırmak için, AB Siber Suç Biriminin Başkanları ile birlikte çalışan Europol, Eurojust ve Avrupa Komisyonu temsilcilerinden oluşan bir uzman grubudur. Avrupa Birliği'nin kolluk ajansı olan Europol, AB Siber Suç Görev Gücü'nde önemli bir rol oynamaktadır.
- Europol bünyesinde barındırılan siber suç veri tabanı sayesinde, AB üye devletlerine, siber suçlarla ilgili soruşturma evrelerinde analitik destek sağlamakta ve AB ve aday ülkeler arasında işbirliği ve bilgi alışverişini kolaylaştırmaktadır.
- İnternet Kullanan Organize Suçların (İOCTA) Stratejik Analizi, siber suç ile ilgili mevcut ve gelecekteki eğilimleri değerlendirerek operasyonel faaliyetler ve AB politikası ilgili bilgilendirme yapmaktadır.
- Internet Suç Raporlama Online Sistemi (ICROS) ve Internet ve Adli Bilişim Uzman Forumu (IFOREX) halen geliştirilmektedir. Bu sistem ve forum, AB üye devlet yetkililerinden gelen siber suç raporlarının merkezi koordinasyonunu sağlayacak, teknik veri ve kolluk kuvvetlerinin eğitimi için ev sahipliği yapacaktır (EUROPOL, 2011).

3.1.4.3.Avrupa Birliği'ndeki teknik uygulamalar

AB, siber güvenliğin sağlanması ve kritik bilgi ve altyapıların korunması için alınabilecek olası yasal, teknik ve idari tedbirleri belirlemek amacıyla;

- Bilgi Toplumu Teknolojileri ve Avrupa Güvenlik Araştırma Programı
- Kritik Bilgi Altyapıları Araştırma Koordinasyon Projesi
- Avrupa Kritik Altyapıların Korunması Programı (European Programme for Critical Infrastructure Protection - EPCIP)

gibi projeler ve programlar yürütmekte ve AB üyesi veya aday ülkelerin yürütmekte olduğu pek çok projeyi desteklemektedir.

EPCIP, Avrupa Komisyonu tarafından 17 Kasım 2005 tarihinde yayımlanan kritik altyapıların korunması ile ilgili "yeşil kitap" ile başlatılan, AB üyesi ülkelerin kritik altyapıların korunmasına yönelik çalışmalarının ortak bir çerçeve etrafında koordine edilmesini ve etkin uyarı ve müdahale sistemlerinin oluşturulmasını amaçlayan bir programdır. Söz konusu raporda, EPCIP'in etkin ve tutarlı şekilde uygulanabilmesini teminen üye ülkelerin tek bir denetleme organı oluşturmaları ve kendi ulusal kritik bilgi ve altyapılarının korunması programlarını EPCIP modeline dayandırmaları istenmektedir.

Ayrıca, AB tarafından EPCIP dâhilinde oluşturulan Kritik Altyapı Uyarı Bilgi Ağı (Critical Infrastructure Warning Information Network) da siber tehditler, kritik altyapılarda bulunan açıklıklar, var olan risklere karşı alınabilecek tedbirler ve izlenebilecek stratejiler hakkında bilgi paylaşımına imkân veren bir platformdur.

Yine AB Komisyonu tarafından Mayıs 2007'de kimlik bilgileri hırsızlığına karşı "Siber Suçlarla Mücadele Üzerine Genel Bir Politikaya Doğru" adlı bir girişim başlatılmıştır.

3.1.4.3.1. Avrupa Şebeke ve Bilgi Güvenliği Ajansı (ENISA)

10 Mart 2004 tarihli ve 2004/460/EC sayılı Avrupa Birliği kararıyla kurulmuş olan Avrupa Şebeke ve Bilgi Güvenliği Ajansı; AB vatandaşlarının, tüketicilerin, şirketlerin ve kamu- özel sektör kuruluşlarının yararına şebeke ve bilgi güvenliğinin gelişmesi için çalışmalar yapmaktadır. Brüksel'deki kurulma periyodundan sonra ENISA faaliyetlerine 2005 yılından beri Girit-Yunanistan'da devam etmektedir (ENISA, 2011a).

ENISA Avrupa Komisyonunun, üye ülkelerin ve iş dünyasının şebeke ve bilgi güvenliği gereksinimlerini karşılamakta ve hem üye ülkeler hem de AB Kurumları için şebeke ve bilgi güvenliği ile ilgili konularda uzmanlık merkezi hizmeti sunmaktadır. Ayrıca Avrupa Birliğinin şebeke ve bilgi güvenliği ile ilgili mevzuatı hazırlanırken ya da yenilenirken teknik destek sağlanmaktadır.

ENISA'nın temel çalışma alanlarını; güvenlik uygulamaları ve servisleri, BOME'ler, kimlik ve güven, esneklik, risk yönetimi, paydaş ilişkileri ve yayınlar oluşturmaktadır (ENISA, 2011b).

Şebeke ve bilgi güvenliği ile ilgili rehber dokümanların yanında ENISA envanter çalışmaları da yapmaktadır. Üye ülkelerde şebeke ve bilgi güvenliği alanında çalışan kurumların iletişim bilgilerinden oluşan bir kim kimdir rehberi hazırlamış ve son olarak 2011 yılında güncellenmiştir (ENISA, Şubat 2011). Ayrıca, Avrupa'daki BOME faaliyetleri hakkında bir envanter oluşturmuş ve belirli periyotlarla güncellenerek yeni versiyonu yayımlamaktadır. Bu envanterde ülkemizde faaliyet gösteren TÜBİTAK UEKAE tarafından oluşturulan TR-BOME ve ulusal akademik ağ kapsamında TÜBİTAK ULAKBİM tarafından kurulan Ulak-CSIRT de bulunmaktadır **Hata! Başvuru kaynağı bulunamadı.**.

3.1.5.G-8

G-8 Dünya üzerinde en gelişmiş sanayiye sahip sekiz ülkenin (ABD, İngiltere, Fransa, Almanya, İtalya, Japonya, Kanada ve Rusya) oluşturduğu bir birlik olup ayrıca Avrupa Birliği de organizasyon bünyesinde kurumsal olarak yer almaktadır. Bu ülkelerin başkanları her yıl düzenli olarak toplanmaktadır. Toplantıların içeriği genellikle teknolojinin gelişme yolu, suç ve terörizm gibi dünya gündemini teşkil eden önemli konulardır.

1995'ten itibaren, G-8 Topluluğu siber suçlarla ilgili çalışmalar yapmaya başlamıştır. Bu konuyla ilgili çeşitli çalışma grupları oluşturulmuş, liderler tarafından birçok bildiri yayımlanmış ve üye ülkelerin adalet bakanları tarafından eylem planları hazırlanmıştır (Turhan, 2006). 1995 yılında Kanada'da düzenlenen zirvede, Organize Suçlar Kıdemli Uzmanlar Grubu (Senior Experts Group on Organized Crime) oluşturulmuştur. Bu grup "Ülkeler Arası Organize Suçlarla Mücadelede Tavsiyeler" adı altında bir rapor yayınlamıştır. Raporda şu hususlar dile getirilmiştir. "Ülkeler iç hukuklarını modern teknoloji ihlallerini cezai müeyyide ile karşılayacak şekilde

yeniden düzenlemelidirler. Problemli konuların da (yetki, adliye makamları, soruşturma, eğitim, uluslararası işbirliğinin sağlanması vs.) etraflıca tanımlanması gereklidir. Ülkeler bu alanda yapılacak çalışmaları teşvik etmeli, teknolojik suçlar ve soruşturmalar ile ilgili problemleri, anlaşmalar ve sözleşmeler yolu ile çözüme kavuşturmalıdır." (Beceni, 2003).

Haziran 1997'de, G-8 Topluluğu bünyesinde "İleri Teknoloji Suçları Alt Komitesi" oluşturulmuştur. Bu komite "Uluslararası Bilgi Ağlarının Kötü Kullanımı" (Misuse of International Data Networks) adında bir rapor hazırlamıştır (Beceni, 2003).

Aralık 1997'de yapılan toplantıda ise "İleri Teknoloji Suçları" tartışılmıştır. Buna göre; bilgisayar sistemlerine yapılan ihlallerin cezai müeyyide ile karşılanması konusunda üye devletlerin iç hukuklarının gözden geçirilmesi ve ileri teknoloji suçlarının araştırılmasının geliştirilmesine yardımcı olunması, karşılıklı yardım anlaşmalarının ve düzenlemelerinin yapılmasının özendirilmesi, yerleri tespit edilemeyen verilerin bilgisayar yolu ile araştırılması ve sınırlar ötesi araştırma ve yardım için yerine getirilmesi önerilen delillerin muhafazası hususlarında çözüm üretiminin teşvik edilmesi kararlaştırılmıştır (Turhan, 2006).

Mayıs 2000 tarihinde Paris'de yapılan toplantıda siber suçlarla ilgili bir takım tavsiye kararları alınmıştır. Toplantının sonuç bildirgesinde; "Elektronik bileşenleri içeren suçun kovuşturulması, araştırılması ve engel olunması için siber suçların değişik sistemler arasında tespit edilmesi ve tanımlanması gerekmektedir. Katılımcılar aşağıda belirtilecek hususların referansında herhangi bir çözümün getirilmesi konusunda mutabakata varmışlardır (Beceni, 2003):

- Gizlilik ve bireysel özgürlüğün korunmasının sağlanması,
- İleri teknoloji suçlarıyla mücadele için hükümetlerin amaçlarının korunması,
- Çalışmaları kolaylaştıracak uygun araçların içerilmesi,
- Siber suçluluğu gösteren şeffaf ve kesin tanımlamaların yapılması,
- Serbest ve adil aktivitelerin sağlanması, özel sektörün gönüllü olarak belirlediği davranış kuralları ve standartların etkinliğinin desteklenmesi,

- Etkinlik ve sonuçlara değer biçilmesi.

G-8 Topluluğu, siber suçların gelecekte en fazla işlenecek suçlar olacağının farkına varması ve özellikle bu suçlardan daha çok G-8 Topluluğu üyelerinin etkileneceğini düşünmesi nedeniyle siber suçlarla nasıl mücadele edilmesi gerektiği ve alınması gereken güvenlik tedbirleri konusunda önemli çalışmalar yapmaktadır.

3.1.6. Ekonomik İşbirliği ve Kalkınma Teşkilatı

Uluslararası bir ekonomi örgütü olan OECD, üye ülkelerin ekonomik ve sosyal gelişimine katkı sağlamak, üyeleri arasında işbirliğini kuvvetlendirmek, küresel ölçekli sorunlara çözüm üretmek üzere kurulmuş bir organizasyondur.

Bilgisayar suçları hakkında ceza hukuku problemlerine ilişkin uluslararası anlamda ilk ayrıntılı çalışma OECD tarafından başlatılmıştır. 1983 yılından 1985 yılına kadar OECD'nin geçici komitesi, bilgisayarlarla ilgili ekonomik suçlarla mücadele konusunda bir uluslararası uyumlaştırmanın mümkün olup olmadığı hususunda tartışmıştır (Sieber, 1998). Eylül 1985'de komite, üye devletlere bilgisayar yoluyla işlenen suçlarda, ulusal ceza kanunlarının göz önüne alınması tavsiyesinde bulunmuştur.

OECD'nin Geçici Komitesi ve ICCP komitesi (International Computer and Communications Policy Committee), üye devletleri siber suçlarla ilgili olarak ortak bir hukuk paydası altında birleştirmek maksadıyla, üye ülkelerin hukuklarının karşılaştırılmasına dayanılarak hazırlanan kurallar listesine göre üye ülkelerin kanunlarında aşağıda yer alan fiilleri suç olarak düzenlemelerini önermişlerdir. Bir başka ifadeyle aşağıda sayılan ihlallerin cezai müeyyide ile karşılanması konusunda fikir birliğine varılması gerektiği bildirilmiştir (Turhan, 2006). Bu ihlaller;

- Giriş, değiştirme, silme ve/veya bilgisayar verilerinin bastırılması ve/veya sermaye veya diğer değerli varlıkların yasa dışı transferi suçunu işlemek kastıyla bilgisayar programları yapılması, (Bilgisayar yoluyla dolandırıcılık);

- Giriş, değiştirme, silme ve/veya bilgisayar verilerinin bastırılması ve/veya sahtecilik suçu işleme kastıyla bilgisayar programları yapılması, (Bilgisayar yoluyla sahtecilik);
- Giriş, değiştirme, silme ve/veya bilgisayar verilerinin bastırılması ya da telekomünikasyon sistemi ve/veya bilgisayar fonksiyonlarının kasten engellenmesi maksadıyla, bilgisayar sistemlerine müdahale edilmesi, (Bilgisayar program ve verilerinde değişiklik yapılması).
- Korunmakta olan, münhasıran bir şahsa ait bilgisayar programını ticari olarak istismar etmek veya piyasaya sürmek maksadıyla, kişilerin bireysel haklarının ihlal edilmesi, (Bilgisayar programlarının telif haklarına aykırı olarak kopyalanması, çoğaltılması ve dağıtılması);
- Güvenlik önlemlerinin ihlali ya da diğer aldatıcı ve zararlı niyetlerle, sistem hakkında yetkili kişinin izni olmadan, bir bilgisayar ve/veya telekomünikasyon sistemine girmenin ve kullanımının engellenmesidir (Telekomünikasyon sistemlerinin, bilgisayarın diğer fonksiyonlarının ve iletişimin değişikliğe uğratılması)

1989 yılında OECD, bilgi sistemleri hakkındaki çalışmalarına özel bir önem vererek devam etmiştir. 26 Kasım 1992'de, OECD Konseyi, Bilgi Sistemleri Güvenliği Tavsiye Yönergesini kabul etmiştir. Yönerge, kamu ve özel sektörü ilgilendirmekte olup, bilgi sistemleri için minimum standartların uygulanması konusuna odaklanmaktadır. Ancak, bilgi sistemlerinin güvenliği konusunda, karşılıklı yardımlaşma, uluslararası alanda suçluların iadesi konularında olduğu gibi, bilgi sistemlerinin yanlış kullanılmasını önlemek amacıyla da yeterli cezai, idari veya diğer müeyyideler talep edilmektedir (Sieber, 1998).

3.1.7. Avrupa Konseyi

Avrupa Konseyinin oluşturulması fikri, II. Dünya savaşından maddi ve manevi büyük zararlar gören Avrupa'nın, benzer trajedileri bir daha yaşamasını önlemek maksadıyla ortaya atılmış ve Avrupa'da tarih boyunca yaşanan gerginliğin ve

çatışmaların yerini güven ve işbirliğinin alması hedeflenmiştir. Bu ortamda 5 Mayıs 1949'da 10 Avrupa ülkesi, Belçika, Danimarka, Fransa, Hollanda, İngiltere, İrlanda, İsveç, İtalya, Lüksemburg ve Norveç Avrupa Konseyini kuran anlaşmayı imzalamışlardır. Türkiye 13 Nisan 1950 tarihinde Avrupa Konseyi'ne üye olmuştur. Kuruluşun bugün 41 üyesi vardır. Avrupa Konseyi savunma konuları dışında toplumları ilgilendiren tüm sorunlara çözüm üretmeye çalışan bir topluluktur. Bu sorunlara örnek olarak, sosyal güvenlik, hukuki işbirliği, insan hakları, yerel yönetimler, bölgesel planlama, medya, eğitim, kültür, spor, gençlik, sağlık, çevre, aile konuları verilebilir. Konseyin bu alanlardaki çalışmaları genellikle sözleşme ya da protokoller hazırlanması ile sonuçlanmaktadır. Sözleşme ve protokoller üye ülke mevzuatlarının uyumlaştırılması, bu suretle ortak normlar ve bir Avrupa Hukuk Düzeni oluşturulması amacına yöneliktir (Avrupa Konseyi, 2011).

Avrupa Konseyi siber suçlar konusunda ilk çalışmalarını 80'li yılların sonlarına doğru gerçekleştirmiştir. Konsey, siber suçlarla ilgili çalışma yapmak üzere bir Uzmanlar Komitesi oluşturmuştur. Konseyin siber suçlarla ilgili olarak böyle bir çalışma başlatmasının hedefi bu suçlarla ilgili olarak ceza kanunlarında hangi fiillerin suç olarak kabul edilip cezalandırılması gerektiğini açık bir şekilde tespit etmek, sivil özgürlük ve güvenlik kavramları arasındaki uyuşmazlığın nasıl aşılacağı konusunda üye ülkelere yol göstermektir.

Uzmanlar Komitesi OECD'nin 1986 yılında yayınladığı raporunu referans alarak burada belirlenen ihlallerin, üye ülkeler nezdinde cezai müeyyide altına alınmasını benimsemiş ve ayrıca bir takım prensiplere ve OECD'nin raporunda belirtilmeyen ihlallere de dikkatleri çekmiştir. Komite çalışmalarının sonucunda OECD'nin raporunda belirlenen ihlallere ek olarak bilgisayarla bağlantılı suçlarla ilgili korunma, engellenme, mağdurlar, usulü bir takım kurallar örneğin uluslararası araştırmalar, veri bankalarına el konulması ve bilgisayar suçlarının soruşturulması ve kovuşturulmasında uluslararası işbirliğine gidilmesi hususlarının eklendiği bir taslak halinde sunulmuştur. Söz konusu taslak üye ülkelere yol gösterici niteliktedir. Daha sonra Avrupa Konseyi Bakanlar Komitesi tarafından 13 Eylül 1989 tarihinde yürürlüğe girmiştir (Turhan, 2006).

Avrupa Konseyinin siber suçlarla ilgili en önemli çalışması Siber Suç Sözleşmesi'dir. Avrupa Konseyi, Konseyin bilgisayar suçlarına ilişkin R (89) 9 sayılı ve bilgi teknolojisiyle bağlantılı ceza usulleri hukuku sorunlarına ilişkin R (95) 13 sayılı tavsiyelerini göz önünde bulundurarak, Kasım 1996'da siber suçlarla ilgilenecek bir uzmanlar komitesi kurmaya karar vermiştir. Devlet ve Hükümet Başkanları tarafından 10-11 Ekim 1997 tarihinde Strazburg'da yapılan İkinci Zirve'de kabul edilen ve yeni bilgi teknolojilerinin gelişimi konusunda Avrupa Konseyinin standartları ve değerlerine dayanan ortak tepkiler verme amacına yönelik Eylem Planını göz önünde bulundurarak sözleşme ile ilgili çalışmalara başlanmıştır. Sözleşme ve açıklayıcı raporu Avrupa Konseyi bakanları tarafından 109. oturumda 8 Kasım 2001 tarihinde kabul edilmiştir. 23 Kasım 2001 tarihinde imzaya açılıp 1 Temmuz 2004 tarihinde yürürlülüğe girmiştir (UNESCO, 2004).

Avrupa Konseyi'nin (89) 9 sayılı Tavsiye kararı belirli bilgisayar kötü kullanım biçimleriyle ilgili ulusal kavramların birbirlerine yaklaşmasını sağlamıştır. Fakat takip eden yıllarda siber suçlarda yeni olgularla mücadelede gerekli verimliliğin sağlanması için "bağlayıcı uluslararası bir araç ihtiyacı" ortaya çıkmıştır. Böyle bir araç çerçevesinde, uluslararası işbirliği önlemlerine ek olarak, maddi hukuk ve usul hukukuyla ilgili sorunlar ve bilgi teknolojisinin kullanımıyla yakından bağlantılı konuların ele alınması gündeme gelmiştir.

Sözleşmenin giriş bölümünde Avrupa Konseyin genel misyonu çerçevesinde siber suçlara karşı etkili mücadelenin cezaî hususlar konusunda artan, hızlı ve verimli bir uluslararası işbirliğiyle gerçekleşeceğine vurgu yapılmaktadır.

Sözleşmenin başlıca amaçları:

- Siber suçlar alanında ülkelerin maddi ceza hukuku unsurlarını ve bağlantılı hükümleri uyumlu hale getirmek,
- Bu suçların ve bir bilgisayar sistemi kullanılarak işlenen ya da delilleri elektronik formda olan başka suçların soruşturulması ve kovuşturulması için gerekli olan yerel ceza usulleri ve yargı yetkilerini sağlamak,

- Hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmak

şeklinde ifade edilmektedir.

Sözleşme; terimler, ulusal düzeyde alınacak önlemler - maddi hukuk ve usul hukuku, uluslararası işbirliği ve diğer hükümler olmak üzere dört bölümden oluşmaktadır. Maddi hukuk konuları kısmında bilgisayar ya da bilgisayarla ilgili suçlar alanında hem suç sayılmayla ilgili hükümler hem de bağlantılı diğer hükümler yer almaktadır. Önce 4 farklı kategoride gruplanan 9 suç tanımlanmakta, sonra ilave yükümlülükler ve yaptırımlar belirtilmektedir.

Önceki bölümde kısaca değinildiği üzere; sözleşmede yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı, bilgisayarlarla ilişkili sahtecilik fiilleri, bilgisayarlarla ilişkili sahtekârlık fiilleri, çocuk pornografisiyle ilişkili suçlar ve telif hakları ve benzer hakların ihlaline ilişkin suçlar suç olarak tanımlanmıştır.

Usul hukuku kısmında öncelikle usule ilişkin bütün yetkiler için geçerli olan ortak şartlar ve önlemler belirlenmektedir. Daha sonra usule ilişkin şu yetkiler belirtilmektedir: saklanan bilgisayar verilerinin hızlı bir biçimde korunması; trafik verilerinin hızlı bir biçimde korunması ve kısmen açıklanması; üretim talimatı; saklanan bilgisayar verilerinin aranması ve bunlara el konulması; trafik verilerinin gerçek zamanlı olarak toplanması; içerikle ilgili verilere müdahale edilmesi. Bu kısmın sonunda yargı yetkisiyle ilgili hükümler yer almaktadır.

Üçüncü bölüm olan uluslararası işbirliği bölümünde, geleneksel ve bilgisayarla işlenen suçlarla ilgili karşılıklı yardımlaşmaya ilişkin hükümler ve iade kuralları yer almaktadır. İki durum için geleneksel karşılıklı yardımlaşmaya değinilmektedir: taraflar arasında hiçbir hukuki temelin (anlaşma, karşılıklı mevzuat vs.) bulunmadığı durumlar ve böyle bir temelin bulunduğu durumlar. Üçüncü bölümde ayrıca, taraflar arasında hızlı yardımlaşmayı mümkün kılmak için 24 saat ve 7 gün açık durumda olacak bir ağın kurulmasıyla ilgili hükümler bulunmaktadır.

Son olarak, dördüncü bölümde -bazı istisnalar dışında- Avrupa Konseyi anlaşmalarındaki standart hükümlerin tekrarlandığı nihai maddeler yer almaktadır.

3.1.8. Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST)

1988 yılında Robert Morris isimli bir üniversite öğrencisinin internet'in büyüklüğünü görmek için internete bağlı bilgisayarlara bulaşacak ve bulaştığı bilgisayarları kendisine bildirecek "wank" solucanının kodunu yazmasından ve bu solucanın internette yayılmasından sonra internetin yüzde onu devre dışı kalmıştır. Oluşan zarar, ABD Genel Muhasebe Ofisinin (GAO) tahminine göre 10M–100M$ arasında olmuştur. Maddi zararın dışında önemli olan nokta ise internette güvenlik algısının yıkılmasıdır. Olayın ardından ABD'de "İnternet Güvenlik Olaylarına Tepki" konulu ulusal bir toplantı düzenlenmiştir. Toplantı sonucunda internet güvenlik problemleri ile ilgili "Güvenilir Bir İletişim Noktası" kurulması önerilmiştir. Öneriye karşılık Savunma İleri Araştırma Projeleri Ajansı (DARPA) görevlendirmesi ile ilk Bilgisayar Olaylarına Müdahale Ekibi (CERT) Koordinasyon Merkezi, internette meydana gelen güvenlik olaylarına müdahale etmek amacıyla kurulmuştur (Eriş, 2008).

Morris solucanından sonra internette olabilecek güvenlik sorunlarının tüm ülke ve kurumları ilgilendirildiği anlaşılmıştır. Bu nedenle ülkeler ve kurumlar arasında işbirliği ve iletişimin arttırılması amacıyla 1990 yılında FIRST kurulmuştur. Şu an 52 ülkeden 249 üyesi bulunan FIRST, bilgisayar olaylarına müdahalede en önemli oluşumlardan biridir ve bu alanda lider olarak kabul edilmektedir. Kanuni olarak FIRST California'da kamu yararına kar amacı gütmeyen bir şirket olarak çalışmalarına devam etmektedir.

FIRST, dünyanın çeşitli bölgelerinden hükümet, özel sektör, üniversite CERT ekiplerinin bir araya gelmesiyle oluşturulmuştur. Olayların önlenmesi, olaylara hızlı bir şekilde müdahale edilmesi gibi alanlarda üye olsun olmasın, ekipler arasında bilgi paylaşımının teşvik edilmesini amaçlamaktadır (FIRST, 2011).

3.1.9. Uluslararası polis teşkilatı (INTERPOL)

Dünyayı daha güvenli bir yer yapmak amacı doğrultusunda polis teşkilatlarının birlikte çalışmalarını sağlamak görevini üstlenmiş bulunan INTERPOL, 190 ülkenin üye olduğu dünyanın en büyük uluslararası polis teşkilatıdır. Genel sekreterliği Lyon, Fransa'da bulunan teşkilat 7/24 esasına göre çalışmaktadır. Aynı zamanda dünya genelinde yedi bölge ofisi ve Birleşmiş Milletler nezdinde New York ve Avrupa Birliği nezdinde Brüksel'de bir temsilcilik bürosu bulunmaktadır. 190 üye ülkenin her biri, kendi yüksek eğitimli kolluk kuvvetlerinden oluşan bir ekibi INTERPOL merkezinde istihdam etmektedir.

INTERPOL, yeni ortaya çıkan siber tehditlere karşı altyapısını güncel tutarak, eğitim ve operasyon odaklı bir siber suç programı yürütmektedir. Bu kapsamda:

- Bölgesel çalışma grupları ve konferanslar düzenleyerek ülkeler arasında bilgi alışverişini teşvik etmek
- Mesleki standartları oluşturmak ve korumak için eğitim ve kurslar düzenlemek
- Uluslararası operasyonları koordine etmek
- Siber saldırı veya siber suç soruşturma durumunda üye ülkelere yardımcı olmak üzere soruşturma ve veritabanı servisleri aracılığıyla küresel bir bilgi altyapısı sunmak
- Diğer uluslararası kuruluşlar ve özel sektör kuruluşları ile stratejik ortaklıklar geliştirmek
- Ortaya çıkan tehditleri tanımlamak ve üye ülkeler ile istihbarat paylaşımı sağlamak
- Operasyonel bilgi ve belgelere erişmek için güvenli bir internet sitesi sağlamaktır (INTERPOL, 2011a).

Birden fazla ülke tarafından yürütülen siber suç soruşturmalarında, polis teşkilatlarının dijital delillere daha hızlı erişimini sağlamak amacıyla, sınır ötesi işbirliği kurulması hayati önem taşımaktadır. Bu bağlamda INTERPOL, ulusal siber

suç birimlerinde çalışan araştırmacılar için üye ülkeler arasında operasyonel teması mümkün olduğu kadar hızlı ve kolay bir hale getirmek için Ulusal Merkez Referans Noktaları (NCRPs) isimli bir bilgi ağı kurmuştur. Bu temas noktaları yedi gün 24 saat bilgi ve/veya yardım taleplerine cevap vermektedir.

INTERPOL, en son çıkan siber suç tipleri ile mücadele alanında strateji, bilgi ve teknolojilerin geliştirilmesi için, Afrika, Amerika, Asya ve Güney Pasifik, Avrupa, Orta Doğu ve Kuzey Afrika'da bölgesel Siber Suç Çalışma Grupları kurmuştur.

Çalışma grupları bünyesinde yürütülen başlıca faaliyetler şunlardır:

- Kendi bölgelerindeki siber suçlardaki son eğilimler hakkında bilgi alışverişinde bulunmak
- Periyodik toplantılar yoluyla üye ülkeler arasında operasyonel işbirliğini arttırmak
- Bölgesel kolluk kuvvetleri için polisiye kaynaklar oluşturmak
- Operasyonel bilgi ve belgelere erişim için güvenli bir internet sitesi geliştirmek

Avrupa çalışma grupları, yaptıkları çalışmalarla, siber suç soruşturma araçlarını ayrıntılı olarak ele alan, INTERPOL Siber Suç Kılavuzunu geliştirerek üye ülkelerin hizmetine sunmuşlardır.

INTERPOL, siber suç soruşturmalarında bilgi ve uzmanlık paylaşımını sağlamak için her iki yılda bir Uluslararası Siber Suç Konferansı'nı düzenlemektedir. Konferans, üye ülkelerin polis teşkilatlarının ev sahipliğinde, kolluk kuvvetleri, akademik uzmanlar ve özel sektör uzmanlarından oluşan katılımcıları siber suçlarla mücadele hakkında güncel konularda sunumlar yapmak ve tartışmalar düzenlemek üzere bir araya getirmektedir (INTERPOL, 2011b).

3.2. Ülke Uygulamaları

Siber suçlar kapsamında gerçekleştirilen ülke uygulamalarına örnek olarak ABD, Almanya, Fransa ve Japonya'daki faaliyetler incelenmiştir.

3.2.1. ABD

İnternetin doğduğu yer olarak ABD bugüne kadar, internet ve bilgisayar dünyasındaki her türlü gelişmeye öncülük ettiği gibi, internetin suç aracı olarak kullanılması ve bu suçların düzenlenmesi olgusunun da ilk olarak ortaya çıktığı yer olma özelliğine sahiptir. Bu özelliğinden dolayı ABD'de siber güvenlik konusunda çalışmalar yürüten çok sayıda kurum/kuruluş bulunmaktadır (Tablo 3.2).

Tablo 3.2 ABD'de siber güvenlik alanında çalışma yapan ulusal kuruluşlar

Ulusal Kuruluşlar	**Çalışma Alanları**
CIA (Merkezi İstihbarat Teşkilatı)	Haber alma ağlarını savunmak, bilgi toplamak.
DHS (İç Güvenlik Bakanlığı)	Federal sivil ağları ve kritik altyapıları korumak, bilgi paylaşımı ve farkındalık, federal müdahale ekiplerini koordine etmek.
DoD(Savunma Bakanlığı)	Askeri ağları savunmak, karşı saldırı hazırlamak.
DOJ (Adalet Bakanlığı)	Federal kovuşturma.
FBI (Federal Araştırma Bürosu)	Federal araştırma.
FTC (Federal Ticaret Komisyonu)	Tüketiciyi koruma.
IC3 (İnternet Suç Şikâyet Merkezi)	Siber suç raporlama, havale merkezi.
NW3C (Ulusal Beyaz Yaka Merkezi)	Kanun uygulayıcısı kurumlara eğitim desteği vermek, FBI'la birlikte IC3'ün yönetimine destek vermek.

Gizli Servis	Ekonomik siber suçları araştırmak.
US-CERT (ABD Bilgisayar Olaylarına Müdahale Ekibi)	Federal sivil ağları (.gov) savunmak, bilgi paylaşımı ve özel sektörle işbirliği.

Amerika Birleşik Devletleri'nde siber suçlarla mücadele için geliştirilen hukuki, polisiye ve teknik uygulamalar ile ilgili bilgiler aşağıda verilmektedir.

3.2.1.1.Hukuki uygulamalar

İnternet yoluyla işlenen suçları tespit, cezalandırma ve önleme amacıyla yapılan hukuki düzenlemeler, bugün için ayrı bir problem sahasının oluşmasına yol açmıştır. Bu problem, yapılan düzenlemelerin gerek anayasal, gerekse evrensel hukuk temelinde bazı hürriyetlerin özüne dokunması tehlikesinin belirmesidir. Bu yüzden, ABD'de bugün için yapılan her türlü hukuki düzenleme, beraberinde bir karşı sivil toplum hareketini de doğurmaktadır. Bir yandan, bu sivil toplum örgütleri (özellikle American Civil Liberties Union) Amerikan Anayasasının Birinci Eki'nde teminat altına alınan, düşünce ve basın hürriyetlerinin ihlalini ve bu özgürlüklerin sansürlenmesini engellemeye çalışırlarken, karşı grubu oluşturan diğer kitlelerce de, artan küresel terörist eylemlerin de baskısıyla, internet yayınlarının sıkı bir takip altına alınması arzulanmaktadır (Çeken, 2002).

ABD'de çeşitli siber suç şekillerini düzenleyen birçok federal ve eyalet düzeyinde yasa kabul edilmiştir. Federal düzeyde yapılan ve bu nedenle bütün ülke çapında uygulaması olan düzenlemelere örnekler aşağıda verilmektedir.

a. **Bilgisayar sahtekârlığı ve bilgisayarların kötüye kullanılması yasası (Computer fraud and abuse act)**

1984 yılında kabul edilen bu yasa, ABD'de artan siber suçları engellemek, en azından artmasını önlemek amacıyla düzenlenmiştir. Başlangıçta söz konusu yasanın kısa vadeli ve dar ölçekli olması amaçlanmıştır. Ancak bilgisayar güvenliğini tehdit eden eylemlerin her geçen gün artması ve yasanın yetersiz kalması nedeniyle 1988,

1989, 1990 ve 1994 yıllarında çeşitli değişiklikler yapılmış ve yasanın kapsamı genişletilmiştir. Bu yasa ile Federal Temel Yasa'nın 18'inci Bölümünün 1030'uncu maddesi değiştirilmiştir (Çeken, 2002). Yasa temel olarak, korumalı bir bilgisayara yetkisiz ve izinsiz erişimi yasaklamaktadır. Yasa ile kamuya ve özel sektöre ait tüm bilgisayarların yanında, kişisel bilgisayarlar da bu korumadan tam olarak istifade edebilmektedir. Yasa ile suç haline sokulan hareketler şunlardır:

- ABD hükümetine zarar vermek veya herhangi bir yabancı ülkeye yarar sağlamak maksadıyla, tasnif edilmiş ve gizlilik dereceli savunma ve dışişleri konularına ilişkin enformasyona izinsiz olarak erişmek,
- Finansal bir kurum veya tüketici araştırma ajanslarından herhangi birinin bilgisayarlarındaki finansal kayıtlara izinsiz ve yetkisiz olarak erişmek,
- Kamu kuruluşlarından herhangi birinin kullandığı bir bilgisayara girerek, bu kuruluşların verdiği hizmeti aksatacak şekilde, burada bulunan bilgileri değiştirmek, bozmak veya ifşa etmek,
- Herhangi bir bilgisayara sahtekârlık veya hırsızlık yapmak maksadıyla izinsiz ve yetkisiz olarak girmek,
- Herhangi bir şekilde kasten veya ihmalen, korumalı bir bilgisayara erişmek, bu tip bir bilgisayara veri veya program göndermek,
- Bilgisayar şifrelerini veya bilgisayarlara erişmekte kullanılabilecek herhangi bir bilgiyi dağıtmak, başkalarının kullanımına sunmak,
- Para veya para hükmünde olan herhangi bir değeri elde etmek maksadıyla, bir bilgisayar veya bilgisayar sistemine zarar verme yönünde tehditler savurmak.

Bu hareketlerden herhangi birinin suç olarak nitelendirilebilmesi için sanığın diğer bir bilgisayara yetkisiz veya mevcut yetkisini aşarak erişmiş olduğunun kanıtlanabilmesi gerekmektedir (Turhan, 2006).

b. **İletişim ahlakı yasası (Communications decency act-CDA)**

Bu yasa, İnternet kaynaklı sorunların çözümlenmesi amacıyla düzenlenen yasalardan birisi olup, getirmiş olduğu hükümler bakımından tarihi bir kilometre taşı olarak kabul edilmektedir (Akdeniz, 2001).

Yasanın temel amacı, İnternet'te yapılan pornografik içerikli yayınlardan çocukların korunmasıdır. Söz konusu yasaya göre İnternet üzerinden müstehcen içeriğe sahip resim, yazı, video vb. materyallerin yayınlanması ve iletilmesi ile şiddet içeren yayınların gerçekleştirilmesi suç olarak düzenlenmiştir. Bunun yanı sıra yasanın uygulanabilmesi için yetkili mercilere, İnternet kullanıcılarının e-posta mesajlarının okunabilmesi ve haber gruplarındaki tartışmalar ile IRC üzerinden yapılan sohbetlerin izlenebilmesi olanağı sağlanmıştır (Sınar, 2001).

Bu yasa ile yürürlüğe giren ve antidemokratik olduğu düşünülen hükümlere karşı kamuoyunda büyük bir tepki meydana gelmiş ve sivil toplum örgütleri American Civil Liberties Union (ACLU- Amerikan Sivil Özgürlükler Birliği) önderliğinde anılan yasaya karşı muhalefet hareketine başlamışlar ve İletişim Ahlakı Yasası ile getirilen bazı hükümlerin Anayasanın 1'inci ekinde teminat altına alınan ifade özgürlüğünü ihlal eder nitelikte olduğu ve yasada yer alan "müstehcen yayın", "ahlaksız" gibi ifadelerin oldukça soyut ve geniş kavramlar olduğu ve bu durum ile ceza normunun belirliliğine ters düştüğü iddia edilerek, ACLU & Reno davası olarak literatüre geçen davayı açmışlardır (Sınar, 2001). Ayrıca bu gruplar yetişkinlerin kendi çocukları için neyin doğru neyin yanlış olduğuna kendilerinin karar verme yetkilerinin de ellerinden alındığını iddia etmişlerdir (Çeken, 2002).

Söz konusu girişimlerin sonucunda Amerikan Federal Yüksek Mahkemesi İletişim Ahlakı Yasası ile getirilen hükümlerin Anayasa'nın 1'inci Eki'ne aykırı oldukları gerekçesiyle iptal edilmelerine karar vermiştir.

c. **Çocuk pornografisinin önlenmesi yasası (Child pornography prevention act – CPPA)**

Çocuk pornografisi Avrupa Konseyi Siber Suç Sözleşmesindeki tanıma göre çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesi olarak tanımlanmıştır. 1996 yılında Amerikan Kongresi tarafından çocukların bu amaçla sömürülmesinin önüne geçmek amacıyla söz konusu yasa çıkarılmıştır.

Anılan yasa ile çocukların görüntülendiği pornografik yayın ve materyallerin elde bulundurulması veya İnternet'te yayınlanması ve bilgisayarlar veya e-posta yoluyla çocuk görüntülerinin bulunduğu cinsel materyallerin ticaret aracı olarak kullanılması yasaklanmıştır. Ayrıca suç teşkil eden çocuk görüntülerinden üç veya daha fazla adedini bizzat bilgisayarında bilerek muhafaza edenler cezalandırılmaktadır.

d. **Çocukların online yayınlardan korunması yasası (Child online prevention act - COPA)**

Bu yasa çocukları pornografik ve müstehcen yayınlardan korumak amacıyla 1998 yılında çıkarılmıştır. Yasa ile normalde büyüklerin erişmesine izin verilen site ve materyallere küçüklerin erişmesinin kolaylaştırılması cezalandırılmaktadır (Çeken, 2002). Amerikan Federal Mahkemesi 22 Haziran 2000 tarihinde Reno & ACLU II davasında verdiği kararda bu yasanın Anayasaya aykırı olduğuna karar vermiştir (Sınar, 2001).

e. **Elektronik haberleşmenin gizliliği yasası (Electronic communications privacy act- ECPA)**

Bu yasa ile radyo haberleşmesi, elektronik posta, özel haberleşme kanalları ve bilgisayar haberleşmesine ilişkin özgürlük ve gizlilik sınırları genişletilmiştir. Yasa ile, resmi makamlar tarafından olduğu kadar, resmi olmayan makamlarca da

yapılmakta olan kanunsuz dinleme faaliyetlerinin önüne geçilmek istenmektedir (Çeken, 2002).

f. İnternet'te kumarın önlenmesi yasası (Internet Gambling Prohibition Act)

Bu yasa ile ABD sınırları içerisinde (kumar oynamanın yasal sayıldığı Las Vegas ve Atlantic City gibi belirli yerler dışında), yasaklanmış bulunan çeşitli şans ve kumar oyunlarının İnternet siteleri aracılığıyla herkes için erişilebilir kılınması üzerine yasa koyucu bir düzenleme yapma ihtiyacı duymuş ve bu şekilde kumar oynatanların 2 yıla kadar hapis cezası ve 10.000 dolara kadar para cezası ile cezalandırılabilecekleri bir yasa çıkarılmıştır (Sınar, 2001).

g. Hüviyet hırsızlığı yasası

Hüviyet Hırsızlığı eylemlerine özgü olarak getirilen yasa Federal Temel Yasanın 1028 nci maddesidir. Bu düzenleme, 1998 yılında kabul edilen Hüviyet Hırsızlığı Yasası (İdentity Theft and Assumption Deterrence Act) ile getirilmiştir. Hüviyet Hırsızlığı Yasası yapılmadan önce 1028 nci madde sadece kimlik bilgileri üzerinde yapılan sahtekârlık eylemlerine ve bu tür belgelerin sahte olarak oluşturulmasına ilişkin bazı tedbirleri içermekteydi, bu tür bilgilerin çalınması ve interaktif ortamlarda, suç aracı olarak kullanılması durumlarına ilişkin herhangi bir düzenleme içermiyordu. Bu yasayla, 1028 nci madde de, 1998 yılında yapılan değişiklikle, doküman üzerinde olsun veya olmasın her türlü sahtekârlık suç haline getirilmiştir. Ayrıca, yasa ile ceza miktarları da arttırılmıştır (Çeken, 2002).

h. Anti-Terörizm yasası (USA Patriot - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)

11 Eylül 2001 tarihinde ABD'de bulunan Dünya Ticaret Merkezi'ne ait kulelere yapılan terörist saldırılardan sonra, Amerikan Kongresi tarafından 26 Ekim 2001 tarihinde yeni bir anti-terör yasası kabul edilmiştir. Yasa, İSS'lere eskiye nazaran,

abonelerinin üye bilgilerini soruşturma makamlarına verme konusunda daha ağır yükümlülükler getirmekte, ulusal güvenliğin gerektirdiği hallerde, hâkim kararı olmaksızın haberleşmenin denetlenebileceğini ve ulusal istihbarat örgütleri ile ulusal olmayan istihbarat örgütleri arasında bu yollardan elde edilen bilgilerin paylaşılabileceğini hükme bağlamaktadır (Çeken, 2002).

Yasanın siber suçlara ilişkin en önemli bölümü, Federal Temel Yasa'nın, daha önceden içeriği "Bilgisayar Sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Yasası" ile belirlenen 1028 nci maddesinde yaptığı önemli değişikliklerdir (Çeken, 2002). Yeni yasa ile yapılan değişiklikler;

- 1028'inci maddede önceden belirlenen ceza miktarlarının arttırılması,
- ABD sınırları dışında bulunan bilgisayarlar kullanılarak gerçekleştirilen ve ABD ticaretini zarara uğratan faaliyetlerin de, 1028'inci madde kapsamına alınması,
- 1028'inci maddede sayılan fiillere teşebbüs edenlerin dahi, bu fiilleri tamamlamış gibi cezalandırılacaklarının belirtilmesi,
- Daha önceden, herhangi bir eyalet mahkemesi tarafından haklarında bilgisayarlar aracılığıyla işledikleri bu tür suçlardan biriyle mahkûmiyet kararı verilenlerin, bu mahkûmiyetlerinin, bu kişilerin daha sonradan, federal düzeyde işleyecekleri suçlarda tekerrüre esas sayılacağının ve bu durumda olanların cezalarının arttırılacağının hükme bağlanmasıdır.

Söz konusu yasada ayrıca siber terörizm suçu kategorisi yaratılmakta ve bu suç faillerinin fiilleri başkasının ölümüne sebep olmuşsa ömür boyu, olmamışsa 15 yıla kadar hapsedilmeleri hükme bağlanmıştır. Yasa ile getirilen siber terörizm suçları:

- Milli güvenlik, milli savunma veya 1954 tarihli Atom Enerjisi Yasasının gereklerine göre erişilmesi yasak olan bilgisayarlara erişerek, buradaki bilgileri yetkili olmayan bir kimseye vermek veya Amerikan çıkarlarına aykırı olduğunu bile bile bir başka ülkenin kullanımına sunmak,

- Federal Temel Yasa'nın 1028'inci maddesinde belirtilen fiilleri gerçekleştirerek toplumun veya bireylerin sağlığına zarar vermek veya bunların sağlığını tehdit eden sonuçların ortaya çıkmasına neden olmak,
- Federal Temel Yasanın 1028'inci maddesinde belirtilen fiilleri gerçekleştirerek, bir federal yönetim organının veya adalet, mili savunma veya milli güvenlik idarelerinin bilgisayarlarına zarar vermek veya bunların zarara uğraması tehlikesine yol açmak (Çeken, 2002).

Bu yasanın en çok eleştirilen yönü, bugüne kadar 11 Eylül saldırılarında herhangi bir siber katkının varlığı ispat edilmemişken, özellikle ABD vatandaşlarının temel hak ve özgürlüklerine getirdiği kısıtlamalar ve uluslararası hukuku ilgilendiren iletişimin izlenmesi, ele geçirilmesi ve siber suçların kovuşturulmasıyla ilgili hükümlerinin içerdiği boyutu olmaktadır. Ancak bu Yasa ile getirilen kısıtlamalar 31 Aralık 2005 tarihine kadar geçerli olacakken ve bu tarihten sonra yasa gereği getirilen kısıtlamalar kendiliğinden ortadan kalkacakken, ABD Kongresi bu yasayı belirli periyotlarla uzatmaktadır (Turhan, 2006).

3.2.1.2.Polisiye uygulamalar

Amerika Birleşik Devletleri'nde siber suçlar ve siber terörizmle mücadele eden pek çok kuruluş ve bu kuruluşlara ait özel birimler bulunmaktadır. Bu çalışmada Amerika için polisiye yöntem olarak FBI tarafından yürütülen çalışmalara yer verilmiştir.

Merkezi Washington'da bulunan Federal Soruşturma Bürosu, (Federal Bureau of Investigation- FBI), ABD'de federal güvenlikten sorumlu kuruluştur. Toplam on madde ile özetlediği sorumluluk ve görevlerinde birinci önceliği terörizm ile mücadele olarak belirleyen kuruluş, siber suçlarla mücadeleye, karşı casusluk ve espiyonaj faaliyetlerinden sonra üçüncü sırada yer vermektedir.

FBI siber suçlarla mücadele konusunda çalışmalarını,

- Bilgisayarlara Saldırı
- Çocuk pornografisi
- Anti-korsanlık / Fikri Mülkiyet Hakları
- Dolandırıcılık / İnternet Suç Şikayet Merkezi

olmak üzere 4 başlık altında önceliklendirmektedir. Bilgisayarlara saldırı başlığı altında doğrudan kullanıcı bilgisayarlarını hedef alan kötücül yazılımlar ve bilgisayar korsanlığı ile mücadele ele alınmaktadır. Bu kapsamda FBI bünyesinde yürütülen faaliyetler:

- FBI bünyesinde siber suçlarla mücadele için bir koordinasyon merkezi olarak Siber Bölüm (Cyber Division) kurulmuştur.
- FBI merkezinde ve 56 saha ofisinde görev yapan özel eğitimli siber ekipler (cyber squads) oluşturulmuştur. Bu ekipler bilgisayar saldırıları, siber dolandırıcılık, çocuk pornografisi ve kimlik hırsızlığı gibi suçlarda uzmanlaşmışlardır.
- FBI'da Siber Eylem Takımları (Cyber Action Teams) ulusal güvenliği ve ekonomiyi tehdit eden siber suçlara ve bilgisayar saldırılarına karşı için uluslar arası alanda haber alma, diğer polis teşkilatları ile işbirliği ve önleme çalışmaları yürütmektedir.
- Ülke çapında federal, eyalet ve yerel alandaki güvenlik güçleri arasında kaynak paylaşımını sağlamak için 93 adet Bilgisayar Suçları Görev Güçleri (Computer Crimes Task Forces) adı altında müdahale ekipleri kurulmuştur.
- Başta Savunma Bakanlığı, İç Güvenlik Departmanı olmak üzere siber suçlarla ilgili benzer çalışmalar yürüten diğer federal kurumlarla, büyüyen bir ortaklık ve işbirliği çalışmaları yapılmaktadır. (FBI, 2011)

1996 yılında FBI bünyesinde bulunan Ulusal Altyapı Koruma Merkezi (National Infrastructure Protection Center - NIPC) ile birlikte çalışarak Ulusal Infragard Programı adında kritik bilgi altyapılarının siber ve fiziksel tehditlerden korunması amacıyla bilgi teknolojileri uzmanlarından oluşan bir pilot proje ekibi kurmuştur.

3.2.1.3.Teknik uygulamalar

Teknik uygulamalar kapsamında Amerika'daki siber güvenlik tatbikatları ve BOME'lere değinilmiştir.

İç Güvenlik Bakanlığı (DHS) tarafından yapılan Cyber Storm III tatbikatı ilki 2006, ikincisi 2008 yılında yapılan tatbikatlar serisinin üçüncüsüdür ve Eylül 2010'da gerçekleştirilmiştir. Cyber Storm tatbikatlarında kritik altyapılara yönelik geniş boyutlu siber saldırı senaryoları üzerinden gerçekleştirilmekte ve müşterek siber hazırlıklılık ve müdahale yeteneklerinin seviyesi gerçekçi ve inanılır olaylar üzerinden ölçülmektedir (DHS, 2009).

Tatbikata ABD ile birlikte Avustralya, Kanada, Fransa, Almanya, Macaristan, Japonya, İtalya, Hollanda, Yeni Zelanda, İsveç, İsviçre ve İngiltere'nin de içinde bulunduğu 13 ülke, ABD Kabinesinden 7 bakanlık, 11 ABD eyaleti katılmıştır. Ayrıca tatbikatta aralarında Bankacılık ve Finans, İletişim, Bilgi Teknolojileri, Ulaşım, Savunma sektörlerinden temsilcilerin de bulunduğu 60 özel sektör kuruluşu yer almıştır (DHS, 2011). Tatbikat sürecinde senaryo kapsamında katılımcılara yöneltilecek 1500 civarı enjeksiyon geliştirilmiştir (Gross, 2010)

Savunma İleri Araştırma Projeleri Ajansı (DARPA); 1988 yılında ortaya çıkan internet solucanı (Morris) neticesinde, Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü bünyesinde, internetten kaynaklanan güvenlik olayları ile mücadele edilmesi amacıyla CERT/CC'yi kurmuştur (Howard ve Longstaff, 1998).

İlk kurulduğunda küçük bir yapı olan ve siber olaylarla mücadele eden CERT/CC'de günümüzde, sistemlerin güvenliğini sağlamak üzere proaktif yaklaşımlar geliştirmek üzere 150 den fazla siber güvenlik uzmanı çalışmaktadır. CERT/CC, ABD'de, hükümet, sektör, kolluk ve akademik çevrelerle işbirliği içinde çalışarak büyük ölçekli ve karmaşık siber tehditlere karşı çözümler üretmek için ulusal seviyede çalışmalar da yürütmektedir. Carnegie Mellon Üniversitesindeki Yazılım Mühendisliği Enstitüsünün, devlet tarafından finanse edilen bir araştırma merkezi

olarak faaliyet göstermesi, CERT/CC'nin çalışmalarının büyük kısmının kamu sektörü ve ulusal güvenlik konularında yoğunlaşması sonucunu doğurmaktadır. Dolayısıyla siber ortamda ulusal güvenliğin sağlanması konusunda CERT/CC'nin uzman bir kuruluş olduğunu söylemek mümkündür (CERT, 2011).

CERT, siber olayların tespit edilmesi bu ve gelecekte meydana gelmesi ihtimali olan olaylara karşı çözüm önerilerinin geliştirilmesi amacıyla internet aktörleri ile birlikte çalışmaktadır. CERT'in misyonu;

- Acil durumlar için güvenilir 24 saat çalışan bir temas noktası hizmeti vermek,
- Güvenlik problemlerini çözmek üzere çalışan uzmanlar arasındaki haberleşmeyi kolaylaştırmak,
- Güvenlik açıklarını tespit eden ve bu açıklıkları gideren bir merkez olmak ve
- Bilgi güvenliğinin anlaşılması ve farkındalığın arttırılması için proaktif çalışmalar yürütmektir (CERT, 2011)

ABD'nin siber altyapısını korumak, siber saldırılara karşı yürütülen mücadele çalışmalarını koordine etmek için 2003 yılında US-CERT kurulmuştur. Merkezi Washington'da bulunan US-CERT, DHS ve kamu-özel sektör işbirliği ile kurulmuştur.

US-CERT, federal ajanslar, hükümet, güvenlik alanındaki uzmanlarla ve diğer ilgililerle işbirliği içinde bilgi paylaşımında bulunarak siber olaylara müdahaleyi koordine etmeyi ve bu yolla siber saldırıları ve güvenlik açıklarını azaltmayı amaçlamaktadır (US-CERT, 2011).

3.2.2.Almanya

Almanya'da siber suçlarla mücadele için geliştirilen hukuki, polisiye ve teknik uygulamalar ile ilgili bilgiler aşağıda verilmektedir.

3.2.2.1.Hukuki uygulamalar

Almanya'da siber suçlar için ayrı fasıllar veya kanunlar yapılmamakta, fiiller hâlihazırda kabul edilen suçlar bazında değerlendirilmektedir. Konuyu bir örnekle somutlaştırmak gerekirse, bilişim sistemlerine karşı mala zarar verme fiilini suç olarak düzenleyen Alman Ceza Kanununun 303a maddesi; mala zarar verme suçunu düzenleyen fasılda yer almaktadır (Değirmenci, 2002).

Alman Ceza Kanununun 202a maddesinde verilerin depolandığı ve işlendiği bilgisayar ağlarına izinsiz olarak girilmesi ve verilerin ele geçirilmesi suç olarak düzenlenmiştir. Anılan suç, bilgisayar sistemlerinde saklanan verilere yönelik olması hasebiyle "sır aleyhine işlenen suçlar" arasında yer almaktadır. Alman Ceza Kanunu bilgisayar sistemlerine izinsiz girilmesini tek başına suç olarak kabul etmemekte, bunun yanında söz konusu suçun meydana gelebilmesi için verilerin de ele geçirilmesini aramaktadır. Kısaca fiil, kendisi veya üçüncü bir kişi lehine, kendisine ait olmayan ve sisteme girmesine izin verilmeyen, emniyete alınmış verilerin ele geçirilmesi halinde suç olarak sayılmaktadır (Önder, 1994).

Yine Alman Ceza Kanununun 263a maddesinde bilişim sistemlerinin kullanılmasıyla işlenen dolandırıcılık suçu hüküm altına alınmıştır. Bu maddeye göre dolandırıcılık suçunun oluşabilmesi için suçu işleyenin kendisi veya üçüncü bir şahıs için hukuka aykırı bir şekilde ekonomik fayda sağlamak amacıyla hareket etmesi gerekmektedir. Kısacası suçun oluşabilmesi için kanun özel kast aramaktadır. Söz konusu maddede dolandırıcılığa sebep olacak fiiller sayılmasına rağmen, bu fiiller tahdidi değildir. Yani sayılan fiiller dışındaki bir fiil ile de dolandırıcılık suçu işlendiğinde cezai müeyyide uygulanacaktır. Bu fiiller; yanlış programlarla, yanlış veya tamamlanmamış verileri kullanarak, verileri yetkili olmadan veya başka suretlerle bilgi işleme yetkisi olmadan müdahale ederek işlenmesidir. Madde metninde, suçun oluşması için verilerin meydana çıkmasını etkilemek suretiyle bir şahsın ekonomik zarara uğramasına sebep olmak da ayrıca ifade edilmiştir (Değirmenci, 2002).

Bilişim sistemleri vasıtasıyla meydana gelen sahtekârlık fiilleri Alman Ceza Kanununun 269 ve 279'uncu maddelerinde düzenlenmiştir. Anılan maddelerde, sahtekârlık suçunun oluşması için, hukukça hükmü haiz bir belgenin bilişim sistemleri aracılığıyla sahte olarak düzenlenmesi veya üzerinde tahrifat yapılması ve bu belgelerin kullanılması yeterli görülmüştür (Turhan, 2006).

3.2.2.2.Polisiye uygulamalar

Federal bir yapıya sahip olan Almanya'da her eyaletin kendi Polis Kanunu vardır. Almanya'nın polis organları şunlardır:

- Federal Polis Birimleri
- Federal Kriminal Dairesi (Bundeskriminalamt)
- Federal Sınır muhafaza (Bundesgrenzschutz)
- Meclis Polisi
- 16 Eyalet Polisi ve eyaletlerin Sahil Güvenlik Polisi (Wasserschutzpolizei)

Tüm eyalet ve Polis birimlerinin suçla mücadele ile ilgili tüm haber ve bilgilerin toplandığı enformasyon merkezi Federal Kriminal Dairesi (BKA)'dir. Bunun yanında BKA, Interpol organizasyonu ve uluslararası ortak polisiye çalışmalarla görevli merkez birimdir. BKA Kriminalistik Enstitüsü ile birlikte ar-ge ve bilimsel araştırma yayınları yayımlar. Uyuşturucu ve ilintili suçlarla mücadele BKA'nın iş hacminin yaklaşık %40'ını oluşturmaktadır. Organize suçlarla ve terörle mücadele diğer ağırlıklı görev alanlarıdır. Bir birimi de Berlin şehrindeki devlet adamlarının korunması ile görevlidir (BKA, 2010).

BKA, Almanya'da siber suçlarla mücadelede polisiye yöntemlerin merkezi konumundadır. Bununla birlikte internetin suçlara karşı taranmasından adli bilişime kadar birçok teknik yöntem BKA bünyesinde uygulanmaktadır. Bu kapsamda siber suçlarla mücadelede İSS'ler ile önemli ölçüde işbirliği yapılmaktadır. İnternet güvenliği konusunda Bilişim Güvenliği Federal Dairesi (BSI) ile birlikte

çalışılmaktadır. Ayrıca BKA tarafından Almanya için siber güvenlik stratejisi isimli bir çalışma da yayınlanmıştır.

BKA yıllık olarak Almanya için siber suç durum raporu yayımlamaktadır. Buna göre 2009 ve 2010 yılındaki suç istatistikleri Tablo 3.3'de verilmektedir.

Tablo 3.3 Almanya suç istatistikleri (2009-2010)

Suç Türleri	2010	2009	Fark	% Fark
Bilgisayar yoluyla dolandırıcılık	27292	22963	4329	18.9
Haberleşme hizmetlerine erişim dolandırıcılık	7993	7205	788	10.9
Bilgisayar yoluyla sahtecilik	6840	6319	521	8.2
Verileri değiştirme / bilgisayar sabotajı	2524	2276	248	10.9
Verilere müdahale / casusluk	15190	11491	3699	32.2
Dar anlamda siber suç	59839	50254	9585	1,19

Kaynak: BKA, 2010

Federal Almanya İçişleri Bakanlığı'nın Federal Kriminal Dairesi (BKA)'ni veri ağlarında siber suçların araştırılması konusunda yetkili ve sorumlu kılması üzerine 1999 yılında BKA bünyesinde siber suçlarla mücadelede en etkin birim olan Veri Ağlarında Olay Bağımsız Araştırma Merkezi Birimi (ZaRD) kurulmuştur. Bu tarihten itibaren 7/24 esasına göre çalışan birim özellikle çocuk pornografisi gibi internet suçlarıyla herhangi bir soruşturmaya bağlı kalmaksızın tarama yaparak mücadele etmekte, elde ettiği bulguları ulusal ve uluslararası adli mercilerle paylaşmaktadır. Birimin kuruluş felsefesi internetin kanunsuz bir alan haline dönüşmesine engel olmaktır.

ZaRD ile yapılan araştırmaların yanı sıra BKA bünyesinde büyük ölçüde olay bazlı bilgisayar ve ağ soruşturmaları yapılmaktadır. Devam eden davalar siber uzmanlar

tarafından takip edilmekte, e-posta yoluyla gelen ihbarlar değerlendirilmektedir. Bu tür olaylarda yerel polis yetkilileri BKA tarafından harekete geçirilmektedir.

3.2.2.3.Teknik uygulamalar

1999 yılında kurulan Bilişim Güvenliği Federal Dairesi (BSI), İçişleri Bakanlığı bünyesinde kurulmuş olup yaklaşık 500 çalışana sahip BİT güvenliği konularında bağımsız ve tarafsız bir kurumdur. Almanya' da iç güvenliğin temel taşlarından biri olan BSI bilişim güvenliği ulusal yetkilisidir ve bilişim güvenliği konusunda üç ayda bir yönetim raporları yayınlamaktadır.

BSI'nin amaçlarından biri toplumda bilgi ve iletişim teknolojilerinin güvenli kullanımını sağlamaktır. IT güvenliği önemli bir konu olarak algılanmakta ve bağımsız olarak yürütülmektedir. BSI kullanıcı ve bilgi teknolojisi üreticilerine, güvenlik konuları, IT sistemleri ve uygulamaları geliştirilmesi sırasında görüşler vermektedir. BSI'nın çalışmaları kapsamında Anti-botnet Danışma Merkezi kurulmuştur.

Anti-botnet danışma merkezi (Botfrei) kullanıcıları bilgilendirmek ve bilgisayarlarını bağlı oldukları botnetlerden kurtarmak için yardımcı olmak üzere internet erişim sağlayıcıları ile birlikte çalışan bir merkezdir. Anti-botnet danışma merkezi (Botfrei); Alman İnternet Ekonomi Derneği ve Bilişim Güvenliği Derneği desteği ile kurulmuş bir projedir.

Botfrei uzmanlarınca sunulan destek basamaklı olarak gerçekleştirilmiştir. Etkilenen kullanıcı internet erişim sağlayıcısından bulaşma hakkında uyarılır, örneğin internet tarayıcısı açıldıktan sonra botnetin varlığından dolayı mesaj alır. Web sitesine davet edilen mağdur kullanıcı ve kendi başına sunulan bilgi ile bilgisayarını temizlemeye çalışır. Sunulan desteğin ikinci aşamasında Botfrei devreye girer ve daha kapsamlı danışmanlık alma ihtiyacı duyan kullanımcılar için gerekli adımlar telefon hattı ile bildirilir. Telefon danışma hattı zararlı programları kendi başına bertaraf edemeyen

kullanıcıları desteklemektedir. Ayrıca kullanıcıya bilgisayarını sürekli nasıl koruması gerektiği de öğretilir.

İnternet Erişim Sağlayıcıları kendi web sitelerinde projeyi tanıtarak etkilenen kullanıcıları bilgilendirmektedir. İnternet Erişim Sağlayıcıları, merkezi telefon danışma hattına sahiptir. Botfrei'nin numarası yetkili İnternet Erişim Sağlayıcısı tarafından kullanıcının bilgisayarına bir kötücül bulaştıktan sonra verilmektedir. Tüm sunulan talimatlar ve DE-Cleaner yazılımı ücretsiz kullanılmakta, telefon hattı için sadece yerel telefon ücreti alınmaktadır (Botfrei, 2011).

3.2.3.Fransa

Fransa'daki siber suçlarla mücadele için geliştirilen hukuki, polisiye ve teknik uygulamalar ile ilgili bilgiler aşağıda verilmektedir.

3.2.3.1.Hukuki uygulamalar

İnternet'in ortaya çıkardığı hukuki sorunlarla ilgili olarak Fransa'daki mevzuat incelendiğinde İnternet'le ilgili olarak ceza hukuku alanında özel bir yasa olmadığı görülmektedir. Fransız yasa koyucular İnternet'le ilgili özel bir kanun hazırlamak yerine Fransız ceza mevzuatında İnternet'i de kapsamına alabilecek genel ifadelere yer vermişlerdir. Örneğin, 1994 tarihli Fransız Ceza Yasası ile küçüklere yönelik olmadığı sürece pornografinin suç teşkil etmeyeceği savunulmakla birlikte yasanın 227-24'üncü maddesi pornografik ve şiddet içerikli yayınların hangi araç ile olursa olsun küçükler tarafından erişilebilir kılınmasını suç olarak düzenlemiştir (Kangal, 2001).

Yine Yasanın 227-23'üncü maddesi ise bir küçüğün pornografik nitelikteki resminin kaydedilmesi ve hangi araçla olursa olsun yayınlanması ve iletilmesi eylemlerini suç olarak düzenlemiştir. Ayrıca Ceza Kanununun 226-8'inci maddesi rızası olmadan sözleri veya resmi üzerinde gerçekleştirilen montajın hangi yollarla olursa olsun yayınlanması eylemi suç olarak kabul edilmiştir. Fransız Ceza Kanununda yer alan

yukarıda belirtilen maddelerde geçen "hangi yollarla olursa olsun" ve "hangi araçlarla olursa olsun" ifadeleri bilgisayar ağlarını ya da İnternet'i de kapsamaktadır (Kangal, 2001).

Fransız hukukunda İnternet üzerindeki suç içerikli yayınlardan dolayı kimin sorumlu tutulacağı sorunu da tartışmalara konu olmuş ve mevcut kuralların gereksinimleri karşılamadığı düşüncesiyle 30 Eylül 1986 tarihli iletişim özgürlüğü Yasasında değişiklik yapan 1 Ağustos 2000 tarihli yeni bir yasa kabul edilmiştir. Bu yasa ile iletişim özgürlüğü Yasasının 2'nci babına "Link Üzerinde özel Haberleşme Dışındaki iletişim Servisleriyle ilgili Hükümler" şeklinde bir 4'üncü başlık eklenmiştir. Toplam 4 maddeden oluşan bu başlık altında İnternet öznelerinin sorumluluğuna ilişkin bir düzenleme rejimi geliştirilmiştir (Sınar, 2002).

21 Haziran 2004 tarihli Fransa "Dijital Ekonomide Güven Kanunu", bilişim ağı hizmetlerinin etkin ve doğru bir şekilde verilmesi ile bilişim suçları ile mücadelede internet servis sağlayıcılarının sorumluluklarının belirleyen bir Kanundur. Yasa İnternetle alakalı olarak aşağıdaki başlıkları içermektedir;

- Yer sağlayıcılara, yer sağlanan içerikle ilgili sorumluluğun azaltılması,
- İçeriğin içerik sağlayıcılar tarafından önbelleğe alınması,
- Elektronik ticaret, çevrimiçi reklam, telefonla satış yapılması ve sözleşmeler,
- Kriptografi, dijital sertifikasyon ve dijital imza,
- Siber suçlar.

Telif Hakları ile İlgili Yasal Düzenleme olan HADOPI kanunu, Fransa'da hazırlanan ve İnternet ortamında yayımlanan fikir ve sanat eserlerinin korunmasıyla ilgilidir. Kanun, korsan film indiren kişilerin İnternet bağlantısının bir yıla kadar kesilmesini öngörüyordu. "Three strikes" sistemiyle ilk olarak abone mail ile uyarılıyor, ikincisinde mektup gönderiliyor ve üçüncüde ise bir yıla kadar internet hesabını kaybedebiliyordu. İnternet ortamında fikir ve sanat eserlerinin korunması için düzenleme yapmayı ve kontrolünü hedefleyen Kanun 9 Nisan 2009 yılında Fransız Ulusal Meclisi tarafından reddedilmiştir. Fransız hükümeti konuyu yeniden

görüşülmek üzere meclise göndermiş ve Kanun 13 Mayıs 2009'da Fransız Senatosunda kabul edilmiştir. Kanun, 10 Haziran 2009 tarihinde Fransız Anayasa Konseyi (Fransa'nın Anayasa Mahkemesi) tarafından İnternetin ifade hürriyetinin bir parçası olduğu ve Fransız hukukunda masumiyet ilkesinin hâkim olduğundan bahisle iptal edilmiştir. Anayasa Konsey'inin, "kamu haberleşme servislerine çevrimiçi ücretsiz giriş insan hakkıdır ve bireylerin bu hakkı sadece hakim kararıyla engellenebilir" demesi üzerine Hükümet kanunun bu maddesini değiştirmiş ve nihayet 22 Ekim 2009 tarihinde Anayasa Konseyi kanunun son halini onaylamıştır. Buna göre HADOPI Kanunu ile kurulan HADOPI Kurumunun İnternet aboneleri üzerindeki bu yetkisi elinden alınıp bu yetki sadece hâkime verilmiştir.

Fransa'da yurtiçi ve yurtdışında erişim engelleme yapılabilmesi ile ilgili olarak kanun çalışmaları yapılmaya başlanmıştır. Çalışmalar Siber Suçlarla Mücadele Merkez Ofisi (OCLCTIC) bünyesinde yürütülmektedir. Filtrelemenin teknik olarak nasıl yapılacağı (Domain, URL, IP) henüz inceleme aşamasında olup avantaj ve dezavantajları değerlendirilmektedir. Engellenen sitelerin, sayfanın niçin engellendiği ve itiraz için başvuru prosedürünü anlatan bir sayfaya yönlendirilmesi düşünülmektedir. Erişim engellemesi yapılacak Domain ve IP adreslerinin listeler halinde erişim sağlayıcılara henüz belli olmayan yöntemlerle iletilmesi düşünülmektedir. Listenin güncellenmesi ve kontrolü OCLCTIC tarafından yapılacaktır. Denetlemelerin nasıl yapılacağı hususunda düşünülen bir yöntem bulunmamaktadır. Engellemeler sadece çocuk ve ailenin korunmasına ilişkin tedbir amaçlı olup Open DNS, proxy veya tünel tarzı teknolojiler kullanılarak içeriğe erişim sağlanması engellenmeyecektir (TİB, 2009).

3.2.3.1.Polisiye uygulamalar

Fransa'daki Siber Suçlarla Mücadele Merkez Ofisi (OCLCTIC), Siber Suçlarla Mücadele Birimi (STRJD) ve Paris Polis Valiliği / Siber Suçlarla Mücadele Birimi (PP/BEFTI) incelenmiştir.

a. Adli polis/Siber suçlarla mücadele merkez ofisi (DCPJ -OCLCTIC)

Daha önceleri sadece mali suçlarla ilgilenen kuruluş 1983 yılından itibaren bilgisayarlarla ilgili suçlarla da ilgilenmektedir. 1994 yılında bilgisayar suçlarıyla ilgili bir birim kurulmuştur. 2000 yılından itibaren OCLCTIC adında merkezi ofis olarak faaliyet göstermektedir. OCLCTIC iç güvenlikten sorumlu Adli Polis (DCPJ) kurumuna bağlıdır. Önceden 5 kişilik teknik destek ekibi, 30 kişilik siber suç soruşturma biriminden oluşan ofiste şu anda tümü polis olan 60 kişi çalışmaktadır.

OCLCTIC'in görev ve sorumlulukları şu şekildedir;

- Kuruluşta eşit sayıda jandarma ve polis çalışanı vardır.
- Merkezi bir birim olduğu için Fransa genelinde koordinasyonu sağlar. Ayrıca siber suçlar konusunda uluslararası taleplerin iletişim noktasıdır.
- İnternet suçlarıyla ilgili gümrük, jandarma ve polis birimlerine teknik destek verir.
- Doğrudan desteğin yanında eğitim de vermektedir.
- Operasyon yetkisi de olan birim, adli otoritelerin izniyle teknik soruşturma başlatabilir ve suç mahallinde inceleme yapabilir.

OCLCTIC'in ihbar kategorileri; çocukların cinsel istismarı, ırkçılık, şiddete özendirme, suç işlemeye teşvik, kaçakçılık, spam, hile, küfür, fuhuş'tur. İhbarlar sadece İnternetten alınmaktadır. Gelen ihbarın uygunluğu kontrol edilmektedir. İhbarın teknik değerlendirmesi için kendileri için özelleştirilmiş bir yazılım kullanılmaktadır. İhbarlar bu yazılım ile incelenmektedir. Site ile ilgili teknik bilgiler (yer sağlayıcı, erişim sağlayıcı, IP, IP lokasyon bilgisi) manuel olarak alınmaktadır. Delillendirme amacıyla sitenin birkaç ekran görüntüsü de alınmaktadır. Daha sonra eğer ihbar içeriği yurt içindeyse kategorisine göre ilgili birimlere, ihbar içeriği yurt dışındaysa INTERPOL veya EUROPOL'e iletilmektedir.

Spam e-postaların sistemlere zarar verecek boyutta olmaması ve kişisel boyutta kalması nedeniyle bir önlem alınmamaktadır. İhbar geldiğinde, e- postaların farklı

ülkelerdeki farklı sistemlerden geçmesi ve ülkelerin mevzuatlarının farklı olması sebebiyle bir işlem yapılmamaktadır. 2001 yılında çıkan "Dijital Ekonomide Güven Kanunu" çerçevesinde erişim sağlayıcılara spam konusunda filtreleme hizmeti vermeleri için yaptırım bulunmaktadır. Ancak Erişim Sağlayıcılar bu hizmeti parayla vermektedirler. Bilinçli müşteriler konunun üzerine giderek hizmeti parasız alabilmektedirler (TİB, 2009).

b. Ulusal Jandarma Hukuki Araştırma ve Belgelendirme Teknik Servisi / Siber Suçlarla Mücadele Birimi (STRJD)

Birimde 270 kişi çalışmaktadır. Adli polis dökümantasyonlarının idaresi yapılmaktadır. Çocukların cinsel istismarıyla ilgili özel bir birimleri bulunmaktadır. OCLCTIC – Pharos ile bağlantı halindedirler. Jandarma 1 Ocak 2009 tarihinden itibaren Milli Savunma Bakanlığından ayrılarak İçişleri Bakanlığına bağlanmıştır, ancak halen askeri statüdedir.

STRJD'nin görev ve sorumlulukları şu şekildedir;

- Kriminoloji alanında veritabanı hazırlamak ve diğer birimlere yardımcı olmak,
- Siber suçla mücadele etmek,
- Dosyalar ve bulgular arasında bağlantıyı sağlamak ve analiz yapmak,
- İnterneti izlemek (web, forum siteleri, p2p uygulamalar) ve ihlalleri aramak,

Birim bünyesinde yapılan teknik uygulamalardan birinde; E-mule adlı uygulamaya bağlanılarak çocukların cinsel istismarı suçunu işlemeye yatkın olanların aşina olduğu anahtar kelimelerin kullanılmasıyla otomatik tarama yapan bir yazılım kullanılmaktadır. Bu yazılım hangi kullanıcının (IP) kaç dosya paylaştığını ve paylaştığı dosyaların inkar edilemezliğini sağlayan hash değerlerini tespit eder. Yazılım daha sonra bu hash değerlerini jandarma, polis ve OCLCTIC tarafından oluşturulan ve güncellenen çocukların cinsel istismarına ait görüntülerin ve hash değerlerinin bulunduğu merkezi bir veritabanından kontrol eder. Bu veritabanı

sadece Fransa içindeki yetkili adli birimler tarafından izlenmekte olup uluslar arası alanda paylaşılmamaktadır.

Forumlar Paris Savcısı tarafından yetkilendirilmiş ve özel eğitimden geçmiş görevliler tarafından takip edilmektedir. Sahte adlar kullanan bu ajanlar forumlarda delillendirme amacıyla döküman elde etmektedirler (TİB, 2009).

c. Paris polis valiliği / Siber suçlarla mücadele birimi (PP/BEFTI)

İletişim ve bilgisayar ağlarına yapılan saldırıları soruşturma birimidir. Adli polis memurlarından oluşan 30 kişinin çalıştığı birimin sorumluluk alanı Paris ve Paris'e en yakın belediyeleri kapsamaktadır. Diğer polis birimlerine, Hakim ve Savcılara teknik destek sağlanmaktadır. Bunun yanında siber suçlarla ilgili soruşturma da yürütülmektedir.

Suçun işlendiğinin düşünüldüğü bilgisayarlara el koyarak kendi birimlerinde kullandıkları özel yazılımlarla suçu işleyenin silemeyeceği türden bilgisayar izleri, delilleri aranmaktadır (TİB, 2009).

3.2.3.2.Teknik uygulamalar

Fransa Ağ ve Bilgi Güvenliği Ajansı (ANSSI), Fransa'nın milli güvenlik kitabı olan "Beyaz Kitap" da vurgulandığı gibi Fransa'nın milli savunma stratejisi içinde yer almaktadır. Ajans, 07.07.2009 tarihinden beri siber savunmanın merkezi olarak faaliyet yürütmektedir. Ajansın bağlı olduğu Milli Savunma Sekreterliğinin adı yakın tarihte "Savunma ve İç Güvenlik Genel Sekreterliği" olarak değiştirilecektir. Personel sayısı 110 olup 3 yıl içerisinde iki katına çıkarılması düşünülmektedir.

ANSSI'nın Görev ve Sorumlulukları şu şekildedir;

- Devlet içinde teknik güvenliği sağlamak.
- Ulusal tüzük ve mevzuat hazırlanmasına destek vermek.

- Uluslararası ilişkileri sağlamak.
- Hükümet içinde güvenlikli iletişim sistemleri kurmak, geliştirmek, denetlemek.
- Hassas şebekelerin (gaz, elektrik, su, iletişim vb.) güvenliğini sağlamak, denetlemek.
- Üst düzey güvenlik sağlayan ürünlerin ve yazılımların geliştirilmesine yardımcı olmak.
- Şifre sertifikalandırma işlemlerini yapmak.

Fransa çapında yetki sahibi olup bölgesel ve il bazlı teşkilatları vardır. Adli bir olayla karşılaşıldığında polise bilgi verilmektedir. Teftişler için 11 mühendis çalışmaktadır. Bakanlıklarla işbirliği, merkezi ve yerel teftişler yapılmaktadır. Güvenlik seviyeleri ölçülmekte ve her yıl 5 bakanlık teftiş edilmektedir.

Operasyonel işlemlerden sorumlu İletişim Sistemleri Güvenliği Operasyon Merkezi (COSSI) adında bir alt birimi vardır. COSSI 7/24 çalışmaktadır. COSSI içinde CERTA adlı bir birim bulunmaktadır. CERTA'nın iletişim sistemlerinin korunması için gerekli bilgilerin ilgilere ulaştırılması ve Fransızca sistem güvenliği dökümanları hazırlanması görevleri vardır (TİB, 2009).

3.2.4. Japonya

Japonya'daki siber suçlarla mücadele için geliştirilen hukuki, polisiye ve teknik uygulamalar ile ilgili bilgiler aşağıda verilmektedir.

3.2.4.1.Hukuki uygulamalar

Japonya'nın teknolojiye olan yakın ilgisinin de etkisiyle, siber suçlar konusunun yaratabileceği tehlikelerin önceden farkına varılmış ve ceza hukukunda gerekli düzenlemeler erken bir zamanda yapılmıştır. Söz konusu düzenlemeler yapılmadan önce, bu düzenlemelerin nasıl yapılacağı konusu doktrinde tartışılmış ve siber

suçlarla mücadelede, klasik ceza normlarının yeterli olamayacağı kabul edilerek, bu konuda yeni suç tiplerinin kabul edilmesi gerektiği konusunda uzlaşmaya varılmıştır. Bunun sonucunda 22 Haziran 1987 tarihinde yürürlüğe giren "Ceza Hukuku Alanında Bazı Hükümlerde Değişiklik Yapılmasına İlişkin Kanun" ile Ceza Kanununa siber suçlarla ilgili yeni suç tipleri eklenmiştir. 1990'lı yıllarda ise, siber-pornografik fiiller Ceza Kanunu'nun 175'inci maddesi kapsamında kabul edilmiştir.

Ayrıca 3 Şubat 2000 tarihinde yürürlüğe giren 1999/128 sayılı "Bilgisayarlara Yetkisiz Erişim Kanunu" (Unauthorized Computer Access Law) ile de, bilgisayar ağları yoluyla işlenen suçlar ayrıntılı bir şekilde düzenlenmiştir (Karagülmez, 2005).

Çocukların zararlı internet içeriğinden korunmasını amaçlayan "Gençlere Güvenli İnternet Kullanımı Sağlayan Çevre Kalkınma Yasası" Nisan 2009'da yürürlüğe girmiştir. Bu yasa mobil telefon operatörlerine filtreleme servislerini zorunlu hale getirerek çocukları internetin yasal olmayan içeriklerinden ve internetteki zararlı bilgilerden korumayı ve bilgi teknolojileri alanında okuryazarlığın geliştirilmesini desteklemektedir. Yasa kapsamında ailelere filtreleme yazılımı kullanarak çocuklarının internet kullanımını izleme, sınırlama, uygunsuz içeriğe erişimi engelleme imkânı verilmektedir. Japonya'da Mobil İçerik Değerlendirmesi ve Gözlemlenmesi Birliği, İnternet Reytingi Gözlem Enstitüsü ve Değerlendirme ve Filtreleme İrtibat Kurulu öz denetim kurulları olarak çalışmalar yapmaktadır.

3.2.4.2.Polisiye uygulamalar

Japonya'da siber suçlar uzun zamandan beri kamuoyunun ilgisini çekmektedir. Siber suçlarla mücadelede Japon yasa koyucularının odaklandıkları siber suçlar şunlardır:

- İzinsiz kimlik ve şifre bilgileri ya da diğer güvenlik açıklarını kullanarak bilgisayar korsanlığı yapmak,
- Bilgisayar virüslerini yaymak, bilgisayarlardaki verilere zarar vermek,
- İnternet üzerinden uyuşturucu ticareti, sahtecilik ve dolandırıcılık.

Japonya'nın siber güvenliğinden sorumlu olan kuruluş Ulusal Polis Teşkilatı (NPA)'dır. Siber Güvenlik Birimi 1997'de kurulmuş, 2000 yılında kapsamlı bir bilgi güvenliği politikası yayımlanmıştır. NPA, 2001 yılında Siber Güç Merkezi adıyla bilinen siber terörizm birimini kurmuştur. Bu merkez 9 ofisiyle Japonya'daki ağ bilgi akışını izlemektedir. Siber Güç Merkezi, 2005 yılında FIRST'e üye olmuştur.

Japonya'da 2009 yılında siber suçların sayısı bir önceki yıla göre 369 (% 5.8) artarak 6690 olarak belirlenmiştir. Ağları kullanarak işlenen suçların sayısı 2009 yılında 3961 olmuş ve bir önceki yıla göre 373 (-8.6%) bir azalma göstermiştir. Ağ kullanarak işlenen siber suçlar arasında, internet ihaleleri, çocuk fahişeliği/pornografi kanunu ihlalleri, Telif Hakları Yasası ihlalleri, müstehcen malzeme dağıtım ve pek çok dolandırıcılık vakası bulunmaktadır. "Bilgisayar Yetkisiz Erişim Yasası"nın İhlali 2009 yılında bir önceki yıla göre 794 (% 45.6) artış göstererek 2534'e yükselmiştir.

İnternet web sitelerinde çok sayıda yasadışı ve zararlı içerik bulunmaktadır. Bu zararlı içerikler Japonya'da çocuklara karşı işlenene suçlar da dahil olmak üzere çok sayıda olaya sebep olmuştur. Haziran 2006'dan bu yana bu tür sorunlar ile başa çıkmak için, internetteki yasadışı ya da zararlı içeriğinin internet kullanıcıları tarafından bildirildiği NPA tarafından finanse edilen Japonya İnternet Yardım Hattı Merkezi kurulmuştur. Merkeze 2009 yılında ulaşan raporların sayısı geçen yıla göre 4540 bir azalma (-3.4%) ile 130.586 olmuştur.

Siber suçların artan tehditleriyle mücadele etmek için uluslararası alanda düzenlenen forumlardan biri olan G8 Yüksek Teknoloji Suç Alt Grubu Forumu ve ICPO konferansında Japonya Ulusal Polis teşkilatı yüksek öncelikli olarak yer almıştır. G8 Topluluğunun 7/24 yüksek teknoloji suç ağının Japonya'daki odak noktası da Ulusal Polis Teşkilatının Siber Suç Bölümü'dür (NPA, 2011).

3.2.4.3.Teknik uygulamalar

Bilgi ve iletişim güvenliği konusunda Japonya'da koordinasyon Kabine Sekreterliği tarafından sağlanmaktadır. Kabine sekreterliği bünyesindeki BT Strateji Merkezi İçerisinde Bilgi Güvenliği Politika Konseyi (ISPC) ve Ulusal Bilgi Güvenliği Merkezi (NISC) siber güvenlik çalışmalarını yürütmektedir. Bu kapsamda kabine sekreterliği özel sektör, devlet kurumları ve bakanlıklar arasında işbirliğini sağlamakta ve gerekli politika ve prosedürlerin hazırlanmasını sağlamaktadır. ISPC Mayıs 2005'te kurulmuştur ve çeşitli bakanlıkların temsilcileri ve özel sektör uzmanlarından oluşmaktadır. ISPC;

- Bilgi Güvenliği ile ilgili stratejileri geliştirmek ve güncelleme,
- Temel stratejiye dayalı şekilde, bilgi güvenliği politikalarının ileriye ve geriye dönük değerlendirmelerini yapma,
- Bilgi güvenliği için devlet çapında tek tip güvenlik kılavuzları geliştirme,
- Devlet çapındaki güvenlik kılavuzlarına dayalı olarak bilgi güvenlik politikaları tavsiye etme

görevlerini yerine getirmektedir.

NISC, ISPC ile birlikte çalışarak;

- Bilgi güvenliği politikası için devlet çapında stratejiler belirleme,
- Devlet kurumlarının bilgi güvenliği üzerine kapsamlı tedbirler belirleme,
- Bilgi güvenliği vakaları meydana geldiğinde ilgili kurumları destekleme,
- Kritik altyapıların bilgi güvenliğini güçlendirme,
- Sektörler arası siber güvenlik egzersizleri gerçekleştirme,
- Diğer ülkelerle uluslar arası strateji ve ilişkiler geliştirme

görevlerini yerine getirmektedir (Brunner ve Suter, 2008).

Japon İçişleri ve İletişim Bakanlığı (MIC) medya ve telekomünikasyon sektöründe düzenleyici olan kurumdur. MIC; İnternet ve IP tabanlı servisleri (örneğin yüksek hızlı internet ve VoIP), geleneksel ve mobil telefon hizmetlerini "Telekomünikasyon İş Yasası" ile düzenlenmiştir. İletişimden sorumlu bakanlık olan MIC bünyesinde

siber güvenlik çalışmaları, Bilgi ve İletişim ile Telekomünikasyon daireleri tarafından yürütülmektedir. MIC'in Bilgi ve İletişim Dairesi bünyesinde başta;

- Bilgisayar virüsleriyle mücadele ve izinsiz erişimin engellenmesi,
- Botnetlerle mücadele ve siber saldırıların kaynaklarının belirlenmesi,
- Güvenlik konusunda araştırma geliştirme faaliyetleri yürütme,
- İnsan kaynaklarının geliştirilmesi,
- Siber güvenlik tatbikatı yapılması,
- Telekomünikasyon firmalarının uymaları gereken güvenlik standartlarının belirlenmesi,
- İlgili kurumlarla uluslararası işbirliğinin geliştirilmesi

olmak üzere çeşitli faaliyetler gerçekleştirilmektedir.

Telekomünikasyon Dairesi ise internetin güvenli kullanımı, zararlı içeriklerin filtrelenmesi ve spam maillerin engellenmesi konularında çalışmaktadır (MIC, 2011).

Japonya çapında bilgi olaylarına müdahale etmek amacıyla kurulmuş BOME'ler kurulmuştur. Bunlardan en önemlileri Ulusal Olay Müdahale Ekibi (NIRT) ve Japonya BOME Koordinasyon Merkezidir (JPCERT/CC).

NIRT Kabine Sekreterliği bünyesinde kurulmuştur ve Japonya'daki kurumların bilgi güvenliği olaylarına müdahale eylemlerini desteklemeyi amaçlamaktadır. NIRT bünyesinde kamudan ve özel sektörden uzmanlar yer almaktadır ve;

- Bilgi olayları hakkında bilgi toplama ve analiz etme,
- Etki azaltma, kurtarma, olayların yeniden meydana gelmesini engelleme konusunda kamu kurumlarıyla birlikte çalışma,
- Kamuyla ilgili kuruluşların ihtiyaç duyduğu uzmanlık ve bilgiyi sağlama,
- Yeni uzmanlar yetiştirme

görevlerine yerine getirmektedir (NISC, 2011).

Japonya'da kurulan ilk BOME olan JPCERT/CC, şebeke servis sağlayıcıları, güvenlik sağlayıcıları, devlet kurumları ve sanayi dernekleri ile koordineli olarak çalışmaktadır. JPCERT bünyesinde;

- Bilgi güvenliği olaylarına müdahale etme,
- Ülke çapındaki ve uluslararası BOME'ler ve ilgili kuruluşlarla birlikte çalışma,
- Yeni BOME kurulumu ve BOME'ler arası işbirliğini sağlama,
- Bilgisayar güvenlik olayları, güvenlik açıkları ve güvenlik yamaları gibi güvenlik bilgileri hakkında teknik bilgi toplayıp yaymanın yanı sıra uyarılar yayınlama;
- Bilgi güvenliği olayları konusunda araştırma ve analiz yapma,
- Bilgi güvenliği teknolojileri konusunda araştırma yapma,
- Bilgi güvenliği farkındalığını ve konu hakkındaki teknik bilgiyi arttırmak için eğitim düzenleme

faaliyetleri gerçekleştirilmektedir (JPCERT, 2011). JPCERT ayrıca Asya Pasifik bölgesinde bilgi güvenliği olaylarına müdahale eden APCERT kurulumunda yer almıştır ve yönetimini gerçekleştirmektedir.

4.TÜRKİYE İNCELEMESİ

Bu bölümde siber suçlarla mücadelede ülkemizin hukuki mevzuatı ile birlikte BTK'nın konu hakkında yapmış olduğu teknik düzenlemeler ele alınarak siber suçlarla mücadelede polisiye yöntemler olarak EGM Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı (KOM) faaliyetlerine yer verilmiştir.

4.1.Hukuki Boyut

Türk hukukunda siber suçlara ilişkin ilk düzenleme, 6.6.1991 tarih ve 3756 sayılı Kanunun 20'nci maddesi ile 13/03/1926 tarihli ve 765 sayılı TCK'nın ikinci kitabına "Bilişim Alanında Suçlar" adıyla 525/a, 525/b, 525/c ve 525/d maddelerinden oluşan bir bap ilave edilmesidir. Bu maddelerin ilk üçünde yasa koyucu tarafından suç tipi olarak belirlenen eylemler ve sonuncusunda fer'i cezalar (ek cezalar) düzenlenmiştir. Bu kanun maddeleri 1.3.1993 tarihinde kanunlaşan Fransız Ceza Kanunu Tasarısından yararlanılarak hazırlanmıştır (Dülger, 2004).

Kanun koyucu TCK'da yapılan değişikliğin ardından, güncel gereksinimleri karşılamak ve karşılaştırmalı hukukta yapılan düzenlemelere paralel düzenlemeler yaparak ülke mevzuatını uyumlaştırmak adına 5846 sayılı Fikir ve Sanat Eserleri Kanununda 7.6.1995 tarih ve 4110 sayılı kanunla değişiklik yapmıştır. Bu değişiklikle "Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları" da "eser" sayılarak, bilgisayar programlarına yönelik bu Kanun kapsamındaki fiillerde suç sayılmıştır (Değirmenci, 2002). Daha sonra 3.3.2004 tarih ve 5101 sayılı Kanunla, 5846 sayılı Kanun'da siber suçları ilgilendiren değişiklikler yapılmıştır (Turhan, 2006).

15.01.2004 tarih ve 5070 sayılı Elektronik İmza Kanunu ile elektronik imzanın geçerliliği kabul edilmiş ve anılan kanunun 16'ncı maddesi ile sahte elektronik imza yapılması ve kullanımı, 17'nci maddesi ile sahte elektronik sertifika yapılması ve kullanılması suç tipi olarak belirlenmiştir (Dülger, 2004).

Yenilenerek 26.09.2004 tarihinde kabul edilip 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunda siber suçlar, "Bilişim Alanında Suçlar" adıyla ikinci kitabın Topluma Karşı Suçlar başlıklı Üçüncü Kısımının 10'uncu Bölümünde 4 madde (m.243-244-245-246) halinde düzenlenmiştir. Yine 5237 sayılı TCK ile birtakım suçların bilişim sistemleri aracılığıyla işlenmesi suçun ağırlaştırıcı sebebi olarak kabul edilmiştir (Turhan, 2006).

4.1.1. 5237 sayılı Türk Ceza Kanununda siber suçlar

5237 sayılı TCK'da siber suçlara ilişkin düzenlemeler, genel olarak 765 sayılı TCK'da yer alan düzenlemelere benzer şekilde fakat daha kapsamlı olarak "bilişim sistemlerine karşı suçlar" ve "özel hayatın gizli alanına karşı suçlar" bölümlerinde düzenlenmiştir. Yine bunların yanında 5237 sayılı TCK'nın bazı bölümlerinde bilişim sistemleriyle işlenmesi mümkün olan suçlara yer verilmiştir. Buna göre 5237 sayılı TCK'da siber suç olarak adlandırılabilecek suç çeşitlerinin yanı sıra bilişim sistemi aracılığıyla işlenebilecek ancak sadece siber suç olarak tanımlanamayacak suç tipleri de mevcuttur (Dülger, 2004).

Bilişim alanında suçlar bölümünde,

- "bilişim sistemine hukuka aykırı olarak girme ve sistemde kalma" (m.243),
- "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (m.244),
- " banka veya kredi kartlarının kötüye kullanılması" (m.245) ve
- "tüzel kişiler hakkında güvenlik tedbiri uygulanması" hususları (m.246)

düzenlenmiştir.

Özel hayatın gizli alanına karşı suçlar bölümünde ise,

- "kişisel verilerin kaydedilmesi" (m.135);
- "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" (m.136)
- "verilerin yok edilmesi" (m.138)

suçlarına yer verilmiştir.

5237 sayılı TCK'nın bazı bölümlerinde siber suçları da kapsayan suç tiplerine yer verilmiştir. Bunlar,

- "haberleşmenin gizliliğini ihlal suçu" (m.132),
- "haberleşmenin engellenmesi suçu" (m.124),
- "hakaret suçu" (m.125),
- "bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu" (m. 142 fkr.2 b. "e"),
- "bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu" (m.158 fkr.1 b. "f")
- "müstehcenlik suçu" (m.226) dur.

a. Bilişim sistemine girme ve orada kalmaya devam etme suçu

Türk hukukunda oldukça yeni bir düzenleme olan 243 ncü madde ile kanun koyucu, bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etmeyi suç olarak kabul etmektedir.

Bu suçla korunan değerler; toplum düzeninin korunması ve bilişim sistemlerinin güvenliğinin sağlanmasıdır. Bilişim sistemlerine yasadışı erişimin önlenmesiyle, sistemi kullananların farklı türdeki menfaatleri korunmaktadır. Bu menfaatlerin başlıcaları; kullanıcıların özel hayatlarının gizliliğinin korunması, özel hayatın dokunulmazlığı, kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuki yararlardır (Dülger 2004 ve Karagülmez, 2005). Ayrıca söz konusu bilişim sistemleri vasıtasıyla (e-posta servisleri vs.) bireylerin haberleşme faaliyetlerine hizmet edilebildiğinden, aynı zamanda bireylerin haberleşme özgürlüklerinin de koruma altına alınmaya çalışıldığı söylenebilir (Doğan, 2005).

Bilişim sistemlerindeki her türlü bilgiye ulaşmak isteyen siber saldırgan çeşitli teknik yöntemlerle bu sistemlere girmeyi ve bir şekilde sistemde kalıcı olmayı hedefler. Örneğin bir bankanın veritabanına internet üzerinden haksız bir şekilde girmeyi başaran saldırgan bir defada elde ettiği verilerle yetinmeyip orada kalıcı olmak için

sisteme kötücül bir yazılım yerleştirebilir. Böylece yerleştirdiği yazılım sayesinde daha sonraki zamanlarda veri hırsızlığı yapabilir. Bu kanun maddesi ile hiçbir veri sızıntısı gerçekleşmemiş bile olsa yasadışı erişim cezalandırılabilmektedir. Ancak bilişim sisteminde kalma süresinin kanunda belirtilmemiş olması süren davalarda bir sorun teşkil etmektedir.

Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçunun maddi unsurunu, hangi yolla olursa olsun bir bilişim sistemine girilmesi ve bilişim sisteminde kalmaya devam edilmesi hareketleri oluşturmaktadır. Sisteme girilmesiyle suç tamamlanmış olmaktadır, ayrıca uzun süre sistemde kalmak ya da bazı verileri ele geçirmek suçun oluşumu için aranmamaktadır (Dülger, 2004).

b. Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu

244'üncü maddenin 1'nci fıkrasında, "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."; 2'nci fıkrasında ise "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır." denilmektedir.

Bu düzenleme ile kanun koyucu bilişim sisteminin işleyişinin engellenmesini, bozulmasını cezalandırmak istemiştir. Maddenin gerekçesinde de, bu maddeyle bilişim sistemine yönelik zarar verme eylemlerinin ayrı bir suç haline getirildiği belirtilmektedir (Karagülmez, 2005).

244'üncü maddenin ilk iki fıkrasında iki ayrı suç düzenlenmiştir. Bu suçları birbirinden ayıran nokta suçların konusudur. İlk fıkrada düzenlenen suçun konusu bilişim sisteminin bütün olarak kendisidir. İkinci fıkrada yer alan suçun konusu ise bilişim sistemini oluşturan verilerdir. Bu nedenle ilk fıkrada yer alan suçun cezası, ikinci fıkrada yer alan suça oranla daha ağırdır. 244'üncü maddenin 4'üncü fıkrasında "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç

oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur." kuralıyla, 1 ve 2'nci fıkralarda tanımlanan fiillerin işlenmesi nedeniyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır (Turhan, 2006).

Maddeye göre, bilişim sisteminin işleyişinin engellenmesinin veya bozulmasının cezası bir yıldan beş yıla kadar hapis cezasıdır. Bilişim sistemindeki verileri bozmanın, yok etmenin, değiştirmenin veya erişilmez kılmanın, sisteme veri yerleştirmenin, var olan verileri başka bir yere göndermenin cezası ise altı aydan üç yıla kadar hapis cezasıdır. Bu fiiller neticesinde kişinin kendisi veya bir başkasına haksız kazanç sağlamasının cezası ise iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasıdır.

Hem eski hem de yeni kanununda bu suç tipi için herhangi bir hafifletici sebep düzenlenmemiştir. Maddenin üçüncü fıkrasında sistemi bozmaya yönelik bu fiillerin banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali ağırlaştırıcı neden olarak düzenlenmiştir. Buna göre söz konusu ağırlaştırıcı durumun gerçekleşmesi durumunda faile verilecek ceza yarı oranında artırılacaktır.

c. Banka ve kredi kartlarının kötüye kullanılması suçu

245'inci maddenin gerekçesinde, banka ve kredi kartlarının haksız, hukuka aykırı olarak kullanılması üzerine bankaların ve kart sahiplerinin zarara sokulmasının ve bu yolla çıkar sağlamasının önlenmesi ve faillerin cezalandırılması amacıyla böyle bir maddeye yer verildiği belirtilmiştir. Ayrıca madde gerekçesinde, bu suçun aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçları ile korunmak istenen hukuki yararın anılan madde ile korunmak istenen hukuksal değerleri oluşturduğu belirtilmektedir. Bunlardan hırsızlık ve dolandırıcılık suçları ile kişilerin mal varlığı, güveni kötüye kullanma suçu ile kişilerin birbirine karşı duyduğu güven, son olarak sahtecilik suçunda ise belgelere olan güven duygusu korunan hukuki değerdir (Dülger 2004 ve Kurt 2005). Bunların yanı sıra, bankaların bu hizmetleri

aracılığıyla yürüyen ticari hayatın ve bankacılık sisteminin güvenirliliğini de korunan hukuki yararlar arasında saymak mümkündür (Turhan, 2006).

Bu suçun faili herkes olabilir. Ancak bir kimsenin fail olarak addedilebilmesi için başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse olması gerekmektedir. Burada mağdur, kredi kartı her ne şekilde olursa olsun elinden alınan veya kendisine verilmesi gereken kart kendisine verilmeyip rızası hilafına kullanılan kişidir. Ayrıca banka ve kredi kartını piyasaya sunan ve bunun karşılığında bireylere kredi veren bankalar da mağdur konumunda olabilmektedir (Dülger, 2004).

Bu madde ile düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun maddi unsuru, başkasına ait (veya sahte oluşturulan veya üzerinde sahtecilik yapılan) bir banka veya kredi kartını sahibinin ya da kendisine iadesi gereken kişinin rızası olmaksızın menfaat sağlamak için kullanmak, kullandırtmak veya başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak ve kabul etmektir (Kurt, 2005).

d. Tüzel kişiler hakkında güvenlik tedbiri uygulanması

246'ncı madde gereği Bilişim Alanında Suçlar başlıklı bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında güvenlik tedbirlerine hükmolunur.

e. Kişisel verilerin kaydedilmesi suçu

TCK'nın 135'inci maddesinin birinci fıkrasıyla, hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi; ikinci fıkrasıyla da kişilerin siyasi, felsefi veya dini görüşlerinin, ırki kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak kaydedilmesi eylemleri suç olarak hüküm altına alınmıştır (Değirmenci, 2002 ve Dülger, 2004).

Bu maddedeki suçlar, ağırlıklı olarak bilgisayar aracılığıyla işlenebilir. Bu durum maddenin gerekçesinde de belirtilmiştir. Söz konusu maddenin gerekçesinde "Çağımızda kişiler ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış veriş yapılan mağazaların müşterilerine ilişkin kayıtlar böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır." denilmektedir (Turhan, 2006).

135'inci madde, TCK'nın "özel hükümler" başlıklı ikinci kitabının "kişilere karşı suçlar" başlıklı ikinci kısmının "özel hayata ve hayatın gizli alanına karşı suçlar" başlıklı dokuzuncu bölümünde yer almaktadır. Yasanın sistematiğine bakıldığında, bu suçla genel olarak kişilerin özel hayatı ve hayatın gizli alanının, özel olarak da kişisel verilerin korunmasının amaçlandığı görülmektedir.

Bu suç fail ve mağdur açısından herhangi bir özellik taşımadığından, bu suçun faili veya mağduru herkes olabilir.

135'inci maddede suçun işlenme şekli ve alanı sınırlandırılmamıştır. Bu suçla her türlü kişisel verinin hukuka aykırı olarak kaydedilmesi fiili cezalandırılmıştır. Ayrıca bu suçun en çok işlenebileceği yer bilişim sistemleri olsa da sadece burada işlenebileceğini söylemek doğru değildir. Yani verilerin kaydedilmesi bir bilişim sistemine ya da veri taşıma aracına sayısal kod halindeki dar anlamda verilerin girilmesi şeklinde olabileceği gibi kişisel bilgilerin bir dosya kâğıdına el yazısı ya da daktilo ile geçirilmesi şeklinde de olabilir (Dülger, 2004).

Söz konusu suç serbest hareketli bir suçtur. Yani verilerin kaydedilmesi işleminin nasıl yapıldığı hususunun bu suçun gerçekleşmesi için herhangi bir özelliği yoktur. Ayrıca, bu suçta neticeye de önem verilmemiştir. Bir başka ifadeyle verilerin kaydedilmesi fiili bu suçun oluşabilmesi için yeterlidir. Yine kayıt etme fiilinin

aleniyete dökülüp dökülmemesinin, bu fiille bir zararın ortaya çıkıp çıkmamasının suçun oluşumunda bir önemi yoktur (Turhan, 2006).

Yasada, bu suçun oluşabilmesi için fiilin hukuka aykırı olarak işlenmesi gerektiği açıkça belirtildiğinden, hukuka aykırılık unsurunun özel olarak araştırılması ve failin gerçekleştirdiği fiilin hukuka aykırı olduğunu bilmesi aranmıştır.

Bu suçun manevi unsuru bilerek ve isteyerek genel suç işleme kastıdır. Madde metninde fiilin hukuka aykırı olarak işlenmesinin vurgulanması nedeniyle failin kastının, fiilin hukuka aykırı olduğunu da kapsaması gerekir (Karagülmez, 2005).

Kanunda kişisel verilerin kaydedilmesi suçunu işleyen failler için öngörülen ceza altı aydan üç yıla kadar hapis cezasıdır. Bu suç tipi için yasada herhangi bir hafifletici sebep düzenlenmemiştir. TCK'nın 137'nci maddesinde özel hayata ve hayatın gizli alanına karşı suçlar bölümünde düzenlenen suçlar için failin kamu görevlisi olması durumunda ya da belirli bir meslek ya da sanatın sağladığı kolaylıktan yararlanma varsa ağırlaştırıcı nedenler öngörülmüştür (Turhan, 2006).

f. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu

TCK'nın 136'ncı maddesinde "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır." hükmüne yer verilmiştir. Bu suç, en yaygın bir şekilde İnternet'te işlenmektedir. Kimlik hırsızlığı olarak da adlandırılan İnternet'teki kişisel verilerin ele geçirilmesi fiillerinde, genellikle müşterilerin ismi, doğum tarihi, sosyal güvenlik numaraları, kredi kartı bilgileri kendi bilgisi dışında ele geçirilmektedir. Daha sonra bu verilerle, haksız kazanç elde etmek üzere, İnternet dolandırıcılığı da dahil olmak üzere pek çok suç işlenmektedir. Ele geçirilen kredi kartı bilgileri ise, çoğunlukla müşteri hesaplarından nakit para transferinde veya kartın sahte bir kopyasının çıkartılmasında kullanılmaktadır (Karagülmez, 2005). Bu suçla korunan hukuki yarar 135'inci maddede düzenlenen hukuki yararla aynıdır.

Bu suçla hukuka uygun olarak kaydedilen veya kaydedilmeyen kişisel verileri hukuka aykırı olarak başkasına verme, yayma veya ele geçirme bağımsız bir suç olarak düzenlenmiştir. Maddenin gerekçesinde de ifade edildiği gibi başkasına verilen, yayılan ya da ele geçirilen verilerin hukuka uygun olarak kaydedilmiş olup olmaması suçun meydana gelebilmesinin koşulu değildir. Veriler nasıl kaydedilmiş olursa olsun bahsi geçen fiillerin gerçekleşmesiyle suç meydana gelmiş olacaktır (Turhan, 2006).

g. Verilerin yok edilmemesi suçu

Madde 138 ile hukuka uygun olarak kaydedilmiş kişisel verilerin kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi, bağımsız bir suç olarak tanımlanmıştır. Bu maddeyle korunan hukuki yarar gerçek kişinin özel hayatı ve buna bağlı olarak kişisel verilerin korunmasıdır. 138'inci madde, sadece kamu tarafından tutulan kişisel verileri değil, hukuka uygun olarak elinde kişisel veri bulunduran özel kuruluşları da kapsamaktadır. Bu sebeple kamu ve özel kuruluşları kendilerinde mevcut olan kişisel verileri kanunların belirlediği sürelere uygun olarak yok edeceklerdir. Bu suçla korunan diğer bir hukuki yarar ise kamu görevinin yerine getirilmesi sırasında disiplin oluşturmak ve kamu yararının elde edilmesini sağlamaktır (Dülger, 2004 ve Turhan, 2006).

Bu suç, verileri yok etmekle sorumlu olan kişinin görevini yerine getirmemesiyle oluşur. Verileri yok etmeme suçu ihmali hareketle gerçekleşmektedir. Yok etme verinin tamamen bir daha geriye döndürülemeyecek şekilde ortadan kaldırılmasıdır. Kısmen yok etmede, verinin kalan kısmı veri niteliği taşıyorsa anılan maddedeki suç gerçekleşir ve buna göre ceza verilir (Turhan 2006).

h. Haberleşmenin gizliliğini ihlal suçu

TCK'nın "haberleşmenin gizliliğini ihlal" kenar başlıklı 132'nci maddesinde:

"(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlali

haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde, ceza yarı oranında artırılır."
hükümlere yer verilmiştir.

Günümüzde haberleşme yoğun olarak, bilişim sistemlerinin sağladığı olanaklar kullanılarak, internet üzerinden gerçekleştirilmektedir. TCK anılan maddelerle bu yeni haberleşme biçimlerinin güvenliğini ve gizliliğini koruma altına almakta ve kanunla bu durumu ihlal edenlerinde karşılaşacakları cezaları tanımlamaktadır.

i. Haberleşmenin engellenmesi suçu

TCK'nın "haberleşmenin engellenmesi" kenar başlıklı 124'üncü maddesinde;

"(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adli para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezalandırılır." hükümlerine yer verilmiştir.

Yukarıda haberleşmenin gizliliğini ihlal suçuna ilişkin açıklamalarda belirtildiği gibi gelişen teknolojik imkanlar ile yeni haberleşme tipleri ortaya çıkmaktadır. TCK'nın 124'üncü maddesinde de yalnızca haberleşme ifadesinin yer alması ve haberleşme araçlarının belirtilmemesi nedeniyle haberleşme hangi araçla gerçekleştirilirse gerçekleştirilsin bunun engellenmesi suç olarak kabul edilmiştir.

j. Hakaret suçu

TCK'nın 125'inci maddesinde düzenlenen hakaret suçu, bilişim sistemleri kullanılarak, internet üzerinden de işlenebilecek bir suçtur. Maddenin ikinci fıkrasında eylemin mağdura yönelik sesli, yazılı veya görüntülü bir iletiyle de işlendiğinde hakaret suçunun gerçekleşeceği kabul edilmektedir.

Ayrıca maddenin diğer fıkralarında hakaret suçunun alenen veya siber alanda yayın yapan basın organları yoluyla işlenmesinin ağırlatıcı nedenlerden olduğu vurgulanmaktadır. Zira internet üzerinden yapılan bir yayın çok geniş bir kitleye ulaşabilmekte ve bir siteden silinerek kaldırılsa bile arama motorlarının arşivinden silinememektedir.

k. Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu

TCK'nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 142'nci maddesinin ikinci fıkrasının "e" bendinde bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçuna yer verilmektedir.

l. Bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu

158 maddenin birinci fıkrasının "f" bendi ile uygulamada siber suçların en sık karşılaşılan türlerinden biri düzenlenmekte ve bilgisayar ağlarıyla gerçekleştirilen hileli işlemler cezalandırılmaktadır.

m. Müstehcenlik suçu

TCK'nın 226'ncı maddesinde müstehcenlik suçu düzenlenmiştir. Bu maddede müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına yönelik düzenlemelere yer verilmiştir. Maddede belirtilen yayınların bilgisayar ağlarıyla yayılması ve paylaşılması mümkün olduğundan bu suç bilgisayar ağları ile işlenebilmektedir.

4.1.2. 5237 sayılı TCK maddelerine ilişkin eleştirisel görüşler

Bilişim suçları olarak değerlendirilen suç tipleri, 5237 sayılı TCK' da suçla korunan hukuksal değer göz önüne alınarak ilgili oldukları bölümlerde korudukları hukuksal değere göre düzenlenmektedir. Koruduğu hukuksal değer karma nitelik gösteren suç tiplerine ise bilişim sistemi ortak alınarak ayrı bir bölümde yer verilmektedir. Ancak banka veya kredi kartlarının kötüye kullanılması suçu koruduğu hukuksal değere göre malvarlığına karşı suçlar bölümünde yer alması gerekirken bu yapılmayarak bilişim sistemlerine karşı suçlar bölümünde düzenlenmektir. Bu durumun düzeltilmesi ve suç tipine ilgili olduğu bölümde yer verilmesi gerekmektedir (Dülger, 2004).

Hem 765 sayılı TCK' da ve hem de TBMM'ye sunulan hükümet tasarısında "verilerde sahtekârlık yapılması suçu" düzenleme altına alınmıştır. Ancak meclis alt komisyonunda değiştirilerek kabul edilen tasarı metninde bu suç tipine yer verilmemiştir; neticede yasa haline gelen 5237 sayılı TCK' da da bu suç tipi yer almamıştır. Suç politikası açısından bilişim sistemi aracılığıyla bu tür belgeler düzenlenip kullanılabileceği ve böylelikle kamunun güveni ihlal edilebileceği için bu suç tipi 5237 sayılı TCK' da düzenlenmeli ve bu suç tipine kamunun güvenine karşı suçlar bölümünde yer verilmelidir. Bu suç tipi, yukarıda belirtilen ilgili bölümde ya bağımsız olarak düzenlenmeli ya da resmi ve özel belgede sahtecilik suçlarının içinde ayrı ayrı düzenlenmelidir (Dülger, 2004).

Bilişim sistemlerinin organize suçlarda ve siber terörizmde kullanılması durumları acilen düzenlenmeli ve bu konu açısından ilgili yasalarda düzenlemeler yapılmalıdır. Bunların yanı sıra ırkçılık, şiddete çağrı, halkı kin ve düşmanlığa tahrik, suça teşvik ve terör örgütlerinin propagandasının bilişim sistemleri aracılığıyla siber alanda yapılması eylemleri hakkında da düzenlemeler yapılmalıdır (Ünver, 2001).

Siber terörizm olgusunun oluşturduğu büyük tehdit dikkate alınarak, veri iletim ağlarından yararlanılmak yoluyla terör eylemleri gerçekleştirilmesi ağırlatıcı neden sayılmalıdır. Çünkü terör eylemi gerçekleştiren eylemciler, klasik suç tiplerinde

kendi yaşamlarını dahi tehlikeye atmaktayken, eylemlerin bilişim sistemleriyle gerçekleştirilmesi hem aldıkları riski hem de tespit edilip yakalanma riskini azaltmakta ve suçun işlenişini kolaylaştırmaktadır. Aynı şekilde organize suç örgütlerinin üyeleriyle haberleşmesi, finansal kaynaklarını kullanması ve aktarması eylemleri de ayrıca düzenlenmelidir ve ağırlatıcı neden sayılmalıdır; yukarıda bu konuda yapılan açıklamalar burası için de geçerlidir. Bu konuda 5237 sayılı TCK' da herhangi bir düzenlemenin olmaması önemli bir eksiklik olarak görülmektedir (Dülger, 2004).

Kanunda bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçuna yer verilmektedir. Teknolojinin her gün ileriye doğru gitmesi yeni siber suç işlenme şekillerinin ortaya çıkarması sebebiyle böyle bir düzenleme yapılması gerekliliği ortaya çıkmıştır. Ancak bilişim sistemiyle gerçekleştirilen hangi tür hırsızlık eylemlerinin bu suçu oluşturacağı da bu düzenlemeden çıkarılamamaktadır. Bilişim sisteminin kullanılmasıyla somut nesnelerin çalınması mı yoksa verilerin çalınması mı bu suçla hüküm altına alınmak istenmiştir? Burada kişinin rızası dışında, failin kendisine veya başkasına yarar sağlamak amacıyla hareket edip kişinin eşya üzerindeki hâkimiyetini bilişim sistemi aracılığıyla sona erdirilmesi fiiliyle bu suç gerçekleşecektir (Turhan, 2006).

Veri iletim ağları üzerinden gerçekleştirilen kumar oynatma eylemi mutlaka ayrı bir fıkrada ve 228. maddenin nitelikli hali olarak cezayı ağırlatan hal seklinde düzenlenmelidir. Bu konuda büyük bir yasal boşluk bulunmaktadır. 5237 sayılı TCK' da bu yönde özel bir düzenleme yoktur. Oysa herkesin ulaşamadığı somut kumarhaneler dahi ülkemizde yasaklanmışken, dileyen herkes bugün siber kumarhanelerde kumar oynayabilmektedir. Her ne kadar 5237 sayılı TCK'nın 228. maddesinde "kumar oynanması için yer ve imkân sağlanması" denilerek geniş bir ifade kullanılıyorsa da yorum sorunlarının yaşanmaması ve uygulamada karışıklığa neden verilmemesi için "sanal alanda bilişim sistemleriyle kumar oynatılmasının" da madde metninde belirtilmesi uygun bir düzenleme olacaktır (Dülger,2004).

Başta Amerika Birleşik Devletleri'nde ve Avustralya'da olmak üzere, istenmeyen elektronik postaların (spam) gönderilmesi eylemleri suç olarak düzenlenmektedir. Bu gerçek anlamda rahatsız edici, veri iletim ağlarındaki trafiğin yoğunluğu arttıran ve kuruluşlar ile kişilerin elektronik posta kutularındaki çok geniş alanları kaplayan dolayısıyla uluslararası ticareti güçleştiren bir durumdur. 5237 sayılı TCK' da bu eylemin de suç tipi olarak düzenlenmesi gerekmektedir (Dülger,2004). Bu bağlamda Avrupa Sınır Ötesi Yayın Sözleşmesi'nin düzenlemesiyle uyum sağlanarak, siber ortamda aldatıcı, yanıltıcı, istismar edici, mal ve can güvenliğini tehlikeye atıcı reklamlara karşı düzenlemeler getirilmeli özellikle kasten can ve mal güvenliğini tehlikeye atıcı reklamların üretilmesi ve internet üzerinden yayınlaması suç haline getirilmelidir (Ünver, 2001).

Siber alanda yer alan kişilerin cezai sorumluluklarına ilişkin olarak mutlaka düzenleme yapılmalıdır. Bugün için ülkemizde bu konuda tam anlamıyla yasal bir boşluk bulunmakta suç ve failler ortaya çıkarılsa dahi yasal boşluk nedeniyle bu kişilere ceza verilememektedir. Ancak bu düzenlemeler yapılırken düşünce özgürlüğüne ilişkin evrensel ilkeler göz önünde bulundurulmalı, özellikle AİHS'nin 10. maddesinde yer alan "ifade özgürlüğü hakkı" ve aynı maddenin 2. fıkrasında yer alan bu hakkın sınırlanabildiği haller çerçevesinde düzenleme yapılmalıdır. Siber alanda yer alan kişilerin cezai sorumluluklarının belirlenmesi düşünce özgürlüğüne ket vurulması anlamını taşımamalıdır (Ünver, 2001).

Ayrıca, ayrı bir yasada internet kişileri olan internet servis sağlayıcıların, erişim sağlayıcıların ve içerik sağlayıcıların ceza hukuku açısından sorumlulukları ayrı ayrı ele alınmalı; içerik sağlayıcılar, basın kuruluşları ya da internette gazetecilik alanında faaliyet gösteren kuruluşlar olabileceği için bunların sorumlulukları bireylerin haber alma hakkı engellenmeyecek şekilde düzenleme yoluna gidilmelidir (Dülger, 2004).

İnternet kişilerinin hukuksal sorumlulukları düzenlenirken veri iletim ağlarıyla sanal basın olarak hareket eden sitelerle kişilerin oluşturduğu ve sanal yayın yapma amacı gütmeyen siteler arasında ayrım yapılmalıdır. Örneğin bir forum odasını yöneten site sahibinin bu siteye gelen yazıları denetlemek ve hepsini okumak gibi bir görevi

yoktur, böyle bir görev yasayla da yaratılmamalıdır; bu nedenle site sahibi siteye gönderilen yazıların suç içermesi halinde söz konusu yazılardan dolayı sorumlu tutulmamalıdır. Bu ayrım gözetilerek bir düzenleme yapılmalıdır (Dülger, 2004).

Bilişim suçlarıyla mücadelede maddi ceza hukukunun ve ceza muhakemesi hukukunun birlikte ele alınmasıyla bir sonuç elde edilmesi mümkündür. Bilişim suçlarının özelliği dolayısıyla uluslararası nitelikte olması, suçun işlendiği yer bakımından sorunların çıkmasına bu da suçun kovuşturmasının nerede yapılacağı sorununa yol açmaktadır. Bu sorunların aşılması ancak uluslararası işbirliğine işlerlik kazandırılmasıyla mümkün olacaktır. Avrupa Konseyi Siber Suç Sözleşmesi'nde bu konuda ayrıntılı düzenlemeler bulunmaktadır. Bu sözleşmeye ülkemiz tarafından da taraf olunması ve 5237 sayılı TCK'nın suçun işlendiği yer konusuna ilişkin maddelerinde bu sözleşmeye paralel gerekli düzenlemelerin yapılmasıyla bu sorunun aşılması mümkün olabilecektir (Sınar, 2004).

Bilişim sistemleri kullanılarak veri iletim ağları üzerinden kişilik haklarına saldırıda bulunulması durumunda özellikle internet aracılığıyla hakaret etme ve sövme cürümleri akla gelmektedir. Bu eylemlerin internet aracılığıyla yapılması çok kısa zamanda çok fazla sayıda kişinin bilgisine ulaşmasını sağlamaktadır, ayrıca özellikle haber siteleri ya da forum alanlarında bu eylemlerin gerçekleştirilmesi halinde bu eylemin sonuçlarını giderici önlemler Basın Kanunu'nda basılı eserlerde olduğu gibi internet açısından bulunmamaktadır. Bu nedenlerle hem bu alana ilişkin önlemler düzenlenmeli hem de siber alanda, özellikle de internette hakaret, sövme, tehdit ve haberleşme özgürlüğünün ihlali gibi suçların islenmesinde bu alanının kullanılması ağırlatıcı bir neden olarak kabul edilmeli ve bu düzenlemeler ile mevcut bilişim suçları arasında ortaya çıkabilecek suçların içtimaı sorunları açık düzenlemelerle çözülmelidir (Karaoğlu, 2004).

Bilişim suçlarıyla ilgili olarak yapılması gereken önemli bir düzenleme de çocukların siber alanda ticari amaçla cinsel istismarının bağımsız bir suç tipi haline getirilmesidir (Ünver, 2001). Çocukların anne-babaları, veli-vasi gibi kişilerce zorlanarak pornografik resim, film gibi materyallere konu edilmesi ve bunların

internet üzerinden pazarlanması ve alınması suç tipi haline getirilmelidir. Ayrıca her türlü çocuk pornografisi içeren materyalin bilişim sistemlerinde bulundurulması, bunların paylaşıma açılması, iletilmesi ve kullanılması suç tipi olarak düzenlenmelidir. Bu eylemlerin suç haline getirilmesinin çok acil şekilde yapılması gerekmesine rağmen TCK' da buna ilişkin düzenleme olan 226. madde bu açıdan son derece yetersizdir (Dülger, 2004). Bu eylemlerin neler olduğu Avrupa Siber Suç Sözleşmesinde tek tek açıklanmıştır.

4.1.3. 5809 sayılı Elektronik Haberleşme Kanunu

10 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun "İlkeler" kenar başlıklı 4 üncü maddesinin (l) bendinde, "İlgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi ilkesi" yer almaktadır.

Elektronik Haberleşme Kanunu ile Bilgi Teknolojileri ve İletişim Kurumu'na; bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, izinsiz erişime karşı şebeke güvenliğinin sağlanması, kişisel veri ve gizliliğin korunması ve elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması görevleri verilmiştir.

4.1.4. 5651 sayılı kanun

1993 yılında İnternet ağına dâhil olan Türkiye, 2001 yılına kadar İnternete önemli bir müdahalede bulunmamıştır. Ancak İnternetin kullanım oranlarının ve buna bağlı olarak sosyal etkilerinin hızla artmasıyla birlikte İnternette yer alan hukuka aykırı ve zararlı içeriğe karşı duyarsız kalmamıştır. 2001 yılından itibaren çeşitli sebeplerle bazı web sitelerinin erişimi engellemiştir. Bu dönemde gerçekleştirilen erişim engellemelerinin İnternet içeriğine müdahale yetkisi veren özel bir kanuna dayanmayışı ve yalnızca genel hükümlerle gerçekleştirilmesi birtakım hukuki tartışmalara yol açmıştır. Mevcut gereklilik ve eleştiriler göz önünde bulundurularak

2007 yılında İnternet içerik politikası hukuki bir zemine oturtulmak istenmiş ve artan bilişim suçlarıyla etkin bir şekilde mücadele etmek amacıyla 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" yürürlüğe koyulmuştur (Keser Berber ve Kaya, 2010).

5651 sayılı Kanun ilk olarak Youtube web sitesinin engellenmesiyle gündeme gelmiştir. Bu siteyi binlerce web sitesinin engellenmesinin takip etmesi, kanunun bir sansür kanunu olarak algılanmasına yol açmıştır. Kanunun içerik, yer, erişim ve toplu kullanım sağlayıcılara ilişkin getirmiş olduğu sınırlayıcı düzenlemeler bu görüşü güçlendirmiştir (Keser Berber ve Kaya, 2010).

4 Mayıs 2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin usul ve esaslar düzenlenmiştir. Kanun kapsamında İnternet ortamında yapılan intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama, 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlara yönelik yayınlara erişimin engellenmesi kararı verilebilmektedir (Turhan, 2010).

Keser Berber ve Kaya (2010), 5651 sayılı Kanuna bazı eleştiriler getirmiştir. Buna göre;

5651 sayılı Kanun'un istenmeyen İnternet içeriğine müdahale etmek için tercih ettiği erişimin engellenmesi yönteminin hukuki olarak hem ölçülülük ilkesi hem de ceza sorumluluğun şahsiliği ilkesine aykırılıklar oluşturduğu dile getirilmektedir.

Ölçülülük ilkesi, sınırlamada başvurulan aracın sınırlama amacını gerçekleştirmeye elverişli olmasını, bu aracın sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçüsüz bir oran içinde bulunmamasıdır. Kanun gerekçesinde açıklandığı üzere 5651 sayılı Kanun, aileyi, çocukları ve gençleri İnternet dâhil elektronik iletişim araçlarının kötüye kullanılmasıyla uyuşturucu ve uyarıcı madde alışkanlığı, intihara yönlendirme, cinsel istismar, kumar ve benzeri kötü alışkanlıkları teşvik eden içerikten korumak amacıyla hazırlanmıştır. Bu amaca ulaşmak için 5651 sayılı Kanunun öngördüğü araç erişim engellemedir. Bu aracın Kanunun öngördüğü amaca ulaşmak için elverişli, zorunlu ve orantılı olmadığı eleştirisi getirilmektedir.

Türk Ceza Kanunu'nun 20. maddesi ceza sorumluluğunun şahsi olduğunu ve kimsenin başkasının fiilinden dolayı sorumlu tutulamayacağını öngörmektedir. IP ve DNS engellemesi teknikleri kullanılarak yapılan erişimin engellenmesinin bu ilkeyi ihlal ettiği öne sürülmektedir.

Ayrıca erişim engellemesi uygulamasının ifade hürriyetini ihlal ettiği, hakkaniyete, ölçülülük ilkesine ve ceza sorumluluğunun şahsiliğine aykırılık teşkil eden bu yöntemlerden bir an evvel vazgeçilmesi gerektiği, bunun yerine hukuka aykırı ve zararlı içerik arasındaki ayrımın Kanun'da kesin olarak yapılarak, hukuka aykırı ve zararlı içerik için ayrı yaptırımların uygulanması gerektiği görüşleri dile getirilmektedir.

4.1.5. 5070 sayılı Elektronik İmza Kanunu

23 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esaslar düzenlenmekte ve elektronik imzanın hukukî yapısı, elektronik sertifika hizmet sağlayıcılarının faaliyetleri ve elektronik imzanın kullanımına ilişkin hükümler yer almaktadır.

Kanunun 5 inci maddesi ile güvenli elektronik imzanın elle atılan ıslak imza ile aynı hukukî sonucu doğuracağı fakat kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmelerinin güvenli elektronik imza ile

gerçekleştirilemeyeceği hüküm altına alınmıştır. Bu doğrultuda, örneğin tapu devrini sağlayan sözleşmeler, araç satışları, mal rejimi sözleşmeleri, vasiyet gibi sözleşmeler, evlenme gibi işlemler elektronik imza ile yapılamamaktadır (Ergün, 2008).

Ayrıca Kanunun 16 ncı maddesinde imza oluşturma verisinin veya aracının ilgilinin rızası dışında elde edilmesi, verilmesi, kopyalanması, bu araçların yeniden oluşturulması, izinsiz elde edilen araçların kullanılması suretiyle izinsiz elektronik imza oluşturulması eylemleri, 17 nci maddesinde ise elektronik sertifikalarda sahtekârlık işlemleri suç olarak düzenlenmiştir (Turhan, 2010).

4.1.6. Türkiye'de kişisel verilerin korunmasına ilişkin düzenlemeler

Türkiye'de kişisel verileri korumayı amaçlayan özel kanuni bir düzenleme henüz yoktur. Ancak, 12 Eylül 2010 tarihindeki Anayasa değişikliği ile Anayasanın 20. maddesine konuyla ilgili bir fıkra eklenmiş ve tarafı olduğumuz Avrupa İnsan Hakları Sözleşmesinin ilgili hükümleri ile birlikte kişisel verilerin korunmasını isteme hakkı, temel hak ve özgürlüklerden birisi olarak Anayasal güvence altına alınmıştır.

Ülkemiz, uluslararası alanda kişisel verileri korumayı amaçlayan 1981 tarihli Avrupa Anlaşmasını imzalamış olmasına rağmen uygunluk kararnamesi henüz imzalanmadığı için söz konusu anlaşma henüz yürürlüğe girmemiştir. Özel bir kanun olmamasına rağmen kişisel verilerin korunması, Türk Medeni Kanunu ve Türk Anayasasında belirtilen ilkeler doğrultusunda gerçekleştirilebilmektedir.

Türkiye'de veri koruması alanında kanunlaştırma hareketi, Avrupa Birliği müktesebatına uyum çerçevesinde Adalet Bakanlığı tarafından kişisel verilerin korunması ile ilgili bir kanun tasarısı ile başlamıştır. Kişisel Verilerin Korunması Kanunu (KVKK) Tasarısına genel olarak bakıldığında, 108 no'lu Avrupa Konseyinin Kişisel Verilerin Korunması Sözleşmesi ve 1995/46 sayılı Avrupa Birliği Veri Koruma Direktifinin temel alındığı görülmektedir. Tasarı Bakanlar Kurulunca 07. 04. 2008 tarihinde kabul edilerek TBMM Başkanlığına gönderilmiştir. Avrupa

Birliği Uyum Tali Komisyonundan geçen tasarı, Adalet Komisyonunda beklemektedir.

Tasarı; kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerinin korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usullerin düzenlenmesini amaçlamaktadır.

KVKK Tasarısı, genel nitelikte hükümler içermekte ve veri korumaya ilişkin sektörel nitelikteki düzenleme ihtiyaçlarını ise bu çerçeveye bağlı kalacak şekilde, ilgili kurum, kuruluş ve meslek birliklerine bırakmayı tercih etmektedir.

Tasarı, kişisel verileri işleme tabi tutulan kişiler ile bu verileri işleme tabi tutan kamu kurum ve kuruluşları ile gerçek ve özel hukuk tüzel kişilerini kapsamaktadır. Söz konusu kişisel veriler, geleneksel dosyalama yöntemiyle işlemede olduğu gibi, otomatik işlemeye tabi tutulduklarında da bu Kanun çerçevesindeki ilke ve kurallara tabi olacaklar; verileri işlenenler ise bu Kanun çerçevesinde çeşitli haklarını kullanabileceklerdir. Kişisel verilerin, kamu kuruluşlarınca, gerçek veya özel hukuk tüzel kişileri tarafından işlenmesi dolayısıyla kişilik hakları ihlal edilenlerin şikâyetleri konusunda Kişisel Verileri Koruma Kurulu karar verecektir. Kişilik hakları ihlal edilen bireyin tazminat hakları ise saklı tutulmuştur. Tasarıda, ihlalin ağırlık derecesine göre idari para cezaları ile ayrıca hapis ve para cezaları öngörülmektedir.

KVKK Tasarısı beş kısımdan oluşmaktadır:
Birinci kısımda (m.1-10); Tasarının amaç ve kapsamı belirlenmiş ve Tasarıda kullanılan terimlerin tanımları yapılmış, kişisel verilerin niteliğine ilişkin ilkeler, kişisel verilerin işlenmesinde hukuka uygunluk sebepleri, özel niteliği olan kişisel veriler ve kişisel verilerin kamu kurum ve kuruluşları tarafından işlenmesi konuları düzenlenmiştir.

İkinci kısımda (m.11-15); veri işleyenlere (veri kütüğü sahibi) verisi işlenen gerçek veya tüzel kişileri aydınlatma yükümlülüğü yüklenmekte ve verisi işlenen gerçek ve tüzel kişilerin hakları ile yurtdışına veri aktarımına ilişkin hususlar belirlenmektedir.

Üçüncü Kısımda ise (m.16-25); Sicil ve Kurula bildirim ve ön inceleme konuları ile özel denetim kuruluşları, istisna getiren hükümler, mesleki davranış kuralları, kişisel verilerin silinmesi ve yok edilmesi konuları düzenlenmektedir.

Dördüncü Kısımda (m.26-33); "Kişisel Verileri Koruma Kurulu"nun oluşumu ile Kurulun yetki ve görevlerine,

Beşinci Kısımda (m.34-39) ise; kişisel verilerin hukuka aykırı olarak işlenmesi durumunda izlenecek soruşturma ve kovuşturma esasları ile uygulanacak idari para cezaları ile hapis ve para cezasına yer verilmektedir.

4.1.7. Ülkemizin Siber Suç Sözleşmesini İmzalama Süreci

23 Ekim 2008 tarihinde Adalet Bakanlığı ve Türkiye Bilişim Derneği'nce Bolu-Abant'ta düzenlenen Siber Suçlar Sözleşmesi konulu seminer sonucu olarak Sözleşme'nin bir an önce imzalanmasının Türkiye'nin diğer ülkelerle etkin bir biçimde işbirliği içinde olması için gerekli olduğunu sonucu basınla paylaşılmıştır (Cihan, 2008).

20-22 Nisan 2010 tarihleri arasında turk.internet.com ve Ankara Barosu işbirliği ile Kocaeli - Kartepe'de düzenlenen 2.İnternet İçerik Düzenleme Çalıştayı'nın sonunda yapılan çalışmalar çerçevesinde hazırlanan "Kartepe Kriterleri" yayınlanmıştır. On üç ilkenin sıralandığı sonuç bildirgesindeki ilkelerden biri de "Bir internet sitesinin tamamına erişimi engellemek yerine, sadece zararlı ve hukuka aykırı içeriklerin engellenmesi yoluna gidilmesi ve bu içerikleri oluşturanların yargılanması sağlanmalıdır. İnternetin uluslararası karakteri göz önüne alınarak diğer ülkelerle işbirliğine gidilmeli, Avrupa Konseyi Siber Suçlar Sözleşmesi imzalanması konusunda çalışmalar hızlandırılmalıdır." şeklinde olmuştur (Hukuki.net, 2010).

10 Kasım 2010 tarihinde Avrupa Konseyi Bakanlar Komitesi Dönem Başkanlığı'nı devralan Dışişleri Bakanı Ahmet Davutoğlu tarafından Sözleşme imzalanmış ve Sözleşmenin onay süreci başlatılmıştır. Bu bağlamda ilgili kurumlar olan Adalet Bakanlığı, İçişleri Bakanlığı, Dışişleri Bakanlığı ve Bilgi Teknolojileri ve İletişim Kurumu'nun temsilcilerinin katılımıyla sözleşmede çekince konulacak ve bildirimde bulunulacak hususların belirlenmesi için çalışmalar devam etmektedir.

Ayrıca Türkiye, Avrupa Konseyi Siber Suç Sözleşmesini imzalamış olmasına rağmen dış politikamızda gözetilen dengeler ve ifade özgürlüğünün kısıtlanması gibi temel nedenlerden ötürü Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesine Ek Protokolü imzalamamıştır.

4.1.6.1.Avrupa Konseyi Siber Suç Sözleşmesi hakkında çekinceler

Siber Suçlar Sözleşmesi, yaklaşık dört yıl süren uzun bir çalışmanın ve birçok taslak metnin sonucu olarak ortaya konulmasına rağmen, gerek sivil toplum kuruluşlarından gerekse ilgili sektörlerden gelen ağır eleştirilere maruz kalmıştır. Bu eleştirilerin odaklandığı noktalar, soruşturma ve araştırma faaliyetlerinin yürütülmesi ile ilgili hükümlerin uluslararası insan hakları belgelerinde çizilen çerçeveyi ihlal etmesi, servis sağlayıcılarına ağır mali ve sosyal sonuçları olan yükümlülükler getirilmesi, sivil toplum örgütlerinin sözleşmenin hazırlık süreci içerisinde yeterli ölçüde görüşlerinin alınmaması noktalarında toplanmaktadır (Türkiye 1. Bilişim Şurası, 2002).

Örneğin sözleşmenin "Şartlar ve Koruma Tedbirleri" başlığını taşıyan 15. maddesinin 2. Fıkrasında "...adli ya da başka nitelikli gözetim..." kavramından bahsedilmektedir. Bu madde ile gerçekleştirilecek faaliyetler özel hayata ve iletişimin gizliliğine müdahale oluşturduğundan, ilke olarak hâkim kararının aranması gerektiğinin vurgulanması uygun olacaktır.

Sözleşmenin 20. maddesi Trafik bilgilerinin gerçek zamanlı olarak toplanması ve 21. maddesi İçerikle İlgili Bilgilere Müdahale Edilmesi başlıklarını taşımaktadır. Her iki madde de, yeterli gizlilik ve güvenlik sağlanmadığı takdirde insan haklarını ciddi şekilde ihlal edebilme tehlikesini taşımaktadır.

Sözleşmenin 19. ve 20. maddelerinin somut suç şüphesi ve hâkim kararı kriterlerine yer vermemesi, iletişim özgürlüğü ve özel hayata saygı ilkelerine açık aykırılık teşkil etmektedir.

Yine, sözleşmenin ulusal egemenliği tehdit eden 32. maddesinde bir ülkenin diğer ülkenin izni olmadan o ülkenin sınırları içerisinde saklanan bilgisayar verilerine erişiminden söz edilmektedir. Maddede "kullanımı herkese açık olan kaynaktan gelen" veya "yetkili kişinin hukuki izni alınarak" erişimden söz edilmekteyse de, vatandaşın kişisel verilerine erişim ve iletişiminin denetlenmesi yerel yargı otoritelerinin tekelinde olan bir durumdur. Devletin yargı yetkisi münhasır ve devredilemez bir yetkidir. Devletin ulusal sınırları içerisinde başka bir devletin o devletin izni olmadan doğrudan doğruya yargı yetkisini kullanması, ulusal egemenliğin ve bağımsızlığın ihlali anlamına gelmektedir. Anılan nedenlerden dolayı sözleşmenin bu maddesinin kabul edilemez nitelikte olduğu düşünülmelidir (Türkiye 1. Bilişim Şurası, 2002).

Ayrıca, sözleşmenin hazırlık aşamasında şeffaflık ve açıklık ilkelerine yer verilmediği, ilk taslak 2000 yılında yayınlandığında bu taslağa birçok eleştiri ve birçok katkı yapma isteği yöneltildiği halde sözleşmenin son hali itibariyle bu eleştiri ve katkıların dikkate alınmadığı, sözleşmenin metninin açık olmadığı ve açıklayıcı metinde de söz konusu boşluğun giderilmediği, sözleşmenin 1981 tarihli Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme ile uyumluluk göstermediği, kişisel verilerin korunması konusuna önem verilmediği, sözleşmenin Avrupa İnsan Hakları Sözleşmesi ile uyum içerisinde olmadığı, temel kişilik haklarına saygı gösterilmediği eleştirileri yapılmaktadır. Ayrıca, Sözleşmenin önsözünde temel insan haklarına saygı ile kanun uygulayıcıları (kolluk kuvvetleri)

arasındaki dengeden söz edilmesine rağmen, sözleşmenin içeriğinde bu dengenin kolluk kuvvetleri lehine bozulduğunun görüldüğü belirtilmektedir (Akdeniz, 2008).

Sözleşmede ön plana çıkan noktanın usule ilişkin hükümler olduğu ve siber suçların bir bölümünün dışında genel olarak siber suçlarla mücadelede kullanılan yetki ve prosedürlere yer verildiği belirtilmektedir.

4.2.Polisiye Boyut

Siber suçlarla mücadelede polisiye yöntemler konusunda ülkemizde İçişleri Bakanlığına bağlı Emniyet Genel Müdürlüğü bünyesinde çalışmalar yürütülmektedir.

Bilişim Suçları ve Sistemleri Şube Müdürlüğü; Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde 2003 yılında kurulmuştur. Bilişim suçları ile mücadele konusunda oldukça fazla tecrübeye sahip olan Şube Müdürlüğü geçmiş tarihlerde taşra teşkilatında ki yapılanması ile birlikte birçok başarılı operasyonlara imza atmış ve bilişim suçları konusunda oluşabilecek boşluğu doldurmaya çalışmıştır. Aynı zamanda Adli Bilişim konusunda uzman personel eğitimine önem vermiş ve 15 bölge merkezinde kurulan Adli Bilişim Büro Amirlikleri sayesinde Türkiye için önemli bir alan olan Adli Bilişim konusunda ihtiyaca cevap vermeye başlamıştır. Siber suçlar ile mücadelenin etkinleştirilmesi için 2007 Nisan ayı itibari ile bahse konu suçların yoğun olarak işlenildiği İstanbul İl Emniyet Müdürlüğü bünyesinde Bilişim Suçları ve Sistemleri Şube Müdürlüğü, diğer 80 ilimizde Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlükleri bünyesinde Bilişim Suçları Büro Amirlikleri kurulmuştur. Ayrıca 08.09.2010 tarihi itibariyle Bilişim Suçları ve Sistemleri Şube Müdürlüğü ikiye bölünerek Bilişim Suçlarıyla Mücadele Şube Müdürlüğü kurulmuş ve işi sadece bilişim suçu olan bir birim haline gelmiştir. Şube Müdürlüğünün görevleri şu şekilde sıralanabilir (KOM, 2007);

- 5237 sayılı Kanunun 243 üncü ve 244 üncü maddelerinde belirtilen suçlarla mücadele etmek ve bu kanunlarda belirtilen diğer suçların işlenmesi

durumunda gerekli çalışmayı yapmak veya gerektiğinde ilgili kurum ve kuruluşlara teknik destek vermek,

- Bilişim sistemleri yoluyla işlenen 5237 sayılı Kanunun 245 inci maddesinin birinci, ikinci ve üçüncü fıkrasında yer alan görev alanına giren suçlarla mücadele etmek,
- 5070 sayılı Elektronik İmza Kanununun 16 ve 17 nci maddelerini kapsayan suçlarla mücadele etmek,
- 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 23 üncü maddesi kapsamındaki suçlarla mücadele etmek,
- Görev alanına giren konularda İl KOM Birimleri tarafından yürütülen mücadeleyi yönlendirmek, çalışmalarla ilgili eksikliklerin giderilmesi için girişimlerde bulunmak,
- Görev alanına giren konularda, Başkanlıkça belirlenen kriterler, ikili ve uluslararası anlaşmalar ile ulusal mevzuat çerçevesinde yabancı ülke makamlarından veya irtibat görevlilerinden gelen talepleri değerlendirmek ve gerekli işlemleri yürütmek,
- Görev alanına giren konularda mevzuat çerçevesinde ulusal veya uluslararası kuruluş faaliyetlerine katılmak ve sonucunda Başkanlığa rapor sunmak,
- Görev alanına giren konularda idari ve hukuki eksikliklerin giderilmesi ve geliştirilmesi yönünde görüş ve önerilerde bulunmak,
- Başkanlık ve İl KOM Birimlerinde karşılaşılan bilişim sistemleriyle ilgili her türlü problemleri çözüme kavuşturabilmek için gerekli alt yapı ve tespit edilen projelerle ilgili analiz çalışmaları yapmak ve uygun çözümleri ortaya koymak,
- Bilişim Suçları veya diğer operasyonel birimlerine Adli Bilişim hizmeti vermektir.

Son yıllarda ülke genelinde artan internet kullanımı, gelişen bilgisayar teknolojisi ve programlama dilleri nedeniyle özellikle siber ortamda dolandırıcılık suçlarında artış gözlemlenmektedir. EGM Teşkilatı, bilişim suçlarının önlenmesine doğrudan veya dolaylı katkı sağlayabilecek kişi ve kuruluşlarla işbirliği yaparak, dünya

standartlarında uygulanan yeni teknolojileri kullanarak suç ve faillerinin tespit edilmesi ve yakalanmasına önem vermektedir (EGM, 2011).

Emniyet Genel Müdürlüğü, Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı verilerine göre 2009-2010 yılları arasında siber suçlara ilişkin olay ve yakalanan şüpheli sayıları Tablo 4.1'de verilmektedir. Buna göre 2010 yılında 2009 yılına göre bilişim suçları ve sistemleri dolandırıcılığı suçunda artış gözlenmiştir. Buna karşın, Bankacılık Düzenleme ve Denetleme Kurulu (BDDK) tarafından internet bankacılığında SMS şifre kullanımının zorunlu hale getirilmesi ile interaktif banka dolandırıcılığı ve internet aracılığıyla dolandırıcılık suçlarının olay ve yakalanan şüpheli sayısında meydana gelen düşüş dikkat çekmektedir.

Tablo 4.1 Suç türlerine göre olay ve yakalanan şüpheli sayıları

SUÇ UNSURU	2009		2010	
	Olay Sayısı	Yakalanan Şüpheli	Olay Sayısı	Yakalanan Şüpheli
Kredi Kartı Sahteciliği ve Dolandırıcılığı	1511	2176	1131	1005
İnteraktif Banka Dolandırıcılığı	550	1113	151	300
Bilişim Suçları ve Sistemleri Dolandırıcılığı	353	534	972	1346
İnternet Aracılığıyla Dolandırıcılık	412	731	71	115
Diğer	45	116	28	134
TOPLAM	2871	4670	2353	2900

Kaynak: EGM, 2011

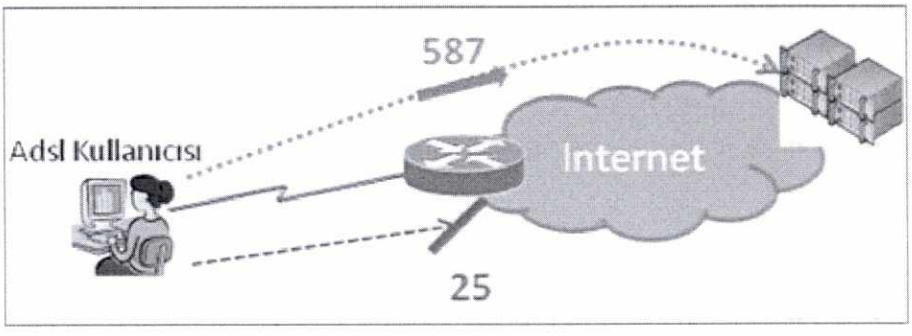
4.3.Teknik Boyut

Ülkemizde Bilgi Teknolojileri ve İletişim Kurumu (BTK) ITU nezdinde ülkemizi temsil eden kurum olması, 5809 sayılı Elektronik Haberleşme Kanunu ile kendisine verilen bilgi, şebeke ve haberleşme güvenliği ile ilgili görevleri dolayısıyla düzenleme faaliyetlerinden farkındalık oluşturma etkinliklerine kadar siber güvenliğin sağlanması ile ilgili çalışmalar yapmaktadır. Bu bağlamda BTK bünyesinde yapılan çalışmalar aşağıda incelenmiştir.

4.3.1.Spam ile mücadele projesi

Spam e-posta gönderimi yaygın olarak ADSL kullanıcılarının bilgisayarlarından mesaj gönderilmek istenen sunucuya doğru 25. port üzerinden bağlanarak yapılmaktadır. Dünyada operatörler tarafından en yaygın kullanılan çözüm Şekil 4.1'de görüldüğü gibi, dinamik IP'li müşterilerin 25. portunun kapatılıp e-posta göndermelerini engelleyerek gerçek e-posta kullanıcıların güvenli başka bir porttan göndermelerini sağlamaktır. Bu yöntem uygulandığında dinamik IP bloklarından gönderilen Spam mesajları azaldığından, Spam mesajların kimlik tespiti ilgili servis sağlayıcı tarafından daha kolay yapılabilmektedir.

Şekil 4.1 Spam ile mücadele projesi



Kaynak: TTNET, 2009

"Spam ile Mücadele Projesi" BTK tarafından 2009 yılı içinde geliştirip uygulanan; TTNET, Çizgi Telekom, Doruknet ve Mynet başta olmak üzere çok sayıda işletmecinin katılımı ve katkılarıyla gerçekleştirilen bir projedir.

Proje ile kimlik doğrulamalı e-posta gönderimine geçiş için, dinamik IP'li kullanıcıların e-posta göndermek için kullandıkları 25. port bloklanıp, kullanıcıların e-posta istemci yazılımları (outlook express gibi) üzerinde "authenticated/kimlik doğrulamalı SMTP" seçeneklerini aktive ederek 587. Port üzerinden e-posta göndermeleri istenmiştir. Proje öncelikle pilot olarak Aydın, Bayburt, Diyarbakır, Giresun, Gümüşhane, Ordu, Rize, Sivas, Tokat, Trabzon illerinde uygulanmış, bu illerde başarılı olunmasının ardından tüm Türkiye genelinde 3 faz halinde yaygınlaştırılmıştır.

Proje sonucunda TTNET'in dünyaya yaydığı günlük spam mesaj sayısı 6.5 milyar düzeyinden 400 milyon düzeyine inmiş ve ülkemiz en çok spam yayan ülkeler sıralamasında oldukça alt sıralara düşmüştür.

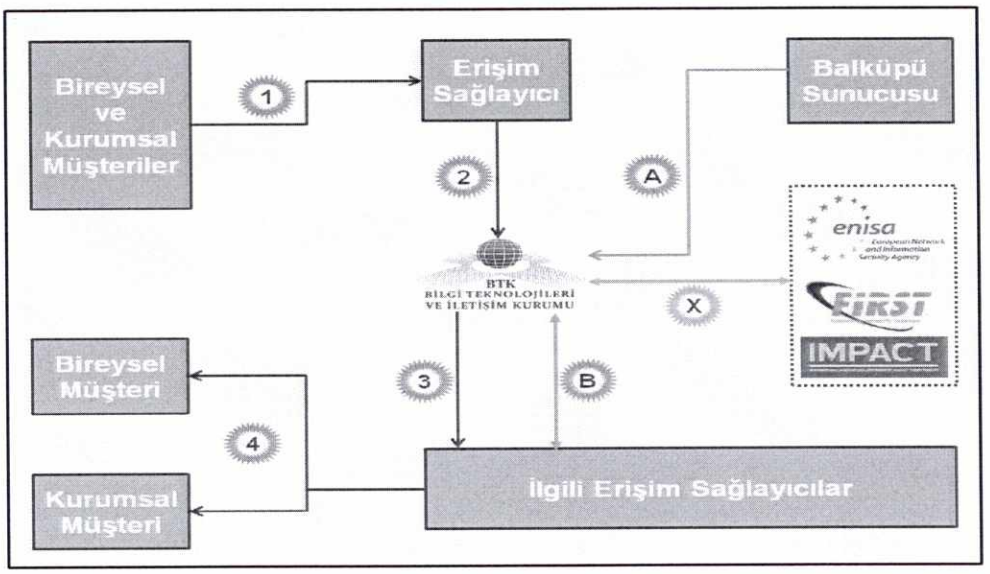
4.3.2.Kötücül yazılımlarla mücadele pilot projesi (KYMP)

Kötücül yazılımlar kullanılarak gerçekleştirilen saldırıların ve oluşan tehditlerin dünyada olduğu gibi ülkemizde de hızla artması nedeniyle bu tür yazılımlarla mücadele edilmesi gereklidir. Kötücül yazılımlarla mücadele konusunda; kötücül içerik yayan veya buna aracılık eden kullanıcıların IP bilgileri tespit edilse dahi; idari, teknik ve hukuki belirsizliklerden ötürü İSS'ler, gerekli önlemlerin alınması konusunda yetersiz kaldıklarından, Kötücül Yazılımlarla Mücadele Projesi BTK tarafından başlatılmıştır.

Bu çerçevede, 13 Mayıs 2010 tarihinde 120 erişim sağlayıcının davet edildiği bir toplantı ile projenin tanıtımı yapılmış ve erişim sağlayıcıların pilot projeye ilişkin görüşlerini bildirmeleri ve gönüllü olarak katılım sağlamaları talep edilmiştir.

Projenin Şekil 4.2'deki çalışma şeması esas alınarak uygulamaya geçirilmesi planlanmıştır.

Şekil 4.2 KYMP çalışma şeması



Kaynak: BTK, 2010

Şekil 4.2'deki adımlarda aşağıdaki işlemler gerçekleşecektir:

1	Saldırıya uğrayan müşteri hizmet aldığı erişim sağlayıcıya başvurur ve saldırıda bulunan IP adreslerini verir.
2	Erişim sağlayıcı, sistemlerindeki ilgili trafik hacmine bakarak saldırı olasılığını teyit eder. Erişim sağlayıcı, • Müşterilerinden aldığı ve teyit ettiği saldırgan IP adreslerini, • Kendisine bir saldırı yapılmışsa saldıran IP adreslerini, • Herhangi bir yolla edindiği saldırgan IP adreslerini BTK'ya iletir.
3	BTK, kendisine iletilen IP adreslerini erişim sağlayıcılara göre ayrıştırır ve bu IP adreslerinden bir saldırı gerçekleştirilme olasılığı olduğu bilgisi ile IP adreslerini ilgili erişim sağlayıcılara iletir. Saldırgan IP adresinin yurtdışından olması halinde BTK bu IP adreslerini yurtdışı çıkışı olan erişim sağlayıcılara iletir.

4	Erişim sağlayıcılar kendilerine iletilen IP adreslerinin tahsisli olduğu müşteriler; • Kurumsal müşteri ise; bu kurumsal müşterinin temas noktasını saldırı gerçekleştirmekte olabilecekleri konusunda bilgilendirir ve tedbir almaya davet eder. • Bireysel müşteri ise; internet bağlantılarını anlık olarak keser ve bu müşteriler internete tekrar bağlandıklarında onları uyarıcı bilgilerin yer aldığı bir internet sayfasına yönlendirir. Yurtdışı çıkışı olan erişim sağlayıcılar kendilerine bildirilen saldırgan IP adreslerinden gelen yurtdışı trafiğini bloke ederler. Yurtdışı bağlantısı olan erişim sağlayıcılar gerekli tedbirleri aldıktan sonra gelen yurtdışı trafiğini engelledikleri saldırgan IP adreslerinin bloklamasını kaldırırlar ve konu ile ilgili olarak BTK'yı bilgilendirirler.
A	Gönüllü erişim sağlayıcılar, kurduğu balküpleri ile köle bilgisayar ağlarının sunucularını belirlemeye olanak sağlayan "bot" yazılımlarını elde ederler ve KBA'ya dâhil olurlar. Elde edilen "bot" yazılımları inceleyen gönüllü erişim sağlayıcılar, köle bilgisayar ağının K&K merkezine erişim sağlayacak bilgilere erişirler.
B	Gönüllü erişim sağlayıcılar eriştikleri bilgileri BTK'ya iletir. BTK bu bilgileri gerekli tedbirleri almaları için erişim sağlayıcılara iletir.
X	BTK, kötücül yazılımlarla mücadele eden ENISA, IMPACT ve FIRST gibi uluslar arası kuruluşlarla işbirliği içinde çalışarak karşılıklı bilgi paylaşımında bulunur.

Proje ile birlikte BTK, kötücül yazılımlarla mücadele eden uluslar arası kuruluşlardan olan IMPACT'e üye olmuştur. Ayrıca, projenin geldiği aşama itibariyle İSS'ler ile bilgi alışverişinde bulunmak maksadıyla TİB bünyesinde oluşturulan platformun test edilme çalışmaları devam etmektedir.

4.3.3. Ulusal Siber Güvenlik Tatbikatı (USGT-2011)

Katılımcı kurumları siber tehditlere karşı alınması gereken önlemler ve olası saldırılar karşısında verilmesi gereken tepkiler konusunda bilgilendirmeyi ve siber güvenlik bilincinin ülke genelinde artırılmasını sağlamayı amaçlayan Ulusal Siber Güvenlik Tatbikatı (USGT), BTK ve TÜBİTAK BİLGEM işbirliğiyle 25-28 Ocak 2011 tarihleri arasında gerçekleştirilmiştir.

Ulusal Siber Güvenlik Tatbikatı; finans, elektronik haberleşme, eğitim ve savunma sektörleriyle silahlı kuvvetler, adli ve kolluk birimleri ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kurum/kuruluşunun katılımıyla gerçekleştirilmiştir. Tatbikatta katılımcı kurumlardan bilgi güvenliği uzmanı, hukukçu ve iletişim uzmanı statüsündeki 197 kişi görev almıştır.

Tatbikatın ilk iki günlük kısmında gerçek saldırılar uygulanırken, son iki günlük kısmında ise yazılı ortamda olası saldırı senaryoları değerlendirilerek teknik, idari ve hukuki süreçler ele alınmıştır. Tatbikatta; 83 gerçek saldırı, 450'nin üzerinde yazılı senaryo değerlendirilmiştir. Tablo 4.2'de tatbikat kapsamında ele alınan gerçek saldırı ve yazılı senaryo faaliyetleri verilmiştir.

Tablo 4.2 Tatbikatta uygulanan enjeksiyonlar

GERÇEK SALDIRILAR		YAZILI SENARYOLAR
Port taraması	27	Elektrik kesintisi
Dağıtık servis dışı bırakma saldırısı (DDoS)	20	Kurum içinden veri sızdırılması
Web sayfası güvenlik denetimi	25	Web sayfasının ele geçirilmesi
Kayıt dosyası analizi	26	Sosyal mühendislik saldırıları
Toplam	*98*	*Toplam* *33*

Kaynak: BTK, 2011

Tatbikata dair genel bilgilendirme sonuçları tüm katılımcı kurumlarla 28 Ocak 2011 tarihinde düzenlenen "Seçkin Gözlemci Oturumu"nda paylaşıldı. Buna göre; Bilgi Güvenliği Yönetim Sistemi (BGYS) eksikliği, saldırı tespit sistemlerinin ve süreçlerinin yetersizliği, güncel olmayan yazılımlar, sistem yöneticilerinin yetersizliği, kurum içi koordinasyon eksikliği, sistem tasarımı aşamasında güvenliğin ihmal edilmesi, iş sürekliliği planlarının bulunmaması, erişim kontrol politikasının olmaması, web uygulamalarında bulunan açıklar, altyapının yetersiz olması gibi sonuçlar elde edilmiştir.

4.3.4. Güvenli Web / İhbar Web / Güvenli İnternet

Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı tarafından "güvenliweb.org.tr" adı altında bir İnternet sitesi oluşturulmuştur. Çocukları, aileleri ve eğitimcileri bilgilendirmek, bilinçlendirmek; internet'in etkin ve yararlı kullanım metotları yanında, barındırdığı tehlikelere karşı farkındalık oluşturmak ve gerekli önlemleri almaya teşvik etmek, Güvenli Çocuk ile çocukların hem eğlenceli vakit geçirmelerine hem de eğlenirken öğrenmelerine, kişisel becerilerinin gelişmesine katkı sağlayacak ve İnternet dünyasını daha yakından tanımalarına imkân verebilecek materyalleri sunmak gibi temek amaçlar doğrultusunda çalışmalar yapılmaktadır.

Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı tarafından 5651 sayılı kanunda belirtilen intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama suçları ile 25/7/1951 tarihli ve 5816 sayılı "Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun" kapsamındaki suç düzenlemeleri çerçevesinde internetteki zararlı içerik hakkında ihbarların yapılabileceği "ihbarweb.org.tr" adresinden hizmet veren bir İnternet ihbar hattı oluşturulmuştur.

Güvenli İnternet, kullanıcıları internetteki uygunsuz içeriklerden ve zararlı sitelerden koruyan ücretsiz ve kullanımı kolay bir sistemdir. 22.11.2011 tarihi itibariyle

uygulanmaya başlanan Güvenli İnternet Hizmetini almak için internet servis sağlayıcılarına başvurmak gerekmektedir. Aile Profili ve Çocuk Profili olmak üzere iki alternatif profil üzerinden işleyen hizmette istenildiği zaman değişikliğe gidilebilir ya da hizmetti kullanmaktan vazgeçilebilmektedir.

Çocuk Profili; pedagoji, sosyoloji ve psikoloji alanlarında uzman akademisyenlerin bulunduğu bir komisyon tarafından belirlenen kriterlere uygun kategorilerdeki sitelere erişilebilen profildir. Çocuk profili ile eğitim, ödev, bankacılık uygulamaları, alışveriş, müzik-oyun-eğlence, haber, e-posta, resmi ve kamu siteleri, tatil, özel şirketler, eğitim kurumları, e-devlet gibi pek çok farklı türden siteye erişilebilmektedir. Aile Profili; kumar, uyuşturucu, fuhuş, müstehcenlik, şiddet, terör, dolandırıcılık, zararlı yazılım gibi kategorilerdeki siteleri engelleyen profildir. Çocuk profiline ek olarak kişisel sitelere, forum ve paylaşım sitelerine erişim sunmaktadır.

4.3.5.Yayınlar

Siber güvenlik konusunda BTK bünyesinde yayınlar hazırlanıp kamuoyuyla paylaşılarak ulusal kapasite gelişimine ve farkındalığın artırılmasına katkı sağlanması amaçlanmaktadır.

SONUÇ VE ÖNERİLER

Siber suçlar, konumdan ve kimlikten bağımsız olmaları, çok hızlı ve kolay bir şekilde işlenebilmeleri ve suç izlerinin kolayca silinebilmeleri gibi karakteristik özelliklere sahiptir. Bu nedenle siber suçların işlenmesi çoğunlukla derin bir uzmanlık gerektirmezken, bunlarla mücadelede takip, tespit ve soruşturma ciddi uzmanlık ve titiz bir çalışma gerektirmektedir.

Teknoloji baş döndüren bir hızla ilerledikçe siber suçların da çeşitlenerek artması kaçınılmazdır. Bu artış beraberinde siber suçlarla mücadelenin zorlaşmasını da getirecektir. Çünkü teknoloji ilerledikçe siber suçların işlenmesi kolaylaşmaktadır. Üstelik suçlunun belirli bir konuma bağlı kalmadan suçun işlenmesi için geçen zamanı neredeyse saniyeler seviyesine inmesi söz konusudur. Bununla birlikte deliller de hızlıca karartılabilmektedir. Bu nedenle bu suçlarla mücadele edebilmek için aynı oranda güncel ve teknolojik araçlar kullanmak zaruridir. Bu araçlar sadece teknik ve polisiye yöntemlerden oluşmamalı aynı zamanda hukuki yöntemleri de kapsamalıdır.

Siber suçların sınır tanımaz doğası, mücadelede sınır ötesi işbirliğini de zaruri kılmaktadır. Bu nedenle bu suçlarla mücadele için hukuksal, teknik ve polisiye yönden işbirliği halinde çalışılırken tüm bu çalışmaların sadece ulusal düzeyde yapılması da sorunun tam olarak çözülmesini sağlayamamaktadır. Bu bağlamda tüm mücadele yöntemleri uluslararası ilişkilerin doğru yürütülmesi ölçüsünde olumlu neticeler verecektir.

Hazırlanan tez çalışması doğrultusunda Türkiye'de siber suçlarla mücadele konusunda yapılması gereken çalışmalara yönelik değerlendirme ve öneriler tezin bütününde izlenen yol takip edilerek hukuki, polisiye ve teknik olmak üzere üç kısımda değerlendirilecektir.

Hukuki Açıdan Öneriler

Siber suçlar teknolojideki gelişimle birlikte sürekli değişen biçimlerde işlenebilmektedirler. Teknik anlamda alınacak tedbirlerin yanı sıra hukuki mevzuatın da değişen ve yeni ortaya çıkan suç tiplerine uyumlu hale getirilmesi gerekmektedir. Bu nedenle siber suçlarla ilgili düzenlemelerin daha hızlı ve sık aralıklarla güncellenmesi sağlanmalıdır. Bu bağlamda ülkemizde siber güvenlik alanında uluslararası gelişmeleri yakinen takip ederek güncel ve kapsamlı çalışmalar yürüten BTK'nın konu hakkında edinmiş olduğu uzmanlık birikimi de dikkate alınarak hukuki düzenlemelerdeki rolü arttırılmalıdır.

Bu çalışmada incelenen ulusal ve uluslararası uygulamalar göz önüne alındığında, ülkemizde yapılan çalışmalara rağmen, siber suçlarla mücadele, politika ve strateji anlamında kurumların yeterince koordine olamadıkları görülmektedir. Bu eksikliğin giderilmesi ve ortaya genel kabul gören bir strateji belgesi konulması için, hukuki, polisiye ve teknik yöntemlerin birlikte tartışıldığı ortak bir platform kurulmalıdır.

Yakın gelecekte siber suçların ve suçluların artış göstermesi, yeni siber suç tiplerinin ortaya çıkması ile birlikte bilişim hukukuna duyulan ihtiyacın artması kaçınılmaz olduğundan, suçluların tespiti ve cezalandırılması süreçlerinin daha fazla başarı elde edilebilmesi için siber suçlar ve bilişim hukuku alanında hizmet verecek özel ihtisas mahkemeleri kurulmalıdır.

Ülkemizde siber suçların soruşturulması ve kovuşturulması aşamasında usul yönünden eksiklikler olduğundan, söz konusu eksikliklerin giderilmesi için mevzuatta siber suç delillerine el koyma ve adli bilişimle ilgili ayrıntılı hükümler hazırlanmalı ve yürürlüğe konulmalıdır.

Ceza kanunumuzda yer alan bazı suç tanımları ile tam olarak neyin kastedildiği anlaşılamamaktadır. Örneğin bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu, bilişim sisteminde kalmaya devam etme suçu bunlardan bazılarıdır. Bu

bağlamda kanunlarımızın gözden geçirilerek bu tip yorumlanması güç ifadelerin değiştirilmesi gerekmektedir.

Bu çalışma kapsamında incelenen, uluslararası hukukta kabul görmüş bazı suç tanımlarının ceza kanunumuzda tam olarak yer almadığı veya içeriğinin yetersiz olduğu görülmektedir. Bu bağlamda aşağıda sayılan güncellemeler yapılmalıdır:

- BTK tarafından teknik anlamda bir proje olarak yapılan spam'la mücadele çalışması sonucunda ülkemizde spam gönderimi ciddi oranda azalmıştır. Bununla birlikte dış hukukta bu yönde düzenlemeler olduğu halde Ceza Kanunumuzda spam gönderimi suç olarak tanımlanmamaktadır. Avrupa Sınır Ötesi Yayın Sözleşmesi'nin düzenlemesiyle uyum sağlanarak, siber ortamda aldatıcı, yanıltıcı, istismar edici, mal ve can güvenliğini tehlikeye atıcı reklamlara karşı düzenlemeler getirilmeli özellikle kasten can ve mal güvenliğini tehlikeye atıcı reklamların üretilmesi ve internet üzerinden yayınlaması suç haline getirilmelidir.
- Suç politikası açısından bilişim sistemi aracılığıyla sahtecilik yapılarak belgeler düzenlenip kullanılabileceği ve böylelikle kamunun güveni ihlal edilebileceği için bu suç tipi 5237 sayılı TCK' da düzenlenmeli ve bu suç tipine kamunun güvenine karşı suçlar bölümünde yer verilmelidir. Bu suç tipi, yukarıda belirtilen ilgili bölümde ya bağımsız olarak düzenlenmeli ya da resmi ve özel belgede sahtecilik suçlarının içinde ayrı ayrı düzenlenmelidir.
- Bilişim sistemlerinin organize suçlarda ve siber terörizmde kullanılması durumları acilen düzenlenmeli ve bu konu açısından ilgili yasalarda düzenlemeler yapılmalıdır. Siber terörizm olgusunun oluşturduğu büyük tehdit dikkate alınarak, veri iletim ağlarından yararlanılmak yoluyla terör eylemleri gerçekleştirilmesi ağırlatıcı neden sayılmalıdır.
- Ceza kanunumuzda siber suçları düzenleyen bölümde yer alan banka ve kredi kartlarının kötüye kullanılması suçu, koruduğu hukuksal değer açısından malvarlığına karşı suçlar bölümünde yer almalıdır.

- Özellikle internet üzerinden gerçekleştirilen "çocuk pornografisine ilişkin her türlü eylem" suç haline getirilmelidir. Bu eylemlerin neler olduğu Avrupa Siber Suç Sözleşmesinde tek tek gösterilmiştir.

Siber suçlar genellikle uluslararası boyutta olduğu için, suçlular hukuk sistemlerindeki boşluklardan yararlanabilmektedirler. Bu nedenle, siber suçlarla mücadele edebilmek için her ülke kendi hukuk sistemi içerisinde yapacağı gerekli düzenlemelerin yanı sıra diğer ülkelerle ortak çalışmalar yürütmesi yararlı olacaktır. Bu bağlamda AB, BM, Avrupa Konseyi, OECD gibi uluslararası kuruluşların yaptığı çalışmalarda aktif rol alınmalıdır.

10.11.2010 tarihinde ülkemiz tarafından imzalanan Avrupa Konseyi Siber Suç Sözleşmesinin siber suçlarla etkili biçimde mücadele edilmesi, siber suçların ulusal ve uluslararası düzeyde belirlenmesi, soruşturulması ve yargıya götürülmesinin kolaylaştırılması, uluslararası işbirliğinin sağlanması için gerekli düzenlemelerin yapılmasını kolaylaştırması gibi nedenlerle siber suçlarla mücadelede fayda sağlayacağı düşünülmektedir. Ancak siber suç sözleşmesine getirilen eleştirilerin odaklandığı soruşturma ve araştırma faaliyetlerinin yürütülmesi ile ilgili hükümlerin uluslararası insan hakları belgelerinde çizilen çerçeveyi ihlal etmesi, servis sağlayıcılarına ağır mali ve sosyal sonuçları olan yükümlülükler getirilmesi, devletin ulusal sınırları içerisinde başka bir devletin o devletin izni olmadan doğrudan doğruya yargı yetkisini kullanması gibi noktalar göz ardı edilmeden Sözleşme hukuki mevzuatımıza uyumlaştırılmalıdır.

Siber suçların günümüzde yaygınlık kazanmasının önemli sebeplerinden biri de bu suçların toplum nezdinde suç olarak görülmemesidir. Bu nedenle, siber ortamda işlenen suçların gerçek hayatta işlenen suçlarla aynı olduğu konusunda genç neslin bilinçlendirilmesi yönünde çalışmalar yapılmalıdır.

Polisiye Açıdan Öneriler

Ülkemizde, diğer dünya ülkelerinde olduğu gibi, Emniyet Teşkilatının siber suçlarla etkili bir şekilde mücadele edebilmesi amacıyla, kolluk kuvvetlerinin faaliyetlerine dayanak teşkil edecek bilişim suçları yasaları çıkarılmalıdır.

Emniyet Teşkilatı ve kamu kurumları arasında koordineli çalışmalar yapılarak, özellikle, siber terör saldırılarına hazırlıklı olma ve müdahale edebilme gücü kazandırılmalıdır. Ayrıca, bu konu ile ilgili özel güvenlik birimleri kurulmalı ve eğitim faaliyetlerinin yürütüleceği enstitüler açılmalıdır.

Siber suçlarla mücadelede kullanılan teknik donanım ve yazılımların kullanımında başarı elde edilmesi için görevli polis memurları gerekli yurtiçi ve yurtdışı eğitimlere gönderilmelidir. Ayrıca bilişim terminolojisi genel olarak İngilizce olduğundan bu alanda çalışan uzmanların dil eğitimlerinin de tam olması sağlanmalıdır.

Ülkemizde adli olaylarda delillere el koyma sürecinde görevli uzman personel sayısında yeterli seviyeye ulaşılamadığı değerlendirilmektedir. Dolayısıyla bu durum, bilişim suçunun failinin bulunmasında etkin sonuçlar alınamamasına sebep olmaktadır. Delil elde etme noktasındaki yanlış uygulamalar soruşturma birimlerinin ciddi emek vererek yaptıkları çalışmaların mahkeme aşamasında geçersiz sayılmasına kadar gitmektedir. Bu bağlamda ülkemizde siber suç soruşturmalarında kullanmak üzere daha fazla sayıda adli bilişim uzmanı yetiştirilmelidir.

Adli bilişim şu an için birkaç özel eğitim kurumu tarafından eğitimi verilen ve sadece bilişim hukuku yüksek lisans programında ders olarak okutulan bir konudur. Bu konuda verilen eğitimlerin artırılması ve yaygınlaştırılması sağlanmalı, adli bilişim uzmanı olmak isteyenlere sertifikasyon yolu açılmalıdır.

Adli bilişimde daha objektif ve uluslararası alanda daha etkin sonuçlar alınması için uygun standardizasyonlar çerçevesinde özel sektörün adli bilişim alanında

çalışmaları desteklenmelidir. Uluslararası akredite adli bilişim laboratuarlarının sayısı artırılmalıdır.

Teknik Açıdan Öneriler

Siber suçlarla mücadelede başarılı olabilmenin en etkin teknik yöntemi ulusal planda siber güvenliğin sağlanmasıdır. Bu alanda ülkemizde birçok kurum ve kuruluş tarafından çeşitli çalışmalar yürütülmektedir. BTK özelinde ülkemizde ulusal siber güvenliğin sağlanması konusunda kritik öneme sahip olduğu değerlendirilen temel ilkeler, yöntemler ve adımlar yayınlanan rapor ve tezlerle ortaya konulmuştur. Bu çalışmaların çıktıları uygulamaya konan projeler, mevzuat çalışmaları ve siber güvenlik tatbikatı ile hayata geçirilmiştir. Bu bağlamda BTK'nın siber güvenliğin sağlanması konusundaki öncü rolü devam etmelidir.

Bilgisayar olaylarına müdahale merkezleri, kritik altyapıların korunması, siber saldırılarla ve kötücül yazılımlarla mücadele edilmesi, siber tehditlere karşı önlemler alınması, siber güvenlik kültürünün oluşturulması ve kişisel verilerin gizliliğinin sağlanması gibi siber güvenlik bileşenleri hakkında yapılan çalışmalar sürdürülmelidir.

Siber güvenlik tatbikatları daha sık aralıklarla yapılmalıdır. Bu konuda yapılan eleştiriler dikkate alınarak daha gerçekçi senaryolar uygulanmalıdır. Ulusal Siber Güvenlik Tatbikatlarının yanı sıra uluslararası boyutta yapılan tatbikatlara da katılım sağlanmalıdır.

5651 sayılı kanun kapsamında kurum ve kuruluşlar tarafından tutulan kayıtların yazılım imkânları kullanılarak merkezi olarak düzenlenmesi sağlanmalıdır. Merkezi olmayan kayıt takip sistemlerinde hem istenen kaydın bulunması zor olmakta hem de tutulan kayıtların anlamlandırılması mümkün olmamaktadır. Ancak, kayıtların tutulması ve düzenlenmesi işinde kullanılan yazılımların kişisel gizliliğin korunması ilkesine göre tasarlanması gerekmektedir.

Siber suçlarla mücadele etmenin bir bileşeni de uluslararası güvenlik standartlarını temel alan çalışmaların yapılması ve bu standartlar çerçevesinde güvenliğin oluşturulmasıdır. Özellikle kamu kuruluşları ve özel işletmelerin, uluslararası bilgi güvenliği standardı olan ISO/IEC 27001 konusunda gerekli adımları atmaları, hem teknik hem de idari anlamda bilgi güvenliği düzeylerini yükseltmelerini sağlayacaktır. Standardın bir kuruluşta uygulama kapsamını belirlemek tamamen uygulayıcıya bırakılmış olup, bu kapsamın zaman içerisinde genişletip daraltılabilmesi konusunda esnek davranılabilmektedir. Bu nedenle, standardı tek bir kişisel bilgisayara sahip bir mahalle bakkalı da, yüzlerce şubesi olan büyük bir banka da uygulayabilmektedir. ISO/IEC 27001 bilgi güvenliği standardı kapsamında verilecek farkındalık eğitimleri sayesinde saldırılara karşı çalışanların farkındalık seviyesi yükselecek ve bu konuda sürekli uyanık kalmaları sağlanacaktır.

Standarda ilişkin sertifikanın alınmasıyla birlikte kurum ve kuruluşların kendi içlerinde ve karşılıklı iş yaptıkları diğer şahıs, kurum ve kuruluşlar nezdinde itibarı da yükselmiş olacaktır. Buna ek olarak, kuruluşlar bilgi varlığı envanterlerinden haberdar olacak ve yapılacak risk analizleri kapsamında da hangi risklerle yüz yüze oldukları netleşecektir. Belirlenecek olan teknik ve prosedürel açıklıklara karşı alınacak önlemler sonucunda kuruluşların iç ve dış saldırılara karşı savunma düzeyleri artırılmış olur.

Teknik önlemlerin vazgeçilmez kavramları olan Firewall, VPN, IDS, IPS, içerik filtreleme ve zafiyet testlerinin yapılması gibi teknik önlemler, aynı zamanda ISO/IEC 27001 standardı kapsamında yapılacak olan çalışmalar arasında yer almaktadır. Ayrıca kimlik doğrulama, kesintisiz bilgiye erişebilme, yetkisiz kişilerin bilgiye erişimlerinin kısıtlanması, bilgi bütünlüğünün sağlanması ve bilginin gizliliği konuları, ISO/IEC 27001 bilgi güvenliği standardının temelini oluşturan kavramlardır. Ancak yapılacak olan çalışmalar ve öngörülen karşı önlemler, yürürlükte olan yasa ve yönetmeliklere aykırı olmamalıdır.

Bilgi güvenliği yönetim sistemi (BGYS) standartı, kurum ve kuruluşların bilgi güvenliği düzeyinin artırılması yönünde sürekli olarak çalışmaların devam

ettirilmesini dayatmaktadır. Bunu sağlamak üzere, standardın PUKÖ (Planla, Uygula, Kontrol Et, Önlem Al) döngüsü uyarınca çalışmalar sürdürülmelidir. İç ve dış denetimler ile yönetimin gözden geçirmesi toplantıları doğrultusunda sürekli iyileştirme yönünde adımlar atılması gerçekleştirilmiş olur. Siber suçları geleneksel anlamdaki diğer suçlardan ayıran en önemli özellik bu suçların işleniş şekillerinin tespitinin zorluğudur. Söz konusu suçlar yepyeni ve çok farklı yollarla işlenebilmektedir. Bu anlamda alınacak güvenlik tedbirlerinin kolay ve hızlı güncellenebilir olması gerekmektedir.

Ayrıca şu unutulmamalıdır ki; insan faktörü ve toplumun eğitilerek farkındalık konusunda bilinçlendirilmesi ile uluslararası standartların uygulanması, siber güvenliğin sağlanmasında en önemli bileşenlerden biridir. Siber ortamda bilgi güvenliğinin sağlanması amacıyla bireysel kullanıcıların eğitimi konusuna önem verilmeli, sosyal farkındalık yaratılarak siber suçlarla etkin şekilde mücadele edilmesi sağlanmalıdır.

KAYNAKLAR

AKBULUT Berrin, 1999, Türk Ceza Hukukunda Bilişim Suçları, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı, Konya

AKDENİZ Yaman, 2001, The Regulation of Pomography and Child Pomography on the Internet. Cyber-rights & Cyber – Liberties, http://www.cyber-rights.org/documents/us_article.pdf, (25.02.2011)

AKDENİZ Yaman, 2008, An Advocacy Handbook for the Non Governmental Organisations, http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf, (25.02.2011)

ALACAKAPTAN Uğur, 1975, Suçun Unsurları, Ankara Üniversitesi Hukuk Fakültesi Yayınları No. 372, Ankara

AVRUPA KONSEYİ, 2001, Siber Suç Sözleşmesi, http://www.coe.int/t/dghl/standardsetting/t-cy/ETS%20185%20turkish.pdf, (15.05.2011)

AVRUPA KONSEYİ, 2011, http://ec.europa.eu/about/index_en.htm, (15.05.2011)

AYDIN Emin D., 1992, Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınları, Ankara

BARROSO David, 2007, Botnets – The Silent Threat, ENISA Position Paper No. 3, European Network and Information Security Agency, http://www.dihe.de/docs/docs/enisa_pp_botnets.pdf, (13.03.2011)

BECENİ Yasin, 2003, Siber Suçlar, http://www.hukukcu.com/bilimsel/kitaplar/yasin beceni/indeks.htm, (19.02.2011)

BENSGHİR Türksel Kaya, 1996, Bilgi Teknolojileri ve Örgütsel Değişim, TODAİE, Ankara

BİRLEŞMİŞ MİLLETLER, 1994, International Review of Criminal Policy Nos 43 and 44 1994: United Nations Manual on the Prevention and Control of Computer-Related Crime, http://www.uncjin.org/Documents/irpc4344.pdf, (10.11.2011)

BKA, 2010, Cybercrime, http://www.bka.de/DE/Publikationen/Jahresberichte UndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true, (12.11.2011)

BOĞAÇ Erkan, SONGÜR Murat, 1999, Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü, Hacettepe-Taş Yayınevi, Ankara

BOTFREİ, 2011, Anti-Botnet-Danışmanlık Merkezi ile ilgili sorular, https://www.botfrei.de/tr/fragen.html, (13.11.2011)

BRUNNER Elgin M., SUTER Manuel, 2008, International CIIP Handbook 2008 / 2009

CERT, 2011, http://www.cert.org/meet_cert/, (15.11.2011)

CİHAN, 2008, Siber Suçlar Sözleşmesi semineri sona erdi, http://www.tumgazeteler.com/?a=4265437, Bolu Cihan Haber Ajansı, (25.02.2011)

CNETNEWS, 2009, Twitter crippled by denial-of-service attack, http://news.cnet.com/8301-13577_3-10304633-36.html, (25.02.2011)

ÇEKEN Hüseyin, 2002, Amerika Birleşik Devletlerinde Siber Suçlar, www.jura.uni-sb.de/turkish/HCeken.html, (19.02.2011)

DEĞİRMENCİ Olgun, 2002, Bilişim Suçları, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı Yüksek Lisans Tezi, İstanbul

DHS, 2009, http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf, (15.11.2011)

DHS, 2011, Department of Homeland Security, http://www.dhs.gov, (15.11.2011)

DOĞAN Koray, 2005, Bilişim Suçları ve Yeni Türk Ceza Kanunu, Hukuk ve Adalet: Eleştirel Hukuk Dergisi, İstanbul

DOKURER Semih, 2001, Ülkemizde Yaşanan Bilişim Suçları ve Geliştirilen Mücadele Yöntemleri, http://www.dokurer.net/files/documents/Bilisim_Suclari_Bursa.pdf , (25.02.2011)

DOKURER Semih, 2005, Bilişim Suçları ve Adli Bilişim, http://www.dokurer.net/files/documents/Adli_Bilisim_Wormy.pdf, (25.02.2011)

DÖNMEZER Sulhi, ERMAN Sahir, 1967, Nazari ve Tatbiki Ceza Hukuku Umumi Kısım, c.1, İstanbul

DÖNMEZER Sulhi, 1994, Kriminoloji, Beta Yayınları, İstanbul

DÜLGER Murat Volkan, 2004, Bilişim Suçları, Seçkin Yayıncılık, Ankara

DÜLGER Murat Volkan, 2005, Yeni Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları ve Bu Suçlarla Mücadelede Alınması Gereken Önlemler, 2.Polis

Bilişim Sempozyumu, Ankara, http://www.dulger.av.tr/assets/pdf/bilisimsuclarionlemler.pdf, (25.02.2011)

EGM, 2011, Faaliyet Raporu 2010, Emniyet Genel Müdürlüğü, http://www.egm.gov.tr/Duyurular2011/Faaliyet_Raporu_2010.pdf, (01.05.2011)

ENISA, 2011a, About ENISA, http://www.enisa.europa.eu/about-enisa, (16.11.2011)

ENISA, 2011b, Who is Who Directory on Network and Information Security, http://www.enisa.europa.eu/publications/studies/who-is-who-directory 2011/at_download/fullReport, (16.11.2011)

ENISA, 2011c, Inventory of CERT Activities in Europe Version2.5, http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe/at_download/fullReport, (16.11.2011)

ERGÜN İsmail, 2008, Siber Suçların Cezalandırılması ve Türkiye'deki Durum, Adalet Yayınevi, Ankara

ERİŞ Mehmet, 2008, TR-CERT Oluşumu, ULAKNET Eğitim ve Çalıştayı Konya, http://www.ulakbim.gov.tr/ulaknet/calistay/08/TR-BOME.pdf, (16.11.2011)

EUROPOL, 2011, The Changing Face of Cybercrime, https://www.europol.europa.eu/content/press/changing-face-cybercrime-521, (15.11.2011)

FBI, 2011, Cyber Crime, http://www.fbi.gov/about-us/investigate/cyber/cyber, (15.11.2011)

FIRST, 2011, About First, http://www.first.org/about, (16.11.2011)

GAO, 2005, Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO-05-434, http://www.gao.gov/new.items/d05434.pdf, (25.02.2011)

GÖZÜBÜYÜK Abdullah Pulat, 1989, Türk Ceza Kanunu Gözübüyük Şerhi C:1, Kazancı Yayınları, İstanbul

GROSS Grant, 2010, Cyber Storm III Simulates Large-scale Attack, http://www.pcworld.com/businesscenter/article/206554/cyber_storm_iii_simulates_largescale_attack.html, (15.11.2011)

HOWARD J.D., LONGSTAFF, T. A., 1998, A Common Language for Computer Security Incidents, www.cert.org/research/taxonomy_988667.pdf, (15.11.2011)

HUFFMAN Mark, 12.11.2006, ConsumerAffairs.com's Top 10 Scams of 2006, ConsumerAffairs.com,http://www.consumeraffairs.com/news04/2006/12/top_ten_ scams.html, (25.02.2011)

HUKUKİ.NET, 2010, 5651 Çalıştayı (20-22 Nisan), http://www.hukuki.net/showthread.php?71314-5651%C7al%FD%FEtay%FD-(20-22 Nisan)&s=e7ede31b78dbf856f32ed9a2c7f99e24, (15.05.2011)

IBM, 2009, IBM X-Force 2008 Trend & Risk Report, IBM Security Solutions, http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf, (15.05.2011)

IBM, 2011, IBM X-Force 2010 Trend & Risk Report, IBM Security Solutions, http://www-935.ibm.com/services/us/iss/xforce/trendreports/, (15.05.2011)

INTERPOL, 2011a, Cybercrime, https://www.europol.europa.eu/content/press/changing-face-cybercrime-521, (15.11.2011)

INTERPOL, 2011b, INTERPOL working parties on IT crime, http://www.interpol.int/Crime-areas/Cybercrime/Meetings, (15.11.2011)

ITU, 2008, Botnet Mitigation Toolkit, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html, (19.02.2011)

ITU, 2009, Understanding Cybercrime: A Guide for Developing Countries (Draft), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf, (19.02.2011)

İNTERNET ÜST KURULU, 2005, İnternet Üst Kurulu SPAM Bildirgesi, Ankara

JPCERT, 2011, About JPCERT, http://www.jpcert.or.jp/english/, (13.11.2011)

KANGAL Zeynel T., 2001, Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu, İÜHFM, C.LIX, S.1-2, İstanbul

KARAGÜLMEZ Ali, 2005, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Seçkin Yayıncılık, Ankara

KARAOĞLU Erol, 2004, İnternet Ortamından Gerçekleştirilebilecek Bir İhlal Turu Olarak Asılsız İsnat, http://www.bilisimhukuku.net/index.php?option=content&task=view&id=337&Itemid=40, (25.02.2011)

KESER BERBER Leyla, 2004, Adli Bilişim (Computer Forensic), Yetkin Yayınları, Ankara

KESER BERBER Leyla, KAYA Mehmet Bedii, 2010, 5651 Sayılı Kanunun Teknik ve Hukuki Açıdan Değerlendirilmesi, http://www.turk.internet.com/portal/yazigoster.php?yaziid=28665, (16.03.2011)

KESER BERBER Leyla, 2011, "Siber Güvenliğin Hukuki Boyutu" isimli sunum, Milli Güvenlik Akademisi, Ankara

KOM, 2007, Bilişim Suçlarıyla Mücadele Şube Müdürlüğü, Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, http://www.kom.gov.tr/Tr/KonuDetay.asp?id =5&BKey=13, (25.02.2011)

KÖKSAL Aydın, 1981, Bilişim Terimleri Sözlüğü, Türk Dil Kurumu, Ankara

KURT Levent, 2005, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayıncılık, Ankara

MCCONNELL INTERNATIONAL, 2000, Cyber crime ... and punishment? - Archaic Laws Threaten Global Information, www.mcconnellinternational.com, (25.02.2011)

MEMİŞ Tekin, 2005, Hukuki Açıdan Kitlelere E-posta Gönderilmesi, Saarbrücken Hukuki İnternet Projesi, www.jura.unisb.de/turkish/TMemis1.html, (25.02.2011)

MIC, 2011, Japon İçişleri ve İletişim Bakanlığı http://www.soumu.go.jp/english/index.html, (15.11.2011)

NICKOLOV Eugene, 2008, Modern Trends In The Cyber Attacks Against The Critical Information Infrastructure, Regional Cybersecurity Forum, Sofia, Bulgaria, http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolov-modern-trends-sofia-oct-08.pdf, (29.04.2011)

NPA, 2011, Police of Japan 2011, http://www.npa.go.jp/english/kokusai/Contents2011.htm, (13.11.2011)

OECD, 2002, Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri: Güvenik Kültürüne Doğru, C(2002/131/FINAL), http://www.oecd.org/dataoecd/42/59/32493366.PDF, (25.02.2011)

OECD, 2006, Task Force On Spam, http://www.oecd.org/dataoecd/63/28/36494147.pdf, (25.02.2011)

OECD, 2009, Computer Viruses and Other Malicious Software, A Threat To the Internet Economy, http://www.oecd.org/document/16/0,3746,en_2649_34223_42276816_1_1_1_1,00.html, (25.02.2011)

OKTUĞ Sema, 2010, Bilgisayar Haberleşmesi Ders Notları, İTÜ Bilgisayar Mühendisliği Bölümü, İstanbul

ÖNDER Ayhan, 1994, Şahıslara ve Mallara Karşı Cürümler ve Bilişim Alanında Suçlar, Filiz Kitapevi, İstanbul

ÖZCAN Mehmet, 2004, Siber Terörizm ve Ulusal Güvenlik, İnternet ve Hukuk, Der: Yesim M. Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, İstanbul

ÖZDİLEK Ali Osman, 2002, İnternet ve Hukuk, Papatya Yayıncılık, İstanbul

PCLABS, 2009, İnternet bankacılığında dikkat edilmesi gerekenler, http://www.pclabs.com.tr/2009/06/02/internet-bankaciliginda-dikkat-edilmesi-gerekenler/, (25.02.2011)

SAĞIROĞLU Şeref, CANBEK Gürol, 2007, Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma, Gazi Üniv. Müh. Mim. Fak. Der. J. Fac. Eng. Arch. Gazi Univ. Cilt 22, No 1.

SINAR Hasan, 2001, İnternet ve Ceza Hukuku, Beta Yayınevi, İstanbul

SINAR Hasan, 2002, İstanbul Bilgi Üniversitesi ve İstanbul Barosu tarafından İnternet ve Ceza Hukuku konulu panelde yapılan konuşması. İnternet ve Hukuk, der. Yeşim ATAMER, ss.277-299, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, ss. 659-669.

SINAR Hasan, 2004, Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme, Prof. Dr. Çetin Özek Armağanı, Galatasaray Üniversitesi Yayınları, İstanbul

SİEBER Ulrich, 1998, Legal Aspects of Computer-Related Crime in Information Society - A Comcrime Study, http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html, (25.02.2011)

SOĞUKPINAR İbrahim, 2006, Bilgisayar Ağları Ders Notları, Gebze İleri Teknoloji Enstitüsü, http://www.gyte.edu.tr/dosya/104/ders/BIL472/BIL472Notlar1-3.pdf, (19.02.2011)

SOPHOS, 2009, Security Threat Report, http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf, (25.02.2011)

SOPHOS, 2011, Security Threat Report, http://www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx (25.02.2011)

SÖZEN, Süleyman vd., 2003, Polisin Görev ve Yetkileri, Anadolu Üniversitesi Yayınları, Eskişehir

SPAMLAWS, 2009, What is Adware (Other Than Annoying)?, http://www.spamlaws.com/ what-is-adware.html, (25.02.2011)

SYMANTEC, 2009, Symantec Internet Security Threat Report Trends for 2008, Volume 14, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, (25.02.2011)

SYMANTEC, 2011, Symantec Internet Security Threat Report Trends for 2010, Volume 16, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf, (25.02.2011)

ŞEN Bilal, 2007, İnternet Suçlarıyla Mücadelede Suç Önleme Anlayışı Ve Bilinçli Kullanıcı, Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, http://www.kom.gov.tr/Tr/KonuDetay.asp?BKey=64&KKey=119, (25.02.2011)

TAN Aydoğan, 2010, Adli Bilişim (Computer Forensic), Edirne Barosu, http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html, (25.02.2011)

TANYOL Tuğrul, 2002, Anarşizm ve İnternet, Cogito İnternet: Üçüncü Devrim, Yapı Kredi Yayınları, İstanbul

TİB, 2009, Siber Suçlarla Mücadele Konusunda Çalışma Ziyareti Fransa 5-10.Ekim.2009, http://www.tib.gov.tr/dokuman/TIB_Fransa_Calisma_Ziyareti.pdf, (10.11.2011)

TURHAN Meltem, 2010, Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri, BTK Uzmanlık Tezi, Ankara

TURHAN Oğuz, 2006, Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), DPT Uzmanlık Tezi, Ankara

TURK.INTERNET.COM, 2011, Siber Suçlardan Kazanılan Para, Yasadışı Yollardan Elde Edilenle Karşılaştırılabilir Boyutlara Ulaştı, http://www.turk.internet.com/portal/yazigoster.php?yaziid=32063, (20.04.2011)

TÜRKİYE 1. BİLİŞİM ŞURASI, 2002, Hukuk Çalışma Grubu Raporu, http://www.scribd. com/doc/19952426/1-Bilişim-Şurası-Hukuk-Raporu, (25.02.2011)

UNESCO, 2004, 4. Staff The COE International Convention On Cybercrime Before Its Entry Into Force, UNESCO.ORG

US-CERT, 2011, http://www.us-cert.gov, (15.11.2011)

ÜNVER Mustafa, CANBAY Cafer, MİRZAOĞLU Ayşe Gül, 2009, Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, BTK, Ankara

ÜNVER Mustafa, CANBAY Cafer, GÜNAYDIN Yüksel, 2010, Köle Bilgisayarlar ve Köle Bilgisayar Ağları (Zombi ve Botnetler), Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, BTK, Ankara

ÜNVER Mustafa, MİRZAOĞLU Ayşe Gül, 2011, Yemleme (Phishing), Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, BTK, Ankara

ÜNVER Yener, 2001, Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C.LIX, S.1-2, İstanbul

YAZICIOĞLU R. Yılmaz, 1997, Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle, Alfa Yayınevi, İstanbul

YENİDÜNYA Ahmet Caner, DEĞİRMENCİ Olgun, 2003, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, İstanbul

YILDIZ Sevil, 2006, Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi, http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler/Sevil %20 YILDIZ/YILDIZ,%20SEV%C4%B0L.pdf, (15.01.2011)

ZAMAN, 2008, İşte şu yollarla bilgisayarınızı ele geçiriyorlar. Tehlikenin adı: Botnet, http://www.zaman.com.tr/haber.do?haberno=732850, (25.02.2011)

ZETTER, K., 2000, "Viruses, the Next Generation", http://pcworld.about.net/ magazine/1812p191id32802.htm (25.02.2011)

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

05.12.2011

(İmza)

Uğur ÖZÜDOĞRU

ÖZGEÇMİŞ

1979 yılında Yalova'da doğdu. İlk, orta ve lise öğrenimini Çınarcık/Yalova'da tamamladı. 2000 yılında Çanakkale 18 Mart Üniversitesi Bilgisayar Mühendisliği bölümünden mezun oldu. Mezuniyete müteakip kamu ve özel sektöre ait çeşitli kuruluşlarda sistem yöneticisi, bilgi teknolojileri uzmanı gibi pozisyonlarda çalıştıktan sonra Mayıs 2008 tarihinde Bilgi Teknolojileri ve İletişim Kurumunda uzman yardımcısı olarak göreve başladı. Bu süre zarfında, siber güvenlik ve kurum sistemleri yönetimi alanlarında çalışmalarda bulundu. Evli ve iki çocuk babasıdır.