I- BÖLÜM

1. BİLİŞİM SUÇLARI ÇALIŞMA GRUBU

18.04.1998 tarihinde Sn Genel Müdürümüz'ün onayıyla kurulan "Bilgisayar Suçları ve Bilgi Güvenliği Kurulu" altında yapılan görevlendirme ile 1.3.1999 tarihinde "Bilişim Suçları Çalışma Grubu" kurulmuştur.

1.1. AMAÇ

Gelişen teknolojilerle birlikte insan ilişkileri de bu teknolojik ortamlara taşınmakta ve bu ortamlarda da hak ihlalleri meydana gelmektedir. Bilişim alanındaki hak ihlallerini araştırmak bu alandaki suç tiplerini belirlemek, ilgili Daire Başkanlıklarının yönetmeliklerinde gerekli düzenlemeleri yapmak üzere "Bilişim Suçları Çalışma Grubu" kurulmuştur.

1.2. ÇALIŞMA PROGRAMI

Bilişim Suçları Çalışma Grubu kurulduğu 1 Mart 1999 tarihinden itibaren kendine 4 aylık bir çalışma programı belirlemiştir.

Bu program:

1) Bilişim suçlarının genel olarak belirlenmesi
2) Belirlenen suç türleri ve bunlara ışık tutacak kaynakların toplanması,
   - **a)** Yerli kaynaklar
     - Konu ile ilgili meri kanunlar
     - Konu ile ilgili meri yönetmelikler
     - Diğer kurum ve kuruluşların yapmış olduğu çalışmalar
       - -Adalet Bakanlığı
       - -Kültür Bakanlığı
       - -BKM (Bankalar Arası Kart Merkezi)
       - -BSA Türkiye (Business Software Aliance)
   - **b)** Yabancı kaynaklar
     - Konu ile ilgili Avrupa ülkelerinin ilgili kanun maddeleri
     - İnterpol vasıtasıyla ulaştığımız ülkelerin polis uygulamaları
     - İnterpol'ün konu hakkındaki çalışmaları
     - Avrupa Komisyonunun (Council of Europe Legal Affairs Committee) konu hakkında hazırlattığı rapor
3) Mevcut kaynakların değerlendirilmesi,
4) Bilişim suçlarının tasnif edilmesi,
5) Daire başkanlıklarının görev alanlarının belirlenmesi,
6) Gerek duyulan Daire başkanlıklarının yönetmeliklerinde değişiklikler yapılması,
7) ***Bilişim suçları kurulu*** adında; Periyodik zamanlarda bir araya gelerek kendi görev alanlarıyla ilgili gelişmelerin diğer üyelerle paylaşıldığı, son gelişmelerin değerlendirildiği ve yeni stratejilerin ortaya konulduğu ve ilgili büro personelinin katıldığı bir kurul oluşturulması ve görev alanlarının belirlenmesi,
8) Çalışmaların bir rapor haline getirilerek ilgili Daire Başkanlıklarından yetkili amirlere bir brifing olarak sunulması, şeklinde belirlenmiştir.

1.3. ÇALIŞMA GRUBUNUN OLUŞTURULMASI

Bu çalışma grubunun içine kendi görev alanlarına göre;

- Teknolojik gelişmeleri takip etmek ve bu konularda yönlendirme yapmak üzere Bilgi İşlem Daire Başkanlığı,
- Yazılım korsanlığı, Bilgisayar sistemleri kullanılarak meydana gelen dolandırıcılıklar ve kredi kartları dolandırıcılığı konusunda düzenlemeler yapmak üzere Kaçakçılık ve Organize Suçlar Daire Başkanlığı,
- Dijital ortamda yayınlanan dergi, gazete ve benzeri yayınları incelemek ve bu konudaki çalışmaları yapmak üzere Güvenlik Daire Başkanlığı,
- Bilişim alanında işlenen suçlarda iz ve deliller konusunda çalışma yapmak üzere Kriminal Polis Laboratuvarları Daire Başkanlığı,
- İnterpol üyesi ülkelerle irtibatı ve karşılıklı bilgi aktarımını sağlamak üzere İnterpol Daire Başkanlığı,
- Üniversitelerle bağlantıları yapmak üzere Polis Akademisi Başkanlığı,
- Yapılacak yönetmelik çalışmalarında bulunmak üzere Hukuk Müşavirliği üyeleri çalışma grubuna dahil edilmişlerdir.

Çalışmaya son şeklini vermek üzere 07.06.1999 –11.06.1999 tarihleri arasında Bilgi İşlem Daire Başkanlığı bünyesinde ortak bir görevlendirme ile bilişim suçlarının tasnifi yapılmış, Daire Başkanlıklarının görev alanları tespit edilmiş ve polisin olay yerinde bilgisayar ve bilgisayar sistemleri ile karşılaştığında yapması gerekenler çalışma grubu sonuç raporu içinde tanzim edilmiştir.

II-BÖLÜM

2. BİLİŞİM SUÇLARININ SINIFLANDIRILMASI

Bilişim alanındaki suç tiplerini incelerken İnterpol ün hazırlamış olduğu "Interpol Computer Crime Manual" esas olmak üzere, Birleşmiş Milletlerin hazırlamış olduğu "United Nations Manual on The Preventation and Control of Computer-Related Crime" kitapçığı ve Avustralya polis teşkilatının hazırlamış olduğu "Minimum Provisions for The Investigation of Computer Based Offences" kitapçıklarından istifade edilerek aşağıdaki suç tipleri belirlenmiştir.

2.1. BİLGİSAYAR SİSTEMLERİNE VE SERVİSLERİNE YETKİSİZ ERİŞİM

2.1.1. Yetkisiz Erişim

Tanım: Bir bilgisayar sistemine yada bilgisayar ağına yetkisi olmaksızın erişmektir.

Açıklama: Suçun hedefi bir bilgisayar sistemi yada ağıdır. "Erişim" sistemin bir kısmına yada bütününe ve programlara veya içerdiği verilere ulaşma anlamındadır. İletişim metodu önemli değildir. Bu bir kişi tarafından bir bilgisayara direkt olarak yakın bir yerden erişebileceği gibi, dolaylı olarak uzak bir mesafeden örneğin bir modem hattı yada başka bir bilgisayar sisteminden de olabilir.

(Interpol Computer Crime Manual,2.Offences, Sf 2)

2.1.2. Yetkisiz Dinleme

Tanım: Bir bilgisayar veya ağ sistemine, sisteminden veya sistemi içinde yapılan iletişimin yetkisi olmaksızın teknik anlamda dinlenmesidir.

(Interpol Computer Crime Manual,2.Offences, Sf 3)

Açıklama: Suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferini içerir.

İletişim;

- Tek bir bilgisayar sistemi içerisinde,
- Aynı kişiye ait iki bilgisayar sistemi,
- Bir biriyle iletişim kuran iki bilgisayar arasında,
- Bir bilgisayar ve bir kişi arasında,

yer alabilir.

Teknik anlamda dinleme, iletişimin içeriğinin "izlenmesi", verilerin kapsamının ya direk olarak (bilgisayar sistemini kullanma yada erişme yoluyla) yada dolaylı olarak (elektronik dinleme cihazlarının kullanımı yoluyla) elde edilmesi ile ilgilidir.

Suçun oluşması için hareket yetkisiz ve niyet edilmiş olarak işlenmesi gerekir. Uygun yasal şartlar çerçevesinde soruşturma yetkililerinin yaptıkları bu kategoriye girmez.

(Interpol Computer Crime Manual,2.Offences, Sf 3)

2.1.3. Hesap İhlali

Tanım: Herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının dijital hesabını kötüye kulanma.

Açıklama: Bu tip suçlar normalde geleneksel suçlardaki hırsızlık, dolandırıcılık suçları gibidir. Pek çok bilgisayar servis şirketleri ve ağları kullanıcılar için yaptıkları ödemeleri ve hesaplarını kontrol etmek amacıyla otomatik faturalandırma araçları temin etmişlerdir. Hesap ihlali, yetkisiz erşim yapılarak başkasının hesabını kullanarak sistemlerden istifade etmek şeklinde olabilir.

(Interpol Computer Crime Manual,2.Offences, Sf 3)

2.2. BİLGİSAYAR SABOTAJI

2.2.1. Mantıksal (Bilgisayar verilerine zarar verme yada değiştirme)

Tanım: Bir bilgisayar yada iletişim sisteminin fonksiyonlarını engelleme amacıyla bilgisayar verileri veya programlarının girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir.

Açıklama: Bir bilgisayar yada iletişim sisteminin fonksiyonlarının çalışmasını engellemek amacıyla verilerin yada programların Zaman Bombası (Logic-Time Bomb), Truva Atları (Trojan Horses), Virüsler, Solucanlar (Worms) gibi yazılımlar kullanarak değiştirilmesi, silinmesi, ele geçirilmesi yada çalışmaz hale getirilmesidir.

(Interpol Computer Crime Manual,2.Offences, Sf 4)

2.2.2. Fiziksel

Tanım: Bir bilgisayar yada iletişim sistemine fonksiyonlarını engelleme amacıyla fiziksel yollarla zarar vermedir.

Açıklama: Bir bilgisayar yada iletişim sistemini oluşturan parçalara sistemin fonksiyonlarını yerine getirememesi amacıyla fiziksel yollarla zarar verilmesidir.

2.3. BİLGİSAYAR YOLUYLA DOLANDIRICILIK

Tanım: Bilgisayar ve iletişim teknolojileri kullanarak verilerin alınması, girilmesi, değiştirilmesi, silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etmek veya mağdura zarar vermektir.

Açıklama: Bilgisayar bağlantılı dolandırıcılık suçları genellikle dolandırıcılığın geleneksel ceza kanunları içerisindeki tanımlarındaki gibi değerlendirilir ve kovuşturması bu kapsamda yapılır. Suçlunun hedefi kendisine veya bir başkasına mali kazanç sağlamak yada mağdura ciddi kayıplar vermektir. Bilgisayar dolandırıcılığı suçları suçluların modern bilgisayar teknolojileri ve ağ sistemlerinin avantajlarını değerlendirmeleri yoluyla klasik dolandırıcılık suçlarından farklılık gösterir.

(Interpol Computer Crime Manual,2.Offences, Sf 6)

2.3.1. Banka Kartları

Tanım: Bankamatik sistemlerinden yapılan dolandırıcılık ve hırsızlık suçlarıdır.

Açıklama: Bankamatik sistemleri (ATM -Automated Teller Machine- olarak da bilinir) genelde bankalar yada benzer finans kuruluşları tarafından kullanılır ve şifreli ağ sistemlerini kullanırlar. Erişim genellikle bir kişisel tanımlama numarası (PIN - Personel Identification Number) girişi gerektiren bir kart yada benzeri bir sistem iledir. Dolandırıcılık bu kartların çoğaltılması, kopyalanması yada iletişim hatlarının engellenmesive dinlenesi yoluyla oluşur.

Uluslararası olaylarda, diğer ülkelerdeki yetkililerle görüşülmesi durumunda sistemin özelliklerinin bildirilmesi çok önemlidir.

(Interpol Computer Crime Manual,2.Offences, Sf 7)

2.3.2. Girdi/Çıktı/Program Hileleri

Tanım: Bir bilgisayar sistemine kasıtlı olarak yanlış veri girişi yapmak veya sistemden çıktı almak yada sistemdeki programların değiştirilmesi yoluyla yapılan dolandırıcılık ve hırsızlıktır.

Açıklama: Bir bilgisayar veri tabanına yanlış veri girmek yaygın bir dolandırıcılık yoludur. Davalar araştırılırken sistemde kullanılan yazılım programlarını da içerecek şekilde tam bir teknik tanımlama yapılmasına ihtiyaç vardır.

Yanlış çıktı daha az yaygındır ve genellikle sahte dokümanların veya çıktıların üretiminde kullanılır. Bu tür suçları araştırırken kullanılan sistem incelenmelidir ve saklı veya silinmiş dosyaları kurtarmak için her türlü çaba gösterilmelidir.

Program hilelerinin tanımlanması teknik açıdan daha zordur. Yaklaşık üç çeşit geniş bilgisayar programı kategorisi vardır:

1) Ticari piyasa için yazılmış yazılımlar ki satışa açıktır.

2) Yukarıda belirtilen şekilde alınmış fakat sonradan belli bir amaç için değiştirilmiş yazılımlar.

3) Belirli bir amaç için özel olarak yazılmış ve satışa yada dağıtıma açık olmayan yazılımlar.

(Interpol Computer Crime Manual,2.Offences, Sf 9)

2.3.3. İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma:

Tanım: Kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerine veya diğer bilgisayar sistemlerine hakkı olmadan girmek.

Açıklama: İletişim servislerinin değişik şekillerde kötü kullanımı olarak tanımlanabilir. Fiil bazen yüksek telefon faturalarının önüne geçmek için işlenebilir.

(Interpol Computer Crime Manual,2.Offences, Sf 10)

2.4. BİLGİSAYAR YOLUYLA SAHTECİLİK

Tanım: Kendisine veya başkasına yasa dışı ekonomik menfaat temin etmek veya mağdura zarar vermek maksadıyla; bilgisayar sistemlerinin kullanarak sahte materyal (banknot,kredi kartı,senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır.

Açıklama: Dijital ortamda tutulan dokümanlar üzerinde değişiklik yapmak sahteciliktir. Bilgisayarlarda tutulan dokümanlarda (İş akış programları, raporlar, personel bilgileri vs) sahtecilik amacıyla yapılan değişikliklerle kişiler kandırılabilmektedir. Bu ve bundan önceki örneklerde bilgisayar sistemleri suçlu aktivitelerin hedefi durumundadır. Fakat bilgisayarlar sahtecilik yapmak amacıyla bir araç olarak da kullanılabilir. Modern yazılımların güçlendirilmiş grafik kapasitesi, ticari alandaki pek çok belgenin sahtesini yapmak için olanak sağlamıştır. Modern teknoloji, özellikle renkli lazer yazıcıların ve fotokopi cihazlarının gelişimi ile daha önceden üretilmesi çok zor olan belgelerin kopyalanmasını mümkün kılmıştır.

(Interpol Computer Crime Manual,2.Offences, Sf 7)

2.5. KANUNLA KORUNMUŞ BİR YAZILIMIN İZİNSİZ KULLANIMI

Tanım: Kanunla korunmuş yazılımların izinsiz olarak çoğaltılmasını, yasadışı yöntemlerle elde edilen bilgisayar yazılımlarının satışını, kopyalanmasını, dağıtımını ve kullanımını ifade eder.

(Interpol Computer Crime Manual,2.Offences, Sf 11)

2.5.1. Lisansız Sözleşme İhlali

2.5.1.1. Lisans Sözleşmesine Aykırı Kullanma

Tek bir bilgisayar için bir yazılımın birden fazla bilgisayarca paylaşılarak kullanılmasıdır. Yazılım lisansları genellikle tek bir bilgisayarla kullanılmak için tanzim edildiğinden, ayrıca ek lisans alınmaması halinde diğer bilgisayarlarca da kullanılması durumunda lisans sözleşmesi ihlal edilmiş olur. Tüm bilgisayarlar için ayrı ayrı lisans alınması şarttır.

2.5.1.2. Lisans Haklarına Aykırı Çoğaltma

Lisans Sözleşmesi ile korunmuş bir yazılımın saklanmış olduğu medya ortamının başka bir medya ortamına kopyalanmasıdır. Genel itibariyle; ödemeden kaçınmak için daha önce satın alınmış

veya yine lisans sözleşmesine aykırı olarak kopyalanmış yazılım, başka bir medya ortamına taşınır. Burada sözkonusu yazılımı kopyalayanda kopyalatanda söleşme ihlali etmiş olur.

2.5.1.3. Lisans Haklarına Aykırı Kiralama

Değişik medyalar üzerine kayıtlı oyun, film ve yazılım programlarının lisans haklarına aykırı olarak kiralanmasıdır.

2.5.2. Taklitçilik

Yazılım taklitçiliği, fikri haklara tabi olan yazılımların, çoğunlukla yasalmış gibi bir görünüme sahip olacak şekilde yasadışı çoğaltılması ve satılmasıdır. Son kullanıcıların aksine, yazılım taklitçileri salt kar amacıyla hareket eder ve para alış-verişi söz konusudur.

Fatura yada benzeri belgeler yazılım taklitçiliğinin saptanması ve izlenmesine olanak vermektedir.

2.5.3. İzinsiz İthalat

Yazılım hakkı sahibinden ve yetkili makamlardan gerekli izni almaksızın, herhangi bir bilgisayar yazılımının ithal edilmesidir.

2.6. YASADIŞI YAYINLAR

Tanım:Yasadışı yayınların saklanmasında ve dağıtılmasında bilgisayar sistem ve ağlarının kullanılmasıdır.

Açıklama: Kanun tarafından yasaklanmış her türlü materyalin Web sayfaları, BBSler, elektronik postalar, haber grupları ve her türlü veri saklanabilecek optik medyalar gibi dijital kayıt yapan sistemler vasıtasıyla saklanması, dağıtılması ve yayınlanmasıdır.

2.7. DİĞER

2.7.1. Ticari Sırların Çalınması

Tanım: Ekonomik kayıp vermek yada yasal olmayan bir ekonomik avantaj sağlamak niyetiyle yetkisi yada herhangi bir yasal sebebi olmaksızın uygun olmayan yollarla bir ticari sırrın kullanımı, transferi, ifşası yada elde edilmesidir.

Notlar: Bilişim suçları ticari sırların hırsızlığını da -özellikle suç bir bilgisayardaki saklanmış verileri ilgilendiriyorsa- kapsayabilir. Endüstriyel espiyonaj olarak da bilinir.

(Interpol Computer Crime Manual,2.Offences, Sf 15)

2.7.2. Verilerin Suistimali

Tanım: Ticari yada mesleki sırların, kişisel bilgilerin yada değerli diğer verilerin kendisine veya başkasına menfaat sağlamak yada zarar vermek amacıyla bu bilgilerin kullanımı, satılması ve dağıtımıdır.

Açıklama: Müşteri bilgileri, hasta bilgileri gibi banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan her türlü kişisel bilginin kendisine yada başkasına menfaat sağlamak veya zarar vermek amacıyla kişilerin rızası dışında kullanılmasıdır.

(Minimum Provisions for The Investigation of Computer Based Offences,sf21)

2.7.3. Sahte Kişilik Oluşturma Ve Kişilik Taklidi

Tanım: Hile yolu ile kendisine veya bir başkasına menfaat sağlamak yada zarar vermek maksadıyla hayali bir kişilik oluşturmak veya bir başkasının bilgilerini kullanarak onun kişiliğini taklit etmektir.

Açıklama: Bilgisayar sistemlerine yetkisiz erişim sağlamak yada kullanma hakkı kazanmak amacıyla gerçek kişilerin taklidi yada hayali kişiler oluşturmak etkili metotlardan biri olarak bilinir. Bu metotta, gerçek kişilere ait bilgileri kullanarak o kişinin arkasına saklanılmakta ve o kişinin muhtemel bir suç durumunda sanık durumuna düşmesine neden olunmaktadır. Ayrıca kredi kartı numara oluşturucu programlar gibi araçlar kullanılarak elde edilecek gerçek bilgilerin hayali kişiler oluşturulmasında kullanılmasıyla menfaat sağlanılmakta ve zarar verilmektedir.

(Minimum Provisions for The Investigation of Computer Based Offences,sf21)

III-BÖLÜM

3. DAİRE BAŞKANLIKLARINA GÖRE GÖREV DAĞILIMI

3.1. ASAYİŞ DAİRE BAŞKANLIĞI

1) Olay yeri incelemelerinde delil toplamada bilgisayar ve ileri teknoloji ürünleri konusunda daha duyarlı olunması ve bu konuda uzman personel yetiştirilmesi, uzman personel olmadığı yerlerde bilgi işlem şubelerinden yardımcı personel alınması,
2) Yapılan uygulamalarda şüpheli kişilerin üzerinden çıkan ileri teknoloji ürünlerinin (databank,disket,cd) incelenmek üzere ilgili birime gönderilmesi ve bu konularda duyarlı olunması,
3) Internet kafelerin denetlenmesi: Her ne kadar bu tür yerlerin açılması belediyeden alınan ruhsatlar ile olsa da Internet vasıtasıyla pornografik yayınlar yapılabileceği gibi yine Internet kullanılarak iç hukukumuza aykırı eylemlerin yapılması muhtemeldir bu konularda da Internet cafelerin belli zamanlar içinde denetlenmesi gerekmektedir,
4) Kanuna aykırı yollarla çoğaltılan veya kanuna aykırı içerik taşıyan cd lerin satışının denetlenmesi;
ile görevlidir.

3.2. BİLGİ İŞLEM DAİRE BAŞKANLIĞI

1) Bilişim teknolojilerini takip ederek, bilişim suçları alanındaki gelişmeleri araştırmak, tanımlarını yapmak ve ilgili daire başkanlıklarına bildirmek,
2) Yerli ve yabancı kaynaklarla (Üniversite, Diğer ülkelerin polis teşkilatları, sivil örgütler) irtibata geçerek bilişim suçlarını incelemek ve ortak çalışmalar yapmak.
3) Virüs, trojan ve benzeri programlardaki gelişmeleri takip etmek ve konu hakkında teşkilatı bilgilendirici bülten hazırlamak,
4) Diğer Daire Başkanlıkları ve illerdeki bilişim suçlarıyla ilgilenen personelin bir araya gelerek karşılıklı bilgi alış verişinde bulunacağı ve ortak kararların alınacağı bilişim suçları kurulunun 4 ayda bir toplanmasını organize etmek,
5) Bilişim alanındaki diğer kuruluşlarla birlikte Bilişim suçlarının tartışılarak teknolojik, kriminolojik ve hukuki boyutunun incelendiği Bilişim Suçları ve Bilgi güvenliği sempozyumunu yılda bir kere düzenlemek ,
6) Bilişim Suçları konusunda uzman personele gelişen teknolojiler hakkında bilgilendirici kurslar açmak;
ile görevlidir.

3.3. GÜVENLİK DAİRE BAŞKANLIĞI

Internet ve dijital ortamda yayınlanan dergi, gazete ve benzeri yayınları incelemek, gerekiyorsa konu hakkında Adalet Bakanlığı ile ortak çalışmalar yapmak ile görevlidir.

3.4. İNTERPOL DAİRE BAŞKANLIĞI

1) Bilişim suçları ile ilgili olarak uluslararası kuruluşlar ve Polis teşkilatlarıyla gerekli koordinasyonu yapmak,
2) İnterpol ve diğer uluslararası kurumlardaki konu hakkında gelişmeleri takip etmek ve ilgili daire başkanlıklarını bilgilendirmek,
ile görevlidir.

3.5. KAÇAKÇILIK VE ORGANİZE SUÇLAR DAİRE BAŞKANLIĞI

1) Kanunsuz olarak bilgisayar yazılımlarının kopyalanmasının ve satışının takibi ve denetlenmesi,
2) Bilgisayar yoluyla dolandırıcılık ve sahtecilik suçlarının takibi ,

ile görevlidir.

3.6. KRİMİNAL POLİS LABORATUVARLARI DAİRE BAŞKANLIĞI

1) Bilişim teknolojileri alanında işlenen suçlarda kullanılan cihaz, araç ve malzemeyi araştırmak, bu suçların oluşumu sonrası delillerini incelemek ve bu konuda görüş bildirmek,
2) Veri depolama medyalarının içerdiği suç delillerini (gizli dosyaları, silinmiş dosyaları, şifreleri, korumalı dosyaları) araştırmak, incelemek ve görüş bildirmek,
3) Veri depolamada kullanılan medyaların bırakabileceği fiziki izleri incelemek ve görüş bildirmek,
4) Bilişim sistemlerinde güvenlik yapılarının incelenmesi, bu sistemler içerisinde oluşabilecek açıkların tespit edilmesi ve bu açıkların istismarı esnasında bırakılabilecek delilleri incelemek ve görüş bildirmek,
5) Gerekli görülen hallerde Bilgi İşlem Daire Başkanlığı ile koordineli olarak bilirkişilik yapmak, ile görevlidir.

3.7. TERÖRLE MÜCADELE DAİRE BAŞKANLIĞI

Internet ortamındaki yasadışı sayfaları kendi yönetmelikleri gereği takip etmek ile görevlidir.

3.8. İSTİHARAT DAİRE BAŞKANLIĞI

Internet ortamındaki yasadışı sayfaları kendi yönetmelikleri gereği takip etmek ile görevlidir.

3.9. POLİS AKADEMİSİ BAŞKANLIĞI

Polis Akademisi bünyesinde kurulacak Polis Bilimleri Enstitüsü altında Bilişim Suçları Araştırma Grubu oluşturarak konunun hukuki ve teknolojik yönünü araştırmak ve üniversitelerle ortak çalışmalar yapmak ile görevlidir.

IV-BÖLÜM

4. BİLİŞİM SUÇLARINDA ARAMA VE ZAPT ETME

Bilgisayar ve haberleşme sistemlerinin kullanımındaki artış ile polis görevlileri yaptıkları tahkikatlar sırasında teknik bilgi gerektiren ileri teknoloji destekli suçlarla karşılaşmaya başlamışlardır. Bilgisayar teknolojileri içeren gelişmiş suçlarda uygulanması gereken arama ve zaptetme yöntemleri geleneksel suç tiplerinde uygulanan yöntemlerden farklıdır. Yinede bu yeni suç tiplerinde yapılması gereken arama yöntemleri ile standart suç tiplerinde yapılan arama yöntemleri arasında bazı paralellikler olabileceği unutulmamalıdır. Diğer suçlarda kullanılan standart soruşturma teknikleri (Şahitler, bilgi veren kişileri bulma gibi) bilişim suçlarında da değerlidir. Bir davada gerekli olan deliller belki de yazılım veya donanım üzerinde olmayabilir, fakat eski yöntemlerde olduğu gibi telefon kayıtlarında, ajandada, çalışma masasında tutulan bir not da olabilir.

Bu tip suçlarla daha etkin olarak mücadele edilebilmesi için bilgisayar teknolojileri hakkında teknik bilgiye sahip olmayan personelin uyması gereken prosedür bu çalışmada belirlenmiştir.

Bilişim suçları yalnızca yüksek bilgisayar teknolojileri içerisinde (Yetkisiz Erişim, Bilgisayar Sabotajı gibi) oluşan bir suç olmayabilir, aynı zamanda bilgisayar teknolojilerini araç olarak kullanarak geleneksel suçlar işleyen suçlularda da benzer bir inceleme gerekebilir. Örneğin bir kaçakçılık suçu sanığının evinde veya işyerinde yapılan aramalarda sanığa ait bilgisayar, databank gibi araçlara rastlanabilir. Bu tip ileri teknoloji ürünü cihazlar içerisinde muhtemelen soruşturmaya ışık tutacak değerli bilgiler bulunabilecektir.

4.1. OLAY YERİNDEKİ İLERİ TEKNOLOJİ CİHAZLARIN ARANMASI VE ZAPT EDİLMESİ:

1) Bir arama izni almadan önce karşılaşılan olayda bilgisayarın oynadığı rol iyi olarak tespit edilmelidir.

- **a)** Bilgisayar suçun bir aracı olabilir. Örneğin bir kalpazan para çoğaltmak için bilgisayarı, tarayıcıyı ve renkli fotokopi cihazlarını kullanabilir.
- **b)** Bilgisayarda bir suçun delilleri (Kaçakçının tuttuğu kayıtlar vs.) saklanabilir.
- **c)** Bilgisayar sanal ortamda meydana getirilen bir suçun işlenmesinde kullanılmış olabilir (yasa dışı yayın yapmak, bir kuruluşun web sayfasını izinsiz olarak değiştirmek vs.).

2) Bilişim suçu içeren bir olaya müdahale ediliyorsa mutlaka teknik bilgi sağlayacak birime (Bilgi İşlem Daire Başkanlığı, Kriminal Polis Laboratuvarları Daire Başkanlığı) danışılarak müdahale yapılmalıdır. İleri teknoloji cihazlarının incelenmesi için özel bir bilgi birikimi gerekmektedir. Bu konuda ehil olmayan kişilerin yapacağı müdahaleler önemli zararlara neden olabilir. Bu konu delil niteliği taşıyan iz ve emarelerin yok edilmesi kapsamında değerlendirilir.

3) Geleneksel bir suçun soruşturması sırasında veya genel asayiş uygulamaları esnasında ileri teknoloji ürünü cihazlara veya malzemelere ulaşılmışsa bu durumlarda ilgili cihazlar ve malzemelere el konularak uzman birimlere gönderilmelidir.

4) İleri teknoloji cihazları pahalı cihazlardır. Ele geçirilmelerinde, zapt veya müsadere edilmelerinde özel bir dikkat göstermek gerekmektedir. Yapılacak bir hata kişilere veya kuruluşlara ait bir çok önemli bilgilerin yitirilmesine ve büyük miktarda maddi zararlara yol açabilir. Bu yüzden ele geçirilenlerle ilgilenecek kişilerin bu konuda eğitilmeleri gerekmektedir.

6) Genel kanının aksine bilgisayar uzmanı diye bir şey yoktur. Yalnızca değişik bilgisayar sistemlerini bilen kişiler vardır. Öncelikle bulacağınız bilgisayar uzmanının ele geçirilen sistemin işletim sistemini bilmeye ihtiyacı vardır. Eğer seçilen uzman Teşkilatımız Personeli değilse yaptıklarını kontrol altında tutmanız ve her hareketin bir kaydının alınmasına özen göstermeniz gerekir. Eğer olayda bir ivedilik yoksa Teşkilatımız içerisinde uzmanlaşmış birimlerimize ulaşmamız daha doğru olacaktır.

5) Günümüzde bilgisayarlar ağlar yardımıyla başka bilgisayarlara bağlıdırlar. Bu yüzden bilgisayardaki delil olabilecek veriler bu bağlantılar yolu ile başka bir yerdeki bir bilgisayara yüklenmiş olabilir. Bu ikinci bilgisayar başka bir ülkede de bulunabilir. İşte burada Interpol devreye girmektedir.

Böyle bir durumun tespiti halinde öncelikle ikinci bir müzakere çıkartılması gerekmektedir. Bu tür olaylarda yapılabilecek en etkili girişim bir istinabe mektubunun hazırlanarak diplomatik kanaldan ilgili ülkeye gönderilmesidir. Tabii aynı zamanda İnterpol kanalını da devreye sokmak gerekir. Unutmayınız ki genel kaide olarak bilişim suçluları bulundukları ülkede yargılanırlar ve iade edilmezler.

4.2. BİLGİSAYARLARLA İLGİLİ BİR TAHKİKATTA İZLENMESİ GEREKEN PROSEDÜR:

1) Yapılacak tahkikatta öncelikle bir plana ihtiyacımız bulunmaktadır.

2) Ele geçirilenler önünüze geldiğinde ne gibi bir yardıma ihtiyacınızın olacağını tespit etmeniz gerekir. Örneğin:

Bilgisayarın sistemi nedir?

İçerisinde ne gibi bilgiler vardır?

3) Olay yerine gittiğinizde mutlaka buranın video veya fotoğraflarını detaylarını kapsayacak açıdan çekin.

4) Olay anında bilgisayar ekranında neler olduğunu tespit edin burada karşı bilgisayar ile olan bağlantı hakkındaki bilgiler bulunabilir.

5) Ele geçirilen tüm bilgiler en kısa sürede bir bilgisayar uzmanına iletilmelidir. Bu şahıs konunun uzmanı olan diğer kişilerle irtibat kurabilir ve sizin için gerekli delilleri yok edebilir.

6) Arama ekibi operasyon konusunda tam eğitimli olmalıdır. Ekip elemanlarının karşılaşacakları teknik malzemeleri tanıdığından emin olun. Günümüzde bilgisayarlar her ebatta olabilmektedir. Yardım için bir bilgisayar uzmanını hazır bulundurun.

7) Büyük bilgisayar sistemlerinin incelenmesi uzun bir süre alabilir. Bilgisayarın incelenmesi için yerinden götürülmesi mümkün değil ise tüm bilgilerin manyetik ortama alınarak götürülmesini sağlayın. Bunun için izin alınması gerekebilir.

8) Aramaya giderken yanınızda manyetik ortam için gerekli malzemeleri götürüyorsanız bunların önceden formatlanarak temizlenmiş olmasına dikkat edin. Ancak hiç kullanılmamış medyaları tercih etmeniz daha doğru olacaktır. Tek bir kez yazılabilir compact diskleri tercih ediniz. Manyetik ortamlarda tutulan bilgiler nem, toz ve elektrostatik etkiler nedeniyle bozulabilir. Bu yüzden bu ortamları taşırken ve saklarken dikkatli olunuz. Bu iş için üretilmiş taşıyıcılar kullanınız.

9) Bilgisayarları dikkatli taşıyın. Üzerinde teyp işareti olan malzemeler ani hareketlerden dolayı zarar görebilirler. Büyük bilgisayar sistemleri sökülecekse uzmanlık gerekir. Özel taşıma ve depolama önlemlerinin alınması gerekir.

4.3. İLERİ TEKNOLOJİ SUÇLARINDA ARAMA:

Hiçbir zaman zanlının bilgisayar sistemine dokunmasına izin vermeyin. Dokunulduğunda tüm bilgileri silecek tek bir tuş olabilir. Aramada zanlının cihazlardan uzak bir yerde kontrol altında bulunması gerekmektedir. Bunun yanında sistem hakkında, açık kapalı olması, şifreler gibi önemli bilgilere sahip olabilir. Fakat sistemin belirli bir şifre girildiğinde otomatik olarak kendini yok etmeye programlanmış olması ihtimali de göz önüne alınmalıdır.

Durumu dondurmak çok önemlidir. İlk yapılması gereken şahısları cihazlardan uzaklaştırmaktır. Telefon ve veri haberleşmesi de kontrol altına alınmalıdır. Hiç kimsenin bir şeyi almasına veya bilgisayarda bir işlemi tamamlamasına izin vermeyin. Çok çeşitli bilgisayar ekranları, yanıp sönen lambalar ve kablo bağlantıları olabilir. Fakat uzman müdahalesine kadar hiçbir şeye dokunmayın. İçeriden yapılacak bir müdahale, uzaktan gelecek olandan daha büyük zarar verebilir. Bilgisayarlar açık bırakıldıklarında tehlikeli değildirler. 7/24 çalışacak şekilde üretilmişlerdir. Teknik ekip gelene kadar zanlıların bir başka yerle irtibata geçmesini önleyin. Çünkü bilgisayar sistemlerine uzaktan bağlanılarak bilgisayarın başında yapılabilecek bütün işlemler yapılabilir. Zanlılar başkalarını uyarıp delillerin yok edilmesine neden olabilir.

Bilgisayara bakın ve modeli ile markasını not edin. Önemli ise bulunduğu yerin bir krokisini çizin. Yardım için ilgili teknik polis birimi veya bir bilgisayar uzmanı ile irtibata geçin. Kimsenin

bilgisayara dokunmasına izin vermeyin. Bunun iki önemli sebebi vardır. Birincisi eğer uzman olmayan birisi bilgisayar ile ilgilenirse daha sonraki aşamalarda uzmanların yapacağı delil toplamasının kalitesi garanti edilemez. İkincisi mahkemeler tarafından delil olarak kabul edilebilecek bilgilerin toplanması mümkün olmayabilir. Kriminal Polis Laboratuvarları Daire Başkanlığı bünyesinde ileri teknoloji ürünü olan cihazlardan elde edilen delillerin mahkemelerde sunumunun sağlanabilmesi üzerinde çalışmalar yapılmaktadır.

Uzmanların bulunması hemen mümkün olmayabilir. Bilgisayar açık ise kapatmak tehlikeli olabilir. Elektrik kesilmesi geçici hafızadaki (RAM) bilgilerin kaybolmasına neden olabilir. Bilgisayarların kurcalanması sonucu bilgilerin silinmesi de mümkündür.

Bilgisayar çalışmıyor gibi görünse de yerinden alınması tehlikeli olabilir. Bilgisayarın önünde her hangi bir ışık yanmıyor, ekranı karanlık veya soğutma fanı çalışmıyorsa da bu bilgisayar kapalıdır anlamına gelmez. Özellikle küçük bilgisayarlar pille çalışıyor olabilir.

Tüm bunlar kontrol edildikten sonra bilgisayarın çalışmadığına kesin emin olduğunuzda tüm kabloları ve fişleri daha sonra tekrar takabilmek üzere işaretleyerek yerlerinden sökün. Bilgisayar değişik parçalardan meydana geliyor ise tüm parçaları araştırma için alın.

Bilgisayarın bağlı olduğu diğer parçaları araştırmak için tüm binayı kontrol edin.

Eğer mümkün ise cihazların fotoğraf ve görüntüsünü kayd edin. Tüm cihazların bulundukları yerlerin kaydedilmesi daha sonraki mahkeme aşamalarında gerekli olabilir.

Cihazları aldığınızda tüm manyetik birimlerin, kitapların, notların ve basılı kağıtların alındığına emin olun. Unutmayın ki şifreler bilgisayarın yanında bulunabilecek küçük kağıt parçalarına yazılmış olabilir. Bunlar daha sonraki işlemler için çok gerekli olabilir. Disketleri ambalajlarından çıkartıp güvenli bir yere koyun.

4.4. DELİLLERİN SAKLANMASI:

Tüm cihazları ve malzemeleri toz, manyetik ortam ve güneş ışığından uzakta normal oda şartlarında saklayın.

V- BÖLÜM

5. SONUÇ:

Bilişim teknolojilerinin gelişimi ile birlikte toplum içerisindeki ilişkiler bu yapılar üzerine kaymaya başlamıştır. Teknolojinin gelişimi beraberinde yeni suç tiplerini ve geleneksel suç tiplerini farklı bir şekilde karşımıza çıkarmıştır.

Ülkemizin iç güvenliğinden sorumlu olan Teşkilatımız meydana gelen bu yeni nesil suç tipleriyle mücadelede kanunların kendisine vermiş olduğu sorumluluklar çerçevesinde gerekli çalışmaları başlatmak ve ivedi bir şekilde konunun üzerine gitmek zorundadır.

Ülkemizde bilişim teknolojilerinin hızla yayılmasıyla bu tip suçların artması kaçınılmazdır. Yeni nesil suç tipleri daha önceki suç tiplerinden farklı olarak ileri teknoloji boyutuna sahiptir. Bu suçlarla mücadele edebilmek için suçun yapısını ve araçlarını cok iyi tanımalı ve bu suçlarla mücadelede ileri teknoloji araçları kullanılması zaruridir.

Bu tip suçlarla mücadele edebilmek için görev ve sorumluluklar, Teşkilatımızın yapısına göre Daire Başkanlıklarına paylaştırılmıştır. Raporda belirtilen görev ve sorumluluklar çerçevesinde yönetmeliklerde düzenlemelere gidilmeli, ilgili personel, yeterli eğitim verilerek alanında uzmanlaşması sağlanmalıdır. Koordinasyonu sağlamak ve etkin olarak mücadele etmek amacıyla ilgili Daire Başkanlıklarının bilişim suçları alanında çalışan personelinin bir araya geldiği "Bilişim Suçları Kurulu" oluşturulmalıdır.

Bu konuda Bilgi İşlem Daire Başkanlığı Bünyesinde Bilişim Suçları Bilgi Bankası oluşturularak, bu alandaki suçların tasnifi ve araştırılmasında sistematik geliştirmek icin çalışmaların başlatılması zarururet arz etmektedir.

Bu konuda uzman eleman yetiştirmek ve konu ile ilgili personele egitim vermek maksadıyla İnterpol'ün her sene düzenlediği "Computer Crime Training Course" larına personel gönderilmesi ve bu konudaki uluslararası toplantılara katılınması ve bu konuda gerekli ödeneğin ayrılması artık zaruret arz etmektedir.

Bilgilerinize arz ederiz.