T.C.
FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
EĞİTİM BİLİMLERİ ANABİLİM DALI

BİLİŞİM SUÇLARIYLA MÜCADELEDE POLİSİN EĞİTİMİ

DOKTORA TEZİ

DANIŞMAN

Prof. Dr. Mehmet TAŞPINAR

HAZIRLAYAN

Çetin GÜMÜŞ

ELAZIĞ - 2008

T.C.

FIRAT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

EĞİTİM BİLİMLERİ ANA BİLİM DALI

BİLİŞİM SUÇLARIYLA MÜCADELEDE POLİSİN EĞİTİMİ

DOKTORA TEZİ

Çetin GÜMÜŞ

Bu tez, / /2008 tarihinde aşağıdaki jüri tarafından oy birliği / oy çokluğu ile kabul edilmiştir.

Danışman	**Üye**	**Üye**
Prof. Dr. Mehmet TAŞPINAR GÜROL	Prof. Dr. Sebahattin ARIBAŞ	Prof.Dr. Mehmet

Üye	**Üye**
Yrd.Doç.Dr. Mehtap YEŞİLORMAN	Yrd.Doç.Dr. Mukadder BOYDAK

Bu tezin kabulü, Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun ... / / ..... tarih ve ..... sayılı kararıyla onaylanmıştır.

Ö Z E T

Doktora Tezi

BİLİŞİM SUÇLARIYLA MÜCADELEDE POLİSİN EĞİTİMİ

Çetin GÜMÜŞ

Fırat Üniversitesi
Sosyal Bilimler Enstitüsü
Eğitim Bilimleri Anabilim Dalı

2008; Sayfa : XVII + 388

Bu araştırmada, bilişim suçları ve polisin bu suçlarla etkin mücadele etmesi için gerekli eğitim organizasyonları çeşitli boyutlarıyla incelenmiştir. Öncelikle, bilişim suçları alanında görev yapan polisin bilişim suçlarındaki mevcut durumunu (eğitim seviyesi, teknik donanım ve ünite vb.) ortaya çıkarmak ve Türk polisinin bilişim suçları alanında genel bir profilinin çıkarılması amacıyla 81 İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlükleri'nde bilişim suçları konusunda görev yapan 379 personele yönelik anket uygulanarak çeşitli veriler elde edilmiş ve ihtiyaç belirlemesi yapılmıştır. Uygulanan anket çalışması ile personelin bilişim suçları konularında kişisel bilgileri, yetkin olduğu konular, mevcut sıkıntılar ve ihtiyaçlar kapsamında kendi görüşlerinin yanı sıra, kurs görme durumları vb. esas alınarak bilişim suçlarına ilişkin yeterlilikleri hakkında anlamlı görüş farklılığı bulunup bulunmadığı araştırılmıştır. Toplam **379** kişiye uygulanan anketlerle çeşitli araştırma bulgularına ulaşılmış ve konuyla ilgili öneriler getirilmiştir. Ayrıca, konu alanı uzmanlarından yararlanılarak personelin bilişim suçlarıyla etkin mücadelesi için uygun eğitim içeriği ile modüller geliştirilmiş ve böylece bilişim suçları eğitimi için temel ve uzmanlık seviyesinde personel yetiştirme kurs programları hazırlanmıştır.

Araştırmadan elde edilen verilere göre **sonuçlar** şöyle özetlenebilir:

Bilişim suçları konusunda Emniyet Teşkilatı'nda görev yapan Kaçakçılık ve Organize Suçlar Şube Müdürlüğü ile Bilgi İşlem Şube Müdürlüğü'ndeki görevlilerin önemli ölçüde eğitim ihtiyacı olduğu tespit edilmiştir.

Bu suçlarla mücadele için ünite, teknik donanım, personel ve eğitim ihtiyacı bulunmaktadır. Adli bilişim alanında personel genel olarak yetkin değildir. Emniyet Teşkilatında, bilişim suçları konusunda idari yapılanmaya gidilmemesi, görev paylaşımı ve kurum organizasyonunda bir takım sorunları ön plana çıkarmaktadır. Suç öncesinde, bilişim suçlarının önlenmesinde teşkilatın ve toplumun farkındalık düzeyinin yeterli düzeyde olmaması önemli bir problem teşkil etmektedir.

Araştırma kapsamında getirilen **öneriler** ise şu şekilde özetlenebilir:

Bilişim suçları konusunda Emniyet Teşkilatı'nda görev yapan Kaçakçılık ve Organize Suçlar Şube Müdürlüğü ile Bilgi İşlem Şube Müdürlüğü görevlilerinin eğitimi için, dünya standartlarına paralellik gösteren eğitim programları geliştirilmeli, sertifikasyon sistemine geçilmeli ve çeşitli eğitim organizasyonlarıyla bilişim suçlarında görev üstlenen polisin eğitim ihtiyacı karşılanmalıdır. Ayrıca, eğitim planlarına alınarak tüm polis teşkilatı personeline yönelik temel seviyede hizmetiçi eğitim programları düzenlenmelidir.

Bu suçlarla mücadele için tüm İl Emniyet Müdürlükleri'nde uygun ortam, teknik donanım, personel ve eğitim imkanları sağlanmalıdır. Adli bilişim alanında personelin yetkinliği artırılmalıdır.

Emniyet Teşkilatında, bilişim suçları konusunda idari yapılanmaya gidilerek görev paylaşımı ve organizasyonu yapılmalıdır. Bilişim suçları konusunda kurumlar arası işbirliği artırılmalıdır. Suç öncesinde, bilişim suçlarının önlenmesinde teşkilatın ve toplumun farkındalık düzeyini geliştirici süreç planlaması yapılarak çeşitli faaliyetler düzenlenmelidir.

Anahtar Kelimeler: Polis, Bilişim Suçları, Suçla Mücadele, İnternet, Eğitim, Öğretim Programı

SUMMARY

Ph. D. Thesis

TRAINING OF THE POLICE AGAINST CYBER CRIME

Çetin GÜMÜŞ

University of Fırat

The Institute of Social Science

And Departmant of Educational Sciences

2008, Page: **XVII + 388**

In this research cyber crime and training organizations necessary for the police against these crimes were investigated in terms of various aspects. First of all, a self-administered survey was conducted including 379 officers who serve at Provincial Directorates of Smuggling and Organized Crimes and Data Processing Branch Offices in 81 provinces in order to determine the existing state of the police (educational status, technical equipment and unit etc.) combatting computer related crimes and to develop a profile of Turkish police in terms of these crimes. By the survey it was tried to ascertain if there were significant differences in the views in regard with their efficiency against cyber crimes based on the personal information of the personnel for cyber crime, topics on which they are competent, actual distresses and requirements as well as their training states. By the surveys including **379** respondents it was reached various research findings and given recommendations in regard with the subject. Moreover, modules were developped with appropriate training contents for efficient combatting of personel against cyber crimes by making use of experiences of the experts and courses programs were made to train personnel at basic and expertise levels.

Results according to the data from the research might be summarized in following way:

It was observed that the staff who are on duty at Provincial Directorates of Smuggling and Organized Crimes and Data Processing Branch Offices needs urgently to be trained.

There are requirements for backdrop, technical equipment and personnel in order to struggle with this kind of crimes. In general, forensic information staff is not competent.

Mission sharing and reorganization in the law enforcement agency are necessary by effecting administorial restructuring in regard with computer related crimes. Consciousness level of agency and public for preventing cyber crimes have to be increased.

Recommendations in frame of the research might be summarized in following way:

Training programs in world standarts should be developped in order to train the staff who are on duty at Provincial Directorates of Smuggling and Organized Crimes and Data Processing Branch Offices, certification system should be introduced and the training need of the police officers who are on duty for cyber crimes and for various training organizations should be met.

Furthermore, in-service training programs at basic level for the personnel at all law enforcement agency should be organized.

In order to combat these crimes provincial security directorates should be supplied with backdrop, technical equipments and personel. Competency of personnel in forensic information shall be provided.

Mission sharing and reorganization in law enforcement agency should be provided by effecting administorial restructuring. Cooperation among the agencies for cyber crime should be strenghtened. Before crimes have been committed activities for increasing consciousness level of the agency and public should be made.

Key Words: Police, Cyber Crimes, Combatting Crimes, Internet, Education, Instructional Program

Ö N S Ö Z

Tüm dünyanın son asrımızda hızla bilgisayarlaşması ile beraber, bizlere hediye ettiği suç ortamlarından birisi de çeşitliliği, kompleksliği, etkisi ve sayısı hızla artan bilişim suçlarıdır. Yine, sürekli değişen dünyada özellikle 1990'lardan sonra günlük hayatın içerisine çok hızlı bir şekilde giren İnternet olgusu; bireylerin, toplumların, devletlerin hayatlarında önemli değişikliklere yol açmıştır ve açmaya da devam edecektir. İnternet olgusuyla birlikte, hayatın her alanında başta A.B.D olmak üzere tüm dünyada olduğu gibi ülkemizde de bilişim suçları günlük hayata damgasını vurmakta ve ülkelerin yaka silktiği konuların başında yer alagelmektedir. Çünkü, devletlerin güvenliğini etkileyen, teröre hizmet edebilen, ayrıca ekonomi ve ticaret dünyansında da büyük maddi kayıplara yol açarak kişilerin günlük hayatını ihlal eden yapısıyla bilişim suçları, yediden yetmişe herkesi içine alan bir tehdit unsuru haline gelmiştir. Ne zaman, nerede, nasıl ortaya çıkacağı belli olmayan, ortaya çıkaracağı maddi külfeti kolayca hesaplanamayan, ayrıca moral faktörleri de oldukça olumsuz etkileyen bu suç türü, çağın vebası olarak tüm dünyada başta kolluk güçleri olmak üzere, bilişim suçları ile mücadele eden tüm ortak paydaları sürekli olarak tedirgin eden, meşgul eden ve önlemler almaya iten bir nitelik kazanmıştır. Türk polisi de, ülkemizde bilişim suçlarıyla mücadelede gecikmeden yerini alma çabasını göstererek bu amaçla çeşitli idari yapılanma, organizasyonlar ve eğitim süreçleri geliştirme gayreti içerisine girmiştir. Bilişim suçlarıyla etkin olarak mücadele edebilmek için personelin eğitim programları geliştirilerek etkin eğitiminin sağlanması ve belli uluslar arası standartlara ulaşarak gerekli ünitelerin kurulması, Emniyet Teşkilatı açısından da büyük önem taşımaktadır. Ülkemizde günlük hayatımıza hızla giren ve artık beraber yaşamak zorunda olduğumuz bilişim suçlarını ve bu suçlarla mücadele eden Türk polisinin yetkinliğini ve eğitimini incelemek Emniyet Teşkilatı açısından son derece önemlidir. Çünkü; incelenen alan ve konular, klasik suç ortamının aksine genel itibariyle kompleks, yeni, zorlukları olan, yol alınması ve geliştirilmesi gereken güncel konulardır. Bilişim suçlarını araştırmak, ünite kurmak ve bilişim suçları için nitelikli personel temin etmek, gerekli eğitim faaliyetleri ile personeli yetiştirmek ve kurum içerisinde istihdam etmek oldukça müşkül, maliyetli ve büyük emek isteyen

hususlardır. Bilişim suçlarıyla etkin mücadele ve bu mücadelede emniyet personelinin eğitimi; toplumsal hayatı ve ülke güvenliğini direkt olarak etkilediğinden dolayı, bilişim suçlarının mümkün mertebe önlenmesi, çözümü ve tehdit unsuru olmasının önüne geçilmesi açısından gerçekten de büyük önem taşımaktadır. Bizlere akademik bakış kazandıran çok değerli öğretim üyeleri/görevlilerinin katkılarıyla bilişim suçları gibi önemli bir konuyu bilimsel olarak incelemek kurum idarecileri ve Emniyet Teşkilatı çalışanlarına önemli katkılar sağlamıştır. Günümüzün hızla değişen ve gelişen koşullarında, üniversite-emniyet işbirliğinin yurt genelinde her zaman ve etkili bir şekilde devam ettirilmesi gerektiği bir gerçektir. Güvenli bilgi toplumu olma ve bilişim suçlarında güçlü olma yolunda yapılan bu çalışmanın emniyet ve eğitim camiasına, ayrıca bilişim ve İnternet dünyasının içinde olan tüm ortak paydalara ve ilgili herkese katkı sağlayacağını umuyorum.

Tez sürecinde tüm çalışmalarımda hiçbir desteği esirgemeyen tez danışmanım Sayın Prof.Dr. Mehmet TAŞPINAR'a teşekkür ederim. Ayrıca, beni sürekli destekleyen ve teşvik eden İl Emniyet Müdürüm Sayın Hüseyin NAMAL'a, kıymetli arkadaşlarım 4. Sınıf Emniyet Müdürleri Mehmet Akif ÇİMEN ve Ali Erkan ALAÇ'a, ayrıca birlikte mesai yaptığımız değerli personelimle beraber Fırat Üniversitesi Eğitim/Teknik Eğitim Fakülteleri'nin çok değerli öğretim üyeleri/görevlilerine en derin şükranlarımı ve saygılarımı sunarım. Bilişim suçlarıyla mücedele ve polisin eğitimi konusunda hazırlamış olduğum anket çalışmasının uygulanması aşamasında bana destek olan başta Emniyet Genel Müdürlüğü olmak üzere, tez kapsamında hazırlanan anketleri dolduran bilişim suçlarında görev yapan 81 İl Emniyet Müdürlüğü KOM ve Bilgi İşlem Şube Müdürlüğü personeline teşekkür ederim. Araştırmada, bilişim suçları eğitimi kapsamında hazırlanan modüllerin geliştirilmesi konusunda desteklerini esirgemeyen konu alanı uzmanlarına da teşekkür ederim.

Ayrıca; tez çalışmam süresince beni sürekli destekleyen ve fedakarlıkta bulunan en başta eşim Münire GÜMÜŞ'e ve çocuklarım Nusret ile Nilgün'e, ayrıca Bilgisayar Öğretmeni kardeşim Gülsüm'e de teşekkürlerimi sunarım.

Kocaeli, Kasım 2008 Çetin GÜMÜŞ

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM

DÖRDÜNCÜ BÖLÜM

BEŞİNCİ BÖLÜM

ALTINCI BÖLÜM

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

BİRİNCİ BÖLÜM

1. GİRİŞ

Günümüz teknolojilerindeki başdöndürücü gelişmeler, tarihteki diğer dönemlerden çok daha ileri ve geniş kapsamlı bulunmaktadır. Teknoloji, artan bir ivme içerisinde ilerlemekte ve en önemli değişiklikler İnternet, bilgisayar ve iletişim teknolojilerinde meydana gelmektedir.

Teknolojideki gelişmeler bireylerin, toplumların, örgütlerin yaşamını kolaylaştırdığı, iktisadi ve sosyal hayata önemli katkılar sağladığı gibi pek çok olumsuzlukları ve yeni suç unsurlarına da beraberinde getirmiştir. Bugün bilgisayar ve İnternet ortamında çeşitli elektronik araç ve gereçlerinin de kullanımıyla özellikle bilişim dünyasının içerisinde daha erken yer alan gelişmiş ülkelerde çeşitli bilişim suçları ile yoğun olarak karşı karşıya kalınmaktadır. Bilişim ortamında saldırganlar; kolayca kişisel verileri elde edebilmekte, şirketlerin, bankaların, kamu kurumlarının sistemlerine girerek büyük zararlar verebilmekte, bilgisayar ortamındaki bilgileri bozabilmekte ya da çalabilmektedirler. Sanal dünyada sahtecilik, dolandırıcılık, pornografi, sabotaj, hırsızlık, kaçakçılık, hakaret, tehdit, devlet aleyhine işlenen ve teröre hizmet eden suçlar gibi birçok suç yoğun olarak işlenegelmekte ve yeni işlenebilecek suç modellerine dünya gebe kalmaktadır.

Bugün artık dünya; devletleri tehdit eden, halkı dehşet ortamına sürükleyebilen, her türlü bilgi bankalarına müdahale edebilen siber terörizmle mücadele etmek durumundadır. Terör örgütleri bilgisayar teknolojisi ve bilgisayar ağlarını kullanarak iletişimlerini kolaylıkla sağlamakta, yıkıcı ve bölücü faaliyetlerini, propagandalarını rahatlıkla elektronik ortam üzerinden sürdürebilmektedirler.

Diğer taraftan, bazı gelişmiş ülkeler bilişim ortamında siber casusluk yöntemlerini yoğun bir şekilde kullanmaktadırlar. Ülkeler veya çıkar gruplarının, askeri ve siyasi bilgilerin yanısıra; sanayi, teknoloji, terör, sağlık, uyuşturucu,

tarihi eser ve çevre gibi bir çok alanı içeren verileri kolayca elde etmeleri ve bu bilgileri ekonomik ve siyasal çıkarları doğrultusunda kullanmaları mümkündür.

Teknolojideki gelişmeler savaş ortamlarını da etkilemiştir. Günümüzün savaş ortamında silah sistemlerinin neredeyse tamamı bilgisayar ve bilgisayar teknolojileri sistemiyle yönetilmektedir. Ülkeler, gelecekte insansız savaşabilecek ileri teknoloji sistem ve cihazları üzerinde çalışmaktadır. Savaşların gelecekte klavye başında, mause tıklamaları ile veya cep telefonu tuşlarıyla gerçekleşmesi muhtemeldir. Hal böyle olunca, bilişim suçlarının ulus güvenliğinin en büyük tehdit kaynağı olması da kaçınılmaz olmaktadır.

Diğer taraftan çocuk pornografisi, kredi kartı kopyalama vb. bilişim yoluyla işlenen asayiş suçları, spam mail, MSN hırsızlığı vb. tehditler her geçen gün hızla artmaktadır. Artan bu tehditlere karşı alınacak önlemler ve düzenlenecek eğitim programlarının geniş kapsamlı ve etkili olması gerekmektedir.

Gelişen teknolojilerin ortaya çıkardığı yeni değerler, bir yandan yeni hukuki yararlar meydana getirirken bir yandan da bunların ihlali, yeni koruma alanlarının ve suçların düzenlenmesini gerektirmektedir. Değişim çok süratli olmakta fakat bu hızlı değişime hukukun ayak uydurması, ortaya çıkan yeni ihtiyaçların karşılanması için gerekli hukuki düzenlemelerin yapılması aynı süratle olmamaktadır. Uluslararası kuruluşlar, diğer dünya ülkeleri ve ülkemiz bilişim hukukunu; sürekli etkili bir mevzuat sistemi içerisinde bulundurmaya gayret göstermektedir.

Bu suçların boyutları doğal olarak kolluk kuvvetlerini de düşündürmektedir. Teknik ve yasal zorlukların yanında operasyonel ve Adliye-Polis-Telekom gibi kurumlar arası koordine zorlukları, uluslar arası işbirliği ve yine bu tür suçlarla ilgili uzman personel yetiştirme zorluğu, kolluğun bu suçlarla mücadelesi açısından önemli engeller teşkil etmektedir. Suçluların teknolojik gelişmeleri kullanarak kazandıkları hızı, kolluk kuvvetleri de yapacakları teknolojik yapılanma, sürekli eğitim organizasyonları, karşılıklı işbirliği ve

çalışma stratejileri ile kazanma yoluna gitmektedirler. Dünyanın neresinde olursa olsun her ülke bilişim ortamında işlenen suçlar konusunda başarılı olmak için; teknolojiyi iyi takip eden, adli bilişimi uygulayabilen, kendisini suç öncesi ve suç sonrası bilişim suçları ile mücadeleye adapte etmiş uzman görevlilere ve konuya motive olmuş yöneticilere gereksinim duyulmaktadır.

1.1 Problem

Günümüz teknolojilerindeki başdöndürücü gelişmeler, tarihteki diğer dönemlerden çok daha ileri ve geniş kapsamlı bulunmaktadır. Teknolojideki gelişmeler; bireylerin, toplumların, örgütlerin, devletlerin yaşamını kolaylaştırdığı, iktisadi ve sosyal hayata önemli katkılar sağladığı gibi pek çok olumsuzlukları, mali külfetleri ve gelişen, değişen yeni suç tehdit ve faktörlerini de beraberinde getirmiştir.

Her yeni gelişen teknoloji insan hayatını kolaylaştırdığı gibi, suç işlemek isteyenlerede bir takım suç işleme olanağı sağlamaktadır. İletişim teknolojisi, bilgisayar ve İnternet'in gelişimi ile birlikte 1990'lı yılların başlarında bilişim suçları ortaya çıkmıştır. Ülkeler, bilişim alanındaki ihlalleri farklı terimlerle karşılamaya çalışmaktadırlar. Bu ihlaller; Amerika Birleşik Devletleri'nde "computer crime", "cyber crime" veya "computer related crime", İngiltere'de "high-tech crime", Almanya'da "computer-kriminalität", İtalya'da "la criminalitá informatica", Fransa'da "la fraude informatique", Türkiye'de ise "bilişim suçları", "siber suçlar" veya "yüksek teknoloji suçları" olarak adlandırılmaktadır (Yazıcıoğlu, 1997). Bilişim suçları kavramı konusunda uluslar arası arenada bir çok tanım bulunmaktadır. Bu da suçun tanımı konusunda yeknesaklığın sağlanamamasına sebep olmakta ve özellikle hukuksal alanda problemlere yol açmaktadır.

Bilişim suçları olgusu hem ülkemizin, hem de dünyanın göz ardı edilemez bir gerçeğidir. Bugün bilgisayar ve İnternet ortamında çeşitli elektronik araç ve gereçlerinin de kullanımıyla özellikle bilişim dünyasının içerisinde daha erken yer alan gelişmiş ülkelerde, çeşitli bilişim suçları ile daha yoğun olarak karşı karşıya kalınmaktadır. Bu suçlarla mücadele etmek ve mücadelede başarı

sağlamak için tüm kurumlarla birlikte yöntemler belirlemek, geliştirmek ve uygulamak, ayrıca organize edilmiş sürekli eğitim faaliyetleri düzenlemek gereklidir. Gerçek hayatta güncel olarak rastlanılan suç tipleri artık dijital ortama taşınmıştır ve bu ortamda da sıkça görülmektedir. Pornografik ve yasadışı yayınlar, MSN hırsızlığı, kredi kartı dolandırıcılığı, telif hakları ile korunan bilgisayar yazılımlarının kopyalanması, e-mail yoluyla hakaret ve tehdit, spam mail vb. suç tipleri artık günümüzde İnternet ve özellikle bilgisayarlar üzerinde yoğun olarak işlenmektedir. Ayrıca yaşanan yüksek teknoloji suçları, bilinen suç tiplerinden farklılık arz etmektedir. Bu yüzden bu tip suçlara, polisler ve suçun soruşturulması esnasında görevli olan herkes daha duyarlı olmak durumundadır. Çünkü elektronik cihazlar, bilgisayarlar ve diğer yüksek teknoloji ürünleri kullanılarak suç; daha kolay, hızlı ve ucuz işlenebilmektedir. Türkiye'nin İnternet ve iletişim ortamına daha fazla katılan yapısıyla, virüs gibi hızla yayılan bilişim suçlarına ve bu suçla mücadeleye ciddi olarak eğilmesi ve önlemler alması gerekmektedir. Bilişim suçlarını önlemede sadece polisin değil, servis sağlayıcılar, bankalar, sivil toplum kuruluşları gibi diğer tüm ortak paydaların ve vatandaşların aktif rol oynaması gerekmektedir. Bilişim suçlarında; toplumsal bazda önleyici tedbirler geliştirme ve bilişim şuurunu güçlendirme, toplumun farkındalık düzeyini artırıcı faaliyetlerde bulunma, büyük önem taşımaktadır. Çünkü, "Önleyici Hekimlik" hizmetlerinde olduğu gibi ve "Önlemek, tedavi etmeten daha iyidir" anlayışında olduğu gibi bilişim suçları da; doğası gereği suç oluşmadan önce alınacak tedbirlerle "Toplum Destekli Polislik" modeli anlayışıyla bilinçlendirme faaliyetleriyle tüm toplum için tehdit olma riskinden arındırılabilecektir. Klasik suçlarda Alo 155'e gelen ihbarlarda olduğu gibi, bu tür bilişim alanındaki suç ortamları içinde polise ve kolluk güçlerine ihbarların gelmesi büyük önem taşımaktadır. Vatandaş boyutunda bilişim suçları alanında düzenlenecek eğitim faaliyetlerinin sağlanması ile, ihbar oranının artacağı bir gerçektir. Ancak, genel olarak vatandaşların ve kolluk güçlerinin yeterli eğitim ve farkındalık düzeyinde olmadıkları da bir gerçektir.

Ülkemiz, tarih boyunca özellikle jeopolitik konumu gereği her zaman için çeşitli devletlerin ve terör örgütlerinin hedefi haline gelmiştir. Günümüzde, terör örgütlerinin kendilerine destek veren dış merkezli bilgisayar sistemleri

aracılığıyla ülkemize yönelik siber saldırı hareketlerinde bulunabilecekleri muhtemeldir. Siber saldırılara karşı, siber saldırı acil eylem planları hazırlanması her ülke için zaruret teşkil etmektedir. Siber terörizme karşı hazırlıksız bir şekilde bulunmak günlük hayatın akışını derinden felce uğratabileceği gibi, ülke güvenliğini ciddi bir şekilde tehdit edebilecektir.

Günümüzde, bilgisayarların ve bilgisayar ağlarının suç işlemek için bir araç olarak kullanılması nedeniyle Emniyet Teşkilatı da, bu yeni suç tipine ve siber terör faaliyetlerine karşı yoğun olarak çalışmalar yapmaktadır. Dünyada ve ülkemizde sürekli gelişen, büyüyen teknolojik tehditler göz önüne alındığında polis, asayişi sağlamak ve görevlerini başarıyla yapmak için gerekli teknik donanımı ve üniteleri kurmak, bilişim suçunun nasıl araştırılması gerektiğini, delillendirmenin nasıl yapıldığını, olay yerinden veriler toplamayı ve bu suçların nasıl önlenebileceğini öğrenmek, bu amaçla eğitim faaliyetleri organize etmek ve bilişim alanında ortak paydalarla etkileşim içerisinde bulunmak durumundadır.

Emniyet Teşkilatı'nda bilişim suçları konusunda, Merkezde; Kaçakçılık ve Organize Suçlarla Mücadele (KOM) Daire Başkanlığı ve başkanlığa bağlı eğitim merkezi TADOC (Turkish International Academy Against Drugs and Organized Crime - Uyuşturucu ve Organize Suçlara Karşı Uluslararası İşbirliği), Asayiş Daire Başkanlığı ve başkanlığa bağlı Suç Araştırma ve Soruşturması Eğitim Merkezi (SASEM), Bilgi İşlem Daire Başkanlığı, İstihbarat Daire Başkanlığı, Terörle Mücadele ve Harekat Daire Başkanlığı, Kriminal Polis Laboratuvarları Daire Başkanlığı, Güvenlik Daire Başkanlığı ve İnterpol Daire Başkanlığı bünyesinde çeşitli görevler yürütülmektedir.

Taşrada ise merkezdeki daire başkanlıklarına bağlı ve koordineli görev yapan başta KOM, Asayiş ve Bilgi İşlem Şube Müdürlükleri bilişim suçları konusunda faaliyetlerini yürütmektedirler. Özellikle İl Emniyet Müdürlüklerinde, KOM Şube Müdürlüğü Bilişim Suçları Büro Amirliği ve Bilgi İşlem Şube Müdürlüğü bünyesinde bilişim suçları konusunda görev ve faaliyetler yürütülmektedir.

Ülkemizde en çon nüfus barındıran il olan, banka ve finans merkezi, bilişim suçlarının en çok yaşandığı illerin başında gelen İstanbul ilinde ise, İstanbul Emniyet Müdürlüğü bünyesinde Bilişim Suçları Büro Amirliği, 2008 yılında Bilişim Suçları ve Sistemleri Şube Müdürlüğü'ne dönüştürülmesi İçişleri Bakanlığı'nın 25/04/2007 tarihli onayı ile uygun görülmüştür. İstanbul Valiliği'nin 29/05/2007 tarihli onayı ile İstanbul Emniyet Müdürlüğü bünyesinde Bilişim Suçları ve Sistemleri Şube Müdürlüğü, 03/09/2007 tarihinde Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı'na bağlı olarak İstanbul Emniyet Müdürlüğü bünyesinde Vatan hizmet binasında faaliyete geçmiştir (İstanbul Emniyet Müdürlüğü, 2008).

Uzman personel yetiştirme zorluğu, kolluğun bu suçlarla mücadelesi açısından önemli engel teşkil etmektedir. Dünyanın neresinde olursa olsun her ülke, bilişim ortamında işlenen suçlar konusunda yüksek teknolojiyi iyi takip eden, kendisini bilgisayar, İnternet ve iletişim konusuna adamış uzman görevlilere gereksinim duymaktadır.

Özellikle bilişim suçları, siber terör vb. alanlarda çalışmalar yapmak ve uzman personel yetiştirmek amacıyla Emniyet Genel Müdürlüğü'ne bağlı TADOC Bilişim Suçları Araştırma Merkezi Başkanlığı çeşitli faaliyetler yürütmektedir. Ayrıca, bilişim suçları ile mücadelede ve meydana gelen olayların çözümlenmesi konusunda başarıyı artırmak amacıyla Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Yüksek Teknoloji Suçları ve Bilişim Sistemleri Şube Müdürlüğü koordinesinde bilişim suçlarıyla ilgili 16 Adli Bilişim Bölge Merkezi kurulmuştur. Ancak, bilişim suçları ile ilgili eğitim programları, tüm bilişim suçları personeline uygulanamamıştır. Teşkilat genelinde, bilişim suçlarında görev yapan tüm personeli kapsayan eğitim ihtiyacı devam etmektedir. KOM, Asayiş ve Bilgi İşlem Şube Müdürlüğü personelinin tamamının belli bir yetkinliğe ulaşması için eğitim görmesi uzun bir zaman dilimine ihtiyaç olduğunu göstermektedir. Şu an için, etkin-yaygın bilişim suçları eğitim organizasyonları düzenlenememektedir. Eğitim konusunda diğer sorunlar, eğitim verecek personelin azlığıdır. Uygun personel belirlemesi

yapılarak ve gerekli şartlar sağlanarak, Bilişim Suçları Eğiticilerinin Eğitimi organizasyonları düzenlenmelidir. Emniyet Teşkilatı gibi hiyererşik yapıya sahip kuruluşlarda üst yönetimin ve idarecilerin de bilişim suçları konusunda eğitim ortamlarında bulunmamaları, bu konuyu verilen önem ve kaynak aktarımını, ayrıca bilişim suçlarıyla etkin mücadeleyi olumsuz etkilemektedir.

Görüldüğü gibi, her geçen gün sayıları artan ve suç tipi olarak farklılık taşıyan bilişim suçlarıyla mücadele edecek ve gelişen-değişen teknolojik suç ortamlarına karşı çözüm bulacak personelin yeterlik ve yetişmesinde sorunlar yaşanmaktadır. Kanun uygulayıcı kurumların bilişim suçlarıyla mücadelede karşısına çıkan en büyük problem, bilgisayar bilgisi ileri düzeyde olan personel eksikliği, yetişmiş personelin etkin olarak kullanılamaması ve kurumda muhafaza edilememesidir.

Bilişim suçlarıyla mücadele, İnternet ortamının gereği olarak bütün bireyleri, toplumları, kurumları ve devletleri direkt olarak etkilediğinden diğer suç tiplerine oranla daha yeni ve daha komplekstir. Bu tür suçlarla mücadele etmek sadece personel eğitimini değil, suç ve suçlu profili, uluslararası işbirliği, ilgili inceleme ünitelerinin kurulması, hukuki altyapı, toplumsal farkındalık ve daha bir çok unsuru içine almaktadır.

Emniyet birimleri tarafından, vatandaşlara yönelik olarak web ortamında çeşitli konularda bilgilendirme faaliyetleri yapılmaktadır. Elbetteki önerilerin yapılmasının yanı sıra toplumsal bilincin, tüm eğitim aşamalarında yaşam boyu eğitim anlayışı içerisinde eğitim yoluyla artırılmasıyla veba gibi salgın bir halde yayılan bilişim suçlarının önüne geçilme imkanı doğacaktır. Aksi takdirde, bilişim suçlarından birey, toplum ve devlet olarak her zaman etkilenmek ve finansal başta olmak üzere bir çok zarara uğrama söz konusu olacaktır.

Taşra yapısına bakıldığında, ülkemizde Emniyet Teşkilatı'nda bilişim suçları ile mücadelede yoğun olarak görevleri bulunan İl Emniyet Müdürlükleri, personel eksikliği, eğitim ve alt yapı gibi oldukça büyük problemlerle karşılaşmaktadır. Büyük illerde, bilişim suçlarıyla diğer illere oranla elbette daha

çok karşılaşılmaktadır. Özellikle son dönemlerde gerek savcılıklardan, gerekse ihbar ya da resmi yazıyla intikal eden bilişim suçları bir hayli arttığı görülmektedir. İmkanların yeterli olmaması ve uzmanlık gerektiren bir konu olması nedeniyle yetişmiş eğitimli personelin az olması ya da bazı birimlerde hiç bulunmaması bu suçlarla mücadeleyi İl Emniyet Müdürlükleri açısından daha da zorlaştırmaktadır. Elbette ki, bilişim suçları ile mücadelenin başarıya ulaşmasında belki de uygun personelin seçimi, personelin eğitimi ve teknik bilgiye sahip olması en önemli ve öncelikli konudur. Emniyet Teşkilatı'nda bilişim suçları konusunda genellikle yeterli bilgi birikimine sahip olmayan personel olduğu için işlenen bir suçta, konuyu dahi anlayamadıkları, iz ve delilleri incelemede yetersiz kaldıkları, yanlış anlaşılmalar nedeniyle ilgisi olmayan insanların mağdur edildikleri görülmektedir. Dünyanın her yerinde olduğu gibi, ülkemizdede kolluğun yeterli eğitimi almaması, delillerin kaybolmasına ve verinin bozulmasına yol açabilecektir. Yetişmiş personel ise, olay yeri çalışması yapabilen, dijital inceleme yapıp, rapor hazırlayabilen personel olarak, geri dönmeyen delil niteliğinde adli mercilere çalışmalar sunabilecektir. Emniyet Teşkilatı'nda aynı zamanda, bilişim suçları konusunda yeterli bilgi birikimine sahip olsa da, bu suçlarla mücadele eden personel sayısının az olduğu ve böylece suç takibi ve önlemesinde yetersiz kalındığı görülmektedir.

Bilişim suçları internet kafeler yönüyle incelendiğinde, ülkemizde bilgisayarlaşma ve İnternet'e bağlanma oranının, diğer ülkelere özellikle AB üyesi ülkelere göre düşük olduğu söylenebilir. Ülkemizde bireyler, ekonomik gerçekler de göz önüne alındığında İnternet ortamından yoğun olarak internet kafeler üzerinden yararlanmaktadırlar. Sayıları hızla artan ve genellikle çocuklarla gençlerin, İnternet'e giriş için en çok internet kafeleri tercih etmeleri göz önüne alındığında internet kafelerin eğitim amaçlı merkezler haline getirilmeleri ve suç unsuru mekanlardan uzak tutulmaları ve bu amaçlarla bu mekanların güvenlik standartları belirlenerek denetlenmesi büyük önem taşımaktadır.

Ülkemizde ve tüm dünya'da siber terör saldırılarının ve çeşitli bilişim suçlarının çoğunlukla İnternet üzerinden yapıldığı göz önüne alındığında, İnternet hizmeti veren ve içeride bululanlara ait herhangi bir kaydın yapılmadığı internet kafelerin de bu suç ortamlarına uygun bir zemin teşkil ettiği bir gerçektir. Bunun için, bu mekanların İçişleri Bakanlığı'nın ilgili genelgelerine ve TCK'na uygun hareket edip etmediklerinin belirlenmesi amacıyla, uzman denetleme kurulları ile internet kafelerin denetlenmesi gerekmektedir. Genellikle öğrenci gençlerin bulunduğu internet kafeler; bilişim suçları, siber terörizm gibi her türlü kötü amaçlı kullanım faaliyetlerinin önüne geçilebilmesi amacıyla etkili denetlenmesi gerektiği halde, belirlenmiş denetim standardı bulunmaması, yeterli teknik bilgiye sahip personel bulunmaması ve belki de devlet otoritesince konuya verilen önem eksikliği nedeniyle etkili olarak denetleme mekanizması bulunmamaktadır.

Bilişim suçları ile mücadele konusunda kanuni ve idari yapılanma büyük önem taşımakla beraber, tek başına ihtiyaçlara cevap vermemektedir. Bilişim suçları konusunda başlı başına bir yasa hazırlanması gerekmektedir. Ülkemizde, diğer ülkelerde olduğu gibi merkezi bir bilişim suçları ünitesi de bulunmamaktadır. Dolayısıyla, her birim kendi görev alanına giren konularda bilişim suçlarına müdahale etmekte ve bu durum, bu suçlarla ülke olarak başarılı bir şekilde mücadele etme aşamasında yeknesaklığı ve bilgi paylaşımını ortadan kaldırarak etkili bir mücadele edilememesine yol açmaktadır. Gerekli teknik donanım ve personelden yoksun olarak belli bir merkezden bilişim suçlarının takip edilmemesi, bu suçların haritasının ve istatistiğinin çıkarılmasında, suç analizi tespiti ve değerlendirilmesinde zorluklar yaşanmasına neden olmaktadır. Bu nedenle, diğer ülkelerde örneğin ABD (CERT) olduğu gibi, ülkemizde de iyi bir şekilde yapılandırılmış, nitelikli personelden oluşturulmuş, çeşitli araştırma birimlerinden oluşan ve kolluğun bilişim suçlarında daha yetkin olmasını sağlayacak (TURKCERT) kurulması büyük önem taşımaktadır.

Bilişim suçlarının çözüme kavuşmasında işbirliğinin rolü büyüktür. Emniyet, Türk Telekom, İnternet Servis Sağlayıcıları, Adliye birimleri ve ilgili

sivil toplum kuruluşlarının birlikte koordineli çalışması bilişim suçları ile mücadele konusunda çok önemli olduğu halde, gerekli işbirliği konusunda eksiklikler mevcuttur. Bilişim suçlarının hedefinin genelde özel şirketler olduğu göz önüne alındığında, suçun yapısından dolayı özel sektörle de işbirliği yapılması gerektiği halde, yeteri kadar işbirliği olduğu görülmemektedir. Özel sektörün tecrübesini bu işe yöneltmesi hem kamu hem de toplum için oldukça faydalıdır. Akgül (2002) bilişim suçları (cyber crime) ve delillerin toplanması konularında on-line işbirliği ağı kurulması gerektiğini belirtmektedir. Ama, gerekli online işbirliği ağının ülkemizde tesis edildiğini söylemek oldukça zordur. Ülkemizde genel olarak bilişim suçlarıyla ilgili ihbarlar ve şikayetler tam olarak ilgili birimlere gelmemektedir. Ancak bunların gelmemesi bu suçların işlenmediği anlamına gelmemektedir.

Bireylerin, bilişim suçları hakkında bilgi sahibi olmamaları, mevzuatı bilmemeleri ve bilişim suçları karşısında hangi merciye başvuracaklarını bilmemeleri de bir gerçektir. İhbar ve şikayet sayısının artması, güvenlik güçlerinin bu konuda gerekli tedbirleri almasına yardımcı olacaktır. Bilişim suçları ile mücadele konusunda İnternet ortamının özelliğinden dolayı uluslararası polis işbirliği de büyük önem taşımaktadır. Ancak, bu işbirliğinin istenen düzeyde olmadığı görülmektedir. Bu durum adaletin yerine gelmemesine, adaletin geç sağlanmasına, bir çok işlenen suçun sonuçsuz kalmasına, maliyeti yüksek maddi zararlar doğmasına ve suçluların cezalandırılamamasına neden olmaktadır. Ayrıca bilişim suçları konusunda, uluslar arası bir tanım yapılmaması da büyük sorun teşkil etmektedir.

Bilişim suçları ile mücadele konusunda en önemli problemlerden biri de, önceden belirlenmiş adli bilişim standartlarının olmayışıdır. İşlemlerin delillendirilmesi ve mahkeme aşamasında delil olarak kabul edilmesinde sorunlar yaşanmaktadır. Delillerin toplanmasında internet servis sağlayıcılara ve internet kafelere önemli görevler düşmekle beraber, genellikle duyarlı olmadıkları görülmektedir. Düzenlenecek mevzuat çalışmalarıyla bilişim suçları konusunda kesin hükümler ile tüm ortak paydaların işin içine dahil edilmesi ve sorumluluklarının belirlenmesi gerekmektedir.

Bilişim suçları ile mücadelede mali imkanların güçlü olması gerekmektedir. Mali imkanların yetersizliği, ilgili ünite ve altyapı kurulması ve bu ünitede görev alacak personelin eğitiminin sağlanmasında olumsuz rol oynamaktadır. Bilişim suçları ile mücadele edecek personelin eğitimi oldukça teknik bir alanı gerektirdiği için maliyeti de yüksek olmaktadır (Karaman, 2003). Emniyet Teşkilatı'nda bilişim suçları ile mücadele konusunda teknik, idari ve eğitime ait ihtiyaçları gidermek üzere yeterli düzeyde bütçe ayrılamamaktadır.

Bilişim suçları ile mücadele konusunda en önemli sorunlardan biri de, özellikle vatandaşların bilinç eksikliği ve farkındalık düzeyinin düşük olmasıdır. Bu nedenle, ülkemizde bilişim suçu mağdurları bu konuda nasıl müracaatta bulunacaklarını ve ilgili mevzuatları genel olarak bilemediklerinden kendi yöntemleri ile mağduriyetlerini gidermeye çalışmaktadırlar. Bu durumda, bilişim suçlarının çözümünde çeşitli sıkıntılara sebep olmaktadır. Ayrıca, bilişim konusunda işlenen suçlarla ilgili vatandaşların şikayetlerini ve mağduriyetlerini direkt olarak iletebilecekleri 2007 Kasım ayından beri fiili olarak görev yapan İnternet Güvenliği Başkanlığı gibi bir birim bulunmakla beraber, yeni kurulan bir müessese olduğu için kamuoyunun bu konuda duyarlı olması zaman almaktadır.

Bilişim suçları konusunda mevcut olan sorunların tespiti oldukça önemlidir. Bunun yanında bilişim suçları ilemücadele edecek polisin eğitimi de bilişim suçlarının önlenebilmesi açısından önemli olduğu düşüncesi ile bu araştırmaya gerek duyulmuştur.

1.2. Araştırmanın Amacı

Araştırmanın genel amacı, dünyada ve ülkemizde farklı şekillerde ortaya çıkan ve sürekli bir artış seyri gösteren bilişim suçlarıyla mücadele aşamasında, öncelikle bilişim suçları sahasında görev yapan polislerle ilgili ihtiyaç tespiti yaparak, polisin bilişim suçlarında mevcut durumunun ortaya çıkarılması sağlamak, ve bu ihtiyaca dayalı olarak temel ve uzmanlık seviyesinde polisin eitimine dönük **öğretim programı** hazırlamaktır.

1.2.1 Araştırmanın Alt Amaçları

Araştırma kapsamında; Emniyet Teşkilatı'nda bilişim suçları konusunda görev yapan 81 İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlüğü personelinin kişisel özellikleri, iletişim teknolojisi ve bilgisayara ilişkin özellikleri, bilişim suçları ile ilgili nitelikleri, bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi düzeyleri ve bu bilgileri gerekli görme düzeyleri konularında çeşitli görüşlerine ilişkin alt amaçlar şu şekilde belirlenmiştir.

1. Emniyet Personelinin Kişisel Özellikleri
   - a- Görevli olduğu il,
   - b- Görevli bulunduğu birim,
   - c- Eğitim durumu,
   - d- Rütbe durumu,
   - e- Emniyet Teşkilatı'ndaki hizmet süresi,
   - f- Bilişim suçları konularındaki hizmet süresi açısından durumları nasıldır?
2. Emniyet Personelinin İletişim Teknolojisi ve Bilgisayara İlişkin Özellikleri
   - a- Evde bilgisayar bulunma durumu,
   - b- Bilgisayar kullanma süresi,
   - c- Günlük bilgisayar kullanım süresi,
   - d- İnternet kullanma süresi,
   - e- Günlük İnternet kullanım süresi,
   - f- Web sitesine sahip olma durumu,
   - g- En çok yararlandığı haberleşme aracı,
   - h- İnternet üzerinden alışveriş veya para transferi **(sanal bankacılık)** yapma durumu,
   - i- İşletim sistemlerindeki güncellemeleri takip edebilme durumu,
   - j- Meslek öncesi, polis eğitim kurumunda bilgisayar ve İnternet kullanımı ile ilgili eğitim alma durumu nasıldır?

3. Emniyet Personelinin Bilişim Suçları ile İlgili Nitelikleri Açısından
   a- İnternet ve güvenliği ile ilgili kaynakları takip edebilme durumu,
   b- Meslek içinde, "Bilişim Suçları" ile ilgili kurs görme durumu,
   c- Bilişim suçları ile ilgili düzenlenen konferans veya seminerlere katılma durumu,
   d- Bilişim suçları ile ilgili eğitim ihtiyaç durumu,
   e- Bilişim suçlarıyla mücadelede, personelin gelişimine etki eden faktörler,
   f- Bilişim suçlarıyla mücadelede yeterli ve yetersiz olunan konular,
   g- Bilişim suçlarıyla mücadele kapsamında yeterli eğitim alınan Konular ve eğitim ihtiyacı gerektiren konular,
   h- Bilişim suçları konusunda bilirkişi olarak görev alma durumu ve görev alınan konular,
   i- Bilişim suçları ile ilgili görev alınan ilginç olaylar,
   j- Bilişim suçlarıyla mücadele kapsamında belirtmek istedikleri diğer konular,
   k- Bilişim suçlarıyla mücadelede, personelin eğitimi konusunda belirtmek istediği konular,
   l- En çok karşılaşılan bilişim suçları,
   m- Bilişim suçlarıyla mücadelede iyi bilinen sistemler,
   n- Bilişim suçları konusunda yetersiz kalma durumu,
   o- Bilişim suçları konusunda yetersiz kalındığında Emniyet Genel Müdürlüğü (EGM) bünyesinde destek alınan birimler,
   p- Bilişim suçları konusunda yetersiz kalındığında dışarıdan destek alınan kurum ve kuruluşlar,
   q- İl Emniyet Müdürlükleri'nde bilişim suçlarıyla mücadelede en yetkin birim,
   r- İl Emniyet Müdürlükleri'nde bilişim suçlarıyla mücadele eden birimlerin daha donanımlı hale getirilme ihtiyacı,
   s- Emniyet Genel Müdürlüğü bünyesinde **"Bilişim Suçları"** ile ilgili bir ünite kurulması konusundaki görüşleri nelerdir?

4. Emniyet personelinin bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi düzeyleri ve bu bilgileri gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?

5. Emniyet personelinin görev yaptığı birime göre, bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi ve gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?

6. Bilişim suçları ile ilgili görev süresi açısından, personelin sahip olması gereken nitelikler konusundaki bilgi ve gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?

7. Bilişim suçları kursuna katılma durumuna göre sahip olması gereken nitelikler konusundaki bilgi ve gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?

1.3. Araştırmanın Önemi

İnternet ve bilgisayar teknolojisi sürekli olarak bir gelişme göstermektedir. Başdöndürücü bir şekilde gelişme kaydeden bilişim teknolojilerinin yaşandığı içinde bulunulan bilgi çağında, bilgiyi iyi kullanabilen toplumların her zaman diğer toplumlardan bir adım daha önde olacakları düşünülmektedir. Bu nedenle, çağımız teknolojisinin son bilişim mucizesi olan İnternet'ten ve bilişim teknolojilerinden zararlarından korunarak ve kötü amaçlı kullanımının önüne geçilerek etik kurallar çerçevesinde istifade edebilme yöntem ve düzenlemelerin tespit edilmesi büyük önem taşımaktadır.

Ancak, günümüzde insan doğası gereği teknolojik gelişmeler içerisinde suç işleme, tüm insanlığın başlıca sorunlarından biri haline gelmiştir. Bilişim suçları gibi bireyi, toplumu, kurumları, devleti ve tüm hayatı etkileyen bu yeni suç türleri için kesinlikle vakit geçirilmeksizin ciddi önlemler alınması ve geniş kapsamlı bilinç altyapısının tesis edilmesi gerekmektedir. Bunun için bireye, kurumlara, üniversitelere, devlete, sivil toplum kuruluşlarına düşen görevler vardır. Bilişim suçlarıyla mücadelede teknolojik alt yapı oluşturmanın,

bilinçlendirmeden daha sonra geldiği gerçeği dikkate alındığında toplumun bilinçlendirilmesi çalışmalarının, veba gibi hızlı bir şekilde yaygınlaşan bilişim suçlarının önlenmesinde bu tür suçlara karşı suç öncesinde en önemli unsur olarak karşımıza çıktığı görülmektedir.

Bilişim suçları konusunda ülke olarak gerekli hukuki ve teknik alt yapı zemininin oluşturulmasında geç kalındığında ve toplumun her kesiminin bu konuda gerekli dikkati sağlanamadığında sorunlar çıkmaktadır. Bireyi, toplumu, kurumları, devleti ve tüm hayatı etkileyen bu yeni suç türleri, hem devlet güvenliğini tehdit edecek, hem de çok ciddi mali külfetler ile toplumsal düzen ve huzuru olumsuz yönde etkileyecektir.

Bilişim suçları konusuna konunun direkt muhatabı polis açısından bakıldığında, günümüzün teknolojik ilerlemeleri ve dolayısıyla teknolojik yeni suç tiplerinin ortaya çıkması gerçeğinden hareketle, polisin görevlerinin gün geçtikçe arttığı, zorlaştığı ve bu durumun böyle devam edeceği görülmektedir. Polisin adliyeye sunduğu delillerin, adli makamlar tarafından kabul görmesi oldukça önemlidir. Bu durum, personelin kendine olan güvenini artıracak ve yeni suç türlerinin çözümünde teşvik edici olacaktır.

Çağımız, polisin en iyi şekilde eğitim görmesini gerektirmektedir. Polisler, suçlulardan daha bilgili ve yetenekli olmak zorundadır. Güvenlik hizmetlerinin kalitesinin artırılması, polisin eğitim düzeyinin yüksek olmasına bağlıdır. Konusunda yetişmiş uzman polis, bilişim suçları gibi ispatın zor olduğu bir alanda, toplumsal adaletin yerine gelmesinde önemli bir işlev görmektedir.

Bugün, başta ABD olmak üzere tüm dünyada bilişim suçları ile mücadele edecek personelin eğitimi üzerinde önemle durulmaktadır. Bu bağlamda, ülke huzur ve asayişinin sağlanmasında en önemli kurumlardan olan polis teşkilatının, bilişim suçlarıyla mücadele edebilmesi için gerekli üniteler kurması ve gelişen çağın koşullarına uygun sertifikasyon sistemine dahil edilmiş model bir eğitim programı geliştirerek polis amir ve memurlarının hizmet öncesi, hizmet içi ve uzmanlık eğitimleriyle yetiştirilmesi büyük önem taşımaktadır.

1.4. Sayıltılar

Bu araştırmada kapsamında geliştirilen bilişim suçları öğretim programı, polisin bilişim suçlarına ilişkin gerekli bilgi ve beceri düzeyini geliştirecek niteliktedir.

1.5. Sınırlılıklar

Araştırma, genel olarak iki boyutta sınırlandırılmıştır.

1. 81 İl Emniyet Müdürlüğü'nün Bilgi İşlem Şube Müdürlüğü'nde görevli 204 kişi ile sınırlıdır.

2. 81 İl Emniyet Müdürlüğü'nün Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü'nde görevli 175 kişi ile sınırlıdır.

1.6. Tanımlar

Adware: Reklam amaçlı olan kullanıcılara istekleri olmadan siteleri açan homepage'ı değiştiren bir programdır.

Anahtarlar (Switches): Ağ anahtarı (İngilizce: switch), bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarından biridir.
Arabellek (memory buffer): Bir cihazda verilerin topluca yazılmadan önce biriktirildikleri bellektir.

Cookie: Web sayfaları tarafından bilgisayarımıza habersizce bırakılan ve bir dahaki girişimizde sayfanın bizi tanımasını sağlayan küçük txt dosyalarıdır.

Cyberpunk: Kripto şifrelerini çözerek sistemlere sızma eylemlerinde bulunanlara kriptografi uzmanlarına denir.
Dat: Dijital manyetik ses depolama ortamıdır.

DoS(Denial Of Service): Bir programın veya bir sistemin askıya alınması yada komple kilitlenmesini amaçlayan bir exploittir.
E-mail tabanlı servisler: Kişiler arasında bilgisayar ortamında haberleşmeyi sağlayan servistir. E-mail gönderilen kişinin adresinin bilinmesi bu servisi kullanmak için yeterlidir. Eğitim amaçlı olarak rahatlıkla kullanılabilen çok yönlü harika bir servistir. Bir eğitsel araç olarak e-mail kullanımının grup tartışmaları, listserver gibi çeşitli seçenekleri vardır.

Exploit: Sistem açığı olarak bilinir. Hackerlar tarafından keşfedilen bu exploitler;

güvenlik konsepti yazıf sistemlere sızmayı sağlayan bir yoldur. Bu yolu kullanabilmek için yazılan script ve master program ları ile exploitler lamerların ve script kiddieslerin kullanımına sunulur.

Fake Mail: Kullanıcıları yanıltmaya yönelik düzenlenen tamamen sahte bir formdur. Güvenerek kişisel bilgilerinizi ve şifrelerinizi girdiğiniz bu tip mailler tamamen sahtedir ve her yazdığınız bilgi aynen bunun size yollayan hacker'ın eline geçecektir.

FTP (file transfer protokol): İki bilgisayar arasında dosya almak/göndermek amacıyla kullanılan bir servistir.

Gopher: Bilgiye hiyerarşik bir yaklaşım sağlayan ve içerdiği menüler aracılığıyla kullanılan bir servistir.

GPRS: GPRS (**G**eneral **P**acket **R**adio **S**ervice), mevcut 2G cep telefonu şebekesi üzerinden paket anahtarlamalı olarak veri iletimi sağlayan teknolojileridir.

Güvenlik Tarayıcıları: Belli bir ağdaki bilgisayarları belli bir düzene göre tarayarak üzerinde çalışan servisler hakkında bilgi edinilmesini sağlayan araçlardır. Elde edilen bilgilerle çalışan servislerin daha önceden bilinen bir güvenlik açığı olup olmadığı tespit edilebilir.

Hack, hacker: İşletim sistemlerinin doğasındaki açık kapıları kullanarak bu açık kapılardan sisteme sızma eylemine "hack", bu eylemi gerçekleştirenlere de "hacker" denir.

Hosting: Hosting veya barındırma, bir web sitesinde yayınlanmak istenen sayfaların, resimlerin veya dokümanların internet kullanıcıları tarafından erişebileceği bir bilgisayarda tutulmasıdır.

Lamer: İnternet üzerinden ücretsiz dağıtılan bazı programlarla "hack" eylemi yapmaya çalışan ama aslında bir şey bilmeyen kişilerdir. Lamerlik, kendisine herhangi bir şekilde "hacker"'lik ithamı yapan grup ve kişilere verilen genel sıfattır.

Log: **B**ilgisayarlarda her işlemin kaydedildiği belgelere denir. TDK'ya göre, bir arada işlenen ve birbirleriyle ilgili olan kayıtların tümüne verilen isimdir.

Kablo Göbekleri (Hubs): OSI katmanında 1. seviyede çalışan ve Türkçesi çoklayıcı olan ağ cihazıdır.

Keylogger: Kendini startup'a yerleştiren ve bazen gizleyen bir programdır. Amacı ise bilgisayarınızda klavye kullanarak yazdığınız herşeyi bilgisayarınızda gizli bir text dosyasına kopyalayan ve sonra bu keyloggerı size bulaştıran sahibine bu text dosyasını email olarak yollayan bir programdır.

Kriptografi: Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür.

Mavi diş (Bluetooth): Mavidiş bilgisayar, çevre birimleri, ve diğer aygıtların birbirleri ile kablo bağlantısı olmadan görüş doğrultusu dışında bile olsalar haberleşmelerine olanak sağlar. Kablo bağlantısını ortada kaldıran kısa mesafe radyo frekansı(RF) teknolojisinin adıdır.

PDA: Dijital Özel Sekreter" anlamına gelen "Personal Digital Assistant" tanımının kısaltması olan PDA, boyutları avuç içine sığacak kadar küçük, başta kişisel bilgilerin saklanabildiği ve iletişim özelliğine sahip elektronik cihazlardır.

Phreaker: Telefon şirketlerinin güvenlik sistemlerini kırarak sistemi kanun dışı yollarla kullanan ya da çıkar sağlayan kişilere denir.

Port Scanner: 65536 tane porta bağlanma girişiminde bulunup hedef bilgisayarın portlarının durumlarını hackerlara bildirmeye yarayan bir araçtır.

Proxy: Belirli servis sağlıyıcıları yada bizzat bir kullanıcının IP sine 80,8080 gibi portlardan bağlanıp üstümüze geçirdiğimiz kullanıcının IP sine proxy denir.

RAM: Bilgisayarın ana bellek birimidir.

ROM: Bilgisayarın çalışması için gerekli olan temel komutların depolandığı yerdir.

Sabit Disk (Hard Disk): Sabit Diskler, veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır. Sabit disk bilgisayarın "veri merkezi"dir.

Sniffer: Türkçe' de koklayıcı anlamına gelen bir kelimedir. Yerel ağdan geçen paketlerin kopyalanması ile şifrelenmemiş olarak geçen bilgileri elde edilmesinde kullanılırlar. Bilgisayar ağlarında veri trafiğini kontrol altında bulundurun bir araçtır. Eğer ağınızda bir sniffer varsa sizde web sayfası üzerinden şifre girişi yaptıysanız, şifrenizin saldırganın eline geçmesi çok kolaydır.

Spam Tool: Bir kullanıcıya isteği olmadan gönderilen reklam veya diğer amaçları gerçekleştirmek üzere geliştirilmiş kimden gönderildiği kullanıcı tarafından anlaşılamayan emaillar yollayan bir program türüdür.

Spoofer: Hackerların systemlere yetkili bir kullanıcıymış gibi kendilerini göstermelerini yarayan bir programdır. En çok kullanılan spoofing yöntemi smurfs ataklarıdır.

Stenanografi: Taşıyıcı dosyada bulunun boşluklardan faydalanarak bu

kısımlara dosyaları şifreleyerek saklama yöntemidir. Taşıyıcı resim ve müzik dosyası olabilir.Taşınan dosyanın ne olacağı önemsizdir.

Telnet: Başka merkezdeki sunucuyu, kendi bilgisayarımız gibi kullanmaya izin veren bir servistir. Dünyada ve ülkemizde elektronik ortama aktarılmış bir çok kitap ve kütüphane kataloğu bu servis ile kullanılmaktadır.

Truva Atları (Trojan): Bilgisayar yazılımı bağlamında Truva atı zararlı program barındıran veya yükleyen programdır. (Bazen "zararlı yük" veya sadece "truva" ibareleriyle de nitelendirilmektedir.) Trojan'ın kendisi bir virüs değildir. Kendi kendini çoğaltmaz, sadece sabit diskteki bilgilere zarar verir. Trojan kendisini zararsız bir program gibi (örneğin bir oyun ya da yardımcı program) gösterir. Görünümü ve ilk çalıştırıldığındaki aktivitesi zararsız bir program gibidir. Çalıştırıldığında verileri silebilir veya bozabilir. Bir trojan, virüs içerebilir ancak kendisi bir virüs değildir. Truva atı yararlı gibi görünen ancak aslında zarara yol açan bir bilgisayar programıdır.

Tuş kaydediciler (Keylogger): Klavyedeki tuş vuruşlarının kaydedilmesi ve bunun sonucunda kişilerin şifre ve kişisel yazışmalarının başkalarına ulaştırılmasını sağlayan yazılımlardır.

WWW (world wide web): 1992 yılında asıl İnternet patlamasını meydana getiren ve İnternet üzerinde kullanımı en zevkli, gelişimi çok hızlı olan hypertext mantığı üzerine dayalı bir servistir.

Virüs: Bilgisayarın çalışmasını engelleyecek, verileri kaydedecek, bozacak veya silecek ya da kendilerini Internet üzerinden diğer bilgisayarlara yayarak yavaşlamalara veya başka sorunlara neden olacak şekilde tasarlanmış yazılım programlarıdır.

Worm: Türkçe anlamı solucan olan bu programlar tıpki virusler gibidir. Programcısının hayal gücü ile sınırlı işler yapabilirler.Bu wormu yazan adamın bulduğu bir açık sayesinde kodlağı bir worm kendisini bu açık sayesinde ve bu açığın olduğu bütün makinelere kopyalar verileri silebilir, şifrelerinizi sahibine yollayabilir.

Yönlendiriciler (Routers): Yönlendirici (İngilizce: *router*), aynı ağ iletişim kurallarını kullanan iki bilgisayar ağı arasında veri çerçevelerinin iletimini sağlayan ağ donanımıdır.

1.7. Kısaltmalar

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

ACPO: Association of Chief Police Officers

ARPANET: Department of Defense Advanced Research Projects Agency - Savunma İleri Düzey Araştırma Projeleri Kurumu

APK: Araştırma Planlama Koordinasyon

ASP: Active Server Pages

ATM: Automated Teller Machine

BBS: Bulletin Board System

BİYESAM: Bilişim ve Yazılım Eser Sahipleri Meslek Birliği

BKM: Bankalararası Kart Merkezi

BMD: Bilişim Muhabirleri Derneği

BSA: Business Software Alliance

BT: Bilişim Teknolojisi

CD-ROM: Compact Disk-Read Only Memory

CERT: Computer Emergency Response Team

CGI: Common Gateway Interface

CIA: Central Intelligence Agency

DDOS: denial-of-service attack

DVD-ROM: Digital Video Disc Read-Only Memory

EGM: Emniyet Genel Müdürlüğü

FBI: Federal Bureau of Investigation

GPRS: General Packet Radio Service

IACIS: International Association of Computer Investigative Specialists

ISP: Internet Service Provider

ISS: İnternet Servis Sağlayıcılar

IT: Information Technology DNS: Domain Name Hosting

Interpol: International Criminal Police Organization

İNETD: İnternet Teknolojileri Derneği

KOM: Kaçakçılık ve Organize Suçlarla Mücadele

LKD:Linux Kullanıcıları Derneği

NASA: National Aeronautics and Space Administration

NATO: North Atlantic Treaty Organization

NSA: National Security Agency

OECD: Organisation for Economic Co-operation and Development

PC: Personal Computer

PDA: Personal Digital Assistant

PIN: Personel Identification Number

PMYO: Polis Meslek Yüksek Okulları

POMEM: Polis Meslek Eğitim Merkezleri

PROMIS: Police Realtime Online Management Information System

RAM: Random Access Memory

ROM: Read Only Memory

SASEM: Suç Araştırma Ve Soruşturması Eğitim Merkezi

TADOC: **T**urkish International **A**cademy Against **D**rugs and **O**rganized **C**rime - Uyuşturucu ve Organize Suçlara Karşı Uluslararası İşbirliği

TBD: Türkiye Bilişim Derneği

TCK: Türk Ceza Kanunu

TDP: Toplum Destekli Polislik

TİB*:* Telekomünikasyon İletişim Başkanlığı

TİEV: Tüm İnternet Evleri Derneği

TK: Telekominikasyon Kurumu

TOEFL: Test of English as a Foreign Language

TÜBİDER: Bilişim Sektörü Derneği

TÜBİSAD: Bilişim Sanayicileri ve İşadamları Derneği

TÜDER: Tüketiciler Derneği

YASAD: Yazılım Sanayicileri Derneği

İKİNCİ BÖLÜM

2. İLGİLİ LİTERATÜR

Bu bölümde, araştırma için genel bir çerçeve oluşturmak amacıyla bilişim terminolojisi, bilişim suçları, bilişim ve hukuk, suç öncesi ve suç sonrası bilişim suçlarıyla mücadele, bilişim suçlarıyla mücadele polis eğitimi gibi konulara ilişkin kaynaklardan elde edilen bilgilere yer verilmiştir.

2.1. Bilişim Temel Terminolojisi (Bilgisayar, Bilişim ve İnternet'in Tanımları ve Bilişim Aygıtları)

Bilgisayar ve iletişim teknolojilerindeki gelişmeler, insanlık tarihi açısından çok önemli bir devrim olarak kabul edilmektedir. İnsan hayatı, her geçen gün gelişen teknolojilere paralel olarak biraz daha kolaylaşmaktadır. Bu gelişmeler; eğitimden ticarete, devlet sektöründen özel sektöre, eğlenceden alışverişe kadar birçok alanda klasikleşmiş anlayışları değiştirmiş ve insanlara yeni bir anlayış yeni bir hayat tarzı kazandırmıştır. Bununla birlikte, insanın bulunduğu her alanda olduğu gibi bu alanda da yeni suç tipleri ortaya çıkmış, suçlular da teknolojinin getirdiği yenilik ve kolaylıkları kullanmaya başlamışlardır. Yeni suç çeşitleriyle birlikte suçlu profilleri ve suç aletleri de değişmiştir.

Bilişim suçlarından bahsedilirken çoğunlukla akla bilgisayar ve internet vasıtasıyla işlenen suçlar gelmektedir. Halbuki diğer iletişim araçları ve bilişim ortamındaki cihazlarla da bu suçlar işlenebilmektedir. Bilişim suçlarından bahsetmeden önce bu suç çeşidinin en önemli vasıtaları olan bilgisayar ve İnternet'ten bahsedilmesi konunun boyutlarının ve öneminin anlaşılması için faydalı olacaktır.

2.1.1. Bilgisayar'ın Tanımı, Temel Parçaları, Çevre Birimleri ve Ağ Erişim Araçları

Bilgisayar; donanım, yazılım ve bileşenlerinden oluşan bir makinadır. Donanım, bilgisayarın ekran, klavye, main board gibi fiziksel ve elektronik yapısını oluşturan ana ve çevre birimlerinin tümüne denir. Yazılım ise, bilgisayarı çalıştırmaya yarayan, fiziksel kısım dışında kalan her şeye denir.

En genel anlamda bilgisayar, belirli verileri kendisine verilen komutlar doğrultusunda işleyen bir elektronik veri işleme aracıdır diye tanımlanabilir (Alkan, Şimşek ve Deryakulu, 1995: 90). Günün gelişen teknolojisine uygun çeşitli ek donanım takılmasına müsait olan bilgisayarlar böylece çok amaçlı işlevselliğini sürdürebilmektedirler.

Bilgisayar temel parçaları şu şekildedir: Merkezi İşlem Birimi (CPU), ROM (Read Only Memory), RAM (Random Access Memory) ve veri depolama birimlerinden oluşmaktadır.

Veri depolama birimlerinden başlıcaları ise şunlardır: Sabit Disk (Hard Disk), Disket, CD-ROM (Compact Disk-Read Only Memory), DVD-ROM, Sıkıstırılmıs Sürücü - Zip Drive, Flash Bellek (Flash Memory), Dat

Bilgisayar çevre birimleri şunlardır: Klavye, Fare, Ekran, Yazıcılar, CD-DVD yazıcılar, Tarayıcılar, Özel Amaçlı Tarayıcılar, Kamera (web cam), Dijital Fotograf Makineleri.

Ağ erişim araçları ise şu şekildedir:

Kablolu erişim: Ağ Kartı-Ethernet Kartı, Modem

Kablosuz erişim: Kızıl Ötesi Erisim Araçları, Mavi diş (Bluetooth), Kablosuz Ethernet Kartları (Wi-Fi), GPRS Modemler.

2.1.2. İnternet'in Tanımı, İnternet Dünyasının Öğeleri, Özellikleri

İnternet

20. y.y'ın son çeyreğinde mikro elektronikte yaşanılan teknolojik değişim ve gelişim rüzgarı, İnternet denilen yüzyılın harikasını ortaya çıkarmıştır. ***Internet*** ya da kısaca ***Net***; tek bir ağ değildir. Aslında İnternet, birbirinden ayrı protokol yapılarına sahip binlerce irili ufaklı ağların toplamıdır. Internet'teki bilgi akışı, bir çok değişik ağdan gelip geçmekte, ulaşacağı yere öylece varmaktadır.

Günlük yaşamın bir parçası olan bu terimin, bugüne değin bir çok tanımı yapılmıştır. Internet; kısaca milyonlarca bilgisayarı birbirine bağlayan geniş tabanlı bir bilgisayar ağı diye tanımlanabilir. Bu ağ, 1969 yılında ARPANET (Department of Defense Advanced Research Projects Agency- Savunma İleri Düzey Araştırma Projeleri Kurumu) olarak kurulmuş çeşitli aşamalardan geçtikten sonra 1990 yılında bugünkü İnternet görünümüne bürünmüştür. Dünya üzerinde İnternet'den başka bir sürü bilgisayar ağı vardır fakat İnternet'i diğerlerinden farklı kılan en büyük özelliği her cins ve kapasitede bilgisayarı kabul etmesidir (Emniyet Genel Müdürlüğü, 1999).

İnternet Dünyasının Öğeleri

İnternet dünyasının en önemli öğelerinden biri "kullanıcı" dır. Diğer bir unsur, Telefon-Telekominikasyon idareleridir. Telefon-Telekominikasyon idareleri, İnternet bağlantısının gerçekleşmesi için gerekli olan, bilgi iletişiminin sağlandığı yerel/ulusal idarelerin sahip olduğu/kontrolünde bulundurduğu iletişim hatlarıdır.

İnternet dünyasının önemli öğelerinden biri de "İnternet Servis Sağlayıcıları"dır. İnternet içerisinde birinci derece önem taşıyan, internet anahtarını da elinde tutan dinamik hüviyetteki hukuk süjesidir. Bir iletişim ağına girmek ve ağda yer alan diğer bilgisayarlarla iletişim kurmak/verileri paylaşmak için gerekli donanıma sahip bir kullanıcı, önce kendisine internet ortamına girmesini sağlayan bir kuruma üye olmalıdır. Bireylerin internete bağlanmalarını, internet üzerinden iletişim kurmalarını ve internetin sağladığı olanakları

kullanmalarını temin eden aracı unsurlara İnternet Servis Sağlayıcılar (ISS) (ISP Internet Service Provider) denir. İnternete geçiş, ISS' ler aracılığıyla olur. Kanunlarımıza göre ISS olmak için özel bir hüküm yoktur. İnternette aracı unsur olan ISS'leri kullanıcıları internete erişimi sağlayan ve/veya elektronik hizmetlerin, kullanıcıların kullanımına sunulmasına aracılık eden gerçek ve tüzel kişilerdir şeklinde tanımlamak mümkündür.

ISS'ler dünyanın farklı ülkelerinde farklı yapılarda olmasına rağmen, internet yalnız erişim, hizmet veren dağıtıcı gibi değil, sunucu kiralama, alan adı sağlama DNS (domain name hosting), sunucu barındırma (hosting), uygulama servis sağlayıcılığı (application service provider), içerik/bilgi sunma gibi hizmetleride vardır.

İnternet Dünyasının Özellikleri

İnternet esasında temel insan haklarına ve özgürlüklerine hizmet etmekte, özellikle "İfade ve İletişim Özgürlüğü"nü sağlamakta ve hatta garantiye almaktadır. Bu nedenle, iletişim özgürlüğünden yararlanmak suretiyle internetin yaygınlaştırılması ve kitle iletişimin en üst düzeye çıkarılması temel amaç kabul edilmektedir. Dünyanın değişik yerlerinde bilgisayarların iletişim protokolleri kullanarak karşılıklı etkileşim içine girdiği, sosyal hayata ilişkin bir çok davranışın dijital ortamda gerçekleştirilebildiği bu ağın karakteristiğine bakıldığında bazı tipik özellikleri ön plana çıkmaktadır.

- Herhangi bir ülke coğrafyasıyla ve ülke hukuku ile sınırlı değildir.
- İnternete bağlanmak için herhangi bir kurumdan izin alınması gerekmez.
- Hemen hemen bütün sosyal ilişkilerin dijital ortama aktarılmış halidir.
- Sanal ortamda gerçek yaşam görülmektedir.
- Kimlik tespiti son derece zordur.
- Bilgiye erişim ile özdeşleşmiş bir kavramdır.
- Her türlü suç ve suç unsurlarına açıktır.

Sağsan (2002: 222), bilgi savaşları kapsamında bu konuyu; saldırıya uğrayan bir ülkenin sınırlarını bilmek, coğrafîk yapısını çözümlemek, hukuksal ve bürokratik olarak yapısını çözümlemek ve geleneksel savaş yöntemlerini kullanmanın önemi kalmamıştır ve saldırı altında kalan ülke, kim tarafından saldırıya uğradığını bilememektedir şeklinde ifade etmektedir.

2.1.3. Bilişim'in Tanımı ve Elektronik Aygıtlar

Bilişim kelime anlamı olarak; insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir (Türk Dil Kurumu, 2008). Bilişim; insanların teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı bir şekilde işlenmesi olarak kabul edilmektedir (İzmir Emniyet Müdürlüğü, 2008). Bilişim, bilgi ve bilginin otomatik olarak işlenmesiyle ilgilenen bir yapısal bilim dalıdır. Bilişim kelimesinin karşılığı olan Informatik (alm.), informatique (fr.) ve bunlardan türetilmiş olan Türkçe enformatik kelimeleri İngilizcedeki computer science ve information systems gibi alanları kapsamaktadır. İskandinav ülkelerinde bilişim biliminin karşılığı olarak datalogi terimi kullanılmaktadır. Bilişim biliminin kökleri matematik, fizik ve elektroteknik'tedir. Bir mühendislik alanı olarak bilişim, verileri aktarabilen, depolayabilen ve algoritmalar yardımıyla verileri işleyebilen matematiksel makineler tasarlamaktadır. Veri işleme ve bununla ilgili iş alanları için genel bir kavram olarak İngilizce "information technology" (IT) yerine Türkçede bilişim teknolojisi (BT) kavramı kullanılmaktadır (Wikipedia, 2008).

Aydın'a göre, bilişim (informatics) aşağıda belirtilen alanları içeren bilim ve teknoloji olarak tanımlanmaktadır. Bilginin ve iletişimin yapısı ve özellikleri; 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 çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleridir.

Elektronik Aygıtlar

Birçok elektronik aygıt bilgileri muhafaza etmek için batarya veya AC Power gibi kesintisiz güç kaynağını gerektiren belleklere sahiptir. Güç kaynağı kapatılırsa veya batarya deşarj edilirse bilgiler kolayca kaybolabilecektir. Elektronik deliller, günüzde kullanılan elektronik aygıtların birçok yeni çeşidinde bulunabilir. Elektronik aygıtlar şu şekilde sıralanabilir (Berber, 2004).

a- Bilgisayar Sistemleri: Bir bilgisayar sistemi tipik olarak, bazen merkezi işlem birimi (Central Processing Unit) olarak adlandırılan bir ana ünitesinden, veri kaydetme aygıtlarından, bir monitörden, klavyeden ve mouse' dan oluşmaktadır. Bilgisayar sistemi bağımsız olabileceği gibi, bir ağ'a da bağlı olabilir. Dizüstü, masaüstü, kule tipi (Tower) sistemler, modüler rafa monte edilmiş sistemler, minibilgisayarlar ve büyük boy (anaçatı) bilgisayarlar gibi farklı birçok bilgisayar sistemi mevcuttur. İlave bileşenler olarak; modemler, yazıcılar, tarayıcılar, yanaşma terminalleri ve harici veri kaydetme aygıtları da unutulmamalıdır. Bilgi işlem fonksiyonlarının ve bilgi kaydetmenin tüm bu çeşitleri; metin işletme, hesaplama yapma, haberleşme ve grafikleri kapsamaktadır. Elektronik deliller daha çok hard drive, depolama cihazları ve araçları üzerine kaydedilmiş dosyalarda bulunmaktadır. Örneğin;

Kullanıcı Tarafından Oluşturulan Dosyalar: Bunlar; adres defterleri, e-posta dosyları, ses/video dosyaları, görüntü/grafik dosyaları, takvimler, internette en çok tercih edilen siteler, veri tabanı dosyaları, elektronik çizelge dosyaları, doküman veya metin dosyalarıdır. Kullanıcı tarafından oluşturulan dosyalar, örneğin; adres defterleri ve veri tabanı dosyaları gibi, kriminal aktivitelere ilişkin önemli deliller ihtiva edebilirler. Adres derfterleri veya veri tabanı dosyaları suç örgütlenmesini, hareketli veya hareketsiz resimler, sübyancılık aktivitelerini, e-posta' lar ise suçlular arasında yapılmış olan heberleşmeleri ispata yarayabilecektir veya bir elektronik çizelgede uyuştutucu madde işi yapanların listeleri bulunabilecektir.

Kullanıcı-Korumalı Dosyalar: Bunlar; sıkıştırılmış dosyalar, yanlış isimlendirilmiş dosyalar, şifleri dosyalar, parola korumalı dosyalar, gizlenmiş dosylar ve steganografidir. Kullanıcıların delilleri bir çok değişik şekilde gizleme imkanları mevcuttur. Örneğin; kendileri için önemli olan bir veriyi şifreleyebilir veya parola korumalı hale getirebilirler. Yine kullanıcılar hard disk üzerinde veya diğer dosyalar içinde veya kasten yanlış bir isim vererek yarattığı bir dosya içinde bir suçun delilini gizleyebilirler. Deliller, bilgisayar işletim sisteminin rutin bir işlevi olarak oluşturulan dosyalar veya diğer veri alanları içinde bulunabilirler. Parolalar, internet aktiviteleri ve geçici yedekleme dosyaları, verilerin çok sık olarak kurtarıldığı ve incelendiği yerlerdir. Bunun yanı sıra bir dosyanın oluşturulduğu tarih ve zaman, değişiklikler, silmeler, erişim, kullanıcı adı veya kimlik bilgileri ve dosya özniteliği gibi, bir dosyanın bileşenleri de delil gücüne sahip olabilir. Hatta bilgisayarın sadece açılması bile bu bilgilerin bazılarında değişiklik yapılması sonucunu doğurabilmektedir.

b- Masaüstü ve Laptop Bilgisayarlar: Elektronik keşif sırasında karşılaşılan bilgisayarların çoğunluğunu masaüstü ya da laptop bilgisayarlar oluşturmaktadır.

c- Bileşenler (Merkezi İşlem Birimi, Hafıza): Merkezi İşlem Birimi (Central Processing Unit – CPU) daha çok çip olarak adlandırılan, bilgisayarların içerisine yerleştirilmiş bir mikroişlemcidir. Mikroişlemci ana bilgisayar kutusu içinde, diğer bileşenlerle birlikte, bir baskılı devre plaketi üzerine yerleştirilmiştir. Bilgisyarlardaki tüm aritmetik ve mantıksal işlevleri yerine getirmektedir. Bilgisayarın işletimini kontrol etmektedir. Bu aygıtın bizatihi kendisi birçok olayın delili niteliğinde olabilmektedir.

Hafıza (Memory)

Bilgisayarın içindeki taşınabilir devre plaketidir. Kullanıcının programlarını ve verilerini bilgisayar işler halde iken depolar. Bu aygıtın da yine bizzat kendisi birçok suçun delili niteliğinde olabilmektedir.

d- Erişim Kontrol Araçları (Akıllı Kartlar, Konektörler, Biyometrik Tarayıcılar, Telesekreterler, Dijital Kameralar):

Akıllı kart, parasal değerleri, şifreleme anahtarlarını veya onay bilgilerini (örneğin; parola), dijital sertifika veya diğer bilgileri saklayabilen bir mikroişlemci ihtiva eden, küçük avuç içi kadar aygıtlardır. Konektörlerde, akıllı kart üzerindeki bilgilere benzer bilgileri ihtiva eden, bilgisayar iskelesine (port) takılabilen küçük aygıtlardır. Biyometrik tarayıcı ise; bireylerin fiziksel özelliklerini (retina, ses, parmak izi gibi) teşhis edilebilen, bir bilgisayar sistemine bağlı araçlardır. Tüm bu aygıtlar bir şifreleme anahtarı olarak bilgisayara veya programlara veya fonksiyonlara erişimin kopntrol altında bulunmasını sağlarlar. Kullanıcı ve kart üzerindeki teşhis/onay bilgileri, erişim seviyesi, yapılanışlar, izinler ve bizzat aracın kendisi delil olarak kullanılabilecektir.

Telesekreterler (Answering Devices)

Telefonun bir parçasını oluşturan veya telefon ve telekomünikasyon hatları (kara hattı) arasında bağlatılı olan elektronik aygıtlardır. Bazı modelleri manyetik teyp veya teypleri kullanırken, diğer bazı modeller ise dijital kayıt sistemlerini kullanmaktadır. Aranan taraf eğer ulaşılamaz durumda ise; arayan tarafın sesli mesajını kaydetmekte veya telefon çağrısına cevap verilmek istenmediğinde kellanılır. Batarya sınırlı bir ömre sahip olduğu için, dataların kaybedilmesi tehlikesi mevcuttur. Bu nedenle delillere nezaret eden kişiye, lavoratuar şefine, adli bilişim uzmanına aygıtın batarya ile çalıştığı konusunda bilgi verilmesi gerekir. Telesekreterler sesli mesajları saklayabilirler ve bazı durumlarda mesajın bırakıldığı tarih ve zaman bilgilerine de ulaşmak mümkündür. Bunlar ayrıca diğer ses kayıtlarını da ihtiva edebilirler. Çağrı yapan kişinin kimlik bilgileri, silinmiş mesajlar, son aranan numara, memo (kısa not), telefon numaraları ve isimler, kasetler elde edilebilecek bilgiler arasındadır.

Dijital Kameralar

Kamera, görüntüler ve videolar için dijital kayıt yapan, saklama aracı ve sohbet donanımı ile birlikte görüntüleri ve videoları bilgisayarlara transfer edilebilen aygıtlardır. Dijital kameralar görüntüleri ve/veya videoları dijital

formatta kaydetmekte ve bunalrı daha sonra izlemek veya düzenlemek için bilgisayar, televizyon gibi araçlara transfer edebilmektedir. Dijital kameralarda yer alan görüntüler, taşınabilir kutucuk, tarih ve zaman damgası ve videolar potansiyel delillerdir.

e- Avuçiçi Aygıtlar (Elektronik Ajanda - PDA): Elektronik ajanda; bilgi işlem, telefon/faks, çağrı sistemi, ağ oluşturma (networking) ve diğer özelliklere sahip küçük aygıtlardır. Her bir çeşidi farklı detay özelliklere sahip olmasına rağmen, her PDA aynı temel tasarımı izlemektedir: PDA'lar minyatür bir klavye ve likid kristal ekran ile birlikte, küçük bir mikroişlemciden oluşmaktadır. Bunlar tipik olarak kişisel düzenleyiciler gibi kullanılmaktadır. Bir avuçiçi bilgisayar normal bir masaüstü bilgisayar sisteminin sahip olduğu tüm özelliklere sahiptir. Bazıları disk sürücü ihtiva etmezken; modern, hard drive veya diğer cihazları taşıyabilen bir PC kart yuvasına sahiptir. Avuçiçi bilgisayarların kendi verilerini diğer bilgisayar sistemleri ile, bir yuvaya oturtularak gerçekleştirilen bağlantı sayesinde, senkronize edebilme özelliği de mevcuttur. Dolayısıyla avuçiçi bilgisayarlar bilgileri saklamaya elverişli olan aygıtlardır. Bellek, batarya sayesinde aktif olarak muhafaza edildiği için ve bataryaların bu aygıtlar bakımından ömrü sınırlı olduğu için, dataların kaybı tehlikesi burada da mevcuttur. Bu nedenle delillere nezaret eden kimse, adli bilişim uzmanı, laboratuar şefi gibi görevli personelin bu konuda bilgi sahibi olmaları gerekmektedir. Bu araçlarda yer alan adres defterleri, takvimler, el yazıları, parolalar, yazılı mesajlar, sesli mesajlar potansiyel delillerdir.

Bir PC'de keşif yapılırken hakim olan düşünce, hard diskteki delilleri değiştirmemek ve bilgisayara el konulduğu sırada kendi durumlarını açık olarak gösteren imgelerin hazırlanmasıdır. Bir elektronik ajanda da veya PDA' da keşif yapılırken ise, bunlarda hard disk mevcut değildir ve burada esas olan düşünce ise; ana bellekteki delillerin mümkün olduğu kadar az ölçüde değişmesine çalışmnaktadır. Bir imgenin hazırlanması olanağı ise ancak uzman yazılımlar kullanıldığında söz konusu olmaktadır.

İzlenecek Yöntem

Bir PDA' ya el konulduğu zaman, aygıtın açılmaması gerekir. Delil çantasına konulmadan önce de aygıtın damgalı bir zarfa yerleştirilmesi gerekir. Bu işlem PDA' nın açılmasını ve içindeki bilgilere erişimini engelleyecektir. PDA, şarj edilebilir tek batarya ile çalışıyorsa, uygun ana şebeke adaptörünün kablolarla, delil çantasından geçecek şekilde aygıta bağlanması, PDA' nın şarj edilir şekilde muhafaza edilmesi bakımından önemlidir. Yapılacak inceleme ortak bellek aygıtları olan IC kartlar, Katıhal (Solid State) Diskleri, SmartMedia kartları ve bellek çubukları, yine ayrıca PDA' yı bir PC' ye bağlamak için kullanılan kablolar veya yuvalar üzerinde de yapılacaktır.

Eğer PDA açık halde bulunursa, burada hemen batarayanın ömrünü muhafaza etmek için, aygıtı kapatmayı düşünmek gerekir. Daha sonra aygıt, yukarıda anlatıldığı şekilde paketlenmelidir. PDA ile ilgili olan herhangi bir güç kaynağına, kabloya veya yuvaya da aynı şekilde el konulması gerekir. Elektronik Ajanda/PDA'nın olay mahallindeki itham edilen kişiye asla geri verilmemesi veya en azından delil kurtarma işlemi tamamen bittikten sonra verilmesi gerekir. Yeniden Başlatma Düğmesine (reset) basılması veya tüm bataryaların çıkarılmasının araçta yer alan tüm bilgilerin tamamen yok olması anlamına geleceği unutulmamalıdır. PDA'yı yetkili bir kişinin keşfin daha ilk aşamalarında incelemesi gerekir. İşlem tamamlanıncaya kadar delilleri korumak amacıyla, bataryaların düzenli zaman aralıklarıyla kontrol edilmesi önem taşımaktadır.

f- Sabit Sürücüler: Manyetik olarak verileri kaydedebilen sert bir plakla kaplanmış olan yalıtılmış kutudur. Bilgisayar içinde olabileceği gibi ayrı olarak da kullanılması mümkündür.

g- Bellek Kartları: Taşınabilir elektronik kayıt araçlarıdır. Karttan güç kesildiğinde dahi bilgilerin kaybedilme riski yoktur. Hatta silinmiş imgelerin bellek kartından tekrar geri kurtarılması dahi mümkündür. Bellek kartları, kredi kartı boyutunda olmalarına rağmen, yüzlerce imgeyi saklayabilmektedir. Bilgisayaralar, dijital kameralar ve avuçiçi bilgisayarlar gibi birçok farklı aygıtta kullanılmaktadır. Örnek olarak; bellek çubukları, akıllı kartlar, çakar bellek (flash memory) ve çakar kartlar (flash card) verilebilir.

h- Modemler: Modem, bilgisayarın diğer bilgisayar sistemleri ve/veya ağlar ile telefon ahtları, kablosuz veya diğer iletişim vasıtları aracılığıyla bağlantısını sağlayarak, elektronik haberleşmeyi kolaylaştıran aygıttır. Modemler dahili, harici, kablosuz, PC kartları şeklinde olabilir. Bizatihi aygıtın kendisi potansiyel olarak delil teşkil etmektedir.

j- Ağ Bileşenleri: LAN/NIC Kartı, Routers, Hubs, Switches, Sunucular, Ağ Kabloları ve Konnektörler, Çağrı Cihazları, Yazıcılar, Taşınabilir Depolama Araçları ve Aygıtları (Flash Disk, CD-DVD-Disket, Sim Kart, Hafıza Kartı), Tarayıcılar, Telefonlar, Cep Telefonları

Yerel Alan Ağı Kartı (Local Area Network) veya Ağ Arayüzü Kartı (Network Interface Card): Bu bileşenler bir bilgisayar ağının göstergeleridir. LAN/NIC kart bilgisayarları bağlamak için kullanılır. Kartlar bilgilerin değiş tokuşu ve kaynakların paylaşımı amacıyla kullanılır. Araçların kendileri potansiyel olarak delil teşkil etmektedir.

Yönlendiriciler (Routers), Kablo Göbekleri (Hubs) ve Anahtarlar (Switches): Bu elektronik araçlar ağ sistemlerinde kullanılmaktadır. Yönlendiriciler, kablo göbekleri ve anahtarlar farklı bilgisayarların veya ağların bağlanması olanağını sağlamaktadır. Genellikle çoklu kablo bağlantıları sayesinde tanınmaktadırlar. Asıl kullanım amaçları ağlar arasındaki veri dağıtımını sağlamak ve bu dağılımı kolaylaştırmaktır.

Sunucular: Bilgisayar ağında başka bilgisayarlara hizmet veren bir bilgisayardır. Dizüstü bilgisayarlarda dahil olmak üzere herhangi bir bilgisayar sunucu olarak yapılandırılabilmektedir. Paylaşımlı kaynak hizmeti sunar. Örneğin; bir ağ için e-posta, dosya depolama, web sayfası hizmetleri ve yazdırıcı hizmetleri gibi.

Ağ Kabloları ve Konnektörler (Bağlaç, Connectors): Network kabloları ve konnektörleri bağlandıkları bileşene bağlı olarak farklı renklerde, kalınlıkalrda ve şekillerde olabilirler. Bir bilgisayar ağındaki bileşenleri birbirine bağlamaya yaramaktadırlar. Bizatihi bu araçlar potansiyel delil niteliğini haizdir.

Çağrı Cihazları (Pagers): Avuç içine sığan büyüklükte, taşınabilir elektronik aygıtlardır, ancak kalıcı olmayan delilleri kapsamaktadır (telefon numarası, sesli mesaj, e-posta gibi). Cep telefonları ve Palmler de çağrı cihazı aracı olarak kullanılabilmektedir. Numerik (telefon numalaraları) ve alphanumerik (metin, e-posta) elektronik mesajların alınması ve gönderilmesi amacıyla kullanılmaktadır. Bu aygıtlarda da bataryaların ömrü sınırlı olduğu için, dataların kaybı tehlikesi gündemdedir. O nedenle ilgili görevlilerin bu konuda uyarılmaları gerekmektedir. Potansiyel deliller olarak; adres bilgileri, e-posta' lar, metin mesajları, seslimesaj erişim numarası, sesli mesaj parolası, borç kartı numaralar, hızlı arama için kaydedilen numaralar, alınan çağrılar için arayan kimsenin kimlik belgeleri, PIN numaraları sayılabilir.

Yazıcılar: Bilgisayara bir kablo ya da kızılötesi bir kapı (iskele) ile bağlı olan ve bilgisayardan gelen verileri kağıt ortama döken aygıttır. Bazı bilgisayarlar, yazdırma işlemi yapılırken birden çok sayfadan oluşan dokümanları alma ve saklama özelliği sunan bir arabelleğe (memory buffer) sahiptir. Bazıları ise bir hard drive' a sahiptir. Printer'lar kullanım log'larını (günlük), tarih ve zaman bilgilerini ve eğer ağ' a bağlı iseler, ağ kimlik bilgilerini ihtiva edebilirler.

Taşınabilir Depolama Araçları ve Aygıtlar: Elektronik, manyetik veya dijital bilgilerin depolanması amacıyla kullanılan araçlardır (örneğin; disketler, CD' ler, DVD' ler, kartuşlar ve kasetler). Bu araçlar üzerine bilgisayar programları, metinler, resimler, videolar, çoklu ortam-multimedia dosyaları vs. kaydedilebilmektedir.

Tarayıcılar: Bilgisayara bağlı olan, bir dokümanı ışınlarla tarayarak, bilgisayara dosya olarak gönderen optik bir aygıttır. Dokümanları, resimleri vs. elektronik dosya haline çevirir. Bunları daha sonra bilgisayar üzerinde yeniden görülmesi, işlenmesi veya transfer edilmesi mümkündür. Aygıtın bizzat kendisi delil olarak kullanılabilmektedir.

Telefonlar: Ya kendi başına veya bir baz istasyonuna (kablosuz) veya doğrudan kara hattına (telekomünikasyon hattına) bağlı olan bir ahizedir. Ya dahili bir bataryadan, elektrikli bir bağlantı ucundan veya doğrudan doğruya telefon sisteminden güç çekmektedir. Kara telekomünikasyon hatlarını, radyo iletimini, hücresel (cep telefonu) sistemleri veya kombinasyonlarını kullanarak, iki yönlü haberleşme sağlamaktadır. Telefonların bilgi depolama özelliği de mevcuttur. Bataryalar sınırlı bir ömre sahip olduğu için, dataların kaybedilmesi tehlikesi burada da mevcuttur. İlgili personelin bu konuda bilgilendirmesi gerekmektedir. Birçok telefon, isimleri, telefon numaralarını, arayan kişiye ait kimlik bilgilerini depolayabilmektedir. Ek olarak; Bazı telefonlar randevu bilgilerini, alınan e-posta' ları ve sayfaları saklayabilmekte ve bir ses kayıt cihazı görevini yerine getirmektedir. Elektronik seri numarası, memo (pot), parola, metin mesajları, seslimesajlar ve web tarama ve saklama özellikleri de mevcuttur.

k- Çeşitli Elektronik Öğeler (Fotokopi Makineleri, Kredi Kartı Okuyucuları, Dijital Saatler, Faks Makineleri): Elektronik aygıtların, olay mahallinde bulunabilecek ancak listelenemeyecek kadar çok çeşitli türleri mevcuttur, Bunun yanı sıra keşfe konu teşkil edebilecek bilginin ve/veya delillerin mükemmel bir şekilde kaynağını oluşturacak çok sayıda klasik olmayan aygıt da söz konusudur. Örnek olarak; kredi kartı okuyucu alet, cep telefonu klonlama ekipmanları, çağrı cihazları, ses kayıt cihazları ve web televizyonları verilerbilir. Faks makinaları, fotokopi makinaları, ve çok işlevli makinalar, dahili depolama aygıtlarına sahip olabilir ve delil değeri taşıyabilecek bilgileri ihtiva edebilirler.

Fotokopi Makinaları: Bazı fotokopi makinaları kullanıcı erişim kayıtlarını ve çekilen fotokopilerin tarihini muhafaza etmektedir. Dökümanlar, tarih ve zaman bilgileri ve kullanıcı kullanım günlükleri (logları) potansiyel deliller niteliğindedir.

Kredi Kartı Okuyucuları: Kredi kartı okuyucuları plastik kart üzerindeki manyetik şeritin ihtiva ettiği bilgileri okumak amacıyla kullanılmaktadır. Bu manyetik şerit üzerinde yer alan, kredi kartının geçerlilik süresinin sona ereceği

tarih, kredi kart numarası, kart sahibinin adresi ve adına ilişkin bilgiler potansiyel delillerdir.

Dijital Saatler: Dijital saatlerin, dijital mesajların kaydedebilen çağrı cihazı fonksiyonuna sahip bir çok farklı çeşitleri mevcutttur. Bu saatler ayrıca adres defterlerini, randevu tarihlerini, e-posta ve notları da depolayabilmektedir. Bazıları ise bilgileri bilgisayarla senkronize edebilme özelliğine sahiptir. Adres defterleri, randevu tarihleri, e-posta' lar, notlar ve telefon numaraları potansiyel delillerdir.

Faks Makinaları: Faks makinaları programlanmış telefon numaralarını ve gönderilen veya alınan belgelerin tarihlerini depolayabilir. Ayrıca bazıları birden çok sayfanın fakslanması söz konusu olduğunda bunalrı önce tarayıp, daha sonra göndermek ya da gelen faksları hafızada saklayıp daha sonra yazdırmak olanağını sağlayan belleğe de sahiptir. Bazıları yüzlerce sayfa gelen ve/veya giden sayfayı depolama özelliğine sahiptir. Belgeler, film kartuşları, telefon numaraları ve gönderildi/alındı logları potansiyel delillerdir.

l- Küresel Konum Sistemleri: Küresel konum sistemleri hedef bilgileri, yol işaretleri ve yönlendiriciler aracığıyla, yapılan seyahat hakkında bilgi temin edebilmektedir. Bazıları önceki hedefleri depolamakta ve seyahat günlüklerini kapsamaktadır. Ev, önceki hedefler, seyahat günlükleri, yol işaret koordinatları, yol işaret adlları potansiyel delillerdir.

m- Suçta Kullanılan Öğelerden Bazıları : Decoder-Encoder, Manyetik Şeritli Kart, Kredi Kartı-Banka Kartı, Slip-Dekont, Pinpad & Skimmer, Sim Kart, Hafıza Kartı, Flash Disk, Manyetik Şeritli Kart (Berber, 2004).

2.2. Bilişim Suçları

Bu bölümde bilişim suçlarının tanımından önce suç kavramı incelenmiş ve ele alınmıştır. Daha sonra, bilişim suçlarının tanımı yapılarak bilişim suçlarının sınıflandırılması, bilişim suçlarının gelişimi ve ortak özellikleri, bilişim suçlarının işlenme nedenleri, bilişim suçluları ve mağdurlarının genel özellikleri, bilişim suçlarında ilgili kurum ve kuruluşlar, siber terörizm, ülkemizde sık karşılaşılan bilişim suçları, bilişim yoluyla işlenen asayiş suçları, bilişim suçlarından örnek olaylar, bilişim suçlarında Emniyet Teşkilatı içerisindeki idari yapılanma, ülkemizde işlenen bilişim suçları istatistikleri, uluslararası platformda ve bazı ülkelerde bilişim suçları konusunda yapılan çalışmalar ve istatistikler, Avrupa Konseyi siber suç sözleşmesi hakkında çeşitli bilgiler verilmiştir.

2.2.1. Suç Nedir? Bilişim Suçları Tanımı

Suç Nedir?

Suç, insanlığın var ola gelmesinden beri var olagelmiş bir olgudur. Tarihte he zaman, her ortamda suç işleme güdüsü, insanoğlunun vazgeçilmez özelliklerinden biri olmuştur. Günümüzde de insanlar, giderek elektronikleşen ve teknolojiye yoğun bir şekilde bağımlılık gösteren yapısıyla, çağın yeni suç türlerinden bilişim suçlarına maruz kalmakta ve bu suçların önlenmesi için yetkililer yoğun bir şekilde önlem almaya çalışmaktadırlar. Teknolojik ortam, giderek artan yapısıyla günlük hayatta yerini aldıkça bu ortamdan kendi menfaatleri doğrultusunda istifade etmeyi düşünecek, bilişim alanında suçları işleyecek bilişim suçlularıda var ola gelecektir. Suçun farklı bilimler tarafından oluşturulmuş farklı tanımları vardır. Suç'u ve unsurlarını bilmek, bilişim suçunu anlamayı da kolaylaştıracaktır.

Suç; evrensellik ve genellik taşıyan bir olgudur. Suç, tarihin en eski devirlerinden itibaren var olmuştur ve ileride de var olmaya devam edecektir. Suçsuz bir toplum bir ütopyadan başka bir şey değildir. İnsanların içinde ihtiraslarla birlikte toplum halinde yaşamanın ortaya çıkardığı çeşitli sosyal çelişkiler, uyumsuzluklar bulundukça suçta var olacaktır. Suç bir bakıma, bazı

kişilerin davranışları ve tutumları ile bunların içinde yaşadıkları grupta yerleşmiş davranış örnekleri ile arasında bir çelişkidir. Bu çelişki her zaman ve her yerde zorunlu olarak var olacağından, suç genel ve evrensel bir olay teşkil eder ve adam öldürme, hırsızlık gibi çeşitli suçların farklılığına rağmen bir çeşit bilimsel yönden gözlemin yapılması kabil ve bilimin konusunu oluşturan bir olay niteliği ile varlığını korur (Dönmezer, 1994 : 49).

Ceza Hukukunda suç, teknik - hukukî yani normatif maksatları karşılar şekilde değişik yazarlar tarafından çeşitli biçimlerde tarif edilmektedir. Ancak bu nevi hukukî nitelikli tariflerin bir olay, bir sapıcı davranış olarak suçun, kriminoloji yönünden de ele alınmasına esas teşkil edip edemeyeceği tartışmalıdır. Teknik hukukî nitelikteki tariflerin sosyolojik bakımından itibarları daha az olmak gerekir; zira bu tariflere göre bir gün bu kanunlar ilga edilecek olursa toplum içinde suçun da kalkacağını kabul etmek gerekecektir. Oysa topluma zarar veren hareketler, kanunlar bunları tarif etmeden önceden de, mevcuttur. O halde önce çözümü gereken problem belirli hareketleri suç haline getirirken kullanılacak ölçüdür. Bu hususta ölçüler verilmesine çalışılmıştır. Sözgelimi Jhering'e göre suç, toplum halinde yaşama şartlarına yönelmiş her türlü saldırılardır (Dönmezer, 1994 : 45).

Bu maksatla sosyolojik nitelikte tariflerin verilmesine de girişilmiştir. Durkheim'e göre "suç kolektif bilincin kuvvetli ve belirmiş tutumlarını (dispositions) ihlâl eden fiillerdir". Thomas ve Znaniecky eserinde sosyal psikoloji yönünden meseleyi almak suretiyle şöyle bir tarif vermektedir: "Suç kişinin kendisini mensubu saydığı grupta, varlığı toplum dayanışması ile çelişki gösteren fiildir". Taft'ın görüşü ise şöyledir: Topluma zarar veren hareketler ya örf ve âdetlerce belirlenmiştir yada grup içinde egemenliği elinde tutanlar, diğer kişilerin, tavır ve hareketlerini uydurmaları için modelleri, örnekleri ve bu suretle moral kuralların tümünü tespit ederler; bu kurallara uyanlara sosyal itibar verir, bunları ihlâl edenlere söz konusu mevkii reddederler (Dönmezer, 1994 : 46).

İnsanlıkla beraber suç da var olagelen bir olgudur. Düzenlenmiş olan mevzuatlara göre, bir eylem suç şartlarını taşıyor ve bu suç bilişim alanında

meydana geliyorsa işte bu suç-bilişim ilişkisi, günümüzde yaygınlaşan ve sürekli önlem alınmasını gerektiren bilişim alanında suçları ve bu konudaki hukuki düzenlemeleri ortaya çıkarmaktadır.

Bilişim suçlarına bir çerçeve çizmek çok zordur. Gelişmekte olan teknoloji bilişim suçlarının da çerçevesini genişletmektedir, bu nedenle bilişim suçlarının tanımını yapmak ve ortak bir tanım üzerinde uzlaşmak oldukça zordur. Tüm dünyada ve ülkemizde, bilişim suçları çeşitli şekillerde tanımlanagelmektedir.

Bilişim Suçları Tanımı

Bilişim suçlarını anlamak ve ilgili düzenlemeleri yapmak için doğru bir tanımlama yapmak önem arz etmektedir. Fakat literatürde, dünya genelinde net bir tanım üzerinde fikir birliğine varılamamıştır. Teknolojideki gelişim ve değişim, tanımlama yapmayı zorlaştırmaktadır.

Bilgisayar suçları ya da bilişim suçları konusunda herkesin ittifak ettiği bir tarif yoksa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris toplantısında yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçları; bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır (Özel, 2002).

Bir diğer tanımda ise bilişim suçları, "Bilgisayar veri ve programlarına izinsiz girilmesi, kullanılması, tahribi veya şok edilmesini, bilgisayardaki kişisel verilerin ifşasını ve sırrın masuniyeti aleyhine işlenen eylemlerdir" biçiminde tanımlanmaktadır (Aydın, 1992).

Avustralya, Sydney Üniversitesi, Bilişim Sistemleri Fakültesi öğretim üyesi Underwood (2008) bilişim suçunu; "Geleneksel suçlardan olan, hırsızlık, dolandırıcılık, sahtecilik ve cinsel istismar gibi suçların, bilgisayar veya bilgisayar ağı kullanılarak işlenmesi" olarak tanımlamıştır.

2.2.2. Bilişim Suçları Sınıflandırılması

İnterpol Genel Sekreterliği'nin hazırlamış olduğu "İnterpol Computer Crime Manual" esas olmak üzere, 11.06.1999 tarihinde hazırlanan Emniyet Genel Müdürlüğü "Bilişim Suçları" raporunda suç tipleri aşağıdaki gibi ele alınmıştır (Emniyet Genel Müdürlüğü, 2000).

1- Bilgisayar Sistemlerine Ve Servislerine Yetkisiz Erişim

a- Yetkisiz Erişim: Bir bilgisayar sistemine yada bilgisayar ağına yetkisi olmaksızın erişmektir. Burada, 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, uzak bir mesafeden örneğin bir modem hattı yada başka bir bilgisayar sisteminden de olabilir.

b- Yetkisiz Dinleme: Bir bilgisayar veya ağ sistemine, sisteminden veya sistemi içinde yapılan iletişimin yetkisi olmaksızın teknik anlamda dinlenmesidir. Burada, suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferinin teknik olarak takip edilmesi ve dinlenmesidir. Teknik anlamda dinleme, iletişim içeriğinin izlenmesi, verilerin kapsamının ya direk olarak (bilgisayar sistemini kullanma yada erişme yoluyla) ya da dolaylı olarak (elektronik dinleme cihazlarının kullanma 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.

c- Hesap İhlali: Herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının bilgisayar sistemlerinde bulanan hesabını kanunsuz olarak kullanmaktır. Bir kişinin, İnternet, telefon veya benzer bir sistemdeki hesabının kişinin rızası olmaksızın kanunsuz olarak kullanılmasıdır.

2- Bilgisayar Sabotajı

a- Mantıksal Bilgisayar Sabotajı: Bir bilgisayar yada iletişim sisteminin fonksiyonlarını engellenme amacıyla bilgisayar verileri veya programlarının sisteme girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir. Bir bilgisayar yada iletişim sisteminin fonksiyonlarına zarar vermek amacı ile verilerin yada programların Zaman Bombası (Logic-Time Bomb), Truva Atları (Trojan Horses), Virüsler, Solucanlar (Worms) gibi yazılımlar kullanılarak değiştirilmesi, silinmesi, ele geçirilmesi yada çalışmaz hale getirilmesidir.

b- Fiziksel Bilgisayar Sabotajı: Bir bilgisayar yada iletişim sisteminin fonksiyonlarına zarar vermek amacı ile sisteme fiziksel yollarla zarar vermedir. Bir bilgisayar yada iletişim sistemini oluşturan parçalara sistemin fonksiyonlarını yerine getirmemesi amacıyla fiziksel yollarla zarar verilmesidir.

3- Bilgisayar Yoluyla Dolandırıcılık

Bilgisayar ve iletişim teknolojileri kullanılarak verilerin alınması, girilmesi, değiştirilmesi ve silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etmek için mağdura zarar vermektir. Suçlunun hedefi, kendisine veya bir başkasına mali kazanç sağlamak yada mağdura ciddi kayıplar vermektir. Bilgisayar dolandırıcılığı suçları suçların modern bilgisayar teknolojileri ve ağ sistemlerinin avantajlarını değerlendirmeleri yoluyla klasik dolandırıcılık suçlarından farklılık gösterir.

a- Banka Kartı Dolandırıcılığı: Kartlı ödeme sistemleri kullanılarak yapılan dolandırıcılık ve hırsızlık suçlarıdır. Kredi kartları, Bankamatik kartları ve benzeri kartlarla yapılan dolandırıcılık suçlarıdır. Kart ödeme sistemleri (ATM-Automated Teller Machine) genelde bankalar veya benzer finans kuruluşları tarafından kullanılırlar. Erişim genellikle bir kişi tanımlama numarası (PIN-Personel Identification Number) girişi gerektiren bir kart yada benzeri bir sistem iledir. Dolandırıcılık bu kartların çalınması, çoğaltılması, kopyalanması yada iletişim hatlarının engellenmesi ve dinlenmesi yoluyla oluşur.

b- Girdi/Çıktı/Program Hileleri: Bilgisayar sistemine kasıtlı olarak yanlış veri girişi yapmak veya sistemden yanlış çıktı almak yada sistemdeki programların değiştirilmesi yoluyla yapılan dolandırıcılık ve hırsızlıktır. Bir bilgisayar veritabanına yanlış veri girmek yaygın bir dolandırıcılık yoludur. Davalar araştırılırken sistem de kullanılan yazılım programları da içerecek şekilde tam bir teknik tanımlama yapılmasına ihtiyaç vardır.

c- İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma: Kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerini veya diğer bilgisayar sistemlerini hakkı olmadan kullanmak. İletişim servislerinin değişik şekillerde kötü niyetli olarak kullanımı olarak tanımlanabilir.

4. Bilgisayar Yoluyla Sahtecilik

Kendisine ve başkasına yasa dışı ekonomik menfaat temin etmek ve mağdura zarar vermek maksadıyla; bilgisayar sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır. Dijital ortamda tutulan dokümanlar üzerinde değişiklik yapmak bir tür sahteciliktir. Bilgisayarlarda tutulan dokümanlarda (İş akış programları, raporlar, personel bilgileri vs) sahtecilik amacıyla yapılan değişikliklerle kişiler kandırılabilmektedir.

5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı

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

a- Lisans Sözleşmesine Aykırı Kullanma: Tek bir bilgisayar için alınan yazılımın birden fazla bilgisayarda lisans haklarına aykırı olarak kullanılmasıdır. Yazılım lisansları genellikle tek bir bilgisayarda kullanmak üzere tanzim edilir. Tek bir bilgisayar için alınan yazılımın lisans hakları çerçevesinde birden fazla bilgisayara kullanılmak üzere kopyalanması ve çalıştırılması yasaktır.

b- Lisans Haklarına Aykırı Çoğaltma: Lisans sözleşmesi ile korunmuş bir yazılımın saklanmış olduğu medya ortamının başka bir medya ortamına kanunsuz olarak kopyalanmasıdır. Genel itibariyle ödemeden kaçınmak için daha önce satın alınmış veya yine lisans sözleşmesine aykırı olarak kopyalanmış yazılımın başka bir medya ortamına taşınmasıdır. Burada söz konusu yazılımı kopyalayan da kopyalatan da sözleşme ihlali yapmış sayılır. Bugün bir çok yerde satılan program, film ve oyun CD'leri bu şekildedir. Bu tür CD lere bakıldığında üzerlerinde Kültür Bakanlığının bandrolü olmadığı ve yazılabilir CD lere kayıt edildiği ve orijinal kutularında olmadığı görülmektedir.

c- Lisans Haklarına Aykırı Kiralama: Değişik medyalar üzerine kayıtlı oyun, film ve yazılımların lisans haklarına aykırı olarak kiralanmasıdır. Oyun, program ve filmleri kiralamaya yönelik özel bir lisansı bulunmadan kiralanmasıdır. Daha çok film ve oyun CD lerinin kiralanması olarak karşımıza çıkmaktadır.

6. Diğer

a- Kişisel Verilerin Suistimali: 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. 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. Kişiler hakkındaki verileri ticarete yönelik kullanmak isteyen bir sistemde, her bilgi para anlamına gelecektir. Kişilere ait verileri, ticari kar amacıyla kullanmak için bilgisayarlar çok kolaylaştırıcı imkanlar sunmuştur. Bazı firmalar kredi kartları ile yapılan alışverişler, telefon konuşmaları, süpermarket kayıtları ve diğer finansal işlemler aracılığıyla sıradan vatandaşın bütün günlük yaşamına ilişkin verileri bilgisayarların hafızalarında depolamaktadır. Örneğin, günlük hayatın olmazsa olmazlarından birisi olan kredi kartı harcamalarından alışveriş alışkanlıklarımız tespit edilerek; bunlar dev firmalara satılarak haksız kazanç elde edilmektedir.

Ayrıca, teknolojinin gelişmesi ve uyduların yeryüzünün her karesini 24 saat gözlemesi, bilgisayarların binlerce milyonlarca insana ait tasnifli veriyi kolaylıkla saklayabilmesi ve yerküre üzerinde bilinmedik, görülmedik dinlenilmedik yer kalmamış olması, insanların sürekli gözetim altında tutulduğu bir “elektronik gözetim” kavramını ortaya çıkarmıştır.

b- Sahte Kişilik Oluşturma ve Kişilik Taklidi: Hile yoluyla kendisine veya bir başkasına menfaat sağlamak yada zarar vermek amacıyla gerçek kişilerin taklit edilmesi veya hayali kişilerin oluşturulmasıdır. 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.

c- Yasadışı Yayınlar: Yasadışı unsurların yayınlanması ve dağıtılması maksadı ile bilgisayar sistem ve ağlarının kullanılmasıdır. 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.

Bu bölümde, bütün dünyayı tehdit altına alan ve hızla artma trendinde olan bilişim suçlarının gelişimi ve ortak özellikleri ele alınmıştır.

2.2.3. Bilişim Suçlarının Gelişimi ve Ortak Özellikleri

2.2.3.1. Bilişim Suçlarının Gelişimi

Her yeni gelişen teknoloji insan hayatını kolaylaştırdığı gibi suçlulara da potansiyel suç işleme olanağı sağlamaktadır. İletişim teknolojisi, bilgisayar ve internetin gelişimi ile birlikte bilişim suçları ortaya çıkmıştır.

Başlangıç (1970-1980): 1970’lerde "phreaker" olarak anılan ve telefon sistemlerine girerek (phreaking) bedava telefon görüşmeleri yapan telefon

hacker'ları ile bilişim suçları duyulmaya başlamıştır (Günay, 1999). 1971'de, John Draper, Cap'n Crunch marka gevrekten çıkan bir oyuncağın çıkardığı ses ile defalarca ücretsiz görüşme yapmayı başarmıştır. 'Captain Crunch' lakabıyla anılan Draper, bu oyuncağın, AT&T'nin uzak mesafe görüşme sistemine erişim için kullanılan tona eşit olan 2600 hertz'lik bir sinyal çıkardığını tespit etmiştir. Draper daha sonra 'blue box' adlı bir cihaz geliştirerek, phreaker'lerin bedava görüşme yapmasını sağlamıştır (Andaç, 2003). Telefon hatlarının yasa dışı kullanımı, telefon şirketlerini harekete geçirmiş ve bilişim suçlarını ilgilendiren yasalar düzenlenmiştir. Bilgisayarların gelişmesiyle telefon hacker'ları ve bilgisayar teknolojisi birleşmiş ve daha güçlü araçlar ortaya çıkmıştır. 1980'lerde bu işe merak salan phreaker ve hacker'lar her türlü sisteme girmeye başlamışlardır.

İlan tahtası sistemleri olarak Türkçe'ye geçen BBS (Bulletin Board System), dönemi (1980-1986): 1978 de, Chicago'lu iki genç, Randy Seuss ve Ward Christiansen, ilk kişisel BBS'i kurmuşlardır (Kurt, 2003). Bilgisayarların modemlerle birbirine bağlandığı BBS ağlarının kullanımının yaygınlaşması ile, dünyanın dört bir yanındaki yüzlerce bilgisayar birbirine bağlanmıştır. BBS ile birlikte yeni nesil, çağdaş saldırganlar ve modern saldırı araçları ortaya çıkmıştır. Bu saldırganlar, web sitelerini ele geçiren, anti sosyal davranışlar sergileyen ve sistem üzerindeki dosyaları yok eden zararlı saldırganlardır. Bunlar, güçlü saldırı araçları ile girilen belirli bir telefon aralığındaki tüm telefon numaralarını çevirerek hatta bağlı modem olup olmadığını tespit edebilmekteydiler (Karaahmetoğlu, 2001).

Ağ dönemi (1987-1994): Bilgisayar ağları ağ döneminde binlerce bilgisayarı içine alacak büyüklüğe ulaşmıştır. Henüz internet servis sağlayıcıları gelişmemesine rağmen, bir çok üniversite ve kuruluş birbirine bağlanmıştır. Bilgisayar ağlarının gelişmesi ile kötü niyetli saldırganlar dosyaları silerek, sistemi çökerterek sistemlere zarar vermeye başlamışlardır. Sonunda Amerikan Devleti bu özgürlükler ortamına müdahalede bulunarak 1986'da Federal Computer Fraud and Abuse Act (Federal Bilgisayar Sahtekarlığı ve Kötüye Kullanma) adı altında bir yasa çıkarmıştır (Kurt, 2003). 2 Kasım 1988'de, babası

National Security Agency'de (NSA) bilgisayar güvenlik uzmanı olan Robert Tapan Morris Morris bu yasa ile tutuklanan ve ceza alan ilk kişi olmuştur. Morris, "internet worm" (Internet solucanı) adını verdiği bir hack yöntemi ile net'e bağlı 6000 bilgisayarı çökerterek internetin onda birini çalışamaz hale getirmiştir (Karaahmetoğlu, 2001). Ancak solucanın bulaştığı bilgisayarlara zarar vermemesi nedeniyle, sadece parasal ceza ödemesine ve amme hizmetinde bulunma cezasına çarptırılmıştır. Amerikan hükümeti bu saldırı sonucunda bilgisayar anti-terörizm takımı olan "Computer Emergency Response Team" (CERT)'in kurulmasına karar vermiştir. Aynı yıl Condor lakablı Kenvin Mitnick; bilgisayar sistemlerinden bir milyon dolar değerinde gizli bilgi ve binlerce kredi bilgisi çalmak, California motor araçları veri tabanına girmek, New York ve California'nın bir çok makineyı birbirine bağlayan bir cihaz olarak adlandırılan hub'larını uzaktan kontrol etmekle suçlanmıştır. Devlet bilgisayarlarına suç amaçla giren ilk kişi ve FBI'nın en çok arananlar listesinde yer alan ilk saldırgandır (Kurt, 2003).

Web dönemi (1995-): Alan isimlendirme sisteminin icadı ile web sistemi doğmuştur. Web'in BBS'nin yerini alması saldırı araçları ve yöntemlerinin dağıtımını daha da kolaylaştırmıştır. Bu konuda yasalar çıkmış, ülkeler saldırı araçları ve saldırganlarla mücadeleye başlamışlardır (Karaahmetoğlu, 2001). 1995 yılında St. Petersburg Üniversitesi mezunu Vladimir Levin, Citibank'ın bilgisayarlarına girerek müşterilerin hesaplarından, yaklaşık 10 milyon doları kendi hesabına aktarmıştır. Levin Heatrow havaalanında İnterpol tarafından yakalanmış ve Citibank paranın büyük kısmını geri almıştır. 2000'lere gelindiğinde DoS (Denial of Service) türü saldırılar gerçekleşmeye başlamıştır. eBay, Yahoo ve Amazon gibi dev internet portallarını veri bombardımanına tutularak çökerten hacker'lar milyonlarca dolarlık zarara neden olmuşlardır. Virüslerin ise, 1999'dan sonra web'de büyük zararlara yol açtığı görülmüştür. 1999 Nisan ayında Çernobil anısına yaratılan CIH virüsü binlerce bilgisayara milyar dolarlarla ifade edilen zararlar verinceye kadar virüslerin bu kadar zararlı olabileceği düşünülmemiştir. 2000'de "LoveBug" 9, "Melisa" 5, 2001'de "Kırmızı Kod" (Code Red) 2,6 milyar dolar zarara sebep olan virüsler olmuştur.

Günümüzde artık saldırganlar ulusal tehdit olmaktan çıkarak uluslar arası tehdit oluşturmaya başlamışlardır. Maddi ve manevi birçok zararından dolayı günümüzde uluslar arası düzenlemelere ve işbirliğine gitmek kaçınılmaz olmuştur. Ülkeler ve uluslar arası kuruluşlar bilişim suçları konusunda çalışmalar yapmaktadırlar. Bilişim suçlarını işleyen bilişim suçlularının da incelenmesinde yarar vardır.

2.2.3.2. Bilişim Suçlarının Ortak Özellikleri

Demirbaş (2005), bilişim suçlarının işlenişi ve doğurduğu sonuçlar dikkate alınarak bu suçların ortak özelliklerini şu şekilde ifade etmiştir.

1) Bilişim suçunun işlenmesinde bilgisayar sistemleri ve teknolojilerinin kullanılması,
2) Yakalanma riskinin çok az olması,
3) Bilişim suçunun sonucunda çok yüksek kazancın kolay ve risksiz olarak temin edilmesi,
4) Yeni suçlar olması nedeniyle gerekli kanun ve düzenlemelerin eksik ve yetersiz olması,
5) Diğer suç türlerine göre daha ağır maddi ve manevi sonuçlar doğurması,
6) Suç mağdurlarının genelde bilinçsiz kullanıcılar ile ekonomi ve finans sektöründen olması,
7) Ekonomik kaybın büyük olması nedeniyle, genelde basit suçlar haricinde güvenlik güçlerine bildirilmemesi,
8) Zarara uğrayan mağdurların büyük kuruluş ve işletmeler olması durumunda itibar ve prestij kaybetme korkusunun baskın gelmesi,
9) Bilişim suçunu işleyenlerin genelde 17-35 yaş arasındaki gençlerden oluşması,
10) Bilişim suçu mağdurlarının ticari faaliyette bulunan kurumlar olması,
11) Suçluların çoğunluğu, bazen fiillerinin deşifre olunmaması için ihbar edilmeyeceğinden, bazen ise, bu fiilleri karşılayacak ceza normunun bulunmamasından cesaretle, eylemlerinin yaptırımsız kalacağına güvenle hareket etmektedir (Demirbaş , 2005: 266).

2.2.4. Bilişim Suçluları, Suç İşleme Nedenleri ve Bilişim Mağdurları

Bu bölümde bilişim suçluları, suç işleme nedenleri ve bilişim mağdurlarının genel özellikleri 3 bölümde incenmiştir.

2.2.4.1. Suçlu Tipleri

Suç işleme eğiliminde bulunan kişi ve/veya kişiler bilgisayar ve donanımlarını kullanarak üçüncül kişi ve/veya kişiler ile kurum ve kuruluşlara zarar vermeyi hedeflemektedirler. Uzaktan erişim ile diğer bilgisayarlara ulaşarak verilerini kullanılamaz hale getirmek, silmek, değiştirmek olabileceği gibi bağlı bulundukları ağı meşgul ederek çalışamaz hale getirmek gibi girişimler işlenen suçlara örnek olarak verilebilir (Aktepe, 2003).

Saldırganları kategorize etmek için bir çok yol vardır. Yine de saldırganları tam olarak gruplamak çok zordur. Saldırganlar yaptıkları işlere ve bilgi seviyelerine göre birkaç farklı tipte adlandırılabilirler. Fakat tüm saldırganların belirli karakteristikleri vardır. Yakalanmak istemezler, kendilerini gizlemeye çalışırlar. Saldırganları yaptıkları işlere göre; “hacker”, “cracker”, “lamer” “cyberpunk”, “phreaker” olarak sınıflanabilir. En çok kullanılan ve bilinen tanımlamalar hacker ve cracker’dır. İşletim sistemlerinin doğasındaki açık kapıları kullanarak bu açık kapılardan sisteme sızma eylemine “hack”, bu eylemi gerçekleştirenlere de “hacker” denir. Teknik bilgileri üst seviyededir. Saldırı kastı olmadan sistemin açıklarını ve eksiklerini bulmak için eylemlerini gerçekleştirirler. “Hacker” ve “cracker” arasındaki temel fark zarar verme kastıdır. Kötü niyetli zarar verme kastıyla veya kendisine yahut bir başkasına çıkar sağlamak için web sayfalarının veya sistemlerin güvenlik duvarlarının, şifrelerinin kırılarak web sayfasına veya sistemlere zarar verilmesine “crack” bu eylemi yapanlara da “cracker” denir. “Lamer”lar ise internet üzerinden ücretsiz dağıtılan bazı programlarla “hack” eylemi yapmaya çalışan ama aslında bir şey bilmeyen kişilerdir (Karaahmetoğlu, 2001). Kripto şifrelerini çözerek sistemlere sızma eylemlerinde bulunanlara kriptografi uzmanlarına da “cyberpunk” adı verilir (Uzun, 1999). Telefon şirketlerinin güvenlik sistemlerini kırarak sistemi kanun dışı yollarla kullanan ya da çıkar sağlayan kişiler de “phreaker” olarak

tanımlanır. Tanımlamalarının değişik olmasına rağmen iyi bir saldırgan tüm bu alanlarda bilgi sahibi olmakla birlikte, içlerinden birinde uzmanlaşmalıdır.

İsveç'te SOLARZ tarafından National Council For Crime Prevention hesabına yapılan bir araştırmada, bilgisayar suçu faillerinin yaş ortalaması 35.2 olarak tespit edilmiştir. Bu faillerin yüzde kırk dördünü bayanlar oluşturmaktadır. İtalya'da Serviziyo Securinet'in 1990-91-92 yıllarına ilişkin olarak yayınlandığı verilere göre ise polis tarafından elde edilen bilgisayar suçu faillerinin 19 yaşından büyük olduğu görülmektedir. Bunların % 25'i 35 ila 45, % 29'u 25 ila 35, % 55'i 19 ila 25 yaşları arasında yer almaktadır. Yine bunların % 38'i işsiz iken % 47 gibi büyük bir çoğunluğu ise üniversiteli öğrencilerden oluşmaktadır. Çalışan kesimin % 43'ü bilgisayarla alakalı bir işte yer almaktadır (Yazıcıoğlu, 1997: 103).

Bilişim suçlarını işleyenler genelde 20-30 yaşları arasındaki gençlerden oluşmaktadır. Bu gençler büyük çoğunluğu erkeklerden oluşan, teknik bilgi düzeyi yüksek kişilerdir (Demirbaş, 2005: 267).

Koltuksuz'a göre (2008), bilişim suçlusunun psikolojik profili şu şekildedir:

- Genç, dinamik, üst düzey eğitimli,
- Zeki, kendisine güvenilen,
- Çoğunlukla sabıka kaydı olmayan,
- İnsanlarla ilişki kurmakta zorlanan,
- Kendini kanıtlamaya gereksinim duyan,
- Ancak bir bilgisayarla varlığını hisseden kişilik (Koltuksuz, 2008).

Pekgözlü'nün (2008), Boni and Kovacich'den (1999) aktardığına göre bilgisayarları ve telekomünikasyon sistemlerini kullanarak internet suçluları; ahlaka aykırı, etik olmayan ve yasadışı amaçlarına ulaşmak istemektedirler. Bu tür suçlular, tipik çalışanlardan, intikam arzulayan insanlardan, kafa gücünü kullanarak çalışan (white-collar) personelden, para canlısı insanlardan, uyuşturucu satanlardan, organize suç işleyen suçlulardan veya borç içinde bulunan kimselerden herhangi biri olabilir. Bu suçluları sınıflandırmak için

mağdurlarına göre pozisyonları kullanılabilir. Dolayısıyla da dahili ve harici tehditler olarak iki tür tehdit tanımlanabilir. Harici grupların bazıları, tedarikçiler veya satıcılar, önceki çalışanlar, bilgisayar korsanları, ilgili iş sahasındaki çalışanlar, rakipler, müşteriler, taşeron şirketler, yabancı ülkelerin örgütleri, politik eylemciler, danışmanlar, bakım görevlilerine benzer dış çalışanlar, dışardan test edenler ve teröristlerdir. Dahili tehdit ediciler ise şirket görevlileri veya şirkete kontratla iş yapan kişilerdir ve kamu veya özel kurumların içerisinden veya bu kurumlar tarafından onaylanmış yerlerden sistemlere erişim hakkı olanlardır. Bunlardan bazıları güvenlik görevlileri, pazarlama personeli, finansal analistler, envanter çalışanları, test ediciler ve yöneticilerdir.

2.2.4.2. Bilişim Suçlularının Suç İşleme Nedenleri

Bilgisayar suçu faillerini suç işlemeye iten sebepler şunlardır:

1) İşten çıkarılma veya işteki çeşitli hoşnutsuzluklar sebebi ile intikam alma duygusu,
2) Önemli biri olma duygusu,
3) Mali zorluklar (İstanbul Emniyet Müdürlüğü, 2006)

Suçluların, suçun doğuşundan beri “fırsatları takip ettiği” bir gerçektir. Bilişim suçları için de, klasik suç tipleri için geçerli benzer sebepleri saymak mümkündür. Fakat kısaca bahsedecek olursak, yaşa göre değişmekle birlikte, bilişim suçlularının suç işlemeye güdüleyecek çeşitli motivasyonları vardır. Bilişim suçluları; intikam almak, kendilerini ispat etmek, zevk almak, merak, çıkar sağlamak, başka bir suç için gerekli argümanları sağlamak gibi sebeplerle suç işleyebilirler. Bu konularda uzmanlaşmış bazı suçlu tipleri; şirketler veya ülkeler, terör ve suç örgütlerince para karşılığı kiralanarak başkaları nam ve hesabına suç işlemektedirler (Özcan, 2003).

Teknolojik açıdan kompleks olmayan bilişim suçlarının bir çoğu, ya macera arayan kişiler tarafından bilinmeyeni keşfetme ya da kendini ispat etme güdüsüyle işlenir. Bilişim alanında işlenen bazı suçlar ise, işlenme frekansı bakımından az sayıda olmasına karşın verdiği zararlar çok büyüktür. Bu tip

suçların kompleks yapısı ve suçu işlemek için teknolojik bilgi düzeyinin yüksekliği göz önüne alındığında suça güdüleyen faktörler de değişir. Bu tür suçları işleyen kişiler uzman kişilerdir ve kendileri veya üye oldukları grupların çıkarları için suç işlerler. Bunları bilişim ortamında izlemek veya yakalamak imkansız denebilecek ölçüde zordur (Özalp, 2002).

2.2.4.3. Mağdurların Genel Özellikleri

Bilgisayar suçlarında bilinmeyen alan oldukça yüksek olup, % 90-95'ler seviyesine ulaşmaktadır. Bunun nedeni, mağdurların bu suçları kamuoyundan saklamak istemelerinden kaynaklanmaktadır; çünkü, şirket seviyesinde gerçekleşen suçlar, kimseye duyurulmadan çözümlenmeye çalışılmaktadır. Bunun nedeni, şirket yöneticilerinin bilgisayar suçları nedeniyle, kolluğun şirketin iç işlerine karışarak, detaylı bilgi sahibi olmalarını istememeleridir. Ayrıca, bu tür bir araştırmanın şirketin prestij yitirmesine neden olacağına da inanılmaktadır. Fiiller, yetkili makamlara bildirilmediklerinden iş dünyası içinde gizli kalmakta ve bu nedenle bazı failler suçlarını toplumdan gizleyebilmektedirler. Bilgisayar suçlarında mağdur durumunda olan bazı şirketlerin ticari yaklaşımları da belirleyici olmaktadır. Örneğin bazı şirketler, yıllık % 5'e kadar olan zararları araştırma yapmaksızın olağan kabul etmektedirler (Demirbaş, 2005: 268).

National Center of Computer Crime Data'nın iki yıl süreyle Kaliforniya'da gerçekleştirdiği bir başka araştırmaya göre ise, bu suçlara ilişkin mağdurların büyük bir çoğunluğunu sıra ile ticari kuruluşlar, bankalar, telekomünikasyon firmaları, kamu kurumları ve bilgisayar üreten firmalar oluşturmaktadır. Bilgisayar suçu mağdurlarının belirlenmesi açısından genel olarak bu suçlardaki rakamların yüksekliğinden ve çeşitli kurum ve kuruluşların değişik emniyet tedbirleri ile sonuca gitmek istemelerinden dolayı bu konuda da diğer hususlarda olduğu gibi çok sağlıklı sonuçlar elde edebilmek pek mümkün olmamaktadır. Ancak suç mağdurları arasında bankaların ticari ve finans kuruluşlarının ve kamu sektörünün diğer kesimlere oranla daha yoğun olarak çeşitli ihlallere maruz kaldığı ifade edilebilir (Yazıcıoğlu, 1997: 107).

Bilişim suçu mağduru olmamak için yapılması gerekenler şunlardır:

- İnternet'e bağlanılan bilgisayarlarda mutlak suretle güvenlik yazılımları (antivirüs programları) kullanılmalıdır.
- Antivirüs programları ve bilgisayarlarda yüklü bulunan ana işletim sistemleri, güvenlik açıklarına karşı ilgili web sitelerine bağlanarak düzenli olarak güncellenmelidir.
- Kullanılan sohbet (chat) programları da düzenli olarak güncellenmeli, bu yazılımların en son versiyonları kullanılmalıdır.
- Genel prensip olarak doğrudan tanışıklık olmayan kimseler ile bağlantı kurulmamalı, eğer bağlantı kuruldu ise de kesinlikle dosya paylaşımı yapılmamalıdır.
- İnternet kullanıcıları chat ortamında başta kredi kartı bilgileri olmak üzere, kesinlikle kendilerine ait bilgileri (isim, adres, telefon) vermemelidir.
- Kullanıcılar, bilgisayarlarını yakinen tanımadıkları kişilere kullandırtmamalıdır.
- İnternet bankacılığı ve e-posta şifreleri mutlak suretli güvenli şifrelerden seçilmeli, bu harf ve rakam gruplarından oluşan güvenli şifreler periyodik aralıklarla düzenli olarak değiştirilmelidir.
- İnternet bankacılık işlemleri toplu kullanıma açık olan internet kafe ve benzeri yerlerde yapılmamalı, kullanıcılar bankacılık işlemlerini evlerindeki ya da işyerlerindeki daha güvenilir olan bilgisayardan gerçekleştirmelidir.
- Bilgisayar kullanıcıları bunun ayrıca bir suç teşkil ettiği bilinci ile korsan yazılım kullanmamalı, lisanslı olmadıkları için düzenli olarak güncellenemeyen bu yazılımların güvenlik açıklarına sebebiyet verdikleri unutulmamalıdır.
- Kullanıcılar internet ortamında bilgisayarlarına müdahale edildiğini anladıkları anda derhal bilgisayarlarının fişini çekerek bağlantıyı koparmalı ve akabinde oluşan güvenlik açığının giderilebilmesi için yetkili bilgisayarcılardan profesyonel yardım almalıdır.
- İnternet ortamında bir suçun mağduru olunduğunda ya da bir suçla karşılaşıldığında derhal polise ihbarda bulunulmalıdır (Emniyet Genel Müdürlüğü, 2007).

2.2.5. Bilişim Suçlarında Başarı ve Çözüm İçin İlgili Kurum ve Kuruluşlar

Bilişim suçlarının, devlet, ülke, vatandaş ve birey bazında önemli bir sorun olmaması ve bu tür suçlardan mali olarak en az etkilenmek için, için mutlak suretle tüm ortak paydaların birlikte işbirliği içerisinde olması ve etkin bir koordine sistemi ile işlemlerini yürütmesi gerekmektedir. Ülke vatandaşlarının, yaşadıkları bir bilişim suçu karşısında nereye müracaat edeceklerini bilmeleri, on-line ihbar hattı ile birey taleplerinin hemen değerlendirilmesi ve yaşanacak sıkıntıların önüne geçilmesi birlikte bu suçlara karşı ortak hareket etme anlayışını güçlendirerek, başarı ve çözüm için önemli bir etken olacaktır.

Bilişim suçlarında başarı ve çözüm için ilgili kurum ve kuruluşlardan bazıları şu şekildedir: Servis Sağlayıcılar, Telekomünikasyon İletişim Başkanlığı (TİB), Bankalararası Kart Merkezi (BKM), Bankalar, İnternet Kafeler, Mynet, Yahoo, Hotmail, Yer Sağlayıcılar, Microsoft, Telekominikasyon Kurumu (TK), Adli Birimler, Emniyet ve Jandarma Birimleri, Internet (Ust) Kurulu, Konuyla İlgili Sivil Toplum Kuruluşları (TİEV Tüm İnternet Evleri Derneği, TÜBİDER Bilişim Sektörü Derneği, TÜBİSAD Bilişim Sanayicileri ve İşadamları Derneği, BİYESAM Bilişim ve Yazılım Eser Sahipleri Meslek Birliği, BMD Bilişim Muhabirleri Derneği, İNETD İnternet Teknolojileri Derneği, LKD Linux Kullanıcıları Derneği, YASAD Yazılım Sanayicileri Derneği, TBD Türkiye Bilişim Derneği, TÜDER Tüketiciler Derneği, İnternet ve Hosting Sorunları Forumu, Bilgi Güvenliği Derneği, Sanal Banka Mağdurları Derneği).

Burada, Bankalararası Kart Merkezi'ne (BKM) yer verilmiştir. Emniyet, Savcılık ve Mahkemelerden gelen kredi kartı taleplerini bankalara aktaran ve bilgi toplayarak bağlantıları emniyet birimlerine bildiren Bankalararası Kart Merkezi, 1990 Yılında 13 kamu ve özel Türk Bankasının ortaklığı ile kurulmuştur. Bankalararası Kart Merkezi, ihtisas polisi uygulamaları gerçekleştirmektedir. Jandarma Genel Komutanlığı ve Emniyet Genel Müdürlüğü ile BKM arasında tesis edilen işbirliği sonucu, her yıl emniyet ve jandarmanın rütbeli bir personeli belirli bir süre için Bankalararası Kart Merkezi'nde görevlendirilmektedir. Bu süre zarfında, Jandarma Genel

Komutanlığı ve Emniyet Genel Müdürlüğü mensuplarının kart sahteciliği ile ilgili konularda uzmanlaşmaları ve BKM, Emniyet ve Jandarma ile ilişkilerin güçlendirilmesi, banka ve kolluk kuvvetleri arasındaki iletişimin geliştirilmesi sağlanmaktadır (KOM Daire Başkanlığı, 2008).

2.2.6. Siber Terörizm ve Organize Suçlar

Bu bölümde siber terörizm, siber terörizm atakları, dünya'da ve ülkemizde siber terör, siber terör ve İnternet kafeler, siber terör ve Emniyet Teşkilatı, Organize Suçlar ve elektronik casusluk ele alınmıştır.

2.2.6.1. Siber Terörizm

Siber Terörizm kavramının yazılı ve görsel medyada, ulusal ya da uluslararası arenada çok fazla kullanılmaya başladığı görülmektedir. Trojanlar, kurtçuklar, virüsler, DNS saldırıları siber terörizmin basit araçları olarak görülebilir. Son yıllarda terör ve terörizm konularına çok büyük bir önem verildiği görülmektedir. Bu ilgi daha çok havaalanı gibi fiziksel alanlara yönelirken, siber terörizm kavramına düşük düzeyde dikkat çekildiği söylenebilir. Bunun 2 temel nedeni vardır. Bu nedenler siber terörizm tartışmalarında yer alan 2 karşıt görüşle açıklanabilir. Bu görüşlerden birincisine göre siber terörizm kimseye zarar vermeyen bir mittir (Forno, 2000). Bu görüşün sahipleri milenyumda ikiz kulelere yönelik gerçekleştirilen eylemlerle anlamını yitirmeye başlamıştır. Daha çok bilgisayar güvenliği konuları ile ilgilenen diğer grup ise sanal ortamda yapılan eylem ve atakların gerçek bir tehdit olduğu görüşündedirler (Denning, 2000). Siber terörizmin, tam bir tanımı üzerinde anlaşmak mümkün olmasa bile, birçok araştırmacı ve akademisyen, siber atak biçimlerinin kategorize edilmesine yönelik, bir bakış açısı geliştirmişlerdir. Meriam Webster sözlüğü terörü, yoğun korku ve şiddet uygulaması olarak terörizmi ise, özellikle zorlama anlamında sistematik terör kullanımı olarak tanımlamaktadır. Desouza ve Hensgen (2003), siber terörizm tanımı olarak aşağıda belirtilen tanımı önermektedir.

"Bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması

aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinliklerdir."

Siber terörizm de, kullanılan araçların kötü ve zararlı olduğunu söylemek mümkün değildir. Adı üzerinde bunlar sadece bir araçtır. Aracın iyi ya da kötü olmasını belirleyen onun kullanılmasıdır. Çünkü, "İnsanları öldüren silah değil, silahı kullanan insandır." Bu durumda, Desouza ve Hensgen'e göre (2003), asıl önem verilmesi gereken; araç değil, onu kullanan insanların (aktörlerin) niyet yada kasıtlarıdır. Hemen hemen bütün ülkelerin gitgide bilgisayar ve iletişim teknolojilerine kaçınılmaz olarak bağımlı olması, içinde bulundukları risk durumlarınında, buna bağlı olarak artmasına yol açmaktadır. Pollitt'in (2002), "Amerika, tamamen bilgisayarlara bağımlıdır. Bu yüzden artan bir şekilde risk altındadır" sözü ülkemiz açısından da benzer anlamlar ifade etmektedir.

Siber Terörizm alanında aktivite gösteren terörist profili gözden geçirildiğinde, bu şahısların genellikle orta sınıftan gelen teknik olarak yetenekli çevirim içi iş sitelerine ve hükümetlerin resmi sitelerine ideolojik veya kişisel çıkar amaçlı saldırıda bulunan kişiler oldukları anlaşılmaktadır. Diğer taraftan, uluslar arası yapıya sahip olması, teknik olarak ehliyetli elemanları içinde barındırması, sanal ortamda planlama ve eğitim verebilmesi, kara para aklama ile de bağlantılı olabilmesi terörist grupların niteliği olarak ortaya çıkmaktadır (Doğan, 2007).

2.2.6.2. Siber Terörizm Atakları

Siber terör ataklarının birinci kategorisi, "basit ve yapılandırılmamış" olandır. Genelde kişisel zevk için üretilen, hedef ayrımı yapmayan, çok hızlı ve etkili yayılarak büyük zararlar veren Kurtçuk (worm) ve virüsler, bu kategori altında toplanmaktadır. İkincisi, çoklu sistemlere karşı daha karmaşık atakları içeren "ileri düzeyde yapılandırılmış olanlardır." Üçüncü olarak, "karmaşık koordinasyona sahip ataklar"dır. Bu ataklar, çok ileri düzeyde yapılmış hedef analizlerine, üstün zeka ve denetime sahiptir. Naval Postgraduate, okul bünyesinde bulunan the Center for the Study of Terrorism and Irregular Warfare araştırmacılarına göre, ileri düzeyde yapılandırılmış bir atağın

gerçekleştirilebilmesi için, bir grup insanın 2-4 yıl arasında çalışması gerekmektedir. Karmaşık koordinasyona sahip ataklar için ise bu süre 6-10 yıl arası olarak ön görülmektedir. Desouza ve Hensgen (2003), siber terörizmi "geleneksel" ve "nadir" ataklar doğrultusunda değerlendirmektedir. Geleneksel olanları açık, nadir olanları ise örtülü ataklar olarak görmektedir. Geleneksel ataklar, virüs ya da kurtçukların (worm) kullanılmasıyla bilgi altyapılarının tahrip edilmesini içermektedir. Easter eggs, time bombs ya da yahoo, eBAy, amazon gibi ünlü siteleri etkileyen DDOS atakları bunlara bir örnek olarak verilebilir. Bu kapsamda değerlendirilebilecek ILOVEYOU, Melissa gibi virüsler de milyonlarca kullanıcıyı etkileyerek milyarlarca dolar hasarın oluşmasına yol açmıştır. Siber törörizmin, diğer bir biçimi olan nadir ataklarda ise terörist gruplar aralarındaki iletişimi kolaylaştırmak için elektronik çıkışları kullanmaktadır. Örneğin, internet üzerinde bulunan tartışma gruplarındaki masum görünen bazı mesajlar, teröristler arasındaki bir iletişim biçimi olarak kullanılabilir. Bu durum bilginin bilgi içinde gizlendiği, steganografi gibi teknikler kullanarak gerçekleştirilmektedir.

2.2.6.3 Dünya'da Siber Terör

Gelişen teknoloji ile birlikte, terör yöntemleri de bu gelişen teknolojilere paralel olarak kabuk değiştirmekte ve dünya üzerindeki tüm ülkeleri bu yeni terör tipi, yani siber terör saldırıları tehdit etmektedir. 11 Eylül 2001 tarihinde ABD'de meydana gelen ve dünyayı etkileyen terör olayı, teröristlerin ve terör gruplarının internet ve teknoloji kullanarak sınır tanımayan bir şekilde eylemlerde bulunulabileceğini göstermiş ve tüm dünya ülkelerinin bu olaydan kendi kendilerine ders almalarını sağlamıştır.

Clarke ve diğerlerine göre (2001), şirketler siber güvenliklerinden daha çok kahveleri için para harcamaktadır. Fakat dijital Waterloo, elektronik Pearl Harbor ve Çernobil olarak nitelendirilen 9-11 olayları ile birlikte siber terörizme yönelik ilginin de arttığı söylenebilir. Ekim 2001'de FBI direktör yardımcısı Ronald Dick (2001), uçak korsanlarının net'i iyi, hem de çok iyi kullandığını belirtmiştir. Siber terörizm kavramı ile siber uzayı kullanan terörist kavramı arasındaki farklılığa literatürde dikkat çekilmektedir. Conway (2002), siber

terörizm sadece enerji, savunma gibi sistemlerin alt yapılarına yönelik bir hareket olarak görülüp değerlendirilmemelidir.

Siber alemin oluşturduğu tehlikenin boyutunu gören ülkeler ise, tehlike karşısında tedbirlerini almaya başlamışlardır. Aşağıda bilişim suçlarına ve siber terörizme yönelik kurulmuş merkez ve birimlerin listesi ülkelere göre yazılmıştır. Bu bürolar dünyanın konuya verdiği önemi de açıkça göstermektedir. Bu ülkelerdeki bazı merkezler ve birimler şunlardır:

Amerika:

Amerika Birleşik Devletleri'nde teknolojik suçlar ve siber terörizmle mücadele eden pek çok kuruluş ve bu kuruluşlara ait özel birimler bulunmaktadır.

1) FBI National Infrastructure Protection Center
2) FBI Computer Crime Squad
3) Information Technology Association of America
4) Trap and Trace Center Authority
5) Carnegie Mellon's Emergency Response Team
6) Commision of Critical Infrastructure Protection
7) CIA Information Warfare Center

Fransa:

1) Haberleşme Sistemleri Güvenligi Merkez Birimi (DCSSI)
2) Haberleşme Teknolojisi kullanılarak yapılan dolandırıcılıkların soruşturulması birimi (SEFTI)
3) Bilgisayar ortamında işlenen suçların bastırılması birimi (BCRCI)
4) Jandarma Genel Komutanlıgı Suç Araştırmaları Enstitüsü (IRCGN)
5) Fransız Istihbarat Örgütü (DST)
6) Iletişim ve Enformasyon ve Teknolojilerinin Kullanımı Suretiyle Işlenen Suçlarla Mücadele Bürosu

Ingiltere ve Hollanda: Cybercops

Irlanda : The Computer Crime Unit

Isviçre: Ulusal Posta ve Telekomünikasyon Ajansı

Kanada: CANCERT (Canadian Computer Emergency Response Team)

Singapur: Computer Emergency Response Team (SINGCERT)

Italya : Posta ve Iletişim Güvenligi Daire Başkanlığı (İstanbul Emniyet Müdürlüğü, 2002).

Diğer ülkelerde ve ülkemizde saldırıya uğrayan ve hack edilen kamuya ait bir çok web sitesi bulunmaktadır. Yine kamuya ait e-mail adresleri terör örgütleri tarafından yoğun bir şekilde e-mail bombardımanına maruz kalabilmekte ve sistem çökertilebilmektedir. Bu konu ile ilgili yaşanmış bazı örnek olaylar şöyle özetlenebilir:

Örnek Olay 1:

Körfez savaşı sırasında Hollanda'lı bir grup genç Pentagon bilgisayarına sızarak, ABD savaş operasyonlarıyla ilgili hassas bilgileri değiştirmiş ya da kopyalamışlardır. Savunma Bakanlığı, bu izinsiz sızmayı tespit edecek önlemlerin yetersizliği yüzünden "problemin boyutunu tespit etmekten acizdir". Bilgisayara giriş, internet dahil bazı networkler içinde gezinme suretiyle başarılabilmiştir (Carter, 1996).

Örnek Olay 2:

1996 yılının Eylül ayında yaşanan web sitesi'nin kırılması olayında kurumun gizli dosyalarına girilememiş olsa da, sitenin içinde yer alan tüm bilgilerin değiştirilmesi bile oldukça büyük bir etki meydana getirmiştir. CIA'ya telefon ederek bu olaydan haberdar olmalarını sağlayan ses, siteyi kıran kişiye aittir. Bu olaydan bir ay önce de ABD Adalet Bakanlığı'nın sitesine girilmiş ve siteye Adolf Hitler'in fotoğrafı yerleştirilmiştir (Topçuoğlu, 2001).

Siber terör eylemleri, tüm dünyada olduğu gibi ülkemizde de bir tehdit kaynağı olarak varolagelmektedir. Gelişmekte olan bir ülke konumunda bulunan Türkiye Cumhuriyeti'ne karşı siber terör saldırılarını incelemekte yarar

bulunmaktadır. Ülkemiz, tarih boyunca özellikle jeopolitik konumu gereği her zaman için çeşitli devletlerin ve terör örgütlerinin hedefi haline gelmiştir. Bu nedenle, ülkemize yönelik olarakta günümüz teknolojilerinden yararlanılarak siber saldırılar yapılma ihtimali ve terör örgütü faaliyetlerinin gerçekleştirilmesi her zaman mevcut bulunmaktadır. Terör örgütlerinin, iletişimlerini İnternet üzerinden gerçekleştirme gayretleri ve İnternet üzerinden propaganda faaliyetleri yürütmeleri de önem teşkil eden diğer bir husustur.

2.2.6.4. Ülkemizde Siber Terör

Günümüzde, terör örgütlerinin kendilerine destek veren dış merkezli bilgisayar sistemleri aracılığıyla, ülkemize yönelik siber saldırı hareketlerinde bulunabilecekleri göz ardı edilmemeli ve olası siber saldırılara karşı bu durum kurumlar koordinasyonunda her zaman yakından gözlemlenmeli ve siber saldırı acil eylem planları ile hazırlıklı bulunmalıdır. Unutulmamalıdır ki, siber terörizme karşı hazırlıksız bir şekilde bulunmak günlük hayatın akışını da derinden felce uğratabileceği gibi, ülke güvenliğini ciddi bir şekilde tehdit edebilecektir.

Ülkemiz aleyhinde faaliyet gösteren zararlı internet sitesi sayısı yaklaşık 8000 civarındadır. Bu sitelerden 150 tanesini aktif olarak faaliyette olup, her gün ortalama 500-1000 bin kişi ziyaret etmektedir. Genelde com, org, net uzantılı olan bu siteler Amerika, Almanya, Hollanda ve diğer Batı Avrupa ülkeleri üzerinden yayın yapmaktadırlar.

Türkiye'de de terör örgütleri İnternet ortamını öncelikle propaganda ve eğitim amaçlı olarak kullanmaktadırlar. Bölücü örgütlerin bu alanda kullandıkları en önemli platform İnternet'tir. Yüzlerce web sitesinden yoğun bir propaganda faaliyeti yürütmektedir. Ülkemizde faaliyet yürüten terör örgütlerinde olduğu gibi uluslararası faaliyet yürüten terör örgütleri de İnternet ortamını etkin olarak kullanmaktadırlar (Özcan, 2003).

Aşağıda bu konuyla ilgili bazı örnek olaylar verilmiştir:

Örnek Olay 1:

2000 yılında Elazığ Emniyet Müdürlüğü İnternet E-mail servisine, *Elazığ Öğretmenevi'ne bomba koyacağım* şeklinde bir e-mail gelmesi üzerine, gelen e-mail adresi incelenerek kişinin ev adresi tespit edilmiş ve Terörle Mücadele Şube Müdürlüğü ekipleri tarafından şahıs yakalanarak, göz altına alınmış ve adli birimlere sevk edilmiştir. (Elazığ Emniyet Müdürlüğü, 2000).

Örnek Olay 2:

Istanbul Emniyeti tarafından 1999 yılında bir terör örgütüne yönelik olarak düzenlenen operasyonda 33 örgüt mensubu, hedef şahıslara ait fotoğraflar ile birlikte yakalanarak gözaltına alınmıştır. Şahısların sorgulamalarında web sitesinde "Örgüt Hedef Listesi" başlığı altında ele geçen fotografları yayınladıkları tespit edilmiştir. Konuya ilişkin olarak yapılan araştırmada yasa dışı örgütün, web sitesinde oluşturdugu hedef listesinden başka "bomba yapımı ve bombalama, silah atış bilgisi, polis takibi ve tarassut, polis sorgusu, kırsalda yön tayini ve ilkyardım" konularında örgüt mensuplarını bilgilendirdiği ortaya çıkarılmıştır (Özcan, 2003).

Örnek Olay 3:

1998 yılında Denizli'de bir terör örgütüne yönelik olarak yapılan operasyonlarda yakalanan teröristlerin ifadelerinde; komşu bir ülkede bulunan örgüt evinde eğitildikleri, kampta askeri ve siyasi eğitimin yanında, uydu telefonu internet üzerinden haberleşme ve şifreli görüşmeler konusunda eğitildikleri, örgütün üst düzey yöneticileri ile uydu telefonlarıyla haberleştikleri mesaj alışverişlerini internet aracılıyla yaptıkları, cihazların şarz işlemlerini güneş ışığından enerji üreten solar sistemi ile sağladıkları anlaşılmıştır (Yamaç, 2003).

Örnek olaylarda da görüldüğü gibi, siber terör unsurları gerek bireysel, gerekse organize gruplar tarafından ülkenin güvenliğine yönelik olarak tehdit unsuru olarak kendini gösterebilmektedir. Bu nedenle, günümüzde ülkemizde de artma eğiliminde bulunan olası siber terör faaliyetlerine karşı, gözlemleyici ve koruyucu unsurların güçlendirilmeye çalışılmasına öncelik verilmelidir.

Ülkemizde de, diğer ülkelerde olduğu gibi saldırıya uğrayan ve hack edilen kamuya ait bir çok web sitesi bulunmaktadır. Yine kamuya ait e-mail adresleri terör örgütleri tarafından yoğun bir şekilde e-mail bombardımanına maruz kalabilmekte ve sistem çökertilebilmektedir. Ülkemizdeki kamu ve özel kurum ve kuruluşları acaba böyle bir siber terörzme karşı hazırlıklı bir durumda mıdır? Sistemlerin güvenliği yönünde, kurumların sistem güvenliklerinin gözden geçirilerek zayıf yönlerin ve açıkların organizeli ve koordineli bir şekilde yeniden kapatılmaya çalışılmasına öncelik verilmelidir.

Terör örgütleri Türkiye'ye yönelik teknolojik eylem hazırlığında bulunmaktadırlar. Terör örgütleri; link hatlarına, bilgi işlem ve veri merkezlerine, bakanlıklara, PTT-Telekom, polis ve askeri birimlerin sistemlerine sanal saldırıda bulunmak için uğraş vermektedirler (Yamaç, 2003).

Bu bilgiler ışığında, küreselleşen dünyada jeopolitik konumumuz da dikkate alındığında, ivedilikle siber güvenlik politikaları ve siber terör acil eylem planları oluşturulması ve siber teröre karşı güvenliği ve iletişimi sağlayan birimler başta olmak üzere tüm ülke de bilinçlendirme eğitimleri düzenlenerek toplumsal bilincin arttırılması, gerekliliği ortaya çıkmaktadır.

Ülkemizde ve tüm dünyada gerek kamu alanında, gerekse özel sektörde yaygın olarak İnternet hizmeti verilen tüm insanların erişimine açık olan internet kafe işletmeleri, siber terör saldırılarında bulunmak isteyenler için ideal mekanlar durumundadır. Ülkemizde ve tüm dünyada genel olarak bu mekanlarda bire bir log kayıtlarının tutulmaması veya şahısların kimlik tespiti istenmemesi nedeniyle, bu mekanlardan suç işlenmesi her zaman mümkün olabilmektedir. Görevliler, bir suç aşamasında internet kafeyi çabaları sonucu tespit etseler bile, bu mekanları suç kapsamında kullananlar çoktan başka bir mekanın yolunu tuttuklarından faillere ulaşmak çoğu zaman mümkün olmamaktadır. Siber terör saldırıları ve internet kafeler arasında her zaman yoğun bir ilişki bulunmaktadır.

Ülkemizde ve tüm dünya'da siber terör saldırılarının çoğunlukla internet üzerinden ve e-mail bombardımanı ile yapıldığı göz önüne alındığında, bu durum internet hizmeti veren internet kafelerin de yukarıda dile getirilen siber terör hareketlerine zemin olabileceği ihtimalini akla getirmektedir. Herkesin kullanımına açık olan ve kötü amaçla kullanıma müsait mekan olan internet kafeler üzerinden kolaylıkla art niyetli kişiler faydalanabilmekte ve malesef kullanıcılar ile ilgili herhangi bir kayıt tutulmadığından dolayı şüphelilere ulaşılamamaktadır. Tüm bu özelliklerden domayı, siber terör ve internet kafeler arasındaki yoğun ilişkiyi ele almakta büyük yarar bulunmaktadır.

2.2.6.5. Siber Terör ve İnternet Kafeler

Ülkemizde, çağımızın en son bilişim mucizesi olan İnternet'in özellikle 1995 yılından sonra öncelikle kamu ve özel sektörde yaygın olarak kullanılmaya başlamasının ardından, sosyal hayatta İnternet hizmetlerinin verildiği yeni bir sektör ortaya çıkmıştır. Bu sektör, ülkenin ekonomik durumu da göz önüne alındığında sayıları hızla artan ve neredeyse her sokak başında hizmete giren internet kafeler biçiminde toplumsal hayatta yerini almıştır.

Eylül 2008 tarihi itibariyle, yurt genelinde yaklaşık 30000 adet internet kafe bulunmaktadır. Ülkemizde bilgisayarlaşma ve İnternet'e bağlanma oranının, diğer ülkelere özellikle AB üyesi ülkelere göre düşük olduğu dikkate alındığında, bireylerin oldukça yoğun olarak internet kafelerden yararlandıkları görülmektedir. Bu nedenle, siber terör eylemlerine karşı özellikle rahat hareket etme özelliğinden dolayı bu mekanların da kullanılabileceği düşünülmelidir. İnternet kafeler ve oyun yerlerine yönelik olarak İçişleri Bakanlığı genelge ile çeşitli düzenlemeler getirmektedir. Bu düzenlemelerden bazıları;

- Devletin ülkesi ve milleti ile bölünmez bütünlüğünü zedeleyici ve anayasal düzeni yıkma amacına yönelik kurulan sitelere erişimin sağlanması,
- İnternet vasıtasıyla diğer bilgisayarlara veya bilgisayar ağlarına kasten zarar verilmesi şeklindedir.

İnternet kafelerle ilgili olarak tüm yurt çapında yapılan yüksek lisans çalışması kapsamında yapılan araştırmada; müşteriler, emniyet yetkilileri ve işletmecilerin İnternet ortamını kullanırken karşılaştıkları sorunlar hakkındaki görüşleri alınmıştır (Gümüş, 2003).

Elde edilen sonuç Tablo:1'de görülmektedir.

Tablo 1: Internet Ortamını Kullanırken Karşılaşılan Sorunlar Hakkında Grupların Görüşleri

Karşılaşılan sorunlar	Müşteriler		Emniyet Yetkilileri		İşletmeciler	
	f	%	f	%	f	%
Bilişim suçları	288	7,90	195	20,68	59	7,48
Hız/Kapasite	922	25,32	81	8,59	230	29,16
Gizlilik	320	8,79	74	7,85	35	4,44
Güvenlik	515	14,15	147	15,59	110	13,94
Bilginin doğruluğu	358	9,84	57	6,05	67	8,49
Sansür	337	9,26	47	4,99	36	4,56
Pornografik yayınlar	683	18,75	292	30,96	190	24,08
Yayın hakları	181	4,96	39	4,13	42	5,32
Diğer	38	1,03	11	1,16	20	2,53
Toplam	3642*	100,0	943*	100,0	789*	100,0

* Araştırmaya katılanlar bu soruda en fazla 3 seçenek işaretlemişlerdir.

Tablo 1'de de görüldüğü gibi özellikle emniyet yetkilileri, bilişim suçları konusunda ağırlıklı olarak görüş belirtmişlerdir. Güvenlik faktörü de, önem sıralamasında her üç grup tarafından üçüncü sırada yer almıştır. Diğer önemli bir sorun, özellikle gençlerin ve çocukların istismar edildiği hızla artma trendinde olan pornografik yayınlardır.

Şu anki mevcut yapılanma itibariyle, kişiye ve bilgisayara ait herhangi bir bilgi kaydının tutulmadığı suç işlemek için ideal mekanlar konumunda bulunan İnternet kafeler üzerinden gerçekleşmesi mümkün olan siber terör eylemlerinin tespiti nasıl sağlanabilecektir? Bu mekanların, her an için ülke güvenliğini derinden tehdit eden bir araç olarak kullanılabileceği gerçeği göz ardı

edilmemelidir. Çoğu ülkede yürürlükte olan bilişim suçları ile ilgili yasa, ülkemizde de hızlı bir şekilde kanunlaştırılmalı ve kolluk ile beraber Telekom yetkililerinin etkili çalışabilmesine ve internet'in kötü kullanımından dolayı cezai müeyyidelerin gerçekleştirilebilmesine zemin hazırlanmalıdır.

Saldırının yapıldığı bilgisayara ulaşan polis bu bilgisayarın bir internet kafe'de oldugunu tespit etmesi durumunda ne olacağı düşünülmelidir. Kim sorumlu? Internet kafe sahibi mi yoksa kim olduğu bilinmeyen meçhul kullanıcı mı? Veya failin bilgisayarına şehiriçi telefon kulubesinden bağlandığını ve saldırıları buradan gerçekleştirdigini düşünelim. Bu durumlarda güvenlik güçlerinin faili tespit etmesi mümkün olmayacaktır (Özcan ve Bal, 2001).

İnternet kafelerde siber suçların işlenmesini engellemek için alınabilecek bazı tedbirler aşağıya çıkarılmıştır (Elazığ Emniyet Müdürlüğü, 2002).

1. Günümüzde İnternet, suç ortamı özelliği taşıması nedeniyle, özellikle de devlete karşı bölücü ve yıkıcı faaliyetlerin izlenmesi açısından mutlak suretle internet kafelerde kurulacak olan yönlendirici bilgisayar (**Server**) vasıtasıyla; emniyet ve jandarma birimlerince kanunun tanıyacağı yetki ile, gerekli teknik altyapı sağlanarak bu mekanlarda gerçekleştirilen işlemlerin gerektiğinde takibinin yapılması sağlanmalıdır.
2. İnternet kafe-oyun yeri içerisinde bilgisayarlar numaralandırılmalıdır. Ayrıca bu mekanlara gelen müşterilerin, **TC KİMLİK NUMARALARI** alınarak bu şekliyle bilgisayar kullanmaları sağlanmalıdır.
3. Hangi Web sitelerinin *devletin ülkesi ve milleti ile bölünmez bütünlüğünü zedeleyici ve anayasal düzeni yıkma amacına yönelik kurulan sitelerden olduğu* belirlenmeli ve bu sitelerin adresleri mutlak suretle İnternet Kafe İşletmelerine kolluk tarafından tebliğ ettirilmelidir.
4. İşletmecilerden, İnternet üzerinden yayın yapan web sitelerinde konusu suç teşkil eden yayınlara girilmemesi için (porno, satanizm, kumar, terörizm vs.) bu mekanlardaki bilgisayarların bu tür yayınları yapan sitelere kapatılması yönünde gerekli önlemlerin alınması amacıyla lisanslı güvenlik yazılımı bulundurmaları sağlanmalıdır.
5. İşletmeler; bilişim suçları, devlet güvenliği vb. türdeki girişimlere duyarsız

kaldıklarında kesinlikle cezalandırılmalıdır. Öncelikli olarak, İnternet kafe açmak isteyenlere yönelik olarak, işletme açma esasları belirlenirken mutlak suretle internet kafe işletmecisinin, belirlenecek eğitim merkezlerinden **"İnternet kafe- oyun yeri işletme sertifikası"** alması koşulu getirilmelidir. Şayet, açılan **İnternet kafe- Oyun Yeri** mesul müdür tarafından işletilecekse, mesul müdürün en az 2 yıllık (elektrik, elektronik, bilgisayar vb.) MYO diploması olması şartı sağlanmalıdır.

6. İnternet kafe-oyun yerlerine yönelik olarak, her vilayetin Türk Telekom, servis sağlayıcı firmalar ve kolluk yetkilileri; koordine halinde İnternet'in özellikle biser terör amaçlı kullanımını önlemek amacıyla komisyon kurmaları sağlanmalıdır.
7. İnternet kafelerin standartları belirlenerek etkili ve düzenli bir şekilde denetlenmesi sağlanmalıdır.
8. İnternet kafeler üzerinden siber terör faaliyetlerinin yürütülmesine karşı olarak, güvenliği ve iletişimi sağlayan birimler başta olmak, internet kafe işletmecileri ve vatandaşlara yönelik olarak tüm ülke çapında bilinçlendirme eğitimleri düzenlenerek toplumsal bilincin arttırılması sağlanmalıdır.

2.2.6.6. Siber Terör ve Emniyet Teşkilatı

Emniyet Teşkilatı bünyesinde bilişim hizmetleri 1982 yılında, Bilgi Işlem Daire Başkanlığı'nın kurulmasıyla atılmıştır. Sanal alemdeki suçları takip etmek için Emniyet Teşkilatı içinde nasıl bir yapılanmaya gidileceği konusunda çalışmalar yapmak üzere 1997 yılında Bilişim Suçları Bürosu kurulmuştur. 2001 yılında bu büro İnternet ve Bilişim Suçları Şube Müdürlüğü olarak değiştirilmiştir. Şube, Bilişim Suçları konusundaki gelişmeleri her yönüyle takip etmekte, bilgisayar sistemlerine izinsiz giriş ve zarar yöntemlerine karşı alınacak tedbirleri araştırmakta, bilişim suçları konusunda yetiştirilecek personelin eğitim standartlarını tespit etmekte ve bilişim suçları konusunda çalışma yapan yerli ve yabancı kuruluşlarla irtibata geçmektedir. 2002 yılında ise, tüm taşra teşkilatında Bilgi İşlem Şube Müdürlükleri bünyesinde İnternet ve Bilişim Suçları Büro Amirlikleri kurulmuştur. 2008 yılı itibariyle, taşra teşkilatında Bilgi İşlem Şube Müdürlükleri bünyesinde İnternet ve Bilişim Suçları alanında bir birim bulunmamaktadır. Taşra teşkilatında, Bilişim Suçları alanında KOM Şube Müdürlükleri bünyesinde Bilişim Suçları Büro Amirlikleri hizmet vermektedir.

İnternet hizmetleri konusunda teknik alt yapının hazırlanması ve Emniyet İnternet sayfasına konulması gerekli bilgilerin belirlenmesi ile “Bilgisayar Suçları ve Bilgi Güvenliği” konularında araştırma yapılması ve bu konudaki yasal boşlukların doldurulması amacıyla; Asayiş, Bilgi İşlem, İnterpol, İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele, Terörle Mücadele ve Harekat Daire Başkanlıkları ve Hukuk Müşavirliğinden konu ile ilgili birer personelden oluşan “Bilgisayar Suçları ve Bilgi Güvenliği Kurulu” Emniyet Genel Müdürü onayı ile 18.04.1998 tarihinde kurulmuştur.

Ayrıca; bilişim suçları, siber terör vb. alanlarda çalışmalar yapmak üzere merkezde Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlar Daire Başkanlığı’na bağlı TADOC Bilişim Suçları Araştırma Merkezi (Ankara) ve 16 İl Emniyet Müdürlüğü bünyesinde “adli bilişim merkezi” kurulmuştur. Ayrıca, taşrada Kaçakçılık ve Organize Suçlar Şube Müdürlüğü bünyesinde bilişim suçları büro amirlikleri kurulmuştur. Aynı idari yapılanma, Asayiş Daire Başkanlığı bünyesinde de sürdürülmektedir.

Birçok terör örgütü internet üzerinden propaganda başta olmak üzere, patlayıcı madde yapımı, örgüt elemanlarının eğitilmesi gibi birçok illegal faaliyet yürütülmektedir. Nitekim Emniyet Teşkilatı’nın çeşitli terör örgütüleriyle mücadelesindeki başarının temelinde bu örgütün bilgisayarlarında yapılan araştırmalar sonucu elde edilen veriler bulunmaktadır. Benzer şekilde uyuşturucu ticareti yapan ve bilgi teknolojilerini kullanan bir şebekenin iletişim ağı bir bilgisayarın içindeki bilgiler sayesinde ortaya çıkarılabilecektir (Özcan, 2003).

Günümüzde, bilgisayarların ve networklerin suç işlemek için bir araç olarak kullanılması nedeniyle Emniyet Teşkilatı da, bu yeni suç tipine ve siber terör faaliyetlerine karşı yoğun olarak çalışmalar yapmaktadır. Siber suçlara karşı alınabilecek önlemler şöyle sıralanabilir.

2.2.6.7. Siber Suçlara Karşı Önlemler

İnternet, geleneksel suçların işlenmesinde yeni bir araç haline gelmesinin yanısıra farklı suç tiplerinin ortaya çıkmasına neden olmuştur. Bu nedenle pek çok ülke mevzuatlarında düzenleme yaparak ya da yeni yasalar çıkarmak zorunda kalmıştır ve bu suçlarla mücadele edecek özel birimler oluşturmaktadır.

Medyanın, finans kuruluşlarının, kamu hizmetlerinin ve iletişimin neredeyse tümüyle bilgisayarlı ortamda gerçekleştirildiği ülkeler giderek artan biçimde siber tehdit altındadır. Bir ülkenin bilişim altyapısı ele geçirildiğinde ya da çalışamaz hale getirildiğinde, ülkenin yaşamsal faaliyetleri durdurulmuş olacaktır. Böylesine büyük çaplı bir saldırı, başarılabildiği takdirde, ülkenin haritadan silinmesine kadar giden bir çöküşün başlangıcı olabilir. Bu nedenle günümüzde ülkeler, mutlaka bu siber tehditlere karşı kendi güvenliklerini sağlamak için çok daha yoğun önlem almak zorunda kalmaktadırlar.

Avrupa Birliği, 2000 yılı içerisinde siber suçlar üzerinde yoğun bir çalışma yapmıştır ve bu çalışmanın sonucunda 8 Ocak 2001 tarihli, bilişim suçları konusunda ortak mevzuat yaratmak amacıyla “İnternet ve Bilgisayar Suçları ile İlgili Sözleşme Taslağı” hazırlamıştır (Küçükgörkey, 2002).

5237 sayılı Türk Ceza Kanunu’nda (TCK) bilişim suçları, “bilişim sistemine girme” (madde 243) “sistemi engelleme, bozma, verileri yok etme veya değiştirme” (madde 244), “banka veya kredi kartlarının kötüye kullanılması” (madde 245), “tüzel kişiler hakkında güvenlik tedbiri uygulanması” (madde 246) madde başlıkları altında düzenlenmiştir. Bilişim suçları sürekli değişkenlik gösteren bir alan olduğu için, zaman içerisinde meydana gelecek yasal boşlukların da, mevzuat düzenlenerek giderilmesi gerekmektedir. Ayrıca, bilişim suçları ile ilgili hükümlerin başka ülkelerde de uygulanması için, yasalar hazırlanırken uluslararası işbirliği ortamı tesis edilmesi şarttır.

Akgül (2002), bilişim suçları (cyber crime) ve delillerin toplanması konularında on-line işbirliği ağı kurulması gerektiğini, bir e-mail’in nereden geldiğinin bilinmesinin zor olduğunu, pek çok yasada değişiklik yapılması gerektiğini belirtmiştir.

Üniversiteler bünyesinde, bilişim suçları araştırma enstitüleri kurulmalıdır. Ayrıca, tüm kamu kurum ve kuruluşlarının internet güvenliği konusunda bir merkezden yürütülmek üzere etkin çalışmalar yürütülmelidir. İnterpol bünyesinde, siber terörizm ile mücadele konusunda birim kurulmalı ve etkinliği artırılmalıdır. Ayrıca, bilişim suçları ve siber terör kapsamında ülkemize ve kurumlara yönelik olarak risk-suç haritası çıkarılmalıdır. İnternet kafeler ve ISS'lerin kuruluşu hakkında yasal bir düzenleme yapılmalıdır. Ayrıca, siber suçlara karşı tüm özel sektör ve kamu kurum ve kuruluşlarının ve bireylerin internet ve network güvenliği konusunda teknik önlemler alması, bu konuda eğitim faaliyetleri düzenlenmesi siber terörden en az etkilenmeyi sağlayacaktır.

Ülkedeki, özellikle güvenlik ve iletişim kurumlarının siber terör eylemlerine karşı gerekli önlemleri almaya ve diğer ülkeler ile işbirliği halinde olmaya çalıştığı kadar, bireylerin de bu tür siber terör eylemlerine karşı bilinçli olmaları veya bilinçli olmaları için eğitim faaliyetleri düzenlenmesi o ülkenin genel güvenliğine olumlu katkıda bulunacak ve ulusal savunma yapısını güçlendirecektir.

Ülkemizde, yoğun olarak internet'e ulaşımın internet kafeler üzerinden gerçekleştiği göz önüne alındığında çeşitli olası siber terör eylemlerinin ve bu mekanlar üzerinden rahatça gerçekleştirilileceği, aynı zamanda fail veya faillerin bu mekanlarda herhangi bir şekilde kaydı tutulmaması nedeniyle neredeyse yakalanmasının imkansız olduğu gerçeği dikkate alınarak, kanun ile bu mekanlar üzerinde etkili denetim gerçekleştirebilmesi sağlanmalıdır.

Elazığ Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü, Bilişim Suçları Büro Amirliği'nce içinde bulunulan bilgi ve teknoloji çağında sayıları hızla artan ve özellikle de çoğunluk olarak gençlerin faydalandığı Elazığ'da faaliyet gösteren internet kafe işletmecilerine yönelik olarak polis merkezlerince tebligat yapılmış ve İnternet'te kişi ve toplum haklarının yanı sıra, devlet güvenliği ihlallerinin ve bilişim suçlarının önüne geçilebilmesi, ayrıca İnternet gibi güçlü bir bilgi ortamında bilgiden, zararlarından korunarak yararlanılması ve bu mekanların vatandaşlara genelgeler doğrultusunda daha iyi hizmet

verebilmelerini sağlamak ve bu şekliyle daha sağlıklı, sorunsuz, eğitim amaçlı bir yapıya kavuşturulmalarını temin ve çeşitli konularda bilgilendirme amacıyla eğitim toplantısı yapılmasının yararlı olacağından hareketle, bir eğitim toplantısı tertip edilmiştir (Elazığ Emniyet Müdürlüğü, 2002).

2.2.6.8. Organize Suçlar

Tüm dünyada olduğu gibi ülkemizde de organize suç örgütleri, yöntem değiştirerek başta İnternet ortamı olmak üzere iletişim teknolojileri üzerinden faaliyetlerini yürütmektedirler. Suç örgütleri, günümüzde genellikle bilinçsiz kullanıcı kesimini hedef kitle yaparak çıkar elde etmeye çalışmaktadırlar.

Organize suç örgütleri, iletişim teknolojilerindeki bu gelişmelerden günümüzde azami düzeyde faydalanarak eylemlerini büyük ölçüde değiştirmişlerdir. Kumar, kredi kartları, ATM, pornografi, şifreli yayınlar vb. bir çok alanda bilişim suçları ulusal ve uluslar arası bağlamda meydana gelebilmektedir.

Dünyada, organize suç örgütleri tarafından ATM'lerdeki şifrelerin ve bilgilerin elektronik cihazlarla elde edilerek yeni kart çıkarılması yoluyla hesapların boşaltılmasının yanı sıra internet bankacılığı ve dijital transfer ile kara para aklama yoluna gidildiğine dair örnek olaylar bulunmaktadır. Organize suç örgütleri, yurt içi ve uluslar arası bağlantılarında internet tabanlı elektronik iletişim ortamlarında yapılan şifreli görüşmeleri kullanmaktadırlar. Bu suretle, ileride aleyhlerinde delil olarak kullanılabilecek dinleme çalışmalarından kurtulmayı amaçlamakta ve interneti güvenli bir iletişim aracı olarak görmektedirler.

Bir Rumen komiser ile mühendisin elebaşı olduğu 'uluslararası bankamatik çetesinin ATM'nin kart girişi sökülüp mikro kamera ve okuyucu yerleştirilmiş lamba düzeneği takılarak karttaki bilgilerin çetecinin laptopuna aktarıldığı uluslararası organize suç olayında şifrenin kamera görüntüsüyle öğrenilip 'kopya kart' üretildiği anlaşılmıştır. Dubai, Tunus ve Sudan'da, ATM'lerden trilyonlar dolandıran 'Rumen çetesi'ni İstanbul polisi çökertmiştir.

Çetenin elebaşı Florin Chırıca'nın Rumen emniyetinden ayrıldığı tespit edilmiştir. İstanbul polisi tarafından, 4 reader kopyalama cihazı, encoder, laptop, 2 ATM kartı baskı cihazı, dijital kamera ele geçirilmiştir (Akşam, 2004).

Dünya üzerindeki çeşitli mafya örgütleri de bilişim ortamını kendi çıkarları doğrultusunda etkin şekilde kullanmaktadırlar. Örnek olarak; organize suç grupları hacker'lar ile işbirliği yaparak, e-ticaret şirketleri ve bankaların bilgisayar sistemlerine girerek müşterilerin kredi kartı numaralarını ve banka hesaplarını elde ettikten sonra bu bilgileri açıklamamak için yüklü miktarda haraç talep etmektedirler. Siber mafyanın yıllık haraç tutarı 700 milyon dolar civarındadır (Özcan, 2003). Bu miktar hızlı bir şekilde artmaktadır. Organize suç örgütleri iletişimlerini ve anlaşmalarını internet üzerinden yaptıkları için yakalanma olasılıkları da azdır.

Dünya üzerinde dolaşan günlük para miktarı 2 trilyon dolar iken, teknolojinin hızı ile bu paranın hızla sanal âleme yönelmesi siber mafyanın iştahını kabartmaktadır. Siber mafya, ülkelerdeki bankaların şubelerine düzenlediği siber soygunlar sonucu milyon dolarları bulan meblağları ele geçirerek kendi sahte hesaplarına yatırmaktadırlar.

Günümüzde ülkeler, ayrıca ulusal güvenlikleri için hacker yetiştirmekte ve organize örgütler de interneti dünyanın farklı köşelerinde uyuşturucu kaçakçılığı için kullanmaktadırlar. Yine insan ticareti, çocuk pornografisi, tarihi eser kaçakçılığı gibi suçlar artık internet üzerinden yapılma ve yapılan online satışların belli bir kısmı kaçak kredi kartı kullanımları yüzünden kaybedilmektedir. Çünkü sanal alemde risk sıfırın altına kadar inebilmektedir.

2.2.6.9. Elektronik Casusluk

Birbirlerinin nefes alışlarını dahi bilmek isteyen ülkeler, başta ABD gibi güçler öncülüğünde sistemler geliştirmektedirler. Bu sistemlerin başında gelen ve NSA (Amerikan Ulusal Güvenlik Ajansı) tarafından geliştirilen küresel "**Elektronik Casusluk"** sistemi, kod adıyla ECHELON'dan ilk kez 1980'lerde söz edilmeye başlanmıştır. ECHELON sistemi, temel olarak dünyanın çeşitli

yerlerinde konuşlandırılmış yer istasyonları vasıtasıyla bütün uydu, mikrodalga, cep telefonu veya fiber optik telefon haberleşmelerini izleyerek bunları NSA'nın çok güçlü bilgisayar sistemine aktarmaktadır.

Koch ve Sperber'in (1996), "Bilgi Mafyası" kitabında dijital bir dünyada geçen gerçek bir polisiye öyküleri bulunmakta ve ihanet, cinayet, bilgisayar casusluğu, gizli servisler, para ve güç konuları yer almaktadır. Kitapta, ABD'nin NSA (Ulusal Güvenlik Dairesi) ile İsrail'in MOSSAD'ı, en üst düzeyde bazı hükümet görevlilerinin yardımlarından yararlanarak küçük bir yazılım firmasından "PROMIS" adındaki bilgisayar programını çalmaları anlatılmaktadır. "PROMIS" adındaki yazılım programı bankaların, holdinglerin ve devlet dairelerinin veri bankalarına fark edilmeden girme imkanı sunmaktadır.

Çok değil yalnızca yirmi yıl öncesine kadar veri suçları, bilimkurgu edebiyatının konusuydu. Oysa bugün, bilgisayar sistemlerine olan bağımlılığımız çok sayıda "hacker", "phreaker" ve "virüs yazarı"nın ortaya çıkışına neden olmuştur. Zayıf kişiliklerini gizleyen, iddialı takma adlar kullanan yirmi yaşın altındaki "hacker"lar epeydir CIA, Pentagon, NASA ve NATO'daki "güvenli" bilgisayar sistemlerine girmektedir. Veri suçları ve Bilgisayar Yeraltı Dünyasını anlatan "Sıfıra Doğru" kitabında, veri suçlarının, bedava telefon kullanımı gibi masum bir girişimden casusluğa ve Amarikan-İngiliz bankalarına her yıl iki milyar paunda mal olan soygunlara kadar geniş bir alan yer almaktadır. Kitapta ayrıca, her geçen gün yeni bir tanesiyle karşı karşıya kalınan bilgisayar virüslerinin ne oldukları, nasıl çalıştıkları ve onları kimlerin niçin ürettikleri ele alınmaktadır (Mungo ve Clough, 2002).

2.2.7. Bilişim Yoluyla İşlenen Asayiş Suçları

Türk Ceza Kanunu'nun 10. Bölümünde "Bilişim Alanında Suçlar" başlığı altında müstakilen düzenlenen bilişim suçlarının haricinde kalan pek çok suç türü, gelişen internet ve bilişim teknolojilerinin parelelinde sanal ortamda da işlenebilmektedir. Örneğin, terör örgütlerine militan kazandırmak ya da bu örgütlere finansman sağlayabilmek için web siteleri açılabilmekte, telif hakları ihlal edilebilmekte, İnternet ortamında fuhşa aracılık ve yer teminine yönelik

faaliyetlerde bulunulabilmekte, hazırlanan web siteleri ile kumar ve yasa dışı bahis oynattırılabilmekte, çocuk pornografisi ve istismarı suçları işlenebilmekte, sanal ortamda tehdit, hakaret hatta dolandırıcılık fiilleriyle karşılaşılmaktadır. Buna benzer çok sayıda örnek verebilmek mümkündür. Özetle, kanunda müstakil bilişim suçu olarak sayılan fiillerin haricindeki pek çok konusu suç teşkil eden fiil bilişim yoluyla işlenebilmektedir. Bu nedenle, bu fiillerin takibi ilgili birimlerce yapılmaktadır. Yani terör örgütlerine ait web siteleri ve bu örgütlerin internet ortamındaki diğer faaliyetlerini Emniyet Teşkilatı'nın terörle mücadele birimleri, internet ortamında ve diğer bilişim teknolojileri kullanılarak yapılan telif hakları ihlalleriyle ilgili tahkikatları Emniyet Teşkilatı'nın güvenlik birimleri ve asayiş suçlarının soruşturulmasını da Emniyet Teşkilatı'nın asayiş birimleri yapmaktadır.

Kısacası, kontür ve kredi kartı dolandırıcılığı, sanal ortamda dolandırıcılık, fuhuş, kumar, tehdit ve hakaret suçları, şantaj ve çocuk pornografisi bilişim yoluyla işlenen asayiş suçlarına örnek olarak verilebilir. Burada, çocuk pornografisi konusu ele alınmıştır.

Çocuk Pornografisi:

Ülkemizde nadiren de olsa çocuk pornografisi olayları yaşanmaktadır. Bilişim suçları kapsamında da, bu konuyla ilgili etkili çalışmalar yapılması gerekmektedir. Emniyet Genel Müdürlüğü Asayiş Daire Başkanlığı, çocuk pornografisi konusunda ve bilişim yoluyla işlenen asayiş suçları konularında yoğun faaliyetler yapmakta ve bu konuda eğitimler düzenlemektedir.

26-28 Mart 2001 tarihleri arasında, aralarında ülkemizinde bulunduğu çeşitli ülkelerin katılımıyla İsveç'in Stockholm kentinde "Adli bakımdan İnternet'te çocuk pornografisiyle mücadele" konulu seminer düzenlenmiştir Seminerde; çocuk pornografisi çeşitli yönleriyle ele alınmış, çocuk pornografisine karşı alınacak tedbirlerin yanı sıra, ülkelerde İnternet ortamında çocuk pornografisiyle ilgili yaşanan örnek olaylar aktarılmıştır. Seminerde ayrıca, ülkelerin bu konuda mutlaka koordineli bir şekilde çalışmalar yapmaları gerekliliği sonucuna varılmıştır (Dokurer ve Kızılsu, 2001).

Avrupa Birliği'de (AB), İnternet sitelerinde çocuk pornosuyla mücadele için özel polis birimleri kurmayı düşünmektedir. Avrupa Parlamentosu'na sunulan rapor ve buna bağlı tavsiye kararında, AB ülkeleri içinde İnternet sitelerindeki çocuk pornosuna ilişkin yayınlarla mücadele için özel polis birimlerinin oluşturulmasının gerekli olduğu belirtilmiştir. AB ülkelerinde oluşturulacak özel polis birimlerinin kendi aralarında etkin bir biçimde işbirliği yapmaları gerektiği savunulan raporda, İnternet kullanıcılarının da polisle işbirliği yapmaları çağrısında bulunulmaktadır (Akşam, 2000).

2.2.8. Bilişim Suçlarında Emniyet Teşkilatı'nda İdari Yapılanma

Bilişim suçlarında gecikmeden yol alınması ve izlenecek stratejilerin belirlenmesi amacıyla Emniyet Teşkilatı'nda 1997 yılından başlanarak, günümüze kadar çeşitli kurullar oluşturulmuş ve idari yapılanmaya gidilmiştir. Bunlardan bazıları şu şekildedir:

Bilgisayar Suçları ve Bilgi Güvenliği Kurulu

"Bilgisayar Suçları ve Bilgi Güvenliği" konularında araştırma yapılması ve bu konudaki yasal boşlukların doldurulması amacıyla; Asayiş, Bilgi İşlem, İnterpol, İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele, Terörle Mücadele ve Harekat Daire Başkanlıkları ve Hukuk Müşavirliğinden konu ile ilgili birer personelden oluşacak Bilgisayar Suçları ve Bilgi Güvenliği Kurulu Emniyet Genel Müdürü onayı ile 18.04.1998 tarihinde kurulmuştur.

Bilgisayar Suçları Çalışma Grubu

Bilgisayar Suçları ve Bilgi Güvenliği Kurulu geleceğin en önemli suç türü olması beklenen Bilgisayar Suçları'nın önemine binaen gerek görülen durumlurda Kurul temsilcilerinden birkaçının görevlendirilmesiyle alt çalışma grupları oluşturmaktadır. Çalışma grubu ilk defa 17-21.05.1999 tarihleri arasında Bilgi İşlem Daire Başkanlığı bünyesinde toplanmış ve çalışma sonrası "Bilişim Suçları Çalışma Grubu Raporu" hazırlanmıştır. Raporda Bilgisayar Suçlarının Tasnifi, Daire Başkanlıklarının görevleri ve Bilgisayar Suçları konusunda olay yerinde yapılması gerekenler belirtilmiştir.

Bilişim Suçlarıyla Mücadelede Daire Başkanlıkları ve TADOC

Emniyet Teşkilatında; Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, Kriminal Polis Laboratuarları, İstihbarat, Asayiş, Bilgi İşlem, Güvenlik, İnterpol ve Sirene, Terörle Mücadele ve Harekat Daire Başkanlığı ve TADOC bilişim suçları konusunda ilgi alanlarına göre faaliyetlerini yürütmektedirler.

Bilgi İşlem Daire Başkanlığı

Emniyet Teşkilatı bünyesinde bilişim hizmetleri 1982 yılında, Bilgi İşlem Daire Başkanlığı'nın kurulmasıyla atılmıştır. Sanal dünyadaki suçları takip etmek için Emniyet Teşkilatı içinde nasıl bir yapılanmaya gidileceği konusunda çalışmalar yapmak üzere 1997 yılında "Bilişim Suçları Büro Amirliği" kurulmuştur. 2001 yılında bu büro İnternet ve Bilişim Suçları Şube Müdürlüğü olarak değiştirilmiştir. Şube, Bilişim Suçları konusundaki gelişmeleri her yönüyle takip etmekte, bilgisayar sistemlerine izinsiz giriş ve zarar yöntemlerine karşı alınacak tedbirleri araştırmakta, bilişim suçları konusunda yetiştirilecek personelin eğitim standartlarını tespit etmekte ve bilişim suçları konusunda çalışma yapan yerli ve yabancı kuruluşlarla irtibata geçmektedir. 2002 yılında ise, tüm taşra teşkilatında Bilgi İşlem Şube Müdürlükleri bünyesinde Sistem İletişim ve Bilişim Suçları Büro Amirlikleri oluşturularak il bazında bu suçlarla mücadele için önlemler alınmıştır. Fakat, Sistem İletişim ve Bilişim Suçları Büro Amirliği'nin tam olarak çalışma şeklinin ne olacağı ile yetki ve sorumlulukların sınırları belirlenmemiştir. 2008 yılı itibari ile tüm taşra teşkilatında Bilgi İşlem Şube Müdürlükleri bünyesinde Bilişim Suçları Büro Amirliği bulunmamaktadır.

Bilişim suçları konusunda, 24 Eylül 2003 tarihli Bilgi İşlem Daire Başkanlığı kuruluş, görev ve çalışma yönetmeliği 6.maddesinde bilişim suçlarıyla mücadele eden birimlere (Asayiş, Güvenlik, İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, Kriminal Polis Laboratuarları, Terörle Mücadele ve Harekat Daire Başkanlığı) eğitim ve teknik destek verilmesi görevi Emniyet Genel Müdürlüğü Bilgi İşlem Daire Başkanlığı'na verilmiştir. Taşra birimleri de hazırlanmakta olan yönetmelik doğrultusunda bilişim suçları büro amirlikleri aracılığıyla bilişim suçları konusunda çalışmalar yapacaktır. İlgili

yönetmelikte, özellikle bilişim suçları ile mücadele kapsamında saldırı tespit ve inceleme büro ile sistem ve ağ güvenliği büro amirlikleri kurulmuştur (Emniyet Genel Müdürlüğü, 2004).

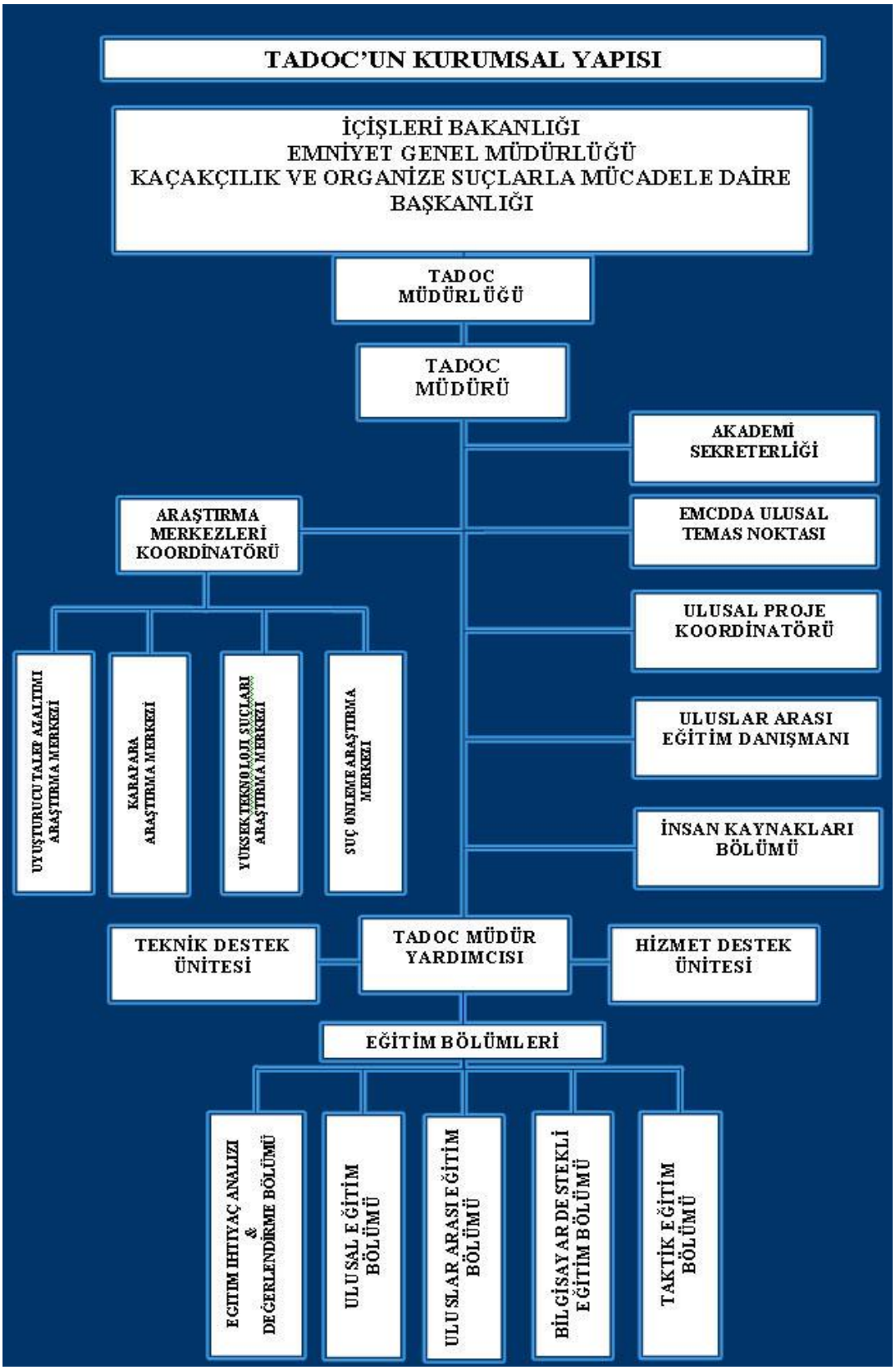
TADOC (Turkish International Academy Against Drugs and Organized Crime)

- Türkiye'nin ulusal ve uluslararası düzeyde uyuşturucu ve psikotrop maddelerin yasadışı üretim, kullanım ve kaçakçılığına karşı süregelen kararlı mücadelesini eğitim sahasında da sürdürmek,
- Organize suç gruplarıyla mücadeleyi, bilimsel veriler ışığında sürekli ve sağlıklı kılabilmek,
- Bölgesel ve uluslararası işbirliğinin kurulması, sürdürülmesi ve geliştirilmesi için uygun bir zemin oluşturmak,
- Değişik ülkelerden ve Ülkemizdeki farklı kurumlardan gelen kursiyerleri kaynaştırma yoluyla, anılan suçlarla mücadele alanında sosyal bir network kurmak, dolayısıyla uluslararası işbirliğinin güçlenmesine katkıda bulunmak gibi amaçlara ulaşmak için,

Birleşmiş Milletler öncülüğünde ve Türkiye-UNODC işbirliği çerçevesinde, 26.06.2000 (Bu tarih her yıl Dünya Uyuşturucu ile Mücadele Günü olarak kutlanmaktadır.) tarihinde Ankara'da Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı'na bağlı olarak Ülkemizin ilk uluslararası nitelikli mücadeleci kurum akademisi olan; “Türkiye Uluslararası Uyuşturucu ve Organize Suçlarla Mücadele Akademisi (TADOC)” kurulmuştur.

TADOC (Türkiye Uluslar arası Uyuşturucu ve Organize Suçlarla Mücadele Akademisi) 2000 yılında kurulmuş ve bünyesinde Bilişim Suçları Araştırma Merkezi faaliyete geçirilmiştir. Bu merkezin ismi 2003 yılında "Yüksek Teknoloji Suçları Araştırma Merkezi" olarak değiştirilmiştir. İl Bilgi İşlem Şube Müdürlükleri’nde ve İl KOM Şube Müdürlükleri’nde çalışan personel ve uygun görülen personeller özellikle TADOC bünyesinde açılan kurslarla "Bilişim Suçları" konusunda eğitim almaktadır.

TADOC'UN Eğitici Kadrosunu başta Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Merkez ve İl Birimlerinde görevli, çeşitli eğitici geliştirme programları ile eğiticilik formasyonu kazandırılan uzman bir kadro oluşturmaktadır. TADOC eğitim programları, programların özelliklerine göre, çeşitli üniversite ve enstitülerde görevli uzman akademisyenler ile yerel ve yüksek mahkemelerde görevli hukuk eğiticileri tarafından desteklenmektedir. Ayrıca, ikili işbirliği anlaşmasına sahip olunan ülkeler ile gerçekleştirilen Uzmanlık Eğitim Programlarında, bu ülkelerin anılan suçlarla mücadele alanında deneyimli uzman eğiticilerinden de faydalanılmaktadır. TADOC'un kurumsal yapısı Şekil 1'de görülmektedir.



Şekil 1: TADOC'un kurumsal yapısı.

1998-2002 yılları arasında Polis-Bilim adamı (Üniversiteler) işbirliği ile oluşturulan "Gelişen Polis Teknolojilerini Araştırma ve Değerlendirme Kurulu", Amerika Birleşik Devletleri, Kanada, Avustralya, Almanya, İngiltere gibi ileri teknolojiye sahip ülkelere geziler yapmış ve araştırma ve değerlendirme çalışmalarının sonuçlarına dayanarak, polis teşkilatının teknolojik yapılanmasında öncelikler olarak değerlendirilen hususlar belirtilmiştir. Değerlendirilen mevcut sistemler arasında polis teşkilatı için daha uygun olduğu düşünülen ABD, Kanada ve Avustralya polis teşkilatlarının sahip olduğu teknolojik yapılanmalar, bilgi güvenliği ve bilişim suçları konularının üzerinde durulmuştur. Emniyet Genel Müdürlüğü ve üniversite öğretim üyeleri ile ortak yürütülen kripto, kripto-analiz, iletişim güvenliği ve bilişim suçları projelerine devam edilmektedir.

Emniyet Genel Müdürlüğü tarafından 1996 yılından beri ABD ve Fransa'ya Bilişim Suçları konusunda lisansüstü eğitimi için personel görevlendirilmiş ve bu personel yurda dönüşlerinde bilişim suçları konusunda çeşitli dairelerde görevlendirilmiştir. Son olarak Emniyet Genel Müdürlüğü, “Bilgisayar Sistemleri ve Bilişim Suçları” ve “Yüksek Teknoloji Suçları” konularında personellerini ABD, Kanada, AB ülkeleri, Avustralya ve Japonya’da yüksek lisans ve doktora eğitimine göndermiştir.

Kriminal Laboratuar Daire Başkanlığı

Polis Kriminal Laboratuar Daire Başkanlığı’nca bilişim suçlarında kullanılan objeler, delil tespiti ve bu delillerin incelenmesi için Data İncelemeleri Şube Müdürlüğü, bu suçların ve delillerin incelenmesine yönelik çalışmaları yürütmektedir.

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, 07.07.1995 tarihli ve 95/7084 sayılı Bakanlar Kurulu kararı ile Merkezde 10 Şube Müdürlüğü ile 3 Büro Amirliği, 80 İli’de Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü ve 31 İlçe’de Kaçakçılık ve Organize Suçlarla Mücadele Grup

Amirliği ile İstanbul İlinde, Mali Suçlarla Mücadele Şube Müdürlüğü, Narkotik Suçlarla Mücadele Şube Müdürlüğü, Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilişim Suçları ve Sistemleri Şube Müdürlüğü olarak 4 ayrı şube ile faaliyetlerine devam etmektedir.

Bilişim Suçları ve Sistemleri Şube Müdürlüğü (Ankara- Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı)

Teknolojinin günlük hayatın vazgeçilmezi olduğu günümüzde, gelişen teknolojiye bağlı olarak suç tipleri değişmiş ya da yeni suç tipleri ortaya çıkarak sürekli yükselen bir ivme ile artış göstermeye başlamıştır. Bu doğrultuda gelişen teknolojinin kötüye kullanılmasının önüne geçmek, bilişim sistemleri kullanılarak işlenen suçlarla daha etkin mücadele etmek ve zaman kaybedilmeden önlenebilmesi ve faillerin yakalanması amacıyla, daha önceden kurulmuş olan Bilgi İşlem Büro Amirliği, 20.04.2003 tarihinde Yüksek Teknoloji Suçları ve Bilişim Sistemleri Şube Müdürlüğü adını altında tekrar yapılandırılmıştır ve 03.01.2006 tarihinde yürürlüğe giren ″E.G.M. Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Merkez ve İl Teşkilatı Kuruluş, Görev ve Çalışma Yönetmeliği″ uyarınca, vizyonu, bilişim sistemlerini ve teknolojiyi bilinçli bir şekilde kullanacak bireylerle birlikte suçluların önüne geçmek, işlenen bütün suçları aydınlatarak bilişim sistemlerinin suçun hedefi veya aracısı olmaktan çıkarmak olan Bilişim Suçları ve Sistemleri Şube Müdürlüğü adını almıştır. Bağlı Büro Amirlikleri ;

1- İdari Büro Amirliği,

2- İstatistik ve Stratejik Analiz Büro Amirliği,

3- Bilgi İşlem Büro Amirliği,

4- Bilişim Suçları ve Teknik Destek Büro Amirliği,

5- Yazılım ve Sistem İletişim Büro Amirliği,

6- Teknik Takip ve İzleme Büro Amirliği’ dir.

Bilişim Suçları ve Sistemleri Şube Müdürlüğü; bilişim sistemlerini art niyetli olarak kullanan ve üçüncü şahısların kimlik, kredi kartı, banka hesap v.b. bilgilerini gerek sosyal mühendislik gerekse de teknoloji yardımıyla ele geçiren kişi, kişiler ve organize örgütler ile mücadele etmektedir. Ayrıca internet üzerinden haksız kazanç elde etmek isteyen, kendini göstermeyi hedefleyen kullanıcıların yetkisiz, izinsiz ve yasadışı olarak bilişim sistemlerine sızmaları, bu sistemlerden veri temin etmeleri, sistemin akışını yavaşlatmaları veya durdurmaları halinde oluşabilecek mağduriyetleri gidermek için gerekli çalışmaları yürütmektedir.

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı'nca "phising" olarak tabir edilen banka ve kredi kartı kurumlarına ait web sitelerinin benzerlerinin yapılması suretiyle yapılan dolandırıcılıklar, "pharming" olarak tabir edilen kullanıcı bilgisayarlarının maniple edilerek bilgisayar üzerinde site yönlendirmesi yapılması suretiyle işlenen dolandırıcılıklar, "smishing" olarak tabir edilen SMS mesajlarının engellenerek ya da maniple edilerek yapılan dolandırıcılıklar ve "vhising" olarak tabir edilen arama suretiyle yapılan dolandırıcılıklar, Ceza Kanunu'nun 158/f Maddesi'nde belirtilen nitelikli dolandırıcılık suçu kapsamında takip edilmektedir.

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde birimlerin suç unsurları ile daha iyi mücadele edebilmeleri amacıyla gelişen teknolojiyi kullanmaları, sürekli iletişim halinde olmaları hedeflenmekte ve ulusal boyutta tüm birimler arasında hızlı ve güvenli bir iletişim altyapısı sistemi kurulması ve yönetilmesi çalışmaları devam etmektedir. Ayrıca, teknolojik hayattaki değişimle birlikte birimlerin her zamankinden daha fazla bilgiye ihtiyacı gerçeğinden hareketle, doğru bilgiye hızlı ve güvenli bir şekilde ulaşabilmesi, mevcut veriler kullanılarak idari, taktik ve stratejik analiz çalışmalarının yapılabilmesi, bütün bunların da henüz suçun ortaya çıkmadan bir araya getirilip değerlendirilebilmesi ve eldeki verilerin daha iyi anlamlandırılmasıyla suçla mücadelede daha etkili tedbirlerin alınacağı bilinci ile birimlerin ihtiyacı olan yazılımların geliştirilmesi çalışmalarıda Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde yürütülmektedir.

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı'na bağlı,

Bilişim Suçları ve Sistemleri Şube Müdürlüğü'nün Misyonu:

1) Türkiye'nin bilişim suçları profilini ortaya koymak,
2) Bilişim suçları faaliyetlerini takip etmek, istihbarat toplamak, değerlendirmek ve operasyon yapmak,
3) Haksız kazancı engellemek,
4) Organize suç gruplarının oluşumunu engellemek,
5) Bilişim sistemlerini ve teknolojiyi endişe duymadan kullanabilecek bir toplum oluşturmak,
6) Ülkeler arasında işbirliğini arttırmak,
7) Kurum içerisinde ve mücadeleci birimler arasında koordinasyon sağlamak,
8) Yurtdışından ülkemize yönelik bilişim suçları tehdidini değerlendirmek, uluslararası işbirliği ile sınır aşan operasyonları organize etmek,
9) Bilişim suçları ile mücadele edecek uzman ve profesyonel personel yetiştirmek,
10) Adli Bilişim hizmetlerini uzman personel ve malzeme desteği ile geliştirmek.

Bilişim Suçları ve Sistemleri Şube Müdürlüğü Hedefleri

1) Bilişim Suçları ile mücadelede ve meydana gelen olayların çözümlenmesi konusunda başarıyı artırmak amacıyla, mevcut 16 Adli Bilişim Bölge Merkezinde görevli uzman personele daha önce verilen yurtiçi, yurtdışı, teknik ve operasyonel eğitim faaliyetlerine ilaveten yeni eğitim faaliyelerinin düzenlenerek etkinlikleri artırılmasıdır.
2) Uluslararası bilişim suçları alanında operasyon faaliyetlerine destek vermek ve mücadeleci kurumlarlarla işbirliğini artırmaktır.
3) Bilişim suçlarıyla sık karşılaşan kurum ve kuruluşlarla işbirliğinin artırılmasıdır.
4) Bilişim suçları konusunda toplumsal farkındalıkların artırılmasıdır.

Bilişim Suçları ve Sistemleri Şube Müdürlüğü Görevleri

1) Türk Ceza Kanununun 243 üncü, 244 üncü, 245 inci (birinci ve dördüncü fıkralar hariç) ve 246. maddelerinde belirtilen Bilişim Suçları ve 158/f Nitelikli Dolandırıcılık suçları hakkında bilgi toplamak, değerlendirmek ve bu faaliyetleri önlemek amacıyla gerekli tedbirleri almak ve ilgili birimlerle müşterek operasyonlar düzenlemek,

2) Görev alanına giren konularda il birimleri tarafından yürütülen mücadeleyi yönlendirmek, çalışmalarla ilgili eksikliklerin giderilmesi için girişimlerde bulunmak,

3) 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,

4) Görev alanına giren konularda mevzuat çerçevesinde ulusal veya uluslararası kuruluş faaliyetlerine katılmak ve sonucunda Başkanlığa rapor sunmak,

5) Görev alanına giren konularda idari ve hukuki eksikliklerin giderilmesi ve geliştirilmesi yönünde görüş ve önerilerde bulunmak,

6) Başkanlık ve il birimlerinin yürüttükleri çalışmalarda, bilişim sistemleriyle ilgili olarak gerekli araştırma, inceleme, tespit ve değerlendirmelerde yardımcı olmak,

7) Başkanlık ve il 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,

8) Başkanlık ve il birimlerinin bilgisayarla çözümlenebilecek her türlü isteklerini çözüme kavuşturabilmek için proje geliştirmek ve uygulama programının üretilmesiyle kullanılmasını sağlamak, yazılımların bakım ve revizyon hizmetlerini yürütmek,

9) Kaçakçılık birimleri için gerekli bilgisayar programlarını yazmak ve geliştirmek,

10) İnternet ve intranet ortamında Başkanlığa ait web sitelerini hazırlamak ve güncelleştirmek,

11) Temin edilen bilişim cihazları ve sistemleri ile ilgili kullanım dokümanları hazırlamak ve eğitim çalışmalarını koordine etmek,

12) Bilişim ağı kurmak, yönetmek ve düzenli olarak bakımını yapmak,

13) Kullanılan veri tabanlarının yönetim ve yedeklemesi işlerini yürütmek,

14) Bilişim Suçları veya diğer operasyonel birimlerine Adli Bilişim hizmeti vermektir.

KOM Daire Başkanlığı'nca; AB'ye uyum sürecine yönelik yürütülen Eşleştirme Projelerinin yanı sıra MATRA Programı kapsamında da çeşitli proje çalışmalarında bulunulmaktadır. Bu bağlamda, 2008 yılları içerisinde **"Bilişim Suçları İle Etkin Mücadele Edilebilinmesi"** başlıklı bir proje çalışması Hollanda'lı yetkililerle birlikte yürütülerek, bilişim suçları konusunda mücadele eden eğiticilerin ve personelin eğitiminin sağlanması amaçlanmaktadır.

28 Ocak - 1 Şubat 2008 tarihleri arasında, 81 İl KOM Şube Müdürlükleri, Bilişim Suçları Büro Amirleri ve Bilişim Suçları Bürolarında çalışan birer memur sınıfı personelin katılımlarıyla "**Bilişim Suçları Soruşturma Teknikleri"** eğitimi Antalya ilinde verilmiştir. Eğitimde temel soruşturma usulleri, adli delillere ilk müdahale ve bilişim suçları konusundaki mevzuat hakkında detaylı bilgiler verilmiştir. Adli dijital delil incelemesi konusunda ülke genelinde oluşturulan 16 Bölge Merkezi personeline dijital delil konusunda ve incelemede kullanılmak üzere satın alınan yazılımların (Encase ve FTK) kullanılması hakkında eğitimler düzenlenmiştir (KOM Daire Başkanlığı, 2008).

Bilişim Suçları ve Sistemleri Şube Müdürlüğü (İstanbul Emniyet Müdürlüğü bünyesinde)

Ülkemizde en çon nüfus barındıran il olan ve bilişim suçlarının en çok yaşandığı illerin başında gelen İstanbul ilinde ise, İstanbul Emniyet Müdürlüğü bünyesinde Bilişim Suçları Büro Amirliği, 2008 yılında Bilişim Suçları ve Sistemleri Şube Müdürlüğü'ne dönüştürülmesi İçişleri Bakanlığının 25/04/2007 tarihli onayı ile uygun görülmüştür. İstanbul Valiliğinin 29/05/2007 tarihli onayı ile İstanbul Emniyet Müdürlüğü bünyesinde "Bilişim Suçları ve Sistemleri Şube Müdürlüğü", 03/09/2007 tarihinde Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı'na bağlı olarak İstanbul Emniyet Müdürlüğü bünyesinde Vatan hizmet binasında faaliyete geçmiştir (İstanbul Emniyet Müdürlüğü, 2008). Şube Müdürlüğü'nün görevleri şu şekildedir:

1) Bilişim Suçları ve Sistemleri Şube Müdürlüğünün görev alanına giren suçların bilişim sistemleri kullanılmak sureti ile işlendiği durumlarla ilgili bilgi toplamak, değerlendirmek ve bu tür faaliyetleri önlemek amacıyla gerekli tedbirleri almak, ilgili birimlerle müşterek operasyonlar düzenlemek ve gerektiğinde mevzuat hükümlerine göre işlem yapmak,
2) Görev alanına giren suç organizasyonlarının faaliyetlerini koordineli olarak izlemek, bilgi toplamak ve değerlendirmek,
3) Operasyonlardan ele geçirilen dijital materyallerin (HDD, Bilgisayar, DVD vb.) imajlarının alınarak gerekli teknik incelemeleri yapmak,
4) İnternet ortamında yapılan suça konu(bilgilerin çalınması, MSN hacklenmesi, site hacklemek vb.) işlemleri yapan kişi/kişileri tespit ederek gerekli tahkikatı yapmak
5) Kişiler arasındaki haberleşmenin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak.
6) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma

cihazı ile kaydeden kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak,

7) Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kişilerin tespit edilerek hakkında gerekli tahkikatı yapmak,

8) Hukuka aykırı olarak kişisel verileri kaydeden kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak,

9) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi/kişilerin tespit edilerek, haklarında gerekli tahkikatı yapmak,

10) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olan kişilerin görevlerini yerine getirmedikleri tespit edildiğinde kişi/kişiler hakkında gerekli tahkikatı yapmak,

11) Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturan kişi/kişilerin tespit edilerek haklarında gerekli tahkikatın yapmak,

12) Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifika oluşturanlar veya bu elektronik sertifikaları bilerek kullanan kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak,

13) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak,

14) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verilerin başka bir yere gönderen kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak,

15) Başkasına ait olan banka yada kredi kartını her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak

veya kullandırarak kendisine veya başkasına yarar sağlayan kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak,

16) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak sureti ile kendisine yada başkasına yarar sağlayan kişi/kişilerin tespit edilerek haklarında gerekli tahkikatı yapmak (İstanbul Emniyet Müdürlüğü, 2008).

Asayiş Daire Başkanlığı:

SASEM, 18 Ağustos 1998 tarihinde KRİMİNAL TEKNİK EĞİTİM VE ARAŞTIRMA ŞUBE MÜDÜRLÜĞÜ adı altında Asayiş Daire Başkanlığı'na bağlı bir eğitim merkezi olarak faaliyetlerine başlamıştır. Asayiş Daire Başkanlığı'nın görev alanına giren konularda, değişen ve gelişen suç türleri ile mücadele edebilmek ve uzman personel yetiştirmek amacıyla yeniden yapılandırılarak, 11 Nisan 2002 tarihinden itibaren Suç Araştırma ve Soruşturması Eğitim Şube Müdürlüğü (SASEM) olarak hizmet vermeye başlamıştır. SASEM bünyesinde bilişim suçları konusunda eğitim faaliyetlerine katılan personel, taşra teşkilatında bu alanda hizmet vermektedir.

2.2.9. Ülkemizde İşlenen Bilişim Suçları İstatistikleri

Bilgisayar kullanımının artması ve bu alandaki teknolojinin gelişmesiyle birlikte sanal alemdeki nitelikli suçlar hızla çoğalmıştır. Hırsızlık, dolandırıcılık, soygun, terörizm, sabotaj ve kaçakçılık gibi pek çok suç dijital ortama taşınmıştır.

Bilişim suçları alanında ülkemiz başta olmak üzere dünya genelinde en sık karşılaşılan suç türleri aşağıdaki gibidir (KOM Daire Başkanlığı, 2008).

- **İnternet Banka Dolandırıcılığı:** İnteraktif bankacılık dolandırıcılığı suçlarını işleyen şahısların kullandığı yöntemler zamana göre farklılık göstermesine rağmen; temelde kullanıcıyı aldatmaya yönelik olanlar ön plana çıkmaktadır. Bu yöntemler; bankaların internet sayfalarının taklit edilmesi (phising), sahte e-posta bildirimleri, cep telefonlarına gönderilen mesajlar (smishing) ya da banka operatörü (vishing) gibi müşterileri

arayan dolandırıcıların bankacılık işlemleri için gereken kişisel bilgiler ile hesap ve kredi kartlarına ait bilgilerin çalınması biçiminde ortaya çıkmaktadır.

- **Banka ve Kredi Kart Dolandırıcılıkları:** En yaygın olarak uygulanan yöntemler şunlardır:

1- ATM cihazlarına düzenekler kurularak kullanıcının kart bilgisinin ve şifresinin alması,

2- Kredi kartları ile ödeme yapılması esnasında özel ekipmanlar kullanılarak kopyalama yapılması

3- Birçok şubesi bulunan büyük mağazaların daha rahat hesap tutabilmeleri için alışveriş yapan müşterilerin kart bilgilerini merkezlerinde depolamaları ve güvenlik zafiyetlerinin bulunması,

4- Art niyetli olarak kurulan internet sistemlerinden alınan hizmetlerle kart bilgilerinin elde edilmesi,

5- Online hizmet veren veya mal satan sitelerden yapılan alışverişlerde, kullanıcıların kart bilgilerinin kaydedilmesi ve yetersiz güvenlik önlemleri ile bilgilerin çalınması.

- **BOTNET saldırıları:** BotNet; Robot Network ağı kavramından türemiş olup, temel hedef köle bilgisayar ağı oluşturmaktır. Botnet sahibi bir saldırgan aynı anda birkaç bilgisayarı kontrol edebileceği gibi binlerce bilgisayarı da kontrol edebilmektedir.
- **Bilgisayar Korsanlığı:** Bilişim sistemine girme, engelleme, değiştirme, verileri yok etmek vs.

Emniyet Genel Müdürlüğü, il emniyet müdürlüklerindeki verileri alarak, Türkiye'deki bilgisayar suçlarının haritasını çıkarmış ve bir rapor hazırlamıştır. Çalışma, takibi şikayete bağlı suçlar, Interpol aracılığıyla intikal eden suçlar ve polisin bizzat ilgilendiği suçlardan oluşmaktadır. 1998 yılında Türkiye'de işlenen bilişim suç sayısı 5 iken, 1999'da bu sayı 15'e yükselmiştir. 2000 yılında 80'i bulan suç dosyasının sayısı, 2001 yılına gelindiğinde 136'yı bulmuştur. Bu

geçen süre içerisinde Adana sahtecilik ve kredi kartı ile internet üzerinden alışveriş ile birinciliğini elden bırakmamıştır. Elde edilen sonuçlar, Türkiye'deki bilgisayar suçlarının, lisans haklarının ihlali, dolandırıcılık, sahtecilik, yasadışı yayınlan ve bilgisayar sabotajı şeklinde geliştiğini göstermektedir (Emniyet Genel Müdürlüğü, 1999).

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı istatistiki verilerine göre kredi kartı sahteciliği ve dolandırıcılığı, banka dolandırıcılığı, bilişim suçları ve dolandırıcılığı konularında 2004, 2005, 2006 ve 2007 yıllarındaki istatistiki bilgiler şekil 2'de belirtilmiştir (KOM Daire Başkanlığı, 2008).

Olay Türü:	2004		2005		2006		2007	
	Olay	Şüpheli	Olay	Şüpheli	Olay	Şüpheli	Olay	Şüpheli
Kredi Kartı Sahteciliği ve Dol.	146	422	195	543	122	241	209	423
Banka Dolandırıcılığı	22	72	9	33	98	172	164	443
Bilişim Suçları ve Dolandırıcılığı	16	31	91	179	4	9	206	421
Toplam	184	525	295	755	224	422	579	1287

Şekil 2: 2004-2005-2006-2007 Yılları Kredi Kartı Sahteciliği ve Dolandırıcılığı, Banka Dolandırıcılığı, Bilişim Suçları ve Dolandırıcılığı

Ülkemizde, basından alınan örneklerle bilişim suçları konusunda gerçekleştirilen bazı operasyon örnekleri 2007 yılı ek-6 ve 2008 yılı ek-7'de belirtilmiştir.

2.2.10. Uluslararası Platformlar ve Bazı Ülkelerde Bilişim Suçları Konusunda Yapılan Çalışmalar

Bilişim teknolojileri üzerinden gerçekleşen ihlaller fiziki bir coğrafyayla sınırlanamamaktadır. Bu ihlallerin gerçekleştiği ortamın bileşenleri dünyanın farklı noktalarında ve farklı hukuk sistemlerine sahip ülkelerin egemenlik yetkisi altında olabilirler. Bu sebepten dolayı bu ortamda işlenen suçlara karşı uluslar arası arenada bir tutarlılık ve sıkı bir işbirliğinin sağlanmak için ülkeler uluslar arası işbirliğine gitmişler bazı anlaşmalar yapmışlardır.

Ülkeler iç hukuklarında düzenlemeye giderlerken üyesi oldukları ve fikir birliğine vardıkları uluslar arası organizasyonların tavsiye kararları doğrultusunda hareket ederek, araştırma ve soruşturma faaliyetlerinde yardımlaşarak ortak davranış biçimleri geliştirmişlerdir. Uluslararası platformda AB, Ekonomik İşbirliği ve Gelişme Teşkilatı (OECD), Birleşmiş Milletler, Avrupa Konseyi ve G8 Bünyesinde bilişim suçları çalışmaları yürütülmektedir. Burada, Avrupa Konseyi'nin bilişim suçları çalışmaları irdelenmiştir.

Avrupa Konseyi Bilişim Suçları Çalışmaları

Avrupa Konseyi'nde bu konuda yapılan ilk çalışma, atadığı uzmanlar komitesinin yaptığı çalışmadır. Komite, OECD'nin 1986 yılındaki raporunu referans alarak çalışmalarını yapmış ve Avrupa Konseyi burada belirlenen ihlallerin üye ülkelerce cezai müeyyide altına alınmasını kararlaştırmıştır. Konseyin böyle bir çalışma başlatmasındaki amaç, ceza kanunları ile düzenlenmesi gerekli olan eylemlerin ne olduğunu açık bir şekilde tespit etmek; sivil özgürlük ve güvenlik kavramları arasındaki uyuşmazlığın nasıl aşılacağı konusunda üye ülkelere yol göstermektir. Komitenin çalışmaları sonucu OECD'nin raporunda belirtilen eylemlere ek olarak bilgisayarla bağlantılı suçlarla ilgili korunma, engellenme, usul ile ilgili bir takım kurallar (örneğin uluslararası araştırmalar, veri bankalarına el konulması ve bilgisayar suçlarının soruşturulması ve kovuşturulmasında uluslararası işbirliğine gidilmesi konuları) ve mağdurların durumu bir taslak halinde sunulmuştur. Üye ülkelere

kanunlaştırma çalışmalarında yol gösterici nitelikte olan bu taslak daha sonra Avrupa Konseyi Bakanlar Komitesi tarafından 13 Eylül 1989 tarihinde benimsenerek yürürlülüğe girmiştir (Beceni, 2002).

Avrupa Konseyi ikinci çalışmasını 1995 yılında gerçekleştirmiştir. Bu çalışmayla, ceza usul yasalarının bilişim teknolojileri ile birleştirilmesiyle ilgili problemler masaya yatırılmış ve bunlara çözüm yolları aranmıştır. Avrupa Konseyinin son ve en kapsamlı çalışması "Draft On Cyber Crime"'dır. Bu çalışma için komisyonlar oluşturulmuş ve Konsey, 1989 ve 1995 yıllarındaki tavsiye kararlarının ışığında son çıkan gelişmeleri de göz önüne alarak üye ülkelerin de ötesinde bilişim suçlarıyla mücadele de global bir konsensus oluşturulmasına zemin hazırlamayı amaçlamıştır.

Yaklaşık iki yıl süren komisyon, alt komisyon çalışmaları ve bir çok taslak metinden sonra, önemli değişikliklere uğrayarak imzalanan sözleşme metni, "siber suç"un tanımı ve sınıflandırılması da dahil, kullanıcıdan sektöre, kamudan sivil topluma çok sayıda kesimi yakından ilgilendiren bir çok konuda düzenleme ve ilkeleri belirtmiştir.

Avrupa Konseyi Siber Suç Sözleşmesi, 23 Kasım 2001'de Budapeşte'de, 26'sı üye ve 4'ü üye olmayan (ABD, Japonya, Kanada ve Güney Afrika) 30 ülke tarafından imzalanmıştır. Sözleşme, genel ilkeler ve tavırlar konumlayan yapısıyla, bilişim suçları konusunda ilk uluslar arası belgedir. Bu konvansiyon; bilgisayar sistemlerinin, ağlarının ve bilgisayar verilerinin gizliliğine, doğruluğuna ve ulaşılabilirliğine zarar verici faaliyetlerin, ayrıca bu sistemlerin, ağların ve verilerin kötü amaçlı kullanımının engellenmesi, ayrıca bu tür faaliyetlerin cezaî niteliklerini belirlemek ve söz konusu cezaî suçlarla etkili biçimde mücadele edilmesi için gerekli yetkilerin temin edilmesini sağlamak, ayrıca, bu tür cezaî suçların hem ulusal hem de uluslararası düzeyde belirlenmesi, soruşturulması ve yargıya götürülmesini kolaylaştırmak ve hızlı ve güvenilir bir uluslararası işbirliğinin sağlanması için gerekli düzenlemelerin yapılmasını temin etmek için gerekli olduğu inancıyla ve "ortak bir suç politikası" geliştirmek amacıyla hazırlanmıştır.

2.2.11. Bilişim Suçları ve Çeşitli Ülkelerde Yapılan Çalışmalar

Amerika Birleşik Devletleri

Amerika Birleşik Devletleri bugüne kadar, internet ve bilgisayar dünyasındaki her türlü gelişmeye öncülük ettiği gibi, bilişim ortamının suç aracı olarak kullanılması ve bu suçların düzenlenmesi olgusunun da ilk olarak ortaya çıktığı yer olma özelliğine sahiptir. Amerika'da bilişim suçlarının geçmişi 1960'lı yıllara kadar uzanmaktadır. İnternetin ve bilgisayarın anavatanı olan Amerika Birleşik Devletleri'nde gerek federal, gerekse eyalet düzeyinde bilişim suçları konusunda bir çok yasa çıkartılmıştır. ABD'de bugün için çeşitli bilişim suçu şekillerini düzenleyen birçok federal yasa kabul edilmiştir. Ancak bunlardan en önemlisi Federal Temel Yasa'nın 18. bölümünün 1030. maddesidir. Bu yasa temel olarak, korumalı bir bilgisayara yetkisiz ve izinsiz erişimi yasaklamaktadır. Yasa metni o kadar geniş kaleme alınmıştır ki, kamuya ve özel sektöre ait tüm bilgisayarlar yanında, kişisel bilgisayarlar da bu korumadan tam olarak istifade edebilmektedir.

Amerika Birleşik Devletleri'nde bilişim suçları ve siber terörizmle mücadele eden pek çok kuruluş ve bu kuruluşlara ait özel birimler bulunmaktadır. Bunlardan bazıları şunlardır; FBI "National Infrastructure Protection Center", "Information Technology Association of America", "Trap and Trace Center Authority" ile "Carnegie Mellon's Emergency Response Team" (CERT) ve bazı üniversiteler bünyesinde kurulan birimler bunların en önemlileridir (Emniyet Genel Müdürlüğü, 1999).

CERT'in Amerika için verdiği istatistikler ilginçtir. İstatistikler, bu suçların bilgisayarın insan hayatına girdiği ilk yıllarda katlanarak arttığını, 1994-1997 arasında yatay seyrettiğini ve nihayetinde 1998'den itibaren internet teknolojisinin insan hayatının her köşesine girmesiyle yeniden katlanarak arttığını göstermektedir. 2003 yılının ilk 9 ayıda dahil olmak üzere bugüne kadar rapor edilen bilişim suçu olay sayısı 297,318'dir. Bu olayların, prestij kaygısı gibi nedenlerle çoğunlukla bildirilmediği düşünülürse bu sayının çok daha fazla olduğu düşünülmektedir.

Tablo 2: ABD'de Meydana Gelen Bilişim Suçları Olay Sayıları (1988-1995)

Yıl	1988	1989	1990	1991	1992	1993	1994	1995
Olay	6	132	252	406	773	1,334	2,340	2,412

Tablo 3: ABD'de Meydana Gelen Bilişim Suçları Olay Sayıları (1996-2003)

Yıl	1996	1997	1998	1999	2000	2001	2002	2003
Olay	2,573	2,134	3,734	9,859	21,756	52,658	82,094	114,855

Tablo 2 ve Tablo 3'te ABD'de meydana çeşitli tarihler arasındaki bilişim suçları olay sayıları görülmektedir. ABD yönetimi, bu suçlarla mücadelenin gerekliliğini anlayarak Temmuz 1996 yılında, A.B.D Başkanı'na bağlı "Commision of Critical Infrastructure Protection" adlı bir komisyon oluşturmuştur (Emniyet Genel Müdürlüğü, 1999). Bu komisyon, elektronik haberleşme ve bilgisayar ağlarının ABD açısından hayati önem taşıdığını, söz konusu ağların dış saldırılara karşı açık olduğunu, öte yandan, kamu ve özel sektörün mevcut tehditleri ciddiye almadığını belirtmiş ve bu ağların korunması için önlemler alınmasının gerekliliğini savunmuştur (Ersanel, 2001). Söz konusu komisyon, suçun takip edilmesi ve araştırılması ile önceden alınacak önlemler konusunda yöntemler tespit etmiştir.

Bununla birlikte, bir çok kamu kurumu ve kuruluşu bu suçlarla mücadele etmede bazı birimler oluşturmuşlardır. Örneğin, CIA "Information Warfare Center" adında ve 1000 kişilik bir personelle 24 saat hizmet veren bir birim kurmuştur. FBI ise, bilgisayar sistemlerine girme ve benzeri suçları takip etmek amacıyla "National Infrastructure Protection Center" ve "Computer Crime Squad"ı oluşturmuştur. Yine Adalet Bakanlığı bünyesinde oluşturulan "Computer Crime and Intellectual Property Section" bu alanda çalışmalar yapmakta, gerekli eğitim faaliyetlerinde bulunmakta ve diğer birimlere destek vermektedir (Emniyet Genel Müdürlüğü, 1999).

Görüldüğü üzere ABD'de mevzuat alanında bu suçlarla ilgili gerekli önlemler alınmış, bunun yanında kolluk kuvvetlerinin bu suçlarla mücadeledeki görev ve sorumluluklarında da gerekli düzenlemeler yapılmıştır.

İsrail

İsrail Emniyet Müdürlüğü, bilgisayar üzerinden işlenen suçlar konusuyla 1996 yılından itibaren ilgilenmeye başlamıştır. Sahtekarlık Büro bünyesinde Bilgisayar Suçları Bölümü kurulmuştur. Anılan bölümdeki görevliler, esasen polis olup bilgisayar konusunda eğitimden geçirilmişlerdir. Bu birim, 1995 yılında yürürlüğe giren "Bilgisayar Yasası ve Polis Soruşturma ve Tutuklama Kanunu" çerçevesinde görev yapmaktadır. Gerektiğinde diğer polis birimlerince yürütülen soruşturmalara yardımcı olmaktadır (Emniyet Genel Müdürlüğü, 1999).

İsrail'de bilgisayar üzerinden işlenen suçlara karşı polis tarafından teknik önlemler alınması söz konusu değildir. Bu alanda diğer devlet kuruluşları ve özel şirketlere yardımcı olunmamaktadır. Söz konusu kuruluşlar kendi imkanları ile korunma sistemlerini oluşturmakta ve işletmektedirler. İsrail hükümeti, bilgisayar suçları ile mücadele konusunda başta ABD olmak üzere, birçok Avrupa ülkesiyle işbirliği anlaşması imzalamış bulunmaktadır.

Fransa

Fransa'da 1998 yılında yeni teknolojiler kullanılarak işlenen suçların maliyeti 14 milyar Frang düzeyine ulaşmış, 1999 yılında ise bu konuda polis ve jandarma makamlarına 3815 olay aksettirilmiştir. Bunların 2450 adedi internet kullanılarak işlenen suçlardır. Kalan 1336 adedi ise telekomünikasyon sistemlerinin kullanımına aittir. Fransız Danıştay'ının 1998 yılında yayınladığı internet konulu raporda, mevcut mevzuatın bilgisayar ortamında işlenen suçlarla mücadeleyi de kapsayacak şekilde geliştirilmesinin yeterli olacağını belirtmiştir. Ancak, bazı özel konularda yeni hukuki çerçevelerin belirlenmesi ihtiyacı doğmuştur. 17 Mart 1999 tarihinde şifreleme sistemi kullanımına ilişkin mevzuatta değişiklikler yapılmıştır. Yine 29 Şubat 2000 tarihinde elektronik imzaların hukuki değer taşımasına ilişkin bir kanun kabul edilmiştir (Emniyet Genel Müdürlüğü, 1999).

İtalya

İtalya'da Bilişim suçları konusunda yasal düzenleme 23 Aralık 1993 tarihinde 547 sayılı kanun ile yapılmıştır. Bilgisayar suçları ile mücadele için 30 Mart 1998 tarihinde Emniyet Genel Müdürlüğü bünyesinde Posta ve İletişim Güvenliği Daire Başkanlığı kurulmuştur. Başkanlık bünyesinde personel, lojistik ve teknik olmak üzere üç bölüm mevcuttur. Taşrada ise 20 ilde doğrudan başkanlığa bağlı olarak görev yapan ofisler bulunmaktadır. Operasyonel işlevi olan teknik bölüm bünyesinde oluşturulan bir çalışma grubunda mühendisler, bilişim teknisyenleri ve örgütlü suç, terörizm, çocuk pornografisi vb. Konularda uzmanlaşmış dedektifler görev yapmaktadır. Bilişim ortamında işlenen suçlar konusunda, ceza yasasında tarif edilen suç teşkil eden eylemler özet olarak şunlardır (Emniyet Genel Müdürlüğü, 1999):

- Yazılımları kısmen veya tamamen tahrip eden, değiştiren, bilgi veya iletişim sistemlerinin doğru çalışmasını engelleyen programlarla saldırıda bulunmak (1 milyon liret- 500$- kadar para cezası).
- Kamu yararına kullanılan tesislerin, bilgi sistemlerinin, veri, bilgi ve yazılımlarının içeriklerini tahrip etmek ve çalışmasını kesintiye uğratmak (1 yıldan 4 yıla kadar hapis).
- Bilgi veya iletişim sistemlerine fiziki olarak veya yazılım aracılığıyla yetkisiz olarak girmek, bilgi almak, alınan bilgileri yaymak, kayıtlar üzerinde tahribat yapmak veya sisteme maksatlı olarak yeni bilgiler ilave etmek (3 yıla kadar hapis ve 10 milyon liret –5000$- kadar para cezası).
- Her türlü iletişimin engellenmesi, mahremiyetinin, ihlal edilmesi, bu amaçla çeşitli cihaz ve sistemlerin kurularak enformatik ve telematik haberleşmenin kesintiye uğratılması, araya girilmesi veya iletişimin içeriğinin değiştirilmesi.

Bu suçlarla mücadele için Posta ve İletişim Güvenliği Daire Başkanlığı bünyesinde oluşturulan grup, sürekli olarak internet üzerinde çalışmakta ve ilgili kanunlarda tarif edilen herhangi bir suç unsuruna rastladıklarında çeşitli yöntemlerle suçlular tespit edilerek, suç ve suçlular adli makamlara intikal ettirilmektedir. Dijital ortamda işlenen her türlü suç bu grubun görev alanına girmektedir (Emniyet Genel Müdürlüğü, 1999). İfade özgürlüğü, kişisel verilerin

korunması, çevrim içi yayıncılık, İnternet hizmet ve içerik sağlayıcıların sorumlulukları, suç teşkil eden içerik ve bilişimle ilgili tüm suçlar göz önüne alındığında bilişim ve hukuk ilişkisi hemen kendini göstermektedir. Ulusal ve uluslar arası boyutuyla bilişim suçları hem mevcut ulusal hukuku hem de uluslar arası hukuku yakından ilgilendirmektedir. Bilişim suçları ve hukuk ilişkisini irdelemekte büyük yarar görülmektedir.

2.3. Bilişim Suçları ve Hukuk

Bilişim suçlarının tüm ülkelerde günlük hayatta yer bulması ve fertlerin, kurum ve kuruluşların, devletin güvenliğini olumsuz olarak etkilemesi ve yüklü mali zararların ortaya çıkmasından dolayı, hukuki alanda da bu suçların yaptırımını bulması ve oluşan suç olgusunun karşılığını bulması için bir çok alanda hukuki düzenlemeler ihdas edilmektedir.

Bilişim suçları, bütün ülkelerin ortak problemi haline geldiğinden ve bilgisayar ağları sayesinde bu suçlar milli sınırları aştığından dolayı ulusal hukuki düzenlemeler bilişim suçları ile mücadelede yetersiz kalmaktadır. Bu nedenle bilişim suçları ile etkin mücadele için ulusal hukuk sisteminin yanı sıra uluslar arası hukuki düzenlemelerin ve bağlayıcılığının sağlanması gerekmektedir. Bu nedenle, özellikle uluslar arası kuruluşlara gerekli mevzuat düzenlemeleri ve işbirliğinin istenen düzeyde olması için önemli sorumluluklar düşmektedir. Ülkemizde, bilişim ve bilişim suçları alanındaki yürürlükte olan mevzuat Ek-1'de verilmiştir.

Bilişim alanındaki başdöndürücü gelişmeler bilgisayarları hayatımızın her alanında vazgeçilmez unsurlar haline getirmiştir. Günümüzde bilgisayarlar toplumun hemen her alanında kullanılır duruma gelmiştir ve İnternet'in gelişmesiyle birlikte, bilgisayar kullanımı bir çok eve de girmiş bulunmaktadır.

Yeni teknolojiler her zaman çözümlerle birlikte yeni problemleri de getirmişlerdir. Bilgisayar teknolojisi yalnızca kamu sektörüne, özel şirketlere ya da bireylere yardım etmemiş, aynı zamanda suçlulara da bilgisayarları yasadışı

yollarda kullanmak için gerekli olan kompleks iletişim bilgisini de sağlamıştır. Bilgisayar teknolojisi suçlulara yasaları ihlal etme fırsatını ve geleneksel suçları teknolojik yöntemler kullanarak işleme şansını vermiştir. Polisin bu yeni ve her geçen gün büyüyen suçla mücadelesini nasıl yapması gerektiği, hangi mevzuata göre çalıştığını bilmesi ve bilişim suçlularını adli birimlere somut deliler ile çıkarması önemli bir konu alanıdır. Bu amaçla, tez çalışması kapsamında temel ve uzmanlık seviyesinde modüller geliştirilmiş ve " bilişm ve hukuk" başlığına içeriğiyle birlikte yer verilmiştir.

Suç öncesinde, bilişim suçları karşısında tedbirler almak belli bir süreci gerektiren, ancak kesinlikle etkili bir faaliyettir. Özellikle, bilişim suçları konusunda toplumun broşür, kitapçık gibi yazılı materyaller hazırlanarak bilgi seviyesinin ve algısının artırılması ya da konferans, panel, sempozyum vb. etkinlikler ile bilişim suçları farkındalık düzeyinin artırılması maliyeti düşük, ancak getirileri fazla olan etkinlikler olarak düşünülmektedir. Toplumu bilinçlendirme faaliyetleri yaparak ve toplumun da desteğini alarak bilişim suçlarıyla mücedeleyi başarıyla sağlayabilen bir Emniyet Teşkilatı, geleceğe hep birlikte daha güvenle bakmayı sağlayacaktır. Unutulmamalıdır ki, klasik suçlarda olduğu gibi, bilişim suçlarında da çözüm için sadece Emniyet Teşkilatı'nın çabaları yeterli olmayacaktır. Bilişim suçlarında da başarı için polis-halk bütünleşmesinin ve işlemesi gereken ihbar (online ihbar) sisteminin rolü yadsınamaz bir gerçektir.

2.4. Suç Öncesi Polisin Bilişim Suçlarıyla Mücadelesi

İnternet aracılığı ile işlenen suçlarla mücadele, internetin ve kullanıcılarının yapısı nedeniyle oldukça güçtür. İnternet suçlarıyla mücadele edebilmek için; bilinçli kullanıcı, mücadelede uzman eğitimli kişiler, yasal mevzuat, mücadelede uluslararası uyum ve işbirliği, yeterli donanım ve teknik altyapı gereklidir. İnternet suçlarıyla mücadelede ele alınması gereken ilk basamak, önleyici güvenlik hizmeti olan suç oluşumunu önlemek ve ayrıca suçun nitelik veya niceliğini azaltabilmektir.

2.4.1. Bilişim Suçlarıyla Mücadelede Suç Önleme Anlayışı

Teknoloji, bir yandan insan hayatını görece kolaylaştırmaya devam ederken, bir yandan da çözülmesi gerekli birtakım problemlere yol açmaktadır. Siber suç olgusu bunlardan sadece biridir. Suç, insanlık tarihi kadar eski bir kavramdır. Her dönemde, dönemin şartlarına göre şekil alan suç ve suçlu kavramı da günümüzdeki dönüşüme paralel gelişmeler göstermektedir. Bilişim teknolojisinin gelişmesi ve bilginin eski devirlere göre daha çok önem kazanması, bilginin ekonomik, sosyal, siyasal değerinin artması, bu değerler üzerinde kolay yoldan hak sahibi olmak isteyen kişileri, bilişim teknolojisi marifetiyle suç işler hale getirmiştir. Ayrıca günümüze kadar suçlu grubunda yer almayan binlerce insan, artık bilişim teknolojisi marifetiyle suç işler hale gelmiştir. Bunun temel sebeplerinden birisi, hayatı kolaylaştıran teknolojinin, suç işlemeyi de kolaylaştırmasıdır (Özcan ve Bal, 2001).

Suçla Mücadele Kavramı

İnternet aracılığı ile işlenenen suçlarla mücadele kavramı, bireyi, tüm toplumu, devletleri ve tüm dünyayı içine alan bir kavramdır. İnternet aracılığı ile işlenenen suçlarla mücadele, İnternet'in ve kullanıcılarının yapısı ve özellikleri nedeniyle oldukça güçtür. İnternet suçlarıyla mücadele edebilmek için; bilinçli kullanıcı, uzman eğitimli kişiler, yasal mevzuat, yeterli donanım ve teknik altyapının yanı sıra, uluslararası uyum ve işbirliği, basın kuruluşlarının ve sivil toplum kuruluşlarının desteği gereklidir. Özellikle suç öncesinde yukarıda sayılan faktörlerin aktif pozisyonda bulunmaları gereklidir.

Bilinçli Kullanıcı

İnternet suçlarıyla mücadelede en önemli unsur belki de bilinçli kullanıcıları yetiştirebilmektir. Bu de yaşama boyu süren eğitim faaliyetleri ile gerçekleşmesi mümkün olan bir durumdur.

Şen'e göre (2003) İnternet ortamında temel sorun; güvenliğin nasıl sağlanacağı bilgisine sahip olmaktan öte, internet aracılığıyla gelebilecek tehlike ve tehditlere karşı duyarsızlık ve bilinçsizliktir. Bilinçlendirme, İnternet'in önemi, İnternet'te bulunan tehlikeler ve bu tehlikelerin sebep olabileceği tehlikelerin

kullanıcılar tarafından bilinmesi sayesinde olabilir. Bu bilinçlenmenin yolu ise "İnternet'teki Risk ve Tehditler" konulu bir eğitim ile mümkün olabilir. Bu eğitimin temel başlıkları şunlardır;

1) Hackerler, lamerlar, crackerlar kimlere denir ve farkları, yetenekleri nelerdir?
2) Sık karşılaşılan bilişim suçları nelerdir ve alana ait mevzuat
3) Dünyadaki ve ülkemizdeki bilişim suçlarından örnekler

Tüm topluma yönelik bilinçlendirme faaliyetleri ise ancak medya organları aracılığıyla mümkün olabilir gözükmektedir.İnternet suçlarının nitelik ve niceliğini azaltmadaki ikinci husus, temel güvenliğin nasıl sağlanabileceğine ilişkin temel teknik eğitimdir. Bu eğitimlerle amaçlanan, evlerin kapı ve pencerelerini kilitlemek ve suç oranını düşürmektir. **"Temel İnternet Güvenliği"** başlıklı eğitimin temel konuları şunlar olmalıdır;

- Fiziksel güvenlik,
- Temel güvenlik açıkları,
- Virüsler, antivirüs programları,
- Şifre seçimi ve şifre koruma,
- Online haberleşme araçları,
- Ağ güvenliği,
- Dosya paylaşma,
- Güvenli e-posta trafiği,
- Casus yazılımlar-spywareler (Şen, 2003).

Polis, görev yaptığı saha olarak genellikle nüfus yoğunluğunun bulunduğu alanda topluma güvenlik ve huzur sağlama görevini üstlenmiştir. Günümüzde suçların çeşitlilik oluşturması ve yeni suç ve suçlu tiplerinin oluşması, suç işlenmesinde giderek artan oranda teknolojik ortamIn kullanılması emniyet birimlerinide bu suçlara karşı daha hazırlıklı olmaya ve bu konuda eğitim gibi, idari yapılanma gibi ve teknik ortam oluşturma gibi çeşitli tedbirler almaya itmiştir.

Adli görevlerini yapan kolluğun, bilişim ortamındaki suçlarla mücadele için suç türlerini tanıması, bu eylemlerin suç teşkil ettiğini, mahiyetini ve ilgili mevzuatı bilmesi gerekir. Bilişim suçları ile etkili bir mücadele için vatandaşların, ailelerin, öğrencilerin, tüm ilgili sektörlerin de Toplum Destekli Polislik Faaliyetleri ile bilinçlendirilmesi önem taşımaktadır.

2.4.2. Toplum Destekli Polislik Faaliyetleri Kapsamında Bilişim Suçları Farkındalık Eğitimi

Toplum Destekli Polislik; güvenlik hizmetlerinin, halkın katılım ve desteğini sağlamak suretiyle etkin ve hızlı bir şekilde yürütülmesini, vatandaş-polis ilişkilerinin geliştirilmesini, suçla mücadelenin güçlendirilmesini ve polislik hizmetlerinin yürütülmesinde çağdaş uygulamaların yaşama geçirilmesini sağlamaktır. Toplumun gönüllülük esasına dayanan desteğini sağlamak ve toplum odaklı hizmet anlayışı içinde, halkın güvenlik hizmetlerinden memnuniyetini artırmak olarak tanımlanmaktadır. Temmuz 2008 itibari ile, Emniyet Teşkilatı'nda 50 İl Emniyet Müdürlüğü'nde Toplum Destekli Polislik Amirliği hizmet vermektedir. Merkez teşkilatı'nda ülkemizin AB'ye üyelik sürecinde, "Toplum Destekli Polislik (TDP) Twinning (Eşleştirme) Projesi" Emniyet Genel Müdürlüğü Asayiş Dairesi Başkanlığı tarafından yürütülmektedir.

Asayiş Dairesi Başkanlığı'nca Mart 2008'de, Toplum Destekli Polislik Büro Amirlerinin katılımıyla verimli bir toplantı gerçekleştirilmiştir. Taşra teşkilatı'nda Toplum Destekli Polislik Amirlikleri, vatandaşlara yönelik başta hırsızlık olmak üzere çeşitli suçlarda bilinçlendirme faaliyetleri yerine getirirken, aynı zamanda kontür dolandırıcılığı, bilişim suçları konuları ve internet kafeler genelgesi gibi hususlarda mağduriyetlerin önlenmesi için yaşanan örnekler ile site, apartman ve mahalle huzur toplantıları, ayrıca okul bilgilendirme toplantıları ile yüz yüze eğitim şekliyle bilgilendirmeler yapmaktadır (Asayiş Daire Başkanlığı, 2008).

Yine, Kocaeli Büyükşehir Belediye Başkanlığı organizasyonu'nda Haziran 2008'de Kocaeli Yöresel Kültürler Fuarı ve Sempozyumu gerçekleştirilmiştir. Kontür dolandırıcılığı, bilişim suçları konuları ve internet

kafeler genelgesi gibi hususlarda bilinçlendirme ve farkındalık düzeyinin artırılarak mağduriyetlerin önlenmesi için Kocaeli Toplum Destekli Polislik Amirliği'nin çalışmaları sempozyumda dinleyicilere aktarılmıştır. Aktarılan 3 konu şu şekildedir.

1. Günlük hayatın vazgeçilmezi İnternet ortamından öğrencilerin, yetişkinlerin dolandırıcılığa uğramaları maddi-manevi zarara girmeleri söz konusu olduğundan bu konuda vatandaşlar bilgilendirilmekte, ayrıca internet kafeler denetlenerek genelgeye uygun hareket etmeleri işletmecilerden ve yararlanıcılardan talep edilmektedir.

2. Günümüzde kontör dolandırıcıları, bir tahkikat veya konuyla ilgili olarak vatandaşları bir sürü telsiz sesinin olduğu bir ortamdan, "polis", "savcı", "hakim" ve "asker" diye aramakta ve maalesef vatandaşlar kendisini arayanın isteği üzerine, işlemlerin yürütülebilmesi için yüklü miktarda kontörü tanımadıkları kişilere göndermektedirler.

3. Cep telefonu aracılığıyla yapılan konuşmalarla dolandırıcılık olayları arttığından, tanınmayan kişilere karşı daha dikkatli davranılması, telefonda ve İnternet'te özel bilgilerin, şifrelerin kimseyle paylaşılmaması ve vakit geçmeden şüpheli durumların güvenlik kuvvetlerine bildirilmesi büyük önem taşımaktadır (Gümüş, 2008).

Gürcan (2007), farkındalık oluşturmada öncelikle "güvenli internet" deniliyorsa kullanıcıların, denetleyicilerin, servis sağlayıcıların "güvensiz internet" de olduğunun farkına varmaları gereklidir, özellikle "farkındalık" (awerness) kavramına bu olgu çerçevesinde yer verilmelidir şeklindeki görüş belirterek farkındalığı artırmada 3 ana değişkeni;

- riskleri anlamak ve mücadele etmek için farklı stratejiler geliştirmek olan güvenlik;
- koruyucu yazılım ve filtreleme programları kullanmak olan emniyet ve
- medyanın gücünü anlayıp etik ve etkili şekilde medyayı yönlendirmek olan okuryazarlık olarak tanımlamıştır.

Bilişim suçlarıyla mücadelede suçun potansiyel muhatabı ve kurbanı olan bilgisayar ve iletişim teknolojilerinin kullanıcıları bu konuda yeterli bilgiye sahip değildirler. Bu konuda bir eğitim çalışması yapılması bilişim suçlarıyla mücadelede çok yararlı olacaktır. Yine bu konuda İnternet servis sağlayıcıları, resmi sivil kurumların, bu suçlara ilişkin gerekli bilgilerin ve mücadele yollarının aktarılası bağlamında üyelerine, kullanıcılarına ve kendilerine İnternet aracılığı ile ulaşacak vatandaşlara sürekli ve düzenli olarak bilgi sunmaları yararlı olacaktır. İnternet kullanıcılarının ve suçun potansiyel mağdurlarının kişisel ve kurumsal verilerin korunmasında mevcut yapı içerisinde neler yapabilecekleri, bu suçlardan nasıl korunacakları konusunda emniyet birimlerinin öncülüğünde eğitim çalışmaları yapılması büyük önem taşımaktadır.

Vatandaşların İnternet ortamında emniyet birimlerine ulaşabilmeleri amacıyla emniyette tüm vatandaşların çok hızlı ve rahat bir şekilde ulaşabilecekleri, şikayette bulunabilecekleri, bilişim suçlarına ilişkin olarak güncel bilgileri takip ederek karşılaştıkları sorunlara cevap alabilecekleri bir İnternet ortamı oluşturulması, polise bu konuda ulaşan vatandaş sayısında önemli bir artış sağlayacaktır. Bilişim suçlarında suçluların yakalanması geleneksel suçlardan farklı olarak çok daha zor olmaktadır. Suçluların yakalanmasında en önemli yol olan ve geleneksel suçlarda “parmak izi v.b.” gibi deliller, bilişim suçlarında “veriler ve bilgiler” olarak ön plana çıkmaktadır.

Sivil toplum kuruluşların yöneticilerinin ve üyelerinin, gönüllülerin, resmi-sivil kurumların ve konunun birebir muhatabı emniyet birimlerinin yerel ve ulusal boyutta ortak katılımlarının sağlanacağı geniş kapsamlı toplum destekli polis faaliyetleri ile bilişim suçlarıyla mücadelede önemli aşamalar kaydedilebilecektir. Emniyet ve diğer kamu kurumları ile sivil toplum kuruluşların birlikte hareket etmeleri daha fazla oranda hedef kitleye ulaşılmasında etkili olacaktır. Halka yönelik olarak emniyet birimlerinin öncülüğünde, sivil toplum kuruluşların da katılımıyla düzenlenecek konferans, paneller, sempozyumlar ile vatandaşlara, internet kullanıcılarına yönelik bilişim güvenliği ve bilişim suçları alanlarında bilinçlendirme imkanı artaya çıkacaktır.

Elazığ Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü'nce, Bilişim Suçları Büro Amirliği tarafından konusu suç teşkil eden PC ve yan ürünleri ile ilgili olarak teknik incelemeler yapılmıştır. Ayrıca, çoğunlukla öğrenciler ve gençlerin yararlandıkları İnternet Kafeler'in mevzuat doğrultusunda hizmet verip vermediklerini kontrol amacıyla denetimler sürdürülmektedir. İnternet Kafeler'in server'larında güvenlik yazılımı bulundurulması gerekmektedir. Bu konularda, İnternet Kafe bilgisayarlarında teknik inceleme yapılmıştır. Suç ortamını asgariye indirmek amacıyla, Bilgi İşlem Şube Müdürlüğü'nce İnternet Kafe işletmecilerine yönelik olarak mevzuatın ve dikkat edilecek hususların değerlendirildiği eğitim toplantıları tertip edilmiştir. Bilgi İşlem Şube Müdürlüğü, Bilişim Suçları Büro Amirliği tarafından korsan cd yapımı ile ilgili olarak Güvenlik Şube Müdürlüğü ile koordineli çalışma yapılmakta ve ilgili bilgisayarlar incelenerek teknik rapor hazırlanmaktadır. Bilişim Suçları konusunda, merkez teşkilatı ile de (Bilgi İşlem Daire Başkanlığı, Kaçakçılık ve Organize Suçlar Daire Başkanlığı) koordineli bir şekilde işlemler yürütülmektedir (Elazığ Emniyet Müdürlüğü, 2002).

Bilişim suçlarıyla mücadelede tüm kamu kurum ve kuruluşlarındaki bireylerin eğitilmeleri, devletin bilişim güvenliğinin sağlanmasında ve e-devlet uygulamalarının sağlıklı bir ortamda yürütülmesinde oldukça önemlidir. Bu amaçla, yapılacak etkinliklerle kamu personelinin bilgisayar, internet ve bu ortamlardaki suçlar konularında eğitilmelerine önem verilmelidir. Kurumlarda bilişim şuurunun eksikliği bir çok bilim adamına göre en önemli problemlerden birisidir. Şen (2007), bilişim suçları uzmanlarından Donn B. Parker'ın "Bilgisayar Güvenliği Yönetimi" isimli kitabında bilişim suçu problemlerinin çözümünü çok net bir şekilde açıkladığını ifade etmektedir.

> "11 yıllık araştırma, danışma hayatım ve tecrübelerimden çıkabilecek tek sonuç, bilgisayar güvenliğinin sadece teknolojik yönünün olmadığı, teknoloji kullanmanın bilgisayar güvenliği için yeterli olmadığıdır. Çözüm, aslında insanların psikolojik ve sosyolojik davranışlarıyla ilgilidir. Dünyanın bir çok yerindeki konferanslarımda ısrarla söylediğim gibi, bilgisayarlar kendi kendilerine hata yapmazlar veya suç işlemezler, aksine sadece insanlar hata yapmaktadırlar. Bu yüzden, bilişim suçu problemine ait çözüm insanlar, davranışları ve tavırları içinde aranmalıdır."

Bilişim suçlarının işlendiği yerlerin başında internet kafe olarak ticari amaçla kurulan işyerleri gelmektedir. Özellikle gençlerin ve öğrencilerin bu makanlardan İnternet erişimi için yararlandıkları ve genel olarak bu kesimin bilişim alanında bilinçsiz olduğu göz önüne alındığında bu mekanların önemi daha da belirgin olarak ortaya çıkmaktadır. İnternet kafe ortamından işlenebilecek bilişim suçlarında, kişilerin herhangi bir kaydının bulunmaması da bu mekanları işleten işletmecilerin sorumluluğunu bir kat daha artırmaktadir. Genelgeler çerçevesinde hareket eden duyarlı bir işletmeci, bilişim suçlarının kendi mekanından işlenmesini önemli ölçüde önleyecektir. Yapılacak yasal düzenlemelerin yanında internet kafe işletmecilerinin eğitilmeleri, bu konuda daha duyarlı ve dikkatli olmalarını sağlayacak ve olası biilişim suçlarının önüne geçilmesinde yarar sağlayacaktır. Bu nedenle, mevzuat düzenlemesinin yapılarak bu mekanları işletecek olan işletmecilerin, Halk Eğitim veya Çıraklık Eğitimi gibi resmi kurumlardan gerekli eğitimi tamamlayarak sertifika almalarının zorunlu hale getirilmesi büyük önem taşımaktadır. İnternet kafe işletmecilerine yasal düzenlemeler vasıtası ile, bilişim alanında suçlarda sorumluluk yüklenmesi, bu suçlarla mücadelede etkililiği artıracaktır. Ancak, temelde önemli olan işletmecilerin bilişim güvenliği ve bilişim suçları alanında gerekli eğitim seviyesine ulaşarak duyarlı olmaları ve bu mekanlardan yararlanan müşterilerine güvenli İnternet hizmeti sunmalarıdır.

Türk Polis Teşkilatı'nın kuruluşunun 157. yıldönümü münasebetiyle "Polisle İlişkilerinizde Rehberiniz" isimli kitapçık, dönemin Emniyet Genel Müdürü Sayın İ.Kemal ÖNAL'ın günümüzde bireyler, aileler, toplumların kullandıkları teknolojiler, anlayışlar sürekli değişiyor ve gelişiyor, ama değişmeyen tek şey dün olduğu gibi bugün de bireylerin ve toplumların entemel ihtiyaçlarından birisi olan GÜVENLİK ihtiyacıdır önsözüyle Araştırma Planlama ve Koordinasyon (APK) Dairesi Başkanlığı yayını olarak Türk vatandaşlarının hizmetine sunulmuştur. Kitapçıkta; polis olma şartlarından, haklarınızı biliyor musunuza, hayat kurtaran trafik kurallarından konut güvenliğine, adli olaylar karşısında izlenecek yol ve yöntemlerden, uyuşturucu konusunda gençlere, anne ve babalara öğütlere, şüpheli paket ve mektuplardan, cinsel tacize kadar bir çok konuda doyurucu bilgiler yer almaktadır (APK Dairesi Başkanlığı, 2002).

Ancak, günlük hayat akışının giderek elektronikleştiği ve dijital dünyanın her yanı sardığı günümüzde, ülkemizde sayıları hızla artan İnternet kafelerden ve klasik suçların neredeyse yerini alan bilişim suçlarından da kitapçıkta bahsedilmesi ile, elbetteki bu konularda öğrencilere, ailelere, tüm vatandaşlara yönelik dikkat çekici bilgi ve önlemler içeren bir yapı kazandıracaktı. Emniyet Teşkilatı personeli ve tüm vatandaşlar için hazıranacak bilişim suçları ile ilgili her kitapçık, broşür ve afişin bu suçların önüne geçilmesinde büyük faydalar getireceği muhakkaktır. Toplum Destekli Polislik hizmetleri çerçevesinde, yüz yüze eğitim şekliyle gerçekleştirilen site, apartman ve mahalle huzur toplantıları, ayrıca okul bilgilendirme toplantılarında bu basılı dökümanların önemli yararlar sağlayacağı düşünülmektedir.

2.4.3. Polisin Suç Öncesinde Bilişim Suçlarıyla Mücadelede Yapması Gerekenler

Bilişim suçları ile mücadele gerçekten de çok zorlu bir iştir. Ancak, hızla yayılan ve zararları etkili olan bu suç türüne karşı ancak bireysel, toplumsal ve hatta sürekli uluslararası işbirliği ile karşı konulabilir. Gerek mali, ve hukuki, gerekse eğitim organizasyonları ve bu konuya yeterli önemin verilmesi ile oluşacak bilinçli ve kararlı mekanizmalar ile bilişim suçlarıyla mücadele edilebilecektir. Beyhan (2003), bilişim suçları ile mücadelede yapılması gerekenleri çeşitli başlıklar altında toplamıştır.

Bilişim suçları ile mücadele konusunda yapılacak idari yapılanma tek başına ihtiyaçlara cevap veremeyecektir. İdari yapılanmanın yanında teknik olarak ihtiyaçlara cevap veren birimler oluşturulmalı, bu birimlerde başta emniyet amiri ve müdürü olmak üzere orta seviye amir ve polis memurları bilgi birikimi ve liyakatlerine göre seçilerek bu birimlerde çalıştırılmalıdır. Şu an itibariyle ülkemizde böyle bir birimin eğitim ihtiyaçlarını karşılaşacak her hangi bir kurum olmadığı için temel eğitimler ülkemizde verildikten sonra bu alanda çalışmaları olan başta A.B.D leri olmak üzere yapılacak ikili anlaşmalarla bu personele teorik ve pratik eğitimin yanında uygulamayı görmek ve öğrendiklerini tatbik edebilmek üzere staj yaptırılarak eğitim ihtiyacı karşılanmalıdır.

Bilişim Suçları olgusu teknolojiyi kullanan ve kullanacak bütün ülkelerin ortak ve öncelikli problemi haline gelmiştir. Bilişim teknolojilerindeki gelişmeler bilgisayar ağları sayesinde milli sınırları aşmış, bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmıştır. Teknolojik gelişmeler ile globalleşen dünyamızda, tüm ülkelerin işbirliği ile bu tip suçlara karşı mücadele etme gereği ortaya çıkmıştır. Bu yüzden Bilişim Suçları konusunda İnterpol, Birleşmiş Milletler ve Avrupa Birliği gibi büyük organizasyonlar tarafından yapılan bir çok çalışma bulunmaktadır. Ayrıca özellikle ABD ve bazı Avrupa ülkeleri kendi bünyelerinde hukuki düzenlemeler ve polisiye yapılanmalarında büyük ilerlemeler göstermiştir.

E-mail yoluyla işlenen (hakaret, tehdit v.s.) bilişim suçlarında yaşanan problemler ise bir hayli fazladır. Ücretsiz mail hizmeti veren servislerden (hotmail, yahoo, dostmail, mynet v.s.) alınan e-maillerin tespiti ise oldukça zor ve hatta imkansızdır. Bunun nedeni ise insanların e-mail adresi alırken, özellikle de bu e-maille suç işlemeyi düşünüyorsa kesinlikle sahte isimler ve adresler kullanmasıdır. Ayrıca bazı internet servis sağlayıcıları internet aboneliği yaparken kişilerin gerçek bilgilerini almamakta, asılsız isim ve adreslerle kayıt yapmaktadırlar. Bu da bahse konu servis sağlayıcılardan abonelik ve e-mail hizmeti alan kişilerin işledikleri suçlarda tespit edilmelerine imkan vermemektedir. Buradan da anlaşılacağı üzere herhangi bir internet kullanıcısı internet abonelik işlemlerini yaptırırken sahte bilgiler verebilmekte ve bununla ilgili herhangi bir yasal yaptırım ve sınırlama bulunmamaktadır.

İnternet kafelerden işlenen suçların önüne geçilmesi için mevzuatta yapılacak değişiklerle internet kafe işleticilerine bir dizi sorumluluk getirilmelidir. Bunlar da; İnternet kafedeki tüm makinaları teknik olarak takip edebilecek bir sistemin kurulması zorunluluğu, kafeden faydalanan insanların kimlik bilgileri, internet erişimi yaptığı tarih, saat bilgileri ve kullandığı bilgisayara kadar kayıtlarının sağlıklı bir şekilde tutulmasının sağlanması, teknolojik sistemler kullanılarak ortamın kameralarla tespiti ve kayıt altına alınması v.b. şeklinde ortaya çıkmaktadır.

Bilişim suçları olgusu hem ülkemizin hem de dünyanın göz ardı edilemez bir gerçeğidir. Bu suçlarla mücadele etmek ve mücadelede başarı sağlamak için tüm kurumlarla birlikte yöntemler geliştirilmeli, belirlenmeli ve uygulanmalıdır. Gerçek hayatta güncel olarak rastlanılan suç tipleri artık dijital ortamda da sıkça görülmektedir. Pornografik ve yasadışı yayınlar, kredi kartı dolandırıcılığı, telif hakları ile korunan bilgisayar yazılımlarının kopyalanması, e-mail yoluyla hakaret ve tehdit v.b. suç tipleri İnternet ve özellikle bilgisayarlar üzerinde yoğun olarak işlenmektedir. Ayrıca yüksek teknoloji suçları, bilinen suç tiplerinden farklılık arz etmektedir. Bu yüzden bu tip suçlara polisler ve suçun soruşturulması esnasında görevli olan herkes daha farklı yaklaşmalıdır. Çünkü elektronik cihazlar, bilgisayarlar ve diğer yüksek teknoloji ürünleri kullanılarak daha kolay ve ucuz suç işlenebilmektedir. Bilişim suçları ile mücadelenin başarıya ulaşabilmesi için personelin eğitimi ve teknik bilgiye sahip olması önemli ve en öncelikli konu olmalıdır. Sonuç olarak Türkiye'nin Bilişim Suçları ile mücadeleye ciddi olarak eğilmesi gerekmektedir.

Emniyet Genel Müdürlüğü; merkez ve taşra teşkilatı bünyesinde kullanılan (Polnet sistemi hariç) bilgisayarlarda, lisanssız işletim sistemlerine, izinsiz çoğaltılmış ofis programlarına ve diğer programlara rastlamak mümkündür. Toplumun genelinde olduğu gibi suç ve suçlularla mücadele etmesi gereken Emniyet Teşkilatı'nın dahi bilişim suçları konusunda yeterince tepkili olmadığını veya bu konuları suç olarak algılamadığı görülmektedir.

Bilişim suçları ile mücadele konusunda ortaya çıkan boşluğu tespit ederek, bu konuda merkez ve taşra teşkilatlarında birimler oluşturan Emniyet Genel Müdürlüğü şu an için toplumun önünde ve önderi konumunda görünmektedir. Ancak oluşturulan birimlerin bilişim suçları ile mücadele edebilmesi için, eğitim ve teknik altyapısının da yeterli olması gerekmektedir. İl Emniyet Müdürlükleri'nde çalışan ve bilişim suçlarında görev yapan çoğu personelin "Bilişim Suçları" konusunda eğitime ihtiyacı olduğundan özellikle taşrada "Bilişim Suçları" ile mücadele güçleşmektedir.

Emniyet Genel Müdürlüğü, bilişim suçları ile mücadeleyi ayrı ayrı birimler halinde bir idari yapılanma ile sürdürmektedir. Bilişim suçları konusunda yapılan çeşitli toplantılarda bazı öneriler geliştirilmiştir.Bunlar şöyle özetlenebilir. Bu suçlarla daha etkin mücadele edebilmek amacıyla ABD'de kurulu olan: Computer Emergency Response Team (CERT) gibi iyi bir şekilde finanse edilmiş "Bilişim Suçları Merkezi" kurulmalıdır. Bu merkezde, teknik ihtiyacı karşılayacak alt birimler oluşturulmalı ve internet vasıtasıyla suç işleyen faillerin tespitini ve suç ile fail arasında illiyet bağını net bir şekilde ortaya koyabilecek teknolojik donanım sağlanmalıdır. Nicelik ve nitelik açısından yeterli ve branşlı personel istihdam edilmelidir. İlgili birimlerde görevlendirilen personelin yurtiçi ve yurtdışı eğitimi sağlanmalıdır. Bilişim suçları konusunda yapılan uluslar arası toplantı, konferans ve eğitime katılım taleplerini karşılamada yeterli bütçe ayrılmalıdır. Bunların yanında diğer bazı öneriler şöyle özetlenebilir.

1. Terör örgütleri lehinde yayın yapan basın, dernek, vakıf ve sivil toplum kuruluşları tarafından internet üzerinde yapılan yayınların geniş kitlelere ulaştırılması yasal açıdan denetimi de zorlaştırmaktadır. Hakkında toplatma veya kapatma kararı verilen yayınlar internet üzerinden yayınlarına devam edebilmektedir.
2. Müstehcen, pornografik ve özellikle de çocuk pornografisine ilişkin cezai müeyyideler caydırıcı bir yaptırıma bağlanmalıdır.
3. İnternet üzerinden yapılan yayınların, Basın Kanunda yapılacak değişiklikle açık bir şekilde bu kanuna dahil edilerek gerekli düzenlemeler yapılmalıdır.
4. Basın ve televizyon yayıncılığını kısıtlayan mevcut yasalar internet ortamında yer alan web sayfalarına uyarlanmalı ve bu konudaki ulusal ve uluslararası yasal düzenlemeler yeniden gözden geçirilmelidir.
5. İnternet'te yer alan verilere ve kişilere ilişkin özel bilgilerin deşifre edilmesi riskine karşı cezai önlem alınmalı ve özel hayatın korunması çerçevesinde tekrar düzenlenmelidir.
6. Uluslar arası alanda internet yolu ile işlenen suçların engellenmesini ve

hatta faillerin iadesini düzenleyen uluslar arası anlaşma yapılmalıdır.

7. İnternet ortamında lisans ve düzenlemeler yoluyla sıkı ve istikrarlı bir denetim mekanizması oluşturulmalıdır.
8. Terörizmin uluslar arası bir problem olduğu, mücadelenin de ancak uluslar arası işbirliğinden geçtiği bilinmeli, bu bağlamda terörizmle mücadele alanında mevcut bulunan uluslar arası anlaşma metinleri bilişim suçları çerçevesinde düzenlenmelidir.
9. Adalet Bakanlığı koordinatörlüğünde, ilgili birimlerin katılımıyla oluşturulacak komisyon çalışmaları ile bilişim suçlarına yönelik yasal bir düzenleme yapılmalıdır.
10. Bilişim sistemine girme, verileri tahrip ve bozma suçu, izinsiz kullanarak haksız yarar sağlama gibi fiiller, ayrıca virüsle sistemlere girerek sistemleri yok etmeye çalışanlar, biraraya gelip sistemlere saldıran, ikiden fazla üyesi bulunan tüm hacker/cracker grupları tebpit edilmeye çalışılmalı, Hacker'lar ile mücadele ve gerektiğinde işbirliği yapılmalıdır.
11. Özellikle bilişim suçları konusunda uzman personel yetiştirilmeli ve gerektiğinde hacker/cracker'larla irtibata geçilerek diyalog kurulmalıdır.
12. Emniyet Genel Müdürlüğü olarak yeni anti-virüs programları geliştirilmeli, kırılması daha zor şifre yazılımları kullanılmalı, elektronik ortamda kişileri ve kurumları gerçek anlamda tanımamıza yarayan e-kimlik ve e-imza gibi yeni teknolojiler geliştirilmelidir.
13. Banka ve kredi kartları ile ilgili dolandırıcılık suçlarında, Bankalar ve Kredi Kartı Merkezleri ile koordineli çalışmalar yapılmalıdır.
14. Bilişim alanındaki suçlar konusunda bu suçların tespiti, delillendirilmesi, insanların bilişim dünyasındaki haklarının korunması amacıyla bu işleri takip edecek hakimlerin, savcıların, polislerin eğitilmesi gerekmektedir. Uluslar arası standartlarda, adli bilişim sertifikasyonlarına sahip "İNTERNET POLİSİ" yetiştirilmelidir.
15. Bilgisayar suçlarında en önemli noktalardan biri; konunun özelliğinden dolayı uluslararası işbirliğidir. Bilişim suçları konusun da İnterpol birimlerinin çalışmalarda bulunması gerekmektedir.

16. İnternet Kafeler de; her türlü bilişim suçlarını işlemeye hazır mekanlar konumundadır. Etkili bir şekilde Bilişim suçları konusun da inceleme yapılmamaktadır. Bu konuda mutlak suretle İnternet Kafeler periyodik olarak denetlenmelidir. Gerekirse, Bilgisayar kullanıcılarının Tarih/Saat, TCKIMLIK NO ve PC NO olarak kaydının tutulması sağlanmalıdır. Kamu ve ülke güvenliğini tehdit edebilecek boyutta işlemler İnternet Kafeler üzerinden de gerçekleşebilmektedir. Tüm kurum, kuruluş ve vatandaşların bu tür siteleri, Emniyet Birimlerine bildirmeleri için medya aracılığıyla bu konuda destek alınmalıdır.
17. Çocuk pornografisi, kumar siteleri vb. konularda web siteleri hassasiyetle incelenmelidir.
18. Bilişim alanındaki suçlar konusunda uluslararası sempozyum, panel, konferanslar düzenlenmelidir.
19. Bilişim alanındaki suçların önlenmesi için, bilişim seferberliği düzenlenmeli ve topyekün bilişim suçlarını önlemek amacıyla bilinçlendirme eğitimleri yapılarak, yaygınlaştırılmalıdır.
20. Bilişim alanındaki suçlar konusunda on-line halk desteği için ortam oluşturulmalıdır

Polis bütün asayişi korumak ve görevlerini başarıyla yapmak için bilişim suçunun nasıl araştırılması gerektiğini ve nasıl önlenebileceğini öğrenmek zorundadır. Suçun yapısından dolayı (çünkü bu tip suçların hedefleri genelde özel şirketlerdir) özel sektörle işbirliği yapılmalıdır. Özel sektörün tecrübesini bu işe yöneltmesi hem kamu hem de toplum için oldukça faydalıdır.

Toplumun bilişim suçunu önemli bir problem olarak görmemesi yeterli kaynak bulunamama sonucunu doğurmaktadır. Kaynak (bütçe ve diğer) sağlayıcılara bilişim suçlarının neler olduklarını ve sonuçlarının neler olabileceğini açık bir şekilde anlatmadan da yeterli miktarda kaynak bulmak mümkün olamayacaktır.

Personeli sürekli eğitim altında tutmak ve onlara gerekli yayınları sunmak kurumları bütçe problemlerine itmektedir. Bir çok kurum bu konulara harcamak

için yeterli ödeneği bulamamaktadır. Fakat, iyi bir planlama ve bazı kaynakları bu yöne aktarmakla bu problem kısmen halledilebilir. Aslında bütçe sıkıntısı, bilişim suçlarının bir çok kurum tarafından etkin bir şekilde mücadele edilmesi gereken bir konu olarak görülmemesinden kaynaklanmaktadır. Üst düzey yöneticilerin bu konuyu çok detaylı bir şekilde değerlendirmeleri gerekmektedir.

Suç öncesinde polise yeterli eğitim (sertifikasyon), donanım ve ünite sağlamak büyük önem taşımaktadır. Toplumun genelinde bilgisayar bilgisi ve ilgisi her geçen gün artmaktadır. Bilgisayarla ilişkisi olan vatandaş sayısı da ilgiye paralel olarak artmaktadır. Bu ilişkide doğal olarak bir kısım yeni ve teknolojik problemleri ortaya çıkartmaktadır. Bütün bunların sonucu olarak polis içerisinde bilgisayar teknolojisi bilgisine ve uzmanlığına olan ihtiyaç da artmaktadır. Problemleri çözebilmek için polis, halktan bu konuda daha bilgili, ilgili ve uzman olmak zorundadır. Polis içinde eğitim bu problemlere en uygun cevap olarak gözükmektedir.

Artık bir çok polis işleminin bilgisayarla yapılmasından ve bilgisayar teknolojisinin çok hızla ilerlemesinden ve değişmesinden dolayı, her bir polis görevlisi düzenli olarak bilgisayar eğitimi almalıdır. Üstelik bu eğitim, bilişim suçlarınının araştırma ve soruşturmasında ayrı bir değer ve önem kazanmaktadır. Polis soruşturmacıları bilgisayarlar, bilgisayar ağları, değişik yazılım paketleri, veritabanları ve elektronik iletişim gübü bir çok konuda bilgi sahibi olmalıdırlar. Eğer bir polis ünitesininin bilgisayar kriminal laboratuvarı varsa, o ünite bilgisayar kriminal analistine veya analistlere sahip olması kaçınılmazdır.

Araştırma yapan personel gerekli ekipmanla techiz edilmelidir. Uygun ekipmanlar ve gerekli araç ve gereçler olmadan iyi bir araştırma yapmak çok zordur. Polis araştırma pesoneline değişik konularla ilgili kitaplar ve bilgisayar bilimi yayınları temin edilmelidir. Bilgisayar bilimi çok dinamik bir bilim olduğundan dolayı, bilgisayar teknolojisi çok hızlı bir şekilde değişmektedir. Mesela, her ay bir çok yeni donanım ve yazılım ortaya çıkmakta ve bilgisayar kullanıcıları arasında yayılmaktadır. Bu gelişmelere yetişebilmek için sürekli eğitim olmak gerekmektedir. Eğitim almanın bir başka yöntemi ise konuyla ilgili

yayınları takip etmektir. Aslında dökümanlar polis araştırma personeline rehberlik etmektedir.

Bilişim suçları ile etkin mücadele için; “Bilgi İşlem” birimlerinin etkinliklerinin arttırılması, sistemlerin ve bilgilerin güvenliğinin sistematik olarak sağlanması gerekmektedir. Kurumsal güvenlik düzeyini arttırmak için güvenlik politikaları ve prosedürlerin belirlenmesi gerekmektedir. Online hizmetler veren kamu kurum veya diğer kuruluşlarda bilişim güvenliğinden sorumlu bilgi işlem yöneticilerinin ve çalışanlarının kurumlarında çalışır vaziyette bulunan bilgisayar ağlarının :

- fiziksel altyapı güvenliğini sağlamalıdırlar,
- güvenlik (firewall) duvarları ile bilgisayar ağlarını korumalıdırlar,
- saldırı tespit sistemleri (internette saldırı tespit sistemleri-intrusion detection technologies for the internet) ile zaman zaman zafiyet taramaları yapmak sureti ile saldırıları çok kısa sürede tespit ederek önlemini almalıdırlar.

Elektronik bir çok işlemin üzerinde döndüğü ve her geçen gün yeni yeni uygulamaların insanlık hizmetine sunulduğu sanal bir dünya olan İnternet’in işlerliğinde İnternet Servis Sağlayıcıların (ISP) da rolü büyüktür.

Bilişim suçlarıyla etkin mücadele edebilme ve suçun önlenmesi, bütünsel bir bakış açısını akla getirmektedir. Suç; her zaman, her yerden, her yaştan ve her eğitim seviyesindeki kişilere, her sisteme yönelik olarak gerçekleşebilecektir. Öyleyse; uzman eğitimli kişiler, yasal mevzuat, yeterli donanım ve teknik altyapı, uluslararası uyum ve işbirliği, basın kuruluşlarının desteği almanın yanı sıra özellikle günün teknolojik tehditlerine göre sürekli olarak bilinçli kullanıcı oluşturma gayreti büyük önem taşımaktadır.

Bilişim suçları ile bilimsel olarak mücadele edilmesi amacıyla, ilk defa 21-22 Ekim 2003 tarihleri arasında ve 14-15 Nisan 2005 tarihleri arasında ikinci kez Polis Bilişim Sempozyumu yapılmıştır. Bu sempozyumda çeşitli üniversitelerden akademisyenler, bilişim firmaları, Adalet Bakanlığı temsilcileri ve Emniyet Teşkilatı mensupları ile P.M.Y.O öğretim görevlileri konuşmacı ve dinleyici olarak katılmışlardır. Sempozyum sonucunda bilişim suçlarının önemi

vurgulanarak, polisin bu konuda alması gereken tedbirler ve atması gereken adımlar ortaya konmuştur.

2.4.4. Bilişim Suçlarıyla Mücadelede Bazı Öneriler ve Alınabilecek Tedbirler

Emniyet Genel Müdürlüğü tarafından, vatandaşlara yönelik olarak web ortamında çeşitli konularda bilgilendirme faaliyeti yapılmaktadır. Aşağıda, bu önerilerden bir bölümü yer almaktadır (Emniyet Genel Müdürlüğü, 2005).

E-mail Adresine Tehdit ve Taciz İçerikli Mesaj Gönderilmesi Durumunda Nereye Müracaat Edilmeli?

Tehdit ve taciz takibi şikayete bağlı suçlardan olduğu için emailinizi header kısmı ile birlikte bir dilekçeye ekleyerek savcılığa müracaat ediniz. Gerekli tahkikat savcılık tarafından yaptırılacaktır.

Kredi Kartı Kullanımında Dikkat Edilecek Hususlar

1- Öncelikle sahip olduğunuz kredi kartını alır almaz şifresini değiştiriniz.

2- Değiştirdiğiniz şifre aritmetik olarak artan veya aynı sayılardan oluşan rakamlar yerine kendinizin kolayca tahmin edileceği bir numara olmalıdır.

3- Kart şifrenizi cüzdanınızda veya kart üzerinde herhangi bir yere kesinlikle yazmayınız.

4- Kart şifrenizi üzerindeki kart numarasını kesinlikle kimseye söylemeyiniz ve göstermeyiniz. Aksi halde kredi kartı bilgilerinizin başka yerlerde başka insanlar tarafından alış verişlerde kullanılması muhtemeldir.

5- Alış veriş yaparken kredi kartınızı Pos cihazından farklı bir cihaza okutturup okutturulmadığına dikkat ediniz, şüphelendiğiniz durumlarda hemen en yakın polis birimine haber veriniz.

6- Bankadan yaptığınız alışverişleri gösteren hesap cetvelini dikkatlice kontrol ediniz. Yapmadığınız alış verişlerde bankaya müracaat ederek olayı bildiriniz ve bu paranın hesabınızdan düşülmesine müsaade etmeyiniz.

7- İnternet üzerinden sıkça alış veriş yapıyorsanız bankadan gönderilen hesap cetvelini kontrol ediniz, sizin kredi kartı bilgilerinizi verdiğiniz sayfa yöneticileri tarafından bu bilgileriniz başka alış verişlerde kullanılabilir.

8- İnternet ortamında alış veriş yaparken bu sitelerin güvenlikli olduğundan emin olunuz. İnternet üzerinden abone yapan ve hizmet veren sayfalardan çok yüksek bir güvenlik sistemi olmadan kesinlikle alış veriş yapmayınız.

9- Bankacılık ve bu tür finans işlemlerini internet üzerinden yaparken bankanın gerekli güvenlik yazılımlarını kullanıp kullanmadığına dikkat ediniz güvenlik yazılımı kullanmayan sitelerden alış veriş yapmayınız ve bankacılık işlemlerini kullanmayınız.

10-İnternet ve telefon bankacılığı sistemlerini kullanırken telefon konuşmanızın dinlenebileceği ortamları kesinlikle kullanmayınız. Şüphelendiğiniz bir durum karşısında hemen banka yetkilileri ve polisle irtibat kurarak gerekli kontrolleri yaptırınız.

Kişisel Olarak Virüslerden ve Bilişim Suçlarından Nasıl Korunulabilir?

1. Bilgisayarınıza lisanslı bir virüs koruma programı mutlaka yükleyiniz. Bu programın virüs güncellemesini yapınız ve makul aralıklarla bilgisayarınızdaki tüm dosyaları virüs kontrolünden geçiriniz.
2. Tanımadığınız diskleri ve CD'leri bilgisayarınıza yüklemeyiniz.
3. Güvenliğinden emin olunmayan internet sitelerinden dosya çekmeyiniz.
4. Çok kritik dosyalarınızı disklere yedekleyiniz ve disklerinizi yazma korumalı hale getiriniz.
5. Kullanmış olduğunuz işletim sistemlerinin açıklarını takip ederek bunların en kısa sürede kapatılmasısnı sağlayınız.
6. Bilgisayarınızda kullandığınız şifrelerinizi kimseyle paylaşmayınız, herhangi bir yere yazmayınız ve tahmin edilmesi kolay şifreler seçmeyiniz.

Kurumsal Olarak Virüslerden ve Bilişim Suçlarından Nasıl Korunulabilir?

1- Kurumların bilgisayar sistemlerinde bulundurdukları bilgiler sınıflandırılmalı ve sınıflandırılan bilgiler neticesinde "Kurumsal Güvenlik Politikaları" belirlenmeli,

2- Oluşturulan güvenlik politikaları çerçevesinde internet ile ilişkili olan veya olması muhtemel bilgiler tespit edilmeli,

3- Tespit edilen bilgiler, güvenlik ihtiyaçlarına uygun olacak nitelikte donanımsal ve yazılımsal güvenlik sistemleri (güvenlik duvarı, anti virus sistemleri, içerik denetim sistemleri vb.) ile koruma altına alınmalı,

4- Kurum Sistem Yöneticileri tarafından yönettikleri sistemlerin özellikleri göz önüne alınarak sistemin açıkları tespit edilmeli ve gerekli yamalar kullanılarak açıkları kapatılmalı, anti virüs sistemleri güncel tutulmalı,

5- Sistem kayıt dosyaları denetlenmeli, yapılabilmesi muhtemel saldırı çeşitleri araştırılmalı ve önleyici tedbirler geliştirilmeli,

6- Kurumlar Bilişim Sistemlerini kuracak, kullanacak, denetleyecek personele yatırım yapmalı ve personel politikaları tekrar gözden geçirilmelidir.

Çocukların İnternet'te Zararlı Sitelere Girememeleri İçin Yapılması Gerekenler

İnternet explorer'ınızın tools menüsünden internet options seçeneğini seçiniz. Karşınıza çıkan ekrandan content menüsünü seçiniz. Karşınıza gelen ekranda Content Advisor menüsünden enable iconuna tıklayın. Karşınıza çıkan ekrandan çocuklarınızın girmesini istemediğiniz sitelerin adreslerini yazarak o sitelere girişi engelleyebilirsiniz (Emniyet Genel Müdürlüğü, 2004).

Elbetteki önerilerin yapılmasının yanı sıra toplumsal bilincin, tüm eğitim aşamalarında yaşam boyu eğitim anlayışı içerisinde eğitim yoluyla artırılmasıyla veba gibi salgın bir halde yayılan bilişim suçlarının önüne geçme imkanı doğacaktır. Aksi takdirde, bilişim suçlarından birey, toplum ve devlet olarak her zaman etkilenmek ve zarara uğramak uzak olmayacaktır.

2.4.5. İnternet Kullanım Etiği

İnternet ortamında, çok büyük bir bilgi bankası bulunmaktadır. Günümüzde bu bilgiler, bireylerin paylaşımına ve kullanımına sunulmuştur. Bu şekliyle paylaşımcılık ve etkileşim artarak devam etmekte ve hızlı değişimler yaşanmaktadır. Allee'e göre de (2000), bilgi kullanıldıkça çoğalır ve bilgiyi paylaşmak tarafların her birinin zenginleşmesini ve bu alışveriş ile kaynaklarını artırmalarını sağlar. İnsanlar bilgiyi beraberce ancak bir güven ve takdir ortamı içerisinde kullanabilir.

Önemli olan sanal, ama aslında gerçek yaşamın kendisi olan İnternet deryasından, etik kurallar çerçevesinde hareket ederek bu bilgi hazinesinden yararlanabilmektir. Bu nedenle ağ üzerindeki her kullanıcının; servisleri, sistemleri kullanmaları konusundaki sorumluluklarını farketmeleri büyük önem taşımaktadır. Kullanıcı, ağdaki her servise ulaştığında yaptığı hareketlerden sorumlu olmak zorundadır.

Ağ'da kötüye kullanım, bir sistemdeki gizli bilgileri hileli yollarla almak, kötü, anlaşılmaz mesajlarla diğerlerini rahatsız etmek, sistemin kaynaklarını kullanıp sistemi yavaşlatmak, ardarda mesajlar postalayarak başkalarının e-posta kutularını doldurmak, ağ üzerinde yasalarla belirlenmiş kuralların dışına çıkmak vb. olarak sayılabilir. Bunun sonucunda, içinde bulunulan ağın durumuna göre, disiplin cezasından işten çıkarılmaya, hesabın silinmesinden hapse kadar kullanıcılar cezalara çarptırılabilir. İnternet'te bazı etik dışı davranışlar şu şekilde özetlenebilir:

- Lisanssız yazılım edinme ve kullanma
- Bilgisayar ortamındaki özel verilere izinsiz erişme
- Başkalarının çalışmalarını kaynak göstermeden kullanma
- Sanal ortamın sağladığı olanakları kullanarak başkalarını rahatsız etme
- Sanal ortamda başkalarının özel verilerine ulaşarak yarar elde etme
- İnternet kafelerde uygunsuz sanal ortamlara girebilme
- Müzik, resim ve film gibi görsel-işitsel materyalleri sahibinin izni olmaksızın kullanma

- İnternet üzerinde yapılan görüşmelerde yanlış bilgi verme
- İnternet üzerinde yapılan görüşmelerde uygunsuz konuşmalar yapma (Gürcan, 2007).

Varol ve Varol'a göre (2001), chat sırasında kullanıcılar yeni sahte kimliklere bürünme ihtiyacı duyabilmektedir. Yapılacak chat; seviyeli oldukları takdirde birliktelik, paylaşım alanları, yeri arkadaşlıklar, yeni kültürleri tanımaya fırsat verecek iken, seviyesiz chat sonucu kavga olayları ve hatta ölüm ile sonuçlanan olaylar olabilmektedir.

İnternet ortamında ister e-mail aracılığıyla, ister web aracılığıyla, isterse diğer on-line chat programları (ıcq, messenger, mirc vb.) mutlaka her zaman İnternet ortamının güzelliğine yakışır kurallar çerçevesinde davranış ve tutumlar sergilenmelidir. Bireylerin, İnternet ortamındaki tutumları ile günlük hayattaki tutumları birbirinden farklı olmamalı ve bu sanal dünyadan etik kurallar çerçevesinde istifade edilmelidir.

Elbetteki bütün kurumlar ve meslek kuruluşları da, bilişim teknolojisinden etkili ve düzenli yararlanabilmek amacıyla herkesçe kabul edilen belli başlı etik kurallara sahip bulunmak durumundadırlar. Bu amaçla, internet ve bilişim etiği konularında yoğun olarak eğitim faaliyetleri düzenlenmesi gerekmektedir. Polisin, suç öncesinde olduğu kadar suç sonrasında da bilişim suçları konusunda aktif bir rol oynaması gerekmektedir. Temel ve uzmanlık seviyesinde tez kapsamında hazırlanan öğretim programlarında yer alan adli bilişim eğitimleri sonunda, bilişim suçları konusunda personelin delillendirme yaparak şüphelileri adli mercilere çıkarma imkanı doğacaktır.

2.5. Suç Sonrası Polisin Bilişim Suçlarıyla Mücadelesi

2.5.1. Adli Bilişim

Adli bilişim, dijital delillerin muhteva ettiği bilgileri; delil inceleme prosedürlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak; delilin

bütünlüğünü koruyarak ve gerçeği açığa çıkarmak amacıyla; kopyalama, belirleme, çözümleme, yorumlama ve belgeleme sürecidir. Adli bilişim böylece,

1. Kopyalama, elde edilen delilin kontamine olmaması için orijinal delilin birebir kopyasının oluşturulmasını,
2. Belirleme, olay yerlerinde bulunan bilişim ile ilintili bulguların tespit edilerek, tüm incelemeler yapılana kadar delil kabul edilmesini,
3. Çözümleme, kopya delil üzerinde, olayla ilgili anahtar kelime gibi mantıksal aramaların yapılmasını,
4. Yorumlama, dijital delil içerisinde bulunan verilerin olayla ilişkisini belirlemeyi,
5. Belgeleme, olay konusu ve bulunan veriler arasındaki ilişkiyi açıklayan rapor yazılmasını kapsamaktadır (Say, 2006).

2.5.2. Bilişim Suçları Araştırma Ekibi Oluşturulması

Shinder'e göre (2002), bilişim suçları araştırma ekibi en az şu kişilerden oluşmalıdır.

Üst düzey operasyon yöneticisi: Bilişim suçlarında olay yerine müdahale konusunda uzman, olay yerinin nasıl çevrilip korunacağını, nerede ve nasıl bir araştırma yöntemi izleyeceklerini planlayan, araştırmadan sorumlu en üst düzey kişidir.

Polis : Olay yerine giriş, olay yerini koruma, ilgili delillerin ve şüphelilerin alınıp gerekli adli işlemlerin yapılmasını sağlar.

Müdahaleci : Olay yerine ilk ulaşan personel, güvenlik görevlisi vb.

Bilişim suçu olay yeri inceleme uzmanları: İlgili delillerin standartlara uygun sekilde bozulmadan toplanıp, aktarılmasını sağlar. Bilişim suçları araştırma ekibi, olay yerinde gerekli bütün işlemleri yaptıktan sonra, elde edilen delilleri bilgisayar adli tıbbı uzmanlarına (Computer Forensic Specialists) iletir.

2.5.3. Bilişim Suçlarında Olay Yeri İncelemesi Yürütülürken Dikkat Edilmesi Gereken Ana Prensipler

Say'ın (2006) ACPO'dan (1999) aktardığına göre, Birleşik Devletler Polis Meslek Grubu, Bilişim Suçlarını Araştırma Ekibi, bilişim suçlarında olay yeri incelemesi yürütülürken dikkat edilmesi gereken ana prensipleri şu şekilde belirtmiştir:

1. Bilgisayar veya diğer ortamlar üzerinde verilerinin değiştirilmesi veya yok edilmesi nedeniyle mahkemeler tarafında kabul edilmeyecek delilller oluşmaması için polis bile olsa yetkisiz kişilerin olay yerine girmesine izin verilmemelidir.
2. Bazı özel durumlarda, orijinal delile erişmek gerekiyorsa, erişecek kişinin konu hakkında ehil ve elektronik delillere gösterilecek ilgi konusunda bilgi sahibi olması gerekir.
3. Üçüncü şahısların delil üzerinde inceleme yapabileceği düşünülerek,delile uygulanan işlemler daha önceden belirlenmiş denetleme prosedürlerine uygun olarak yapılmalı ve yapılan işlemler kayıt altına alınmalıdır.
4. Olay yerinden sorumlu olan uzman, tâbi olduğu kanunlar ve yönetmelikler hakkında bilgi sahibi olmalıdır.

2.5.4. Nelere El Konulması Gerekir?

- Ana Bölüm: Genellikle ekranın ve klavyenin bağlı olduğu kutu
- Ekran, klavye ve mouse (Sadece belirli davalarda gereklidir. Şüphe halinde uzmana danışılması gerekir)
- Bağlantı uçları, kablolar (lead) (Sadece belirli davalarda gereklidir. Şüphe halinde uzmana danışılması gerekir)
- Güç kaynağı ünitesi
- Bilgisayarın içine yerleştirilmemiş hard diskler
- Makinanın arkasına bağlanmış konnektörler (dongle)
- Modemler (Bazıları telefon numaraları ihtiva etmektedir)
- Harici sürücüler ve diğer harici aygıtlar
- Kablosuz ağ kartları

- Dijital kameralar
- Disketler
- Yedekleme kasetleri
- JAZ/ZİP karttuşları
- CD' ler
- DVD' ler
- Bilgisayara bağlı olmayan hard diskler
- PCMCIA kartlar
- Bellek çubukları ve bellek kartları (Berber, 2004: 13).

Ekipmanların incelenmesinde yardımcı olması açısından bilgisayar donanım, yazılım ve el kitaplarının, parola ihtiva edebilecek herhangi bir şeyin, anahtarların müsadere edilmesi; yazıcılara, çıktılara ve yazıcı kağıtlarına eğer forensik inceleme için gerekli ise el konulması gerekir. Bilgisayar donanım, yazılım el kitapları ve kullanma klavuzlarının da bu kapsama dahil edilmesinin abartılı olduğu düşünülebilir. Ancak işlem yapmak ve delilleri incelemek doğrudan bu özel yazılım ve donanımlara ve/veya el kitabında yazılı olan talimatlara olabilir. Bilgisayar teknolojisi son derece hızlı değiştiği için, diğer başka kaynaklardan benzer veya güncelliğini kaybetmiş donanım veya talimatları elde etmek imkansız olabilir (Berber, 2004: 13).

2.5.5. Olay Yerinde Rastlanılması Durumunda Delillere Uygulanacak Prosedürler

Olay yerinde bir bilgisayarın, açık veya kapalı olma durumuna göre uzman personel tarafından dikkat edilecek hususlar aşağıya çıkarılmıştır.

2.5.5.1. Olay Yerindeki Bilgisayarın Kapalı Olması Hali

- Ekipmanların bulunduğu yerin güvenlik altına alınması ve kontrol altında tutulması.
- Yazdırma işlemi yapan yazıcıların bu işlemi bitirmelerini engellememek.
- Olay mahallinde bulunan insanları, bilgisayarlardan ve güç kaynaklarından uzaklaştırmak
- Hiçbir durumda bilgisayarı açmamak.

- Bilgisayarın kapalı olduğundan emin olunuz. Bazı ekran koruyucular bilgisayarın kapalı olduğu izlenimi verebilirler, ancak hard drive ve monitör aktivite ışıkları aygıtın açık olduğuna işaret edebilir.
- Bazı laptop bilgisayarların kapakları açıldığında, çalışmaya başladığını unutmayınız.
- Bataryayı laptop bilgisayardan çıkarın.
- Tüm bileşenlerin fotoğrafını çekin veya kameraya kaydedin. Eğer kamera yoksa sistemin ayrıca bir taslak planını (kroki) çizin.
- Daha sonra bilgisayarı yeniden kolayca kurabilmek için, tüm kablo ve kapıların (port), ekipmanların etiketlenmesi.
- Tüm parçaların işaretlendiğinden ve etiketlendiğinden emin olunuz. Bunu yapmazsanız veya eksik yaparsanız, ekipmanlar adli bilişim uzmanı tarafından reddedilecektir.
- İnceleme yerinde parolaların yazılı olabileceği not defteri, günlük veya herhangi bir kağıt parçası bulunup bulunmadığını araştırınız.
- Kullanıcılara herhangi bir parolanın mevcut olup olmadığını sormayı planlayın, eğer verilirse bunları doğru bir şekilde kaydedin
- Bilgisayar ekipmanları ile ilgili olarak yapılan her hareketi ayrıntılı olarak not edin (Berber, 2004: 11).

2.5.5.2. Olay Yerindeki Bilgisayarın Açık Olması Hali

- Ekipmanların bulunduğu ortamı emniyet altına alın.
- Ortamda bulunan insanları bilgisayarlardan ve güç kaynaklarından uzaklaştırın.
- Eğer varsa, modem bağlantısını kesin
- Eğer bilgisayarın ağ'a bağlı olduğuna inanıyorsanız, incelemeden sorumlu olan kişiden, kurum içi (in-house) adli bilişim analistlerinden veya harici uzmanlardan tavsiyeler alınız.
- Bilgisayarların sahiplerinden/kullanıcılarından tavsiye almayınız.
- Tüm bileşenlerin (bağlantı uçları dahil) bulundukları şekilde fotoğraflarını çekin veya kameraya alın. Eğer kamera yoksa, sistemin bir krokisini

çizin ve bilgisayarı sonradan tekrar kolayca kurabilmek için tüm kabloları ve kapıları (port) etiketleyin.

- Diğer tüm bağlantı kablolarını çıkarın.
- Ekipmanları dikkatlice çıkarın ve her bir ekipmanı numaralandırın. Ana Ünitenin, ekranın, klavyenin ve diğer ekipmanların farklı numaralara sahip olması gerekir.
- Tüm parçaların etiketlerle işaretlendiğinden emin olunuz. Bunun yapılmaması veya yanlış yapılması adli bilişim uzmanı tarafından ekipmanların kabul edilmemesine sebep olabilecektir.
- Ortamda parolaların yazılı olduğu günlük, not defteri veya herhangi bir kağıt parçası bulunup bulunmadığını kontrol edin.
- Kullanıcılara herhangi bir parolanın mevcut olup olmadığını sormayı düşünün, eğer verirlerse bunları doğru bir şekilde kaydedin.
- Bilgisayar ekipmanlarına ilişkin olarak yapılan her hareketi ayrıntılı olarak not edin.
- Ekranda görünen şeylerin fotoğrafını çekin veya ekrandaki şeylerin içeriği hakkında yazılı notlar hazırlayın.
- Klavyeye dokunmayın mouse'ı kliklemeyin ve ekran karamış durumda ise veya bir ekran koruyucu görünüyorsa, incelemeden sorumlu kişiden ekranı tekrar geri yüklemek isteyip istemediklerini sorulmalıdır. Eğer istemiyorsa, mouse' ın kısa süreli olarak hareket ettirilmesi ekranı geri yükleyecektir veya ekran koruyucunun parola korumalı olduğunu gösterecektir. Eğer ekran geri yüklenirse; fotoğraf, kamera veya not alarak içeriğini kaydedin. Eğer parola korumalı yazısı görünürse, mouse' a artık hiç dokunmadan aşağıdaki şekilde hareket edin, Bu durumda zamanı ve mouse' ın kullanımı aktivitesini kaydedin.
- Herhangi bir uzmana ulaşmanız mümkün değilse, hiçbir programı kapatmadan bilgisayarın arkasındaki güç kaynağı kablosunu çıkarın. Bilgisayarın kapatılması eylemi, eğer kaydetme işlemi yapılmamışsa, az miktarda delilin kurtarılamaması anlamına gelebilmektedir (Berber, 2004: 12).

2.5.6. Dijital Deliller ve Özellikleri

Dijital deliller, oldukça yeni bir kavramdır. Dijital deliller hakkında, bilimsel olarak bir çok farklı tanımlamalar mevcuttur. Chisum, (1999) dijital delilleri "bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler" olarak tanımlamıştır.

Casey, (2000) dijital delilleri, bir suçun islendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir iliski sağlayan veriler olarak tanımlamıştır. Shinder (2002) ise dijital delili, bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgiler olarak tarif etmiştir.

Say'ın (2006) Ashcroft'dan (2001) aktardığına göre, Birleşik Devletler Adalet Bakanlığı, Ulusal Adalet Enstitüsü'nün belirlediği dijital delillerin yapısal özellikleri şu şekildedir.

1. DNA ve parmak izi gibi latenttir.
2. Kolaylıkla değiştirilebilir, bozulabilir veya yok edilebilir
3. Dünya çapında bir alana dağılmış olabilir.
4. Zamana bağlı olabilir.

Adli bilişim alanında, bir takım donanım ve yazılımlar kullanılmaktadır. Bu yazılımlar aracılığıyla, personel gerekli inceleme ve araştırma sürecini sürdürebilmektedir.

2.5.7. Adli Bilişim Alanında Kullanılan Gereçler

Adli Bilişimde Kullanılan Yazılımlar

Adli bilişim dalında kullanılan yazılımlar bazen kendilerini has donanım kullanılmasını gerektirirler. Bu tür yazılımlar kullanım sırasında gereken esnekliği azalttıkları için pek tercih edilmezler. Veri kurtarma yazılımları adli bilişimde en çok kullanılan yazılım türüdür. Çünkü genellikle şüpheli delil üzerinde bulunan normal yazılımlar ile görülemeyen silinmiş verileri bu tür yazılımlar ile kurtarmak mümkündür (Say, 2006).

Encase, Encase İle İmaj Alma İşlemi

Adli Bilişim dünyasında en çok kullanılan veri kurtarma yazılımı Encase'dir. Dünya çapında 15,000 araştırmacı tarafından kullanılmaktadır. En büyük 50 bilişim firmasının 40'ı Encase yazılımını aktif olarak çalışanlarının bilgisayarlarında kurulu bulundurmaktadır. Encase yazılımı genellikle kanun kuvvetleri, hükümetler ve kurumsal şirketler tarafından kullanılmaktadır. Dünya ülkelerindeki birçok mahkemeler tarafından resmi veri kurtarma ve raporlama yazılımı olarak kabul görmektedir. Encase yazılımı ile birçok farklı dijital medyanın imajı alınabilir. Bunlardan en sık kullanılan medya türü bilgisayar sabit diskleridir. Günümüzde yüksek kapasitelere sahip olan modern sabit diskler Encase tarafından kolaylıkla imajlanabilmektedir. Adli bilişimde, elektronik delillerin mutlaka kopyaları üzerinde çalışılması gerektiğinden elde edilen delillerin güvenilir bir yöntemle imajlarının alınması gerekmektedir. Encase sahip olduğu özellikler ve doğrulama algoritmaları sayesinde bu görevi profesyonel bir şekilde yerine getirebilmektedir (Say, 2006).

2.5.8. Delillerin Toplanması

Uzunay'ın (2005) IACIS'dan (1999) aktardığına göre, bir bilişim suçu olayının başarılı bir şekilde yargılanması için doğru, kabul edilebilir ve hukukun delil ve delillendirmeye yönelik prosedürlerini izlemek çok büyük önem arz etmektedir. IACIS tarafından dijital delillerin toplanmasına yönelik belirlenmiş standartlar şunlardır:

- Orijinal deliller ilk bulundukları durum ve sartlara benzer sartlarda korunmalıdır.
- Orijinal delillerin bütünlüğünü bozmamak için mümkünse bire bir kopyası alınmalıdır.
- Kopyanın üzerine alınacağı medya "Adli Tıp yönünden steril – Forensically sterile" olmalıdır, yani üzerinde daha önceden herhangi bir data bulunmamalıdır ve virüs ve diğer zararlı kodlara karsı kesinlikle temiz olmalıdır.
- Deliller mutlak suretle etiketlenmeli, korunmalı ve belgelendirilmelidir.
- Adli inceleme esnasındaki bütün basamaklar ve yapılan islemler yazılı hale getirilmelidir.

2.5.9. Delillerin Taşınması

Say'ın (2006) ACPO'dan (1999) aktardığına göre, elde edilen delillerin laboratuara taşınırken her hangi bir zarara uğramamaları için azami gayret gösterilmeli ve her delil için ayrı ayrı aşağıdaki tedbirler alınmalıdır.

Bilgisayar Kasası

- Dikkatli taşınmalıdır.
- Karayolu ile taşınacaksa dik tutulmalı ve sarsıntılara maruz kalmamalıdır.
- Manyetik alanlardan (hoparlör, telsiz, ısı) uzak tutulmalıdır.

Ekran

- Cam kısmı yumuşak bir yere konarak taşınmalıdır.

Sabit Disk

- Manyetik alanlardan uzak tutulmalıdır.
- Anti statik torba, sert kâğıt kesekâğıdı veya hava alan plastik torbalarda taşınması gerekir.

Disket ve Kaset

- Manyetik alanlardan uzak tutulmalıdır.
- Katlamayınız veya bükmeyiniz.
- Disketlerin üzerine etiket yapıştırmayınız.

El Bilgisayarı

- Manyetik alanlardan uzak tutulmalıdır.
- Anti statik torbalarda taşıyınız.

Klavye, Fare ve Kablolar

- Delikli plastik torbalarda taşınabilir.
- Ağır nesnelerin altına koymayınız.

Parmak izi alınacak delillerin korunması

- Elektronik deliller üzerinde yüksek voltaj oluşturduğu ve delillerin zarar görmesine neden olacağından, parmak izi almak için alüminyum tozu kullanılmamalıdır.
- Normal oda şartlarında saklanmalıdır.
- Sıcak, soğuk, nemli veya rutubetli ortamlarda bırakılmamalıdır.

Piller

- Birçok bilgisayar, sistem ayarlarını saklamak için dahili piller kullanırlar. Piller kısa devre edilir veya biterse bu ayarlar yok olacaktır. Pillerin ömürlerinin ne kadar olduğunu anlamak tam olarak mümkün değildir. Modern bilgisayarların pillerinin raf ömürleri ortalama 24 aydır. Bu nedenle modern bilgisayarlardan daha ziyade eski model bilgisayarlara bu konuda dikkat etmek gerekir. Bazı adli kopyalama yazılımları CMOS (Complementary Metal Oxide Semiconductor) ve ROM (Read Only Memory) bilgilerini kopyalayabilmektedir. Eğer bu bilgiler adli bilişim uzmanı tarafından kopyalanırsa bu konuda endişelenmeye gerek kalmaz. Dizüstü bilgisayarlara özel önem verilmelidir. Çünkü bu tür bilgisayarların hem ana pil ünitesi hem de CMOS pil ünitesi vardır.

2.5.10. Belge Hazırlama ve Raporlama (Dokümantasyon)

Say'ın (2006) Maher'dan (2004) aktardığına göre, adli bilgiler eğer düzgün raporlanmaz ve sunulmaz ise değerleri sınırlandırılmış olur. Genellikle bütün raporlarda basitçe; delilin neden incelendiği, nasıl incelendiği ve sonuç bilgileri bulunur. Adli bilişim ekspertiz raporu yazmak, delile uygulanan süreçlerin kaydedilmesini ve daha önceden belirlenmiş olan standartlara uyulmasını gerektirir. Ekspertiz raporu aşağıdaki bilgileri de kapsamalıdır.

1. Olayın detaylarını doğru olarak tanımlamalıdır.
2. Yargı organlarının anlayacağı basitlikte olmalıdır.
3. Yasal inceleme prosedürlerine uygun nitelikte olmalıdır.
4. Cümleler tek anlamlı olmalı, yanlış anlaşılmaya meydan
5. vermemelidir.
6. Cümlelere kolayca referans gösterilebilmelidir. Gerekli yerlerde

7. madde işaretleri ve numaralandırma kullanılmalıdır.
8. Rapor, sonucunu tam olarak kapsayan bilgiyi içermelidir.
9. Gerektiğinde uygun fikirler ve tavsiyeler belirtilmelidir.
10. Tüm raporu özetleyen bir sonuçla bitirilmelidir.

2.6. Bilişim Suçları ile Mücadelede Polis Eğitimi

Tüm dünyada olduğu gibi, bilişim suçlarında başarı ve etkin mücadelenin sağlanması bu suçların çözümünde görev alan polis amir ve memurlarının da eğitimi büyük önem taşımaktadır. Polis, kendisini genel olarak eğittiği, yetiştirdiği ve bilinç artırımını sağladığı ölçüde; bu yeni ve sürekli karmaşıklaşan suç türü ile etkin olarak mücadele edebilecektir.

Maltais (2005)'e göre, teknolojiyle ilgili özelliklerden biri onun sürekli ve inanılmaz hızla evrilmesidir. Uzmanların söylediklerine göre son 30 yılda üretilen bilgi 5000 yıldır üretilen bilgiden çoktur. Yapılan tahminlere göre toplam bilgi birikimi her beş yılda iki kat artmaktadır. Neil Postman'ın belirttiği gibi teknoloji değişikliği bir katkı değildir, ekolojiktir. Yeni teknoloji hiçbir katkıda bulunmamakta, her şeyi değiştirmektedir. İleriye doğru yol aldığımızdan Batı ekonomileri iş gücü yoğunluklu olmaktan bilgi/zihin ağırlıklı olma dönüşümünü sürdüreceklerdir. Güvenlik güçlerinin yeni teknolojilere ayak uydurmaları ve suç işleyenlerin bunları nasıl kullandıkları önemlidir (Maltais, 2005).

Güçlü ve güvenli bir emniyet teşkilatının oluşturulması, güvenlik hizmetlerinin etkili ve verimli bir şekilde sunulması ve polislerin meslek yaşamına kendilerine güvenerek başlamaları ancak iyi bir eğitimin verilmesiyle sağlanacaktır. Çünkü geçmişin polislik anlayışı ve yaklaşımları ile bugünün ve geleceğin güvenlik ihtiyaçlarına ve sorunlarına çözüm bulabilmek güç olacak ya da yanlış çözümler bulunacaktır. Bugünden yarının toplumuna hizmet verebilecek nitelikte polislerin yetiştirilmesini sağlayacak önlemleri alarak, eğitim programlarını çağın değişen ve gelişen koşullarına göre hazırlanmak zorundadır. (Cerrah ve Semiz, 1998, s.10).

Bilişim suçlarıyla mücadele etmek durumunda olan polisin bu alandaki eğitimi, giderek yaygınlaşmakta olan bu yeni ve hızla çoğalan suç türüyle başarılı bir şekilde mücadele edebilmesi ve yetkinlik kazanması amacıyla büyük önem taşımaktadır.

2.6.1. Bilişim Suçlarıyla Mücadelede Polis Eğitiminin Önemi ve Niteliği

Günümüzde insanlık, yeni bir çağın eşiğinde olup hızlı bir değişim ve gelişim içerisindedir. Her alanda bir değişim ve gelişim yaşanmaktadır. Bu nedenle bireylerin bu hızlı gelişim ve değişime ayak uyduracak şekilde eğitilmeleri zorunludur. Toplumda yaşanan bu hızlı değişime polisin de ayak uydurması gerekmektedir. Hızla değişen çevresel koşullar ve toplumsal dinamizm hemen her alanda olduğu gibi polis teşkilatında da daha nitelikli insan gücüne duyulan ihtiyacın artmasına sebep olmaktadır. Polis hizmetlerinde etkililiğin artması için, polisin eğitiminin ve uygulamaların da yeniden düzenlenmesi gerekmektedir. Ayrıca vasıflı, meslek gruplarına göre mesleğinde yetişmiş nitelikli insan gücünün kalkınmadaki yer ve önemi de son derece açıktır.

Çağdaş polis eğitiminde polise bazı roller verilmektedir:

1. Polis, polislik mesleğinin teknik ve uzmanlık gerektiren yönlerini, taktik ve inceliklerini bilen, tekniklerini iyi kullanabilen, iyi atış yapabilen, kamu düzenini temin eden temel “güvenlik mühendisi” dir.
2. Polis, mesleki teknik bilgilerle birlikte, çalıştığı toplumun yapısal özelliklerini, inceliklerini ve duyarlılıklarını iyi kavrayıp bunlara yardımcı olacak, suça yönelimli insanları devlete kazandıracak bir sosyal hizmet uzmanı, sosyal hastalıkları tedavi eden bir sosyologdur. Çünkü günümüzde sosyal olayların çözümünde kaba kuvvetin ve kuralların yerini sosyal ve psikolojik metotlar almaya başlamıştır (Göksu, 2000, s.165).

Polis, görevi gereği toplumdaki huzurun baş koruyucusudur. Adalet, yargı organlarından önce polis tarafından gerçekleştirilir. Çünkü haklının haksızdan,

suçlunun suçsuzdan ayrılması görevi ile sorumlu olan yargı organı bu kararı verirken, polisin kendisine vereceği kanıtlara önemli ölçüde ihtiyaç duyacak ve kararını polisin getirdiği kanıtlar üzerine oturtacaktır. Polisin bu görev bilincine sahip olması ve saygınlık kazanabilmesi, büyük önem taşımaktadır. Polisin bu önemli işlevinin bilincinde olan gelişmiş ülkeler polise çağın bütün olanaklarını tanımış, eğitimine, modernizasyonuna öncelik vermiştir. Günümüzde tüm ülkelerde akılcı ve bilimsel polislik uygulamaları ön plana çıkmış bulunmaktadır. Bilimsel polislik anlayışı çerçevesinde emniyet teşkilatının görevlerini etkin ve verimli bir şekilde gerçekleştirebilmesi, büyük ölçüde polis memurlarının ve amirlerinin çağın gereklerine göre eğitilmesine ve temel polislik eğitiminin sağlıklı bir şekilde verilebilmesine bağlıdır.

Polisin görevleri, günümüzün teknolojik ilerlemeleri ve dolayısıyla teknolojik yeni suç tiplerinin ortaya çıkmasıyla gün geçtikçe artmakta ve zorlaşmakta olup, gelecekte daha da artacaktır. İçinde bulunduğumuz çağ, bu durumlarda dikkate alındığında polisin en iyi şekilde eğitim görmesini gerektirmektedir. Polisler, suçlulardan daha bilgili ve yetenekli olmak zorundadır. Özellikle, bilişim suçları gibi alanların çözümünde ve başarı yakalanmasında polis, bilişim suçlularından bir adım daha önde olmak zorundadır. Geçmişte yaşanmış olan olaylar polisin eğitimine verilmesi gereken önemi daha da artırmıştır. Güvenlik hizmetlerinin kalitesinin artırılması polisin eğitim düzeyinin yüksek olmasına bağlıdır. Genel olarak polisin, bilişim suçları karşısında eğitim faaliyetleri ile yetkin hale gelme çabaları görülmekte ise de, özellikle taşra teşkilatında bilişim suçları gibi yeni ortaya çıkan suç türlerine karşı yetersiz kaldığı görülebilmektedir.

Polis eğitim kurumlarında ve emniyet müdürlüklerinde personelin hizmet içi eğitim programlarının, bilişim suçları da dikkate alınarak düzenlenmesi gerekmektedir. Gelişmiş ülkelerde olduğu gibi ülkemizde de, özellikle genel olarak bilinç eksikliğida göz önüne alındığında bu tür suçlarla karşı karşıya kalma riski bulunmaktadır. Diğer dünya polislerinde olduğu gibi Türk polisinin de, bilişim suçları ve bu suçlarla mücadele alanında yoğun çaba sarfetmesi gerekliliği ortadadır. Polisin, ihtiyaç belirlemesi yapılarak günün koşullarına

uygun eğitim içeriği ile oluşturulmuş temel ve uzmanlık seviyesinde eğitim programları ile yetiştirilmesi gerekmektedir.

Polis eğitim kurumlarında bilgisayar eğitimi uygulamalı olarak bilgisayar labaratuarlarında verilmekte ise de, bilişim suçlarına yönelik olarak müfredat içerisinde her hangi bir düzenleme bulunmamaktadır. Bu durum, çağın gelişen teknolojileri, yeni suç türleri ve adli bilişim alanında personelin verimini olumsuz olarak etkilemektedir. Çağımızın değişen ve gelişen ihtiyaçları doğrultusunda polisin hizmet öncesi mesleki temel eğitiminin yeniden gözden geçirilmesi gerekmektedir.

Bir toplumsal kurumu ya da örgütsel yapıyı oluşturan bireylerin sahip olduğu nitelikler, o kurumun başarı ya da başarısızlığında en belirleyici etmen durumundadır (Cerrah ve Semiz, 1998, s.4). Özellikle toplumla yakın ilişki içerisinde bulunan ve güvenliğin sağlanmasından birinci derecede sorumlu olan polisin rolünün önemli ölçüde değişmesi, polisin mesleki temel eğitimini daha da ön plana çıkarmaktadır.

2.6.2. Bilişim Suçlarıyla Mücadelede Eğitimin Sınıflandırılması

Bilişim alanındaki suç ve suçlularla mücadelenin yakın gelecekte polis için ne kadar önemli bir konu olduğu açıktır. Bunun için özellikle bu suçlarla mücadelede yeterli teknik ve hukuki altyapı, uluslar arası işbirliğinin yanı sıra eğitilmiş personelin önemi büyüktür.

Bilişim suçlarıyla mücadelede etkili olabilmek, başta kolluk ve adliye birimleri olmak üzere oldukça geniş bir çevreyi içine almaktadır. Devlet organları, sivil toplum kuruluşları, internet kafeler, evdeki anne ve tüm vatandaşların bilgisayar ve İnternet eğitimleri almaları ve bu konuda bilinçlenmeleri, bilişim suçları ile mücadelenin şüphesizki ana kaynağı olacaktır.

Bilişim suçları ile mücadelede eğitim 5 başlık halinde incelenebilir.

1. Hizmet Öncesi Polis Eğitimi
2. Hizmet İçi Eğitimde Bilişim Suçları Eğitimi (Temel Eğitim,

Uzmanlık Eğitimi)

3. Bilişim Suçları Güncelleme Eğitimi
4. Bilişim Suçları'nda Uzaktan Eğitim
5. Bilişim Suçları'nda Yurt Dışı Eğitimi

2.6.2.1. Hizmet Öncesi Polis Eğitimi

Günümüzde bilim ve teknoloji alanındaki ilerlemeler baş döndürücü bir hız kazanmıştır. Kişiler ve kurumlar bu ilerleme, gelişme ve yeniliklere ayak uydurmakta zorlanmaktadırlar. Bilişim suçları gibi, çözümü uzmanlık gerektiren suçların önlenmesi ve işlenen suçların tespiti amacıyla, bu tür suçlarla ileride karşılaşacak ve çözümünde uğraş verecek olan polisin hizmet öncesi yeterli bilgisayar eğitimi alması büyük önem taşımaktadır. Emniyet Teşkilatı bünyesinde, eğitim kurumlarında bulunan bilgisayar sınıfları Tablo 4'te görüldüğü gibidir (Eğitim Daire Başkanlığı, 2008).

Tablo 4: Eğitim Kurumlarında Bulunan Bilgisayar Sınıfları

EĞİTİM KURUMU	SINIF SAYISI
POLİS AKADEMİSİ	4
POLİS KOLEJLERİ	6
PMYO	38
POMEM	16
TOPLAM	**64**

Emniyet teşkilatında ki eğitim yapısı incelendiğinde, Türk polis teşkilatının mevcut amir kaynağı Polis Koleji ve devamı olan Polis Akademisi olduğu görülmektedir. Teşkilatın memur kaynağı ise çeşitli illerde bulunan Polis Meslek Yüksek Okulları (PMYO) ve Polis Meslek Eğitim Merkezleri (POMEM) dir.

Özellikle, Polis Meslek Yüksek Okulu'ndaki iki yıllık sürede, polis memuru adaylarına bilişim alanındaki verilecek olan eğitimin, daha sonraki meslek hayatlarında bilişim suçları ile mücadelede önemli bir yeri olduğu düşünülmektedir. Yakın gelecekte bilişim suçları ile mücadele polisin görev alanında önemli yer tutacağı gerçeğinden yola çıkarak, polisin temel eğitiminde, bilişim ve Internet suçları konusunda polis memuru adaylarının yeterli derecede bilinçlendirilmesi gerekir. Bu nedenle gerekli program geliştirme faaliyetleri ile ilgili olarak reorganizasyona gidilmesi gerekmektedir. Bilişim Suçları ile etkili mücadele için, şu sorulara cevap bulunması gereklidir.

1) Bilişim Suçları ile etkili mücadele için polis, bu konuya önem vermekte midir?
2) Bilişim Suçları ile etkili mücadele için polis, gerekli inceleme birimleri ve ünitelerini kurmuş mudur?
3) Bilişim Suçları ile etkili mücadele için polis, kurmuş oldukları merkezlerde etkili eğitim faaliyetleri gerçekleştirebilmekte midir?
4) Bilişim Suçları ile etkili mücadele için polis, vatandaşa yönelik önleyici tedbirler almakta mıdır?
5) Bilişim Suçları ile etkili mücadele için Akademi/Polis Meslek Yüksek Okullarında verilen Bilgisayar eğitimi yeterli midir?
6) Bilişim Suçları ile etkili mücadele için Akademi/Polis Meslek Yüksek Okullarında bilgisayar eğitimi veren eğitici personelin yeterlikleri istenen düzeyde midir?
7) Bilişim Suçları ile etkili mücadele için Akademi/Polis Meslek Yüksek Okullarında bilgisayar eğitimi için fiziki ortam ve personel yeterli midir?
8) Bilişim Suçları ile etkili mücadele için polisin uzmanlaşması sağlanmakta mıdır?
9) Bilişim Suçları ile etkili mücadele edecek polisin seçimi nasıl gerçekleştirilmektedir?
10) Bilişim Suçları ile etkili mücadele edecek polisin hizmetiçi eğitimleri yeterli midir?
11) Bilişim Suçları ile etkili mücadele edecek polisin uzmanlık eğitimden geçirilmesi gerçekleştirilmekte midir?

12) Bilişim Suçları ile etkili mücadele edecek polis yurtdışındaki bilişim suçları mücadele tekniklerini izleyebilmekte midir?
13) Bilişim Suçları ile etkili mücadele edecek polis, bilimsel ve akademik yayın ve sempozyumları takip edebilymekte midir?
14) Bilişim Suçları ile etkili mücadele kapsamında tüm polislerin genel PC temel eğitim düzeyi nasıldır? PC Eğitim seviyeleri yükseltilebilmekte midir?
15) Bilişim Suçları ile etkili mücadele için polisin üniversite, Telekom, ISS ve ilgili çevrelerle diyaloğu tesis edilmiş midir?
16) Bilişim Suçları ile etkili mücadele için polisin uluslararası işbirliği ve etkileşimi sağlanmakta mıdır? (Karaman, 2003).

Vatandaşların günlük hayatta Internet'i kullanma oranı çeşitli ülkelerde Türkiye'ye göre yüksek olmakla beraber, Türkiye'de bu alanda hızlı bir artış olduğu görülmektedir. Bunun için polisin temel eğitiminde en azında bilgisayar, Internet ve Internet suçları konusunda temel bilgiler verilmesi çağdaş polis eğitimi açısından oldukça yerinde olacağı düşünülmektedir. 9 Mayıs 2001 tarihli 4652 sayılı Polis Yüksek Öğretim Kanunu ile polis memurlarının temel eğitimi iki yıla çıkarılmış ve daha önce olmayan bazı dersler programda yerini almıştır. Bu derslerden birisi de bilgisayar dersidir. Bilgisayar dersi, iki yıl içinde Mesleki Teknik Yazışma ve Bilgisayar adı altında sadece iki saat olarak verilmektedir. Ayrıca bu dersi veren kişiler genellikle. alt rütbedeki (Komiser yardımcısı, komiser) kişiler olmaktadır. Bu derste genelde bilgisayar kullanımı öğretilmeye çalışılmaktadır. Bilişim suçları konusunda bir bilgi verilmemektedir (Karaman, 2003).

PMYO'larında bilişim suçlarının eğitimi ile ilgili diğer çarpıcı bir eksiklik de, ikinci sınıflarda okutulan polisin görev ve yetkileri ve polis etiği kitabında kısada olsa bilişim suçlarına yer verilmesine rağmen, Müfredat programda bilişim suçlarına yer verilmemiştir. Emniyet teşkilatının memur ihtiyacını karşılayacak olan personeli yetiştiren eğitim kurumu olan PMYO'larında bugünün ve yakın gelecekte polisin en önemli suç mücadele alanlarından birisi de bilişim suçlarıdır. Bu alanındaki suç ve suçlularla daha başarılı ve çağdaş

olarak mücadele edebilmek için yapılması gerekenler konu başlıkları ile şu şekilde sıralanabilir.

1) PMYO'larında verilen bilgisayar dersleri, iki yıl süre ile mesleki teknik yazışma dersinden ayrı olarak verilmesi gerekir.
2) Bilgisayar derslerini verecek olan eğitimciler, bilgisayar ve bilişim suçları konusunda uzman kişilerin olması gerekir.
3) PMYO'larında kitaplar ve müfredat program bir birinden farklı olmamalı. Müfredat programlarda bilişim suçları ve mücadele yöntemleri konusunda bilgi verilmelidir.
4) PMYO'larında bilgisayar sınıfları İnternet'e bağlı olmalı, polis memuru adaylarına Internet kullanma imkanı sağlanmalıdır. Bazı okullardaki polis memuru adaylarının dışarıda Internet kullanmaları disiplin suçu sayılmamalıdır.
5) PMYO'larında kişi başına düşen Internet sayısı her okulda farklı farklı olmaktadır. Bu sayının PMYO'larında eşit şekilde dağıtılması gerekir. PMYO'larında ortalama kişi başına düşen bilgisayar sayısı 100 polis memuru adayına 5,81 bilgisayar düşmektedir. Bu sayının imkanlar elverdiği ölçüde artırılması gerekir.
6) PMYO'larında öğrenmeyi kolaylaştırmak için bilgisayar destekli işitsel ve görsel eğitime ağırlık verilmelidir.
7) İnternet üzerinden yasa ve ahlak dışı yayınların yapıldığı, kredi kartları üzerinden sahte kimlikle alışverişlerin yapıldığı, ülke güvenliğini tehdit eden ve toplumun ahlak kurallarına uymayan web sayfalarının artığı, yasa dışı terör örgütlerinin ve organize suç şebekelerinin haberleşme aracı olarak kullanıldığı Internet, polisin de en az bu kullanıcılar kadar bilmelidir ki bunlarla mücadele edebilsin. Özellikle bu alandaki temel bilgiler PMYO'larında yeterli seviyede verilmesi gerekir (Karaman, 2003).

2.6.2.2. Hizmet İçi Eğitimde Bilişim Suçları Eğitimi

Polisin mesleki eğitiminde önemli olan, toplumun güvenlik ihtiyaçlarının karşılanması amacıyla güvenlik hizmetlerine ilişkin bilgi, beceri ve pratik uygulama yetenekleri kazandırmak suretiyle personelde fiziksel, duygusal, sosyal, ekonomik ve teknolojik gelişmelerin sağlanması sürecinin devamlılığıdır. Hizmet içi eğitim her meslek için geçerlidir. Ancak, kamunun düzenini sağlayan

ve koruyan polisler için hizmet içi eğitimin ayrı bir önemi ve yeri vardır. Çünkü, bir ülkede demokratik hukuk devleti ilkelerinin işlemesinde, kamu düzeni, iç huzur ve güvenliğin sağlanmasında ve bunun devamının tesis edilmesinde Emniyet Teşkilatı görevlileri önemli görevler üstlenmektedirler. İşte bu görevlerinin yerine getirilmesi amacıyla Emniyet Teşkilatı personelinin çağın gelişme ve değişmelerine adapte olarak, hukuk devleti ilkelerine bağlı, insan haklarına saygılı, polis-halk ilişkilerinde güçlü, bilgi ve becerilerini sürekli yenileyen bilgili ve kültürlü bireylerden oluşması için etkin ve verimli hizmet içi eğitim faaliyetleri belirli periyodik aralıklarla gerçekleştirilmektedir. Hizmet içi eğitiminin sağladığı yararları kurumsal ve bireysel yararlar olmak üzere iki kategoride toplanabilir (Taymaz, 1981: s.15).

Kurumsal Yararlar ;

- Hizmetin kalitesi ve verimlilik artışı sağlanır.
- Kurumun kendisini yenilemesi kolaylaşır.
- Yenilik ve gelişmelere kolaylıkla uyulur.
- İş güvenliği sağlanır, iş kazaları azalır.
- Amortisman, bakım ve onarım giderleri azalır.
- Kurum, hizmet ettiği toplumda saygınlık kazanır.
- Kurumda iletişim ve ilişkilerin sağlanması kolaylaşır.
- Üst kademe veya alanlara personel hazırlanır.
- Personel arası anlaşmazlıklar ve disiplin sorunları azalır.
- Personelin işinden ve başkalarından şikayeti eksilir.

Bireysel Yararlar ;

- Bireyin işinde güven duygusu gelişir.
- Bireyin morali yükselir, huzurlu çalışma sağlanır.
- Hizmet içinde kurumda yükselme olasılığı artar.
- Bireyin işinde memnuniyetsizliği azalır.
- İş yerinde insan ilişkilerinde gelişme olur.
- İş arkadaşları arasında iletişim daha kolaylaşır.
- Geleceğe daha güven ve ümitle bakılır.
- Kurum içinde ve dışında saygınlık kazanılır.

- Öğrenme yolu ile bireysel doyum sağlanır.
- İşinde sınama-yanılma süresi kısalır.
- Birey işinde isteklenir ve güdülenir.
- Rahat ve emin iş yapma olanağı sağlanır.

Bilim ve teknikte yaşanan hızlı gelişmeler sosyal, iktisadi ve kültürel sahalarda değişmelere yol açmaktadır. Bu değişmeler nedeniyle bireylerin öğrenmesi gereken bilgi ve becerilerde de büyük artışlar olmuştur. Bu bilgileri yalnızca örgün eğitim sistemi ile bireye kazandırmak mümkün olmamaktadır. Bu nedenle, çeşitli eğitim kademelerinden geçerek meslek hayatına başlayan bireylerin öğrenim sıralarında edindiği bilgi ve becerilerin eksikliği ile yeni değişiklikler ve bu bilgilerin meslek alanlarında yetersiz kalmaları sebebiyle bireylerin hizmet içi eğitim faaliyetleri ile yaşam boyunca eğitilmeleri zorunluluk arz etmektedir.

Tüm kamu ve özel sektör kuruluşlarında olduğu gibi Emniyet Teşkilatı'nda da hizmetlerin daha etkin, seri ve verimli hale getirilmesi ancak çağdaş bilişim teknolojilerinden yararlanarak, bilgi çağı toplumunda gelişen ve değişen bilgileri güncel olarak takip etmek ile olasıdır. Toplumun bireylerine güvenlik hizmeti sunan Emniyet Teşkilatı Mensuplarının bilgiye daha da açık ve üretken hale getirilebilmesi ancak en üst seviyede eğitimli ve bilgili personel ile mümkündür. Kişilerin bilgilerini artırmak, becerilerini geliştirmek, davranışlarına olumlu bir yön vererek örgütsel verimliliği artırmak, hizmet içi eğitimle sağlanabilir.

Yaşadığımız çağ, hızla gelişmekte olan bilim ve teknolojinin yarattığı köklü aşamalara sahne olmaktadır. Bu değişimin doğal bir sonucu olarak toplumsal kurumların yapılarında ve modern insanın yaşantısında da büyük değişmeler olmuştur. Bu sürekli değişen ve gelişen ortamda, toplumun düzen ve güvenliğini bozan suçların izlenme yöntemi de değişmiş, emniyet teşkilatına doğrudan görev veren yasaların dışında, burada sayılamayacak kadar birçok yasa polise çeşitli ve ek görevler yüklemiştir.

Bu koşullar altında, Türk toplumunun düzen ve güvenliğinin sağlanması ve sürdürülmesi, bu görevleri yerine getirebilecek güce sahip ve nitelikte eğitilmiş personelle mümkün olabilir. Bunun için, eğitim çalışmaları "... kurs, seminer, panel, forum gibi değişik tekniklerin kullanılması ile ve çoğu zaman da iş başında sürüp gider (Kalkandelen, 1979) gerçeğinden hareketle bilişim suçları ile etkili mücadele için, organizasyonlu hizmet içi eğitim programları ile sürekli eğitim faaliyetleri düzenlenmelidir.

Meslek öncesi eğitimde bireyin kazanmış olduğu bilgi ve beceriler, alanlarındaki değişme ve gelişmeler karşısında yetersiz kalmaktadır. Bu yetersizliğin ortadan kaldırılması hizmet üretiminde istenilen verimin sağlanmasında en büyük rolü üstlenen bireyin istenilen niteliklere sahip olabilmesi eğitimin sürekliliği ile elde edilir. Bireylere mesleklerindeki yenilikler ve gelişmeler hizmet içi eğitim yolu ile kazandırılabilecektir. Emniyet Teşkilatı bünyesinde, Türkiye genelinde (merkez, taşra, okullar) bulunan bilgisayar sınıfları Tablo 5'deki gibidir (Eğitim Daire Başkanlığı, 2008).

Tablo 5: Türkiye Geneli Bilgisayar Sınıfları

YER	**SINIF SAYISI**
MERKEZ	3
İLLER	35
OKULLAR	64
TOPLAM	**102**

Emniyet Genel Müdürlüğü, Bilgi İşlem Daire Başkanlığı hizmet içi eğitim kapsamında sürekli olarak amir ve memur personele yönelik olarak bilgisayar kursları düzenlemektedir Hizmet içi eğitim kapsamında belirlenmiş olan müfredat standartları şu şekildedir: PC Temel Eğitimi (Windows XP, Word 2003, Excel 2003, İnternet), Web Tasarım Eğitimi, Ms Access Eğitimi, Visual Basic. Ayrıca, bilgisayar kullanmayı bilmeyen bir personelin, istediği bilgiye

ulaşamayacağı ve dolayasıyla bilgiden yararlanamayacağı gerçeğinden hareketle, polisin etkin ve verimli bilgisayar kullanımını sağlamak amacıyla ülke genelinde polis bilgisayar eğitimi ve okur-yazarlığı kampanyası düzenlenmiştir.

Tablo 6'da 2007 yılı bölge merkezleri eğitim durumu yer almaktadır (Eğitim Daire Başkanlığı, 2008).

Tablo 6: 2007 Yılı Bölge Merkezleri Eğitim Durumu

2007 YILI BÖLGE MERKEZLERİ EĞİTİM DURUMU					
BÖLGE MERKEZİ	**GENEL TOPLAM**				
	KURS SAYISI	**KURS SAATİ**	**KURSİYER SAYISI**		
			AMİR	**MEMUR**	**TOPLAM**
ADANA	43	892	5	667	672
ANKARA	11	340	3	112	115
ANTALYA	7	270	1	169	170
BURSA	13	349	6	99	134
DİYARBAKIR	42	337	200	287	487
ERZURUM	17	464	3	283	259
İSTANBUL	67	399	1	2195	2196
İZMİR	19	66		458	458
SAMSUN	41	2034	3	466	469
VAN	15	405		193	193
GENEL TOPLAM	275	5496	222	4902	**5.153**

Emniyet Genel Müdürlüğü Bilgi İşlem Daire Başkanlığı 10 adet bölge merkezi ile; yani her bölge ili, civarındaki illere hizmet götürme yöntemiyle tüm teşkilata yönelik çalışmalarını yürütmekte ve eğitim faaliyetlerini devam ettirmektedir. Adli bilişim alanında da, özellikle KOM Daire Başkanlığı belirlenen bölge merkezleri ile, bilişim suçları eğitimlerini belirlenen illere yönelik olarak sürdürmektedir.

Emniyet Teşkilatı personelinin, Eylül 1997 ve Mayıs 2008 arasındaki tarihlerdeki kursiyer sayıları Tablo 7'de yer almaktadır. Yaklaşık 90000 personelin, çeşitli alanlarda bilgisayar kursu görmeleri Emniyet Teşkilatı adına

oldukça güzel bir neticedir. Sürekli hizmet içi eğitim faaliyetlerinde bulunan teşkilat personeli, bilişim suçları alanında da etkili bir şekilde mücadele edebilecektir (Eğitim Daire Başkanlığı, 2008).

Tablo 7: 1997(Eylül) ile 2008 (Mayıs) Arasında Toplam Kurs Gören Personel Sayısı

TOPLAM KURS GÖREN PERSONEL SAYISI			
	1997(Eylül) - 2007	2008 (Mayıs)	TOPLAM
KURS YERİ	KURSİYER SAYISI		
MERKEZ	12.002	520	12.522
BÖLGE MERKEZLERİ	74.160	1.660	75.820
FİRMALAR	1.357	0	1.357
GENEL TOPLAM	87.519	2.180	89.699

Bilişim suçlarının yasal manada takibini yapan emniyet birimlerinin bu konuda özel bir eğitim almaları ve uzmanlaşmaları gerekmektedir. Halkın huzur ve güvenliğinin teminatı olan Polis Teşkilatı'nın verimlilik ve etkinliğinin artırılması, dünyada gelişen teknolojik yenilik ve imkanların yakından takip edilerek en üst seviyede kullanımı ile mümkün olacaktır. Günümüzde suçluların bile, genel olarak teknolojik imkanlardan yararlanarak amaçlarına ulaştıkları gerçeği, polis için teknolojinin önemini daha da artırmaktadır. Güvenlik örgütleri, teknolojinin getirdiği olanaklardan en çok yararlanabilecek birimlerin başında gelmektedir.

Karaman'ın (2003) Robinson'dan (2000) aktardığına göre, bugün polisin bilişim suçları ile mücadele edebilmesi için, bu alanda iyi eğitilmiş personel ve son model bilgisayarlara (hardware) ve programlarına (software) sahip sistemlere ihtiyaç duyulmaktadır. Bunun için, başta ABD olmak üzere bilişim

suçları ile mücadele edecek personelin eğitimi üzerinde önemle durulmaktadır. Fakat bilişim suçları ile mücadele edecek personelin eğitimi oldukça teknik bir alanı gerektirdiği için maliyeti de yüksek olmaktadır. Yine, Karaman'ın (2003) Mccaul'dan (2001) aktardığına göre, Amerika'da Teksas eyaletinde bilgisayar suçları ile ilgili olarak polis memurlarına verilen eğitimin kişi başına maliyeti 35 bin $ 'dır. Bu şekilde ileri teknoloji eğitimi almış personel çok yüksek para teklifi ile özel sektörde iş imkanı bulabilmektedir (Karaman, 2003).

Bir kaç yıl sonra bu şekilde ileri teknoloji eğitimi almış olan kişiler özel sektöre kayabilmektedir. Bu sorun sadece ABD'de değil diğer ülkelerle beraber aynı şekilde Türkiye'de de Emniyet Teşkilatında da yaşanmaktadır. Bu şekilde ileri teknoloji eğitimi almış personelin çalışma şartları ve ücret sistemi dışarıdaki şartlara göre uyumlu hale getirilmesi personelin verimli çalışma açısında önemli bir konudur.

Polisin temel eğitiminde diğer dünya ülkelerinde de ciddi anlamda bilişim suçları ile ilgili eğitim verildiği görülmemektedir. Çünkü bu alan oldukça özel bir alan olmakta ve teknolojik altyapı bilgilerine sahip olmak gerekmektedir.

Hizmet içi eğitim kapsamında aşağıdaki amaçlar doğrultusunda, bilişim suçları eğitimi gerçekleştirilmesi gereklidir.

1. Adli ve kolluk çevrelerinin görüşlerine göre bilişim suçları ve suçluları konusunda sınıflandırma var mıdır, yeterli midir?
2. Emniyet Teşkilatı'nda ki ilgili birimlere göre bilişim suçlarıyla mücadele aşamaları, saldırı yöntemleri ve saldırı tespit yöntemleri nelerden oluşmaktadır? Ayrıca, suç teşkil eden olayların delillendirme süreci nasıl gerçekleştirilmektedir?
3. Emniyet Teşkilatı'nda ki ilgili birimlere göre, bilişim suçlarıyla mücadelede yaşanan problemler, yapılması gerekenler ve çözüm yöntemleri nelerdir?

4. Baro ve adli çevrelere göre bilişim suçları ve mevcut hukuk değerlendirmesi nasıldır? Polisin, bilişim suçlarıyla mücadelede başarısı için yapılması gereken hukuki ve yasal düzenlemeler nasıl olmalıdır?
5. Emniyet Teşkilatı'nda ki ilgili birimlerde bilişim suçları konusunda teknik altyapı ve donanım tesis edilmiş midir?
6. Kamunun, internet kafe işletmecilerinin, adli birimlerin ve halkın bilişim suçlarıyla mücadelede aktif tutulmasını sağlamak için hangi düzenlemelerin yapılması gerekmektedir?
7. Bilişim suçlarıyla ilgili suç analizi tespiti için güncel istatistiki verilerin, suç haritalarının elde edilebileceği bir organizasyon oluşturulmuş mudur?
8. Bilişim suçları ile etkin mücadele yapılabilmesi amacıyla, toplumun tüm kesimine yönelik olarak bilişim şuurunun gelişmesine katkıda bulunacak düzenleme ve faaliyetler yapılmakta mıdır?
9. Uluslararası platformda ve bazı ülkelerde bilişim suçları konusunda yapılan çalışmalar ve geliştirilen eğitim programları hangi düzeydedir?
10. Emniyet Teşkilatı ilgili personellerine göre, bilişim suçları ile mücadelede Emniyet Teşkilatı içerisinde idari yapılanma ve organizasyon yeterli midir?
11. Bilişim suçları ile mücadelede polis amir ve memurlarının teknik yönden eğitimi yeterli midir?
12. Bilişim suçları konusunda ilgili birim ve çevrelerin görüşlerine göre polisin eğitimine dönük bir eğitim programı geliştirilmiş midir? Yeterli midir?

Emniyet birimlerinin eğitimi, suçlarla mücadelede ve suçluların yakalanmasında bilgisayar sistemlerini ve ileri teknoloji ürünlerini çok iyi derecede kullanarak, kaybı çok kolay olan suç kanıtlarına ve suçlulara hızlı ulaşılmasını sağlayacaktır. Bu amaçla, Emniyet Genel Müdürlüğü tarafından uzman personel yetiştirilmesi amacıyla TADOC merkezi açılmış ve TADOC bünyesinde Bilişim Suçları Araştırma Merkezi kurulmuştur. Burada, özellikle

Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlar Daire Başkanlığı organizasyonunda, uzman personel yetiştirmek amacıyla eğitim programları düzenlenerek uzmanlık eğitimi eğitim faaliyetleri gerçekleştirilmektedir. “Bilişim Suçları Eğitimi Temel Seviyede Personel Yetiştirme Kursu” programı, günde 6 saat olmak üzere toplam 90 saat süresince (3 haftalık) eğitim boyunca uygun personele verilmektedir (Ek-9).

Yine, bilişim suçları konusunda Emniyet Teşkilatı’nın genel olarak başarılı olabilmesi için, ülke genelindeki tüm personele yönelik olarak temel eğitim seviyesinde bilgi verilmesi gerekmektedir. Böylece, polisin bilişim suçlarına aşinalığı ve farkındalık düzeyi artırılarak, bu suçlarla etkili bir şekilde mücadele etme imkanı doğacaktır. Araştırma kapsamında, konu alanı uzmanlarının da görüşleri alınarak hazırlanan “Bilişim Suçları Eğitimi Uzman Seviyede Personel Yetiştirme Kursu” programı, günde 6 saat olmak üzere toplam 600 saat süresince (5 aylık) eğitim boyunca uygun personele verilecektir (Ek-10).

Bu amaçla, İl Emniyet Müdürlüklerinin hepsinde günün teknolojisine uygun bilgisayar ve adli bilişim laboratuarlarının kurulması gerekmektedir. Ayrıca, bilgisayar laboratuarlarındaki kurslarda eğitimci olarak görev alacak kişilerin, hem teknik konularda bil1gisayar eğitimleri hem de eğitimin etkililiğini artırmada bilişim suçları eğiticilerinin eğitimi kursundan geçirilmesi önem taşımaktadır.

2.6.2.3. Bilişim Suçları Güncelleme Eğitimi

Bilişim suçlarıyla mücadelede bilgilerin güncellenmesi büyük önem taşımaktadır. Düzenlenecek sürekli eğitim faaliyetleri ile uygun personele, uygun eğitim verilmesi ve mevcut yeni su türü ve risklere karşı on-line ortamda eğitimlerin düzenlenmesi, tüm teşkilatta bilişim suçlarında görev yapan personele büyük faydalar sağlayacaktır. Aynı zamanda, bilişim suçları, tüm dünyayı giderek tehdit eden bir yapı içerdiğinden dolayı, ülkeler bu konuda uluslar arası işbirliği gerçekleştirme yönünde çaba sarf etmektedir. Uluslar arası arenada, bilişim suçlarında birlikte eğitim faaliyetleri yapılabildiği ve bu suçlarla mücadelede gerekli işbirliği ortamı (mevzuat, antlaşmalar, teknik yardımlaşma)

sağlanabildiği takdirde, bilişim suçları yönüyle doğan zararların büyük ölçüde azalacağı düşünülmektedir.

Günümüzde bilim ve teknik alanındaki hızlı gelişmeler insanları bu gelişmeleri yakından izlemeye zorlamaktadır. Belirli eğitim kuruluşlarını bitirmiş olanların edindikleri bilgiler, bütün ömürleri boyunca yeterli değildir. Başarı için yenilikleri yeni gelişmeleri izleme zorunluluğu vardır.

Bu bağlamda insan ilişkilerinin çeşitlendiği ve karmaşık hale geldiği, toplumun plüralist bir yapıya dönüştüğü günümüzde; hak, hukuk, insan, suç ve suçlu kavramları ile birlikte polisin yeni fonksiyonları ve bilhassa polis eğitiminin yeniden yapılanması hususu önem kazanmıştır. Çünkü, globalleşen dünyada gerçekleşen hızlı gelişmeler ve suç tipleri polisin eğitiminin tekrar sorgulanmasını gerektirmektedir ve polisin toplumdaki, hatta dünyadaki değişim ve gelişmeye ayak uydurması zorunludur. Ayrıca, kamu düzeni açısından, önleyici polislik ve suç sonrası polisliğin önemi unutulmadan esas amacın suç oluşmadan önce gerekli önlemlerin alınarak kamu düzeninin bozulmasının önüne geçmek olduğu göz ardı edilmemelidir. Amaç, suç oluşmadan önce gerekli önlemleri alabilmektir. Bilişim suçları gibi ülkemizde yoğun olarak artmakta olan yeni suç tipleriyle mücadelede kolluğun mevcut gelişmeler doğrultusunda güncelleme eğitimine tabi tutulması işte bu nedenle büyük önem taşımaktadır.

2.6.2.4. Bilişim Suçları'nda Uzaktan Eğitim:

Emniyet Teşkilatı'nda bilişim uzmanlarının, Bilişim Suçları Uzmanı veya Adli Bilişim Uzmanı olarak çalışabilmeleri için sanal dünyadaki suçlarda olay yerinde nasıl davranılacağı, dijital delillerin nasıl toplanacağı, delillerin zarar görmeden ve orijinalliği bozulmadan nasıl inceleneceği, incelenen medyaların dökümasyonunun nasıl yapılacağı ve delillerin nasıl muhafaza edilerek adli mercilere teslim edilmesi gerektiğini bilmeleri gerekmektedir.

Uluslar arası alanda kabul görmüş Computer Forensics(Adli Bilişim), Digital Investigations (Dijital İnceleme), Cyber Crime Investigations (Siber Suç

İncelemesi) vb. gibi alanlarda sertifikasyonlar mevcuttur. Bilişim Suçları ve Adli Bilişim alanında uluslar arası alanda en çok kabul görmüş sertifikasyonlardan bazıları şu şekildedir:

1. Computer Forensic Computer Examiner (CFCE): http://www.iacis.com/
2. Certified Information Forensics Investigator (CIFI): http://www.iisfa.org/
3. EnCase Certified Examiner (ENCE) http://www.guidancesoftware.com
4. Certified Computer Examiner (CCE): http://www.certified-computer-examiner.com
5. Certified Computer Crime Investigator (CCCI): http://www.htcn.org/
6. Professional Certified Investigator (PCI): http://www.asisonline.org/ (Ekizer, 2007).

2.6.2.5. Bilişim Suçları'nda Yurtdışı Eğitimi

Emniyet Genel Müdürlüğü'nün ihtiyacı olan alanlarda bilimsel çalışmalarda bulunmak üzere 657 sayılı Devlet Memurları Kanunu'nun 78, 79 ve 80. maddeleri ve "Yetiştirilmek Amacıyla Yurtdışına Gönderilecek Devlet Memurları Hakkındaki Yönetmelik" hükümleri ve Bakanlar Kurulu Kararı ile tanınan kontenjanlar çerçevesinde, Emniyet Teşkilatı'nın ihtiyaç duyduğu alanlarda yetiştirilmek ve bilimsel çalışmalarda bulunmak üzere 1999 yılında itibaren lisansüstü ve Kısa süreli (Hizmetiçi) eğitimlere personel gönderilmektedir. Emniyet Genel Müdürlüğü'nce "Yurtdışı Lisansüstü Eğitim" başvuru şartları şu şekilde belirlenmiştir (Eğitim Daire Başkanlığı, 2008).

- Emniyet Hizmetleri sınıfı personeli olmak
- Adaylık dahil en az üç yıl çalışmış olmak
- Son üç yıllık sicil döneminde olumlu sicil almış olmak
- Son üç yıl içinde kademe ilerlemesinin durdurulması cezasını almamış olmak
- Haklarında meslekten veya memuriyetten çıkarma cezasını gerektirecek suçlardan dolayı devam eden adli veya idari soruşturması bulunmamak
- Askerlikle ilgisi bulunmamak
- Askerliğini yapmış ise, başvuruda bulunduğu yılın 01 Ocak tarihi

itibariyle (40) yaşından gün almamış olmak. Askerlik yapmamış ise 1111 sayılı Askerlik Kanununun 35/E maddesi gereğince Eğitim Dairesi Başkanlığı'nca belirlenecek yaş kriterine sahip olmak

- Daha önce yurtiçinde aynı konuda veya yurtdışında aynı düzeyde eğitim veya öğrenim görmemiş olmak
- Yeterli yabancı dil bilgisine sahip olmak: son başvuru tarihinden önceki iki yıl içerisinde; İngilizce için en az (213) puanlık geçerli TOEFL veya en az (7,5) puanlık IELTS belgesine, Fransızca için ilgili ülke kurumunun yaptığı sınavlarda alınan eşdeğer belgeye sahip olmak
- Yetiştirilmek Amacıyla Yurt Dışına Gönderilecek Devlet Memurları Hakkında Yönetmelik hükümlerine göre geri çağrılmamış olmak,
- Talebi birim amirliğince uygun bulunmak.

Emniyet Genel Müdürlüğü'nün yurtdışı lisansüstü eğitime gönderilen personelin eğitim aldığı konulardan bazıları şu şekildedir:

Adli Görüntü,
Ses ve Konuşma Analizi,
Adli Tıp- Adli Bilimler,
Bilgisayar Sistemleri ve Bilişim Suçları,
Bilgisayar ve Bilgisayar Suçları,
Bilişim Suçları ile Mücadele,
Elektronik İstihbarat Uygulamaları,
Enformasyon Sistemleri Yönetimi,
İleri Teknoloji Suçları,
Mali Suçlarla Mücadele,
Olay Yeri İnceleme,
Organize Suçlar,
Organize Suçlarla Mücadele,
Suç Analizi,
Suç ve Suçlu Sosyolojisi/Psikolojisi,
Suçlu Profilleri ve Suç Profili Çıkarma,
Terörizm ve Uluslararası Kuruluşlar,

Uluslar arası Terör Örgütleri,

Uluslararası Terör Örgütleri ve Bağlantıları,

Uluslararası Terörizm ve İnsan Hakları,

Yüksek Teknoloji Suçları,

Yüksek Teknoloji Suçlarıyla Mücadele (Eğitim Daire Başkanlığı, 2008).

2.6.2.6. Bilişim Suçları'nda Polisin Eğitimi Amaçlı Öğretim Programı Geliştirme

Bu araştırma ile bilişim suçları konusunda görevli olan emniyet mensplarının hedef eğitim ihtiyaçlarının belirlenmesi için ihtiyaç analizi de yapılmıştır. Buna göre program geliştirmenin temel aşaması olan ihtiyaç analizi konusunda kısaca bilgi vermek te yarar vardır.

İhtiyaç analizi süreci şöyle özetlenebilir.

İhtiyaç analizi bir eğitim programı geliştirmenin öncelikli sürecidir.. Tamamen ARGE süreci olan İhtiyaç analizinde cevaplanması gereken 3 temel soru vardır. Yetişecek birey;

- Ne bilmeli? (Bilişsel özellikler)
- Ne yapabilmeli? (Devinsel özellikler)
- Nasıl bir insan-birey olmalı? (Duyuşsal özellikler)

İhtiyaç analizi için üç boyutlu ARGE yapılması gerekir. Bunlar;

- Toplumun ihtiyaçları,
- Bireyin ihtiyaçları,
- Konu alanının ihtiyaçları dır.

Bunların özellikleri şöyle özetlenebilir (Demirel, 2000: 80-81; Ertürk, 1993: 32-41; Oliva, 1997: 145; Saylan, 1995: 81-82; Saylor, Alexander and Lewis, 1981: 19; (Taşpınar, 2007; 19 -23).

Toplumun ihtiyaçları genel olarak "nasıl bir insan/birey? sorusuna toplumsal açıdan bakılması demektir. Toplumun bireyden beklentileri, değerleri, felsefesi, inançları gibi esasların dikkate alınarak, hazırlanacak eğitim programının hedefleri ortaya konulmalıdır. Aksi halde sistemden yetişen bireylerin toplumun beklentilerine cevap verebilmesi mümkün olmayacaktır. Örneğin toplumun bilişm suçlarından korunma konusunda bireylerden

beklentileri, bu konuda eğitim alacak kişilerin ne tür niteliklere sahip olmasını bekledikleri ilgili toplum kesimlerinden alınabilecek bilgiler yer alabilir.

Bireyin ihtiyaçları ise "nasıl bir birey? sorusuna, eğitimi alacak kişi açısından bakılması demektir. Bir başka deyişle, bireyin ne tür bir eğitim ihtiyacı içinde olduğunun ortaya çıkarılmasıdır. Birey genel olarak toplumun beklentilerine uygun niteliklere sahip olmak, toplumsal iş bölümüne katılmak, üretici kimlik kazanmak, iyi bir vatandaş olmak ister. Bunları eğitim sistemi yoluyla sağlamak mümkündür. Örnek vermek gerekirse bilişim suçları konusunda eğitim almak isteyen bir bireyin sahip olmayı istediği bilgi ve becerileri ile kişilik özelliklerinin belirlenmesi, hazırlanacak eğitim programının amaçlarının oluşturulmasına kaynaklık eder.

Konu alanının ihtiyaçları, programı hazırlanacak olan alanla ilgili ihtiyaç analizi etmektir. Söz konusu alanla ilgili olarak mevcut bilimsel ve teknolojik düzey nedir?, bu alanda yetişecek bir birey ne tür bilgi ve becerilere sahip olmalıdır? Bu alanda hazırlanacak bir eğitim-öğretim programının başlıca konu alanları neler olmalıdır? gibi sorulara cevap aranmalıdır. Örneğin bilişim suçları konusunda mevcut bilimsel ve teknoloik düzey nedir? Bu soruların cevapları genel olarak programın amaçlarını ortaya koyacaktır. Bu amaçlar aynı zamanda bireyin ve toplumun ihtiyaçları ile de tutarlılık gösterecektir.

Yukarıda sözü edilen üç boyutta yapılan ihtiyaç analizi çalışması bir AR-GE çalışması niteliğindedir. Yapılacak araştırma kapsamında çeşitli sorulara cevaplar aranır. Genel duruma ilişkin olarak, bilişim suçları eğitimine ilişkin mevcut durum, yapılan ve yapılacak olan eğitim etkinlikleri, bu konuyla ilgili bireylerin eğitim ve bilinç düzeyleri, sahip olamaları gereken niteliklere sahip olma durumları, beklentileri vb. pek çok boyutta veri toplanabilir.

İhtiyaç analizi yaklaşımları

İhtiyaç analizi yapılırken dört temel yaklaşım benimsenmektedir. Bunlar şöyle özetlenebilir (Demirel, 2000: 84-85).

1. **Farklar yaklaşımı:** Beklenilen bilgi-beceri düzeyi ile mevcut olan düzeyin karşılaştırılması demektir.

2. **Demokratik yaklaşım:** Çoğunluğun ve toplumdaki baskı gruplarının istekleri ihtiyaç analizine yön verir.

3. **Analitik yaklaşım:** Gelecekte ortaya çıkması muhtemel olan durumlar dikkate alınarak ihtiyaçlar belirlenir. Bu durum bilimsel ve teknolojik gelişmeleri yakından izlemeyi gerektirmektedir.

4. **Betimsel yaklaşım:** Eğitim yaşantılarından ortaya çıkan durumla ilgilenir. Eğitimde olması gereken bir olgunun olmaması sonucu ortaya çıkan zarar ile olması halinde elde edilecek yarar karşılaştırması yapılır.

Belirlenen ihtiyaçlar konusunda ilgili kesimlerin görüşlerinin alınması ve gerekli değerlendirmenin yapılması için de farklı teknikler kullanılmaktadır. Bu teknikler ve uygulama biçimleri şöyle özetlenebilir (Demirel, 2000: 90-108).

İhtiyaç Belirleme – Değerlendirme Teknikleri

Delphi Tekniği-Anket Geliştirme: Gelecekte nelerin olabileceğine ilişkin görüş alma esasına dayalı bir uygulamadır. Konu ile ilgili seçilmiş uzmanlar yüz yüze gelmeden, kendilerine posta ya da elektronik ortam da ulaştırılan anketleri cevaplarlar. Uygulama birkaç açık uçlu soru ile başlar. Ortak ve farklı görüşlere göre anket her aşamada yeniden yapılandırılıp, uzmanlara bir kez daha sunulur. Sonuçta geleceğe dönük ortak ve farklı düşünceler belirgin hale gelebilmektedir. Örneğin "bilişim suçları öğretim programında başlıca konular neler olmalıdır?" gibi bir soru ile başlayan bir uygulama olabilir.

Progel (DACUM) Tekniği: İngilizce "**D**eveloping **A** **Cu**rriculu**m**" sözünün, tercümesi olan **pro**gram **gel**iştirme kelimesinden türetilmiş bir isimdir. Bir meslek ile ilgili programın geliştirilmesi amacıyla ilgili uzmanların bir araya gelerek çalışmalar yaptığı bir uygulamadır. Mesleğin tanımı ile başlanır. Daha sonra mesleğin ana yeterlik alanları ve bunların işlemleri (gözlenebilir davranışları) belirlenir. Bunlar gözden geçirilir, giriş yeterlikleri belirlenir, belirlenen işlemlerin önemi, yapılma sıklıkları, güçlük düzeyi vb. belirlemeler de yapıldıktan sonra, ortaya çıkan ürün belirli bir komisyon ya da meslek danışma kurulu gibi bir organ tarafından değerlendirilir ve kesin şekli verilerek kullanılmaya başlanır. Örneğin, bilişim suçları öğretim programı katkı sağlayabilecek uzmanlar bir araya getirilip böyle bir çalışma yapılabilir.

Meslek (İş) Analizi: DACUM tekniğine benzer ancak daha fazla zaman alır. Öncelikle programın ihtiyaçları belirlenir. Sonra mesleğin analizi yapılır. Bu aşamada mesleğin tanımı, işlemler, işlem basamakları, bunlarla ilgili gerekli bilgi, beceri, tutum ve alışkanlıklar belirlenir. Program tasarısı hazırlanır, gerekli değerlendirmelerden sonra uygulamaya başlanır.

Testler: Özellikle öğrenme ihtiyaçlarını ortaya çıkarmak amacıyla kullanılır. Ayrıca öğrencilerin başlangıçtaki bilgi düzeylerini (bilişsel giriş davranışları) belirlemek amacıyla da kullanılır. Elde edilen sonuçlara göre ihtiyaçlar belirlenmiş olur. Bu tür bir boyut öntest – sontest modellemeli araştırmalar için de temel oluşturur.

Gözlem: Gerçek ortamda doğal biçimde öğretmen, öğrenci, sosyal çevre ve ortam gözlenir. Veriler gözlem formuna kayıt edilir. Veriler istatistiksel metotlarla analiz edilerek ihtiyaçlar konusunda gerekli değerlendirmeler yapılır.

Görüşme: En çok kullanılan tekniklerden biridir. Görüşme yüz yüze olduğu gibi yazılı formlar biçiminde anket soruları olarak da organize edilebilir.

Kaynak tarama: Geliştirilecek program ile ilgili olabilecek her tür literatürden veri toplanması ihtiyaçların belirlenmesi için önemli sonuçlar ortaya çıkarır. Bu kapsamda önceden uygulanan programlar, düzenlenen raporlar, yapılan araştırmalar-tezler vb. pek çok kaynak taraması yapılıp, veriler değerlendirilir.

Bu araştırmada yapılan ihtiyaç analizinde yukarıda belirtilen yaklaşımlardan gerekli olanlar kullanılmıştır. Öncelikle literatür taramasına dayalı bilişim suçları eğitimi konuları belirlenmiş ve bunlarla ilgili personelin bilme-gerekli görme düzeyini belirlemeye dönük anket hazırlanmış ve uygulanmıştır. Anket sonuçları SPSS programında değerlendirilmiş ve gerekli içerik çalışmasına zemin oluşturmuştur. Belirlenen içerik öğretim programı formunda hazırlanmış ve uzman yargısına sunulmuştur. Bu çalışma belirli ölçüde delphi tekniği yapılanmasına sahiptir. Çünkü hazırlanan programın eleştirisine ilişkin yarı yapılandırılmış sorular oluşturulmuştur. Sorular, 8 uzmana e-mail ile gönderilmiş, bir bölümüne de yüz yüze görüşme sonucunda uygulanmıştır. Bu sorular şunlardır:

1. Hazırlanan modüllerin amaçları bilişim suçları eğitimi alacak polisin ihtiyaçlarını karşılayabilecek düzeyde midir?
2. Modüllerin içeriği bilişim suçları eğitimi açısından yeterince kapsamlı mıdır?
3. Modüllerin içeriği ile amaçları tutarlı mıdır?

4. İçerik yeterince açık, anlaşılır, ilgi çekici, güncel ve katılımcıların düzeylerine uygun mudur?
5. İçeriğin öğrenilmesi için önerilen süre yeterli midir?
6. Modüllerde yer alan değerlendirme programın amaçlarına ulaşma düzeyini belirleme, kapsam geçerliliği vb. açılardan yeterli midir?
7. Hazırlanan modülleri biçimsel özellikleri (görünüm, sayfa dizaynı, yazı karakteri, resim vb.) açılardan nasıl değerlendirirsiniz?
8. Bunların yanında belirtmek istediğiniz başka bir husus varsa lütfen yazınız?

Bu araştırma da, polisin bilişim suçları ile ilgili mevcut durumunu ortaya koyması açısından oldukça önemlidir. Bunun yanında yukarıda sözü edilen bilişim suçları eğitimlerinin daha işlevsel yapılabilmesi, içeriklerin yenilenmesi açısından da önemli katkı sağlaması beklenmektedir.

2.6.3. Kanada'da Bilişim Suçları Eğitimi

Kanada'da polis güvenlik güçleri Kanada Polis Koleji ya da diğer bölgesel eğitim merkezlerinde eğitim görmektedirler. Ayrıca bölgesel yapıda altı kuruluş eğitim vermektedir. Atlas Okyanusu eyaletleri için Atlantik Polis Akademisi, Kırsal eyaletler için Saskatchewan Polis Koleji, İngiliz Columbiası için BC Adalet Enstitüsü, Ontario için Ontario Polis Koleji ve Quebec için Quebec Ulusal Polis Okulu bulunmaktadır (Maltais, 2005).

Kanada'da Bilişim Suçları Hizmet içi Eğitimi

Polislerin hizmet içi eğitiminde, bir takım güçlükler bulunmaktadır. Saskatchewan polis merkezinden soruşturmaya yanıt veren bir katılımcı bu tür kursların gereksinime, önceliğe ve bütçeye bağlı olduğunu belirtmiştir. Atlantik Polis Akademisinde hizmet içi polis memurları için bilişim suçlarına ilişkin yalnızca bir kurs bulunmaktadır. Quebec Ulusal Polis Okulu, Quebec eyaleti içinde mesleğe yeni katılanlara yönelik kurslar düzenlemekle birlikte bu kurslarda bilişim suçlarıyla ilgili konular yer almamaktadır. Ontario Polis Kolejinde de durum bundan farklı değildir. Saskatchewan Polis Kolejinin 2005 yılında servis içi memurlar için açtığı kurslarda da bilişim suçlarıyla ilgili konular yer almamaktadır. Canadian Police College (CPC)'deki eğitim olanaklarının

güçlü olması bilişim suçlarıyla ilgili olarak diğer polis örgütlerini kendi olanakları içinde eğitim vermelerine neden olmuştur. Örnek olarak Ontario'daki London Polis Örgütü böyle bir çözüme gitmiştir. Araştırma kapsamında, memurlardan görüşlerini belirtmeleri istenmiştir. Araştırma kapsamında yapılan soruşturma ve görüşmeler, bizzat güvenlik güçleri elemanlarının kendi ağızlarından Kanada güvenlik güçlerinin bilişim suçlarıyla mücadelesinde neyin doğru, neyin yanlış olduğunu belirleyen genel izlenimleri yansıtmaktadır (Maltais, 2005).

- New Brunswick polis örgütünden 3 no.lu katılımcı tüm örgüt üyelerine verilen bilişim suçlarıyla ilgili eğitimin yıl başına bir tam gün olduğunu belirten tek katılımcıdır. Başka bir polis örgütü de tehdit amaçlı elektronik postalarla ilgili suç araştırması ve bilgisayar müsaderesi konularında eğitim verdiklerini belirtmektedir. Prens Edward Adası polis teşkilatından 4 no.lu katılımcı ise teşkilat görevlilerinin "elektronik posta izleme" eğitimi aldıklarını iletmektedir.

- Polis örgütlerinden en çok Ontario Eyalet Polis Teşkilatı'nın (OEPT) verilen eğitimlerden yararlandığı görülmektedir. Bu teşkilattan 5 no.lu katılımcı her uygun fırsatta eğitim aldıklarını belirtmektedir. "Kurs imkanı ortaya çıktığında elektronik suç birimindeki görevliler için onlara katılmak zorunlu olmaktadır." Eyalet polis teşkilatı olan OEPT'in eğitim için yeterli düzeyde tahsisatı bulunmakta ve çok sayıda görevliyi bilişim suçları konusunda eğitilmek üzere kurslara göndermektedir. Kurslardan en çok yararlanmalarının bir nedeni eğitim yerinin aynı ilde olması, bir diğeri de OEPT'nin bilişim suçlarına en yüksek önceliği tanımasıdır.

KPK'nin sunduğu eğitimlerden yararlanmanın güçlüğü karşısında diğer polis örgütleri bilişim suçuyla ilgili eğitim gereksinimlerini kendi olanaklarıyla karşılamak zorunda kalmışlardır. Örneğin, London (Ontario) Polis Teşkilatı 2003 yılında böyle bir uygulamaya gitmiştir. 2003 yılı iş planında belirtilen amaçlarından bir tanesi internet suçlarıyla ilgili araştırmacı yetiştirmektir. Yıllık gözden geçirme belgelerinde yetişmiş araştırıcı sayısında yüzde yüz artış olduğu belirtilmektedir (London Polis Teşkilatı, 2003; Maltais, 2005).

Canadian Police College (CPC)'deki ve Atlantic Police Academy'de düzenlenen bazı bilişim alanında kurslar ek-2'de belirtilmiştir.

ÜÇÜNCÜ BÖLÜM

3. İLGİLİ ARAŞTIRMALAR

Bu bölümde ulaşılabilen kaynaklara göre bilişim suçları, İnternet ortamında güvenlik, firewall, telif hakları, İnternet ve hukuk, kolluğun bilişim suçlarında eğitimi vb. konularda yapılan araştırmalar hakkında çeşitli bilgiler verilmiştir. Bu bölüm; 1. Yurt içinde 2. Yurt dışında yapılan araştırmalar olarak iki bölüm halinde incelenmiştir.

3.1. Yurt İçinde Yapılan Araştırmalar

Karaahmetoğlu, 2001 yılında "İnternet Güvenliği Kavramları ve Teknolojileri" konulu yüksek lisans tezi hazırlamıştır. Çalışmada, internet güvenliği kavramları ve teknolojileri üzerine uygulanabilir bilgi güvenliği çözümü elde edilmiştir. Bu bilgi güvenliği çözümü maliyet, ölçeklenebilirlik, tutarlılık, gizlilik ve güvenirlik ölçütlerini sağlamaktadır. Tez çalışması kapsamında bilgi güvenliği çözümünün oluşturulmasında ilk olarak kurumun güvenlik ihtiyaçları belirlenmiş ve bu ihtiyaçlar doğrultusunda, bilgi güvenliği çözümlerinin vazgeçilmez elemanları olan firewall, saldırı sezme sistemleri, virüs tarama sunucuları, şüpheli dunum sezme sunucuları ve yüksek şifreleme teknolojileri kullanılmıştır. Ayrıca, çalışmada yeni gelişen teknolojiyle beraber bilginin çalınması ve kişilerin, kurumların aleyhine kullanılması tehlikesi vurgulanarak, İnternet üzerinde bilginin güvenliğini sağlayacak kavramların, yöntemlerin ve teknolojilerin geliştirilmesi gerektiği belirtilmiştir.

Değirmenci, 2002 yılında "Bilişim Suçları" konulu yüksek lisans tezi hazırlamıştır. Tez kapsamında, bilgisayar ve bilişim sistemleri tanımlanmış, bilişim sistemlerinin toplum hayatında kullanımı, bu kullanımın olumlu ve olumsuz yönleri ve bilişim alanında yapılan uluslararası çalışmalar irdelenmiştir. Ayrıca, bilişim suçları ile ilgili tanımlamalar, bilişim suçları alanında ülkemizde ve uluslararası hukukta yapılan tasnifler ve yaşanan ilginç örneklerle bilişim suçlarının işleniş şekilleri, bilişim suçları konusunda uluslararası hukukta düzenlemeler, bazı ülkelerin ceza kanunları ve TCK'da bilişim suçları tez çalışmasında incelenmiştir.

Dülger, 2004 yılında “Türk Ceza Hukuku’nda Bilişim Suçları” konulu yüksek lisans tezi hazırlamıştır. Çalışmada, bilişim suçlarının çok daha sık ve bu günden öngörülemeyen çok daha farklı alanlarda işleneceğinin kaçınılmaz olduğu ve bu nedenle bu suçlarla hem hukuksal yönden, hem teknik yönden, hem de güvenlik yönünden işbirliği halinde mücadele yürütülmesi gerektiği vurgulanmıştır. Ayrıca, ülkemizde ve yabancı ülkelerde bilişim suçları konusunda yapılan özellikle ceza hukuku alanındaki yasal düzenlemelerin tek başına bu suçların önlenmesinde yeterli olmayacağı belirtilmiştir. Çalışmada, üç yasa ile (TCK, FSEK, EİK) düzenlenen bilişim suçlarının kendi alanında ya da diğer suç tipleriyle içtima sorunlarının ortaya çıktığı belirtilmiştir. Yine, İnternet’te yer alan kişiler olan içerik sağlayıcı, erişim sağlayıcı ve servis sağlayıcıların ceza hukuku açısından sorumluluklarının ilgili yasalar ya da özel bir yasayla belirlenmesi gerektiği vurgulanmıştır. Sanal terörizm olgusuna karşı, ülkemizde hukuksal alanda hiçbir yaklaşım bulunmadığı ve bilişim suçlarıyla daha etkin mücadele edebilmek için Avrupa Siber Suç Sözleşmesi’ne ülkemizin dahil olunması çalışma kapsamında ifade edilmiştir.

Kurt, 2005 yılında “Bilişim suçları ve TCK’daki uygulaması” konulu yüksek lisans tezi hazırlamıştır. Tez kapsamında, hukuk sahasında yer alanların bilişim sahasını kavrayabilmeleri için ana hatlarıyla teknik bilgiler sunulmuş, bilişim alanının belirlenmesi, hangi unsurlardan oluştuğu, suçun işleniş şekilleri, bilişim suçlarının tasnifi, gerekli tanımlamalar ve hangi eylemlerin bilişim suçu olduğu tespit edilmeye çalışılmış, bilişim suçlarında dünyada görülen ilk vakalar incelenmiş, konunun uluslararası boyutu ve Türk hukukunda bilişim suçlarıyla ilgili yapılan çalışmalar irdelenmiştir. Çalışmada, “bilişim suçu” ile “bilgisayar suçu” ayrımı ortaya konularak, her iki tanımlamanın paralellik gösteren ve ayrışan noktalarına vurgu yapılmıştır.

Ayrıca, tez kapsamında Türk Ceza Kanunu’nda bilişim suçlarının klasik ceza teorisinin benimsemiş olduğu usul çerçevesinde tüm yönleriyle şerhedilmesi amaçlanmıştır. 5237 sayılı Türk Ceza Kanunu’ndaki bilişim suçları ve uygulamayı şekillendiren Yargıtay kararları incelenmiş, bilişim suçlarıyla mücadele edecek olan uygulamacıların zihinlerinde kanuni metinlerin

canlanabilmesi için Yargıtay'ın son beş yıllık kararların tamamına yer verilmiştir. Böylece, kanun uygulayıcıların karşılaşılan her yeni ve değişik olaylar karşısında çıkarımlar yapmasına yardımcı olunmuştur.

Önemli, 2005 yılında "İnternet suçlarıyla mücadele yöntemleri" konulu yüksek lisans tezi hazırlamıştır. Çalışmada, İnternet suçlarıyla mücadelede ülkelerin ve uluslar arası kurumların uyguladıkları yasal ve kurumsal yöntemler incelenmiştir. Bu bağlamda, ülkemizdeki mevcut yasal ve kurumsal düzenlemeler de incelendikten sonra uygulanan mevcut düzenlemeler neticesinde tespit edilen sorunlar çözüm önerileriyle birlikte irdelenmiştir. Çalışmada şu sonuçlara ulaşılmıştır: Olayların çözümünde bazen ulusal hukuk kuralları yeterli olmamaktadır. Bir ülkeye göre suç olan unsur, diğer ülkeye göre suç olmamakta ya da bir ülkeye göre delil olan bir durum, diğer ülkeye göre delil olmamaktadır. Yine suçun işlendiği yer konusunda sorunlar bulunmaktadır. Bu nedenle uluslar arası bazı kurallara ihtiyaç duyulmaktadır. İnternet suçlarıyla mücadelede önemli bir yer tutan diğer unsur, uluslar arası işbirliği konusudur. Mevcut kanunların eksikliklerinin giderilmesi, İnternet servis sağlayıcıların yetki ve sorumluluklarının belirlenmesi, uzman birimlerin kurulması ve uluslar arası kuruluşların çalışmaları, suçlarla mücadelede diğer önemli hususlardandır.

Savaş, 2005 yılında "İnternet Ortamında Yapılan Hukuki Sözleşmeler ve Bunların Hukuki Sonuçları" konusunda doktora tezi hazırlamıştır. Tez çalışmasının konusunu internet ortamında kurulan sözleşmeler ve bunların hukukî sonuçları oluşturmaktadır. Bu bağlamda elektronik sözleşmelerin kurulması için öncelikle internet ortamı incelenmiştir. Tez çalışmasında elektronik ticaret konusu, İnternet ortamında yapılan hukukî işlemler, internet ortamında kurulan sözleşmeler, elektronik sözleşmelerde şekil konuları ele alınmıştır. Daha sonra elektronik imza olarak isimlendirilen dijital imza konusu alt yapısı ve işleyişi ile birlikte şekle ilişkin genel prensiplerle karşılaştırılarak incelenmiştir. Son olarak da yeni yürürlüğe giren elektronik imza kanununun genel bir değerlendirilmesi yapılmıştır.

Yıldız, 2006 yılında “Suçta Araç Olarak İnternet’in Teknik ve Hukuki Yönden İncelenmesi” konusunda doktora tezi hazırlamıştır. Çalışmada, internetin teknik özellikleri hakkında genel bilgiler verilmeye çalışılmıştır ve bugün için geçerli olan internetin fonksiyonları irdelenmiştir. Tez kapsamında, internetin hukuki düzenleme altına alınması ve bilgisayar sistemlerine karşı yapılan saldırıların teknikleri açıklanmış, ayrıca internet sujelerinden internet servis sağlayıcıların cezai sorumluluklarının olup olmadığı, yerine getirdikleri fonksiyonlar göz önüne alınarak irdelenmiştir. Karşılaştırmalı hukukta ve uluslar arası çalışmalarda internet suçlarının hangi yöntemlerle düzenlenmiş olduğu ve uluslararası alanda internet suçlarının düzenleyen tek belge olan Avrupa Konseyi Siber Suç Sözleşmesinin hükümleri tez kapsamında incelenmiştir. Ayrıca, özel hayatın gizliliği ve korunması, günümüzde büyük tartışmalara yol açan mahremiyet ve kişisel verilerin korunması konuları tez kapsamında ele alınmıştır.

Tulum, 2006 yılında “Bilişim Suçları ile Mücadele” konusunda yüksek lisans tezi hazırlamıştır. Tez çalışmasında, bilgisayar ve internet ile ilgili temel kavramlar ele alınarak genel bilgiler verilmiş, daha sonra bilişim suçlarının tanımı, özellikleri, sınıflandırılması, bilişim suçları failleri ve mağdurlarının genel özellikleri ele alınarak bilişim suçlarının ulusal ve ulusalüstü hukuktaki durumu, bu suçlarla mücadele yöntemleri, alınan ve alınması gereken tedbirler ve çözüm arayışlarına yer verilmiştir. Tez çalışmasında, ahlaki değerleri, insanlığı ve ülkeleri tehdit eden bilişim suçlarının tüm ülkelerin ortak problemi haline geldiği ve mevcut hukuk kurallarının modern teknolojinin yarattığı olumsuzlukları gidermede yetersiz kaldığı vurgulanmıştır. Bilişim suçları ile mücadelede, milli menfaatler ve ulusal güvenlik için geleceğin teknolojilerine de cevap verebilecek esnek çözümlerin üretilmesi, yasal tedbirlerin yanısıra, her kurum ve kuruluşun kendi içerisinde özel tedbirler geliştirerek, güvenlik kurallarını önemsemeleri önerilmiştir.

Karakurt, 2006 yılında “Bilişim suçları ile mücadelenin uluslar arası boyutu ve Türkiye’ye yansıması” konulu yüksek lisans tezi hazırlamıştır. Tez kapsamında, bilişim suçları ile mücadele çerçevesinde uluslararası alanda

yapılan çalışmalar ve bu çalışmaların Türkiye'deki yansıması incelenmiştir. Ayrıca, bilişim suçları olarak adlandırılan siber tehdit tanımlanarak, boyutlarını belirlemek ve bu konada mücadele etmekle görevli olan kanun uygulayıcılarına bağlı olarak, uluslar arası alanda ve Türkiye'de bilişim suçları ile mücadelede yapılan çalışmaları tespit etmek, değerlendirmek, mücadelede yaşanan zorluklar ve problemleri ortaya koymak ve bu mücadelede neler yapılması gerektiğine ilişkin çözüm önerileri sunmak amaçlanmıştır. Tez çalışmasında bilişim suçları ile mücadelede teknik, yasal, operasyonel sorunlar ortaya konulmuştur.

Dijle, 2006 yılında "Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı" konulu yüksek lisans tezi hazırlamıştır. Tez kapsamında, bilişim suçlarının her geçen gün arttığı, yaygınlaştığı ve ciddi bir tehlike oluşturduğu belirtilmiş ve bilişim suçları ile mücadele hakkında bilimsel çalışmaların yapılması gerektiği vurgulanmıştır. Tez çalışmasında, bilişim suçları çeşitli yönleri ile incelenmiş ve bilişim suçlarının kapsamı, tanımlaması ve sınıflandırılması açıklanarak, hukuki boyutu, polisiye uygulamaları üzerinde durulmuştur. Tez kapsamında, Türkiye'de bilgisayar ve İnternet ile profesyonel olarak daha çok öğretim elemanları ve üniversite öğrencilerinin ilgilendiği düşünülerek öğretim elemanları ve üniversite öğrencilerine e-posta ile adresi duyurularak web sitesi vasıtasıyla bir anket uygulanmıştır. Böylece eğitimli insanların bilişim suçu ve bilişim suçları ile mücadele hakkındaki görüşleri değerlendirilmiştir.

Yavuz, 2006 yılında "Novel Methods For Security Mechanisms and Key Management Techniques in Wireless Networks Based On Signcryption and Hybrid Cryptography – Kablosuz Ağlarda Güvenlik Mekanizmaları ve Anahtar Yönetim Teknikleri İçin Signcryption and Hybrid Kriptografi Temelli Yeni Yöntemler " konulu yüksek lisans tezi hazırlamıştır. Tez kapsamında, kablosuz iletişim ağlarında güvenliğin sağlanmasının güvenlik sistemlerinin en zorlu problemlerinden biri olduğu, yine kablosuz ağların yerel sabit ağlara nazaran gizli dinleme ve aktif saldırılara karşı daha korunmasız olduğu vurgulanmıştır. Ayrıca, kablosuz ağların özellikle enerji ve bant genişliği olanakları bakımından

sınırlı olduğu ve bu durumun kablosuz ağlarda güvenliği temin etmeyi güçleştirdiği ve özellikle üye sayısının çok fazla olduğu ve üyelerin sisteme giriş-çıkışlarının sık gerçekleştiği dinamik karakteristikteki kablosuz ağlarda büyüdüğü belirtilmiştir. Tez çalışmasında, güvenlik sistemlerine üç temel noktada yenilik getirilmiştir: Yapısal tasarım, bütünleşik anahtar yönetim teknikleri ve kriptografik yaklaşımlar.

Çekiç, 2006 yılında "İnternet Aracılığıyla İşlenen Suçlar" konusunda 3 bölümden oluşan yüksek lisans tezi hazırlamıştır. Tez kapsamında, birinci bölümde bilgisayar ve bilgisayara ilişkin kavramlar, bilişim sistemleri, internet ve internete ilişkin süjeler ile internetin yapısal özellikleri açıklanmıstır. İkinci bölümde bilişim suçu, bilişim suçlarının yapısı ve alınması gereken tedbirler açıklanmıştır. Üçüncü bölümde ise Türk Hukuk sisteminde düzenlenen bilişim suçları ele alınarak incelenmeye çalışılmıştır. Ayrıca Bilişim suçları dışında içerik itibariyle internet aracılıgı ile işlenebilecek diğer suçlarda açıklanmıştır.

Say, 2006 yılında "Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuarlarda İncelenmesi" konusunda yüksek lisans tezi hazırlamıştır. Tez kapsamında, bilişim suçlarının vuku bulduğu olay yerlerinden elde edilen delillerin toplanması, elde edilen delillerin data inceleme labouratuvarına sevki ve laboratuvarda incelenmesi konusunda bir yaklaşım yolu gösterme ve saha personeli tarafından sık yapılan yanlış davranışları düzeltme amaçlanmıştır. Araştırmada, öncelikle suç kavramı tanımlanmış, konunun uzmanı olan yerli ve yabancı kriminolog ve sosyologların tanımlarına yer verilmiştir. Ayrıca, bilişim suçlarının tanımı yapılmış ve tanımlama yapılırken dikkat edilmesi gereken hususlar belirtilmiştir. Çalışmada, bilişim suçunun meydana geldiği yer olan olay yerinde, olay yeri inceleme uzmanının delillere müdahale etme konusunda dikkat etmesi gereken noktalar belirtilmiş ve elektronik delillerden, dijital deliller elde edilmesi ve dijital delillerin nihai olarak incelendiği yer olan data inceleme laboratuvarında, delillerin bütünlüğünün bozulmaması ve karartılmaması için alınması gereken önlemlerle beraber adli bilişim ekspertiz raporu yazma esasları çalışmada ele alınmıştır.

Gaziler, 2006 yılında “İnternet Bankacılığı ve Kullanımının Etkinliği” konusunda yüksek lisans tezi hazırlamıştır. Tez çalışmasının konusunu internet bankacılığı kullanımının etkinliği ve internet bankacılığı kullanımının eğitimle ilişkisinin araştırılması oluşturmaktadır. Üç bölümden oluşan çalışmanın birinci bölümünde internet bankacılığı konusu araştırılmıştır. Bu bölümde, internet bankacılığının tanımı, tarihçesi, hangi ihtiyaçların sonucunda ortaya çıktığı, dünyada ve ülkemiz finans piyasalarındaki durumu, internet bankacılığının bankaya ve müsterilere sağlayacağı imkanlar incelenmistir. Çalışmanın ikinci bölümünde internet bankacılığı ve güvenlik konusu araştırılmıştır. Bununla birlikte internet bankacılığında karşılaşılan sorunlar, internet bankacılığında gerçeklesen saldırılar ve bu saldırılara karşı bankaların ve internet bankacılığı hizmetini kullanan müşterilerin alabilecegi önlemler yine bu bölümde incelenmiştir. Son bölümde ise banka müşterileri üzerinde yapılan “internet bankacılığı kullanım etkinliği, eğitim ilişkisini ortaya koymaya yönelik” bir araştırmaya ve çalışma sonucunda elde edilen bulgu ve değerlendirmelere yer verilmiştir.

Dilek, 2007 yılında “Bilişim Suçları ve Türk Hukukundaki Yeri” konusunda yüksek lisans tezi hazırlamıştır. Tez kapsamında, ülkemizde bilişim suçlarıyla ilgili kanun ve mevzuatların yeterli olmadığı, gelişen teknolojiyle birlikte yeni düzenlemelere ihtiyaç duyulduğu ve toplumumuzun bu suçlarla ilgili bilgisinin de yetersizliği nedeniyle bilişim suçlarının ülkemizde günden güne çoğaldığı tespit edilmiştir. Tez çalışmasında, suç teknikleri ve bilişimle ilgili kavramlar incelenmiş, bilişim suçlarının tanımı ve bu suçların sınıflandırılması yapılmıştır. Daha sonra virüs, Truva Atı, Hacker gibi kavramlar irdelenerek bu suçların hukuk sistemin içerisindeki yerine değinilmiş, son olarak bilişim suçlarının yabancı ülkelerdeki yasal ve idari yapılanmasından söz edilmiştir. Tez çalışmasında, bilişim suçlarında mevcut yasaların yetersiz olduğu, gerekli hukuki düzenlemelerin teknolojik gelişmeler karşısında zorlandığı ortaya konmuş, ancak kanunlarla birlikte toplumunda bilişim konusunda bilinçlenmesi ve eğitilmesi gerektiği vurgulanmıştır.

Dilek, 2007 yılında “Bilişim Suçları” konusunda yüksek lisans tezi hazırlamıştır. Tez kapsamında, konu ile ilgili genel olarak temel terim ve kavramların açıklanmasından sonra bilişim alanında işlenen suç tipleri ayrıntılı olarak incelenmiş, uluslar arası kuruluşların konu ile ilgili yaptıkları çalışmaları, mukayeseli hukukta bilişim suçlarının düzenlenişi, bazı ülkelerdeki durum ve bilişim suçları konusunda ülkemizdeki yasal düzenlemeler, bilişim suçlarının tasnifi, unsurları ve ceza hukuku açısından genel bir değerlendirme yapılmıştır.

Gürcan’ın (2007) belirttiğine göre, ASAGEM tarafından “Türkiye’de Ailelerin İnternet Kullanım Durumları” araştırması yapılmıştır.

- Araştırmanın evrenini, İnternet erişimine sahip ya da İnternet kullanan ailelerdeki anne ve babalar ile bu aileler içerisinde İnternet’e erişebilen 18 yaş altı çocuklar oluşturmaktadır. Örnekleme birimi hane halkı olarak belirlenmiştir.
- Araştırmanın örneklem büyüklüğü; Türkiye kent nüfusunu temsil eden, İstatistiki Bölge Birimleri Sınıflaması (İBBS) 2. Düzey (26 bölge)’den 26 il seçilerek, ülke genelinde tahmin verebilecek düzeyde tasarlanmıştır. Ankara, İstanbul, İzmir, Adana ve Bursa kent nüfusunun büyüklüğünden dolayı seçilmiş iller olarak saha çalışmasına dahil edilmiştir.
- Toplanan anket sayısı 2000 anne, 2000 baba ve 819 çocuk olmak üzere toplam 4819’dur.

Araştırma kapsamında, Internet kullanım durumu ortaya çıkarılmıştır.

- Araştırmaya katılan her beş aileden dördünün evinde en az bir bilgisayar bulunmaktadır.
- Araştırmaya katılan bireylerin yaklaşık % 77’sinin İnternet kullandığı belirlenmiştir.
- İnternet kullanmayanların yaklaşık % 76,7’sini anneler; % 22,8’ini babalar; % 0,6’sını çocuklar oluşturmaktadır.

Araştırma kapsamında, Internet kullanım süreleri ortaya çıkarılmıştır.

- Araştırmaya katılan aile bireylerinin %51’i günde en az bir kez İnternet’i kullanmaktadır.

Araştırma kapsamında belirlenen, İnternet/Bilgisayar kullanımının neden olduğu psikososyal sorunlar ise şunlardır:

- Aile bireylerinin İnternet'te güvenlik ve etik açısından tehlike oluşturabilecek içeriklerin neler olduğuna ilişkin görüşleri incelendiğinde, en fazla soruna pornografi, şiddet, terör içerikli siteler ve kumar oynama siteleridir.
- Aile bireylerinin İnternet'te güvenlik ve etik açısından karşılaştıkları sorunların neler olduğuna ilişkin görüşleri incelendiğinde, en fazla karşılaşılan sorunun virüs yazılımları ve Web sayfalarında gezinirken şiddet, terör ve pornografi gibi içeriklerle istek dışında karşılaşılması olduğu ortaya çıkmıştır.

3.2. Yurt Dışında Yapılan Bazı Araştırmalar

İsveç'te SOLARZ tarafından National Council For Crime Prevention hesabına yapılan bir araştırmada, bilgisayar suçu faillerinin yaş ortalaması % 35.2 olarak tespit edilmiştir. Bu faillerin yüzde kırk dördünü bayanlar oluşturmaktadır. İtalya'da Serviziyo Securinet'in 1990-91-92 yıllarına ilişkin olarak yayınlandığı verilere göre ise polis tarafından elde edilen bilgisayar suçu faillerinin 19 yaşından büyük olduğu görülmektedir. Bunların % 25'i 35 ila 45, % 29'u 25 ila 35, % 55'i 19 ila 25 yaşları arasında yer almaktadır. Yine bunların % 38'i işsiz iken % 47 gibi büyük bir çoğunluğu ise üniversiteli öğrencilerden oluşmaktadır. Çalışan kesimin % 43'ü bilgisayarla alakalı bir işte yer almaktadır (Yazıcıoğlu, 1997: 103)

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

sektörünün diğer kesimlere oranla daha yoğun olarak çeşitli ihlallere maruz kaldığı ifade edilebilir (Yazıcıoğlu, 1997: 107).

Şen, 2001 yılında “Criminal Justice Responses To Emerging Computer Crime Problems” konulu yüksek lisans tezi hazırlamıştır. Tez çalışmasında, bilgisayarla alakalı suçlar; bilgisayar suçları, internet suçları ve siber terörizm olarak üç ana alanda incelenmiştir. Çalışmada, başarıya ulaşmak için yürütme organlarının bilgisayar suçları incelemelerini yapabilecek düzeyde teknik ve analitik donanıma sahip çalışanları işe almaları gerektiği vurgulanmıştır. Polis kurumlarının, bu özel çalışanlar olmadan inceleme yapamayacağı ve bilgisayar suçlarını verimli ve gerekli biçimde inceleyemeyeceği, uygun insanları alıp uygun eğitimi vermenin, uygun araç gereç temin etmenin iyi inceleme ve araştırma ekipleri kurmanın ilk adımları olduğu çalışma kapsamında belirtilmiştir.

Araştırma; ayrıca polis kurumlarının, kurum bilgisayarlarında yüksek hassasiyetli bilgiler sakladıklarını ve değerlendirdiklerini, bu bilgileri suçlu erişiminden korumaları gerektiğini vurgulamaktadır. Çalışmada, şirketlerin, bilgisayar suçu kurbanlarının; olayları yürütme memurlarına iletmeleri gerektiği, bilgisayar suçları araştırmalarının geniş kapsamlı olarak yapılması ve kanıtların dikkatle toplanıp saklanması gerektiği vurgulunmışarı. Ayrıca, bir çok bilgisayar suçu bilgisayar ağlarıyla alakalı olduğu için, müfettişlerin ağlar hakkında bilgi sahibi olmaları gerektiği çalışmada vurgulanmaktadır. Uluslararası bilgisayar suçlarıyla mücadele için, uluslar arasında bilgisayarla alakalı suçların belirlenmesi ve değerlendirilmesi konusunda bir işbirliği ve görüş birliği olması ve bu uluslar arasında iyi düzenlenmiş çözümler, müşterek işbirliği anlaşmaları ve muhtemel yeni cezai müeyideler geliştirecek uluslar arası bir çatı geliştirilmesi gerektiği çalışma kapsamında vurgulanmıştır.

Erdönmez, 2002 yılında “Investigation Of Computer Crimes” konulu yüksek lisans tezi hazırlamıştır. “Bilgisayar Suçlarının Araştırılması”nın konu edildiği çalışmanın ilk bölümünde bigisayara ilişkin suçların oluşumu ele alınmıştır. Bilgisayara ilişkin suçlara ayrıntılı bir girişten sonra bu tür suçların en

yaygın olanları incelenmiş ve suçluların özellikleri, onları suça iten güdüler belirlenmiştir. İkinci bölümde bigisayara ilişkin suç araştırmalarının genel süreci özetlenmiştir. Bilgisayara ilişkin suç tanımlaması yapıldıktan sonra suçlular ve soruşturma süreçleri ele alınmış ve suçluların özellikleriyle suça iten güdüler belirlenerek konuyla ilgili bir örnek olay incelemesine yer verilmiştir. Son bölümde yüksek teknolojiyi kullanan suçlarla güvenlik güçlerinin mücadelesi tartışma konusu yapılmıştır.

Moore, 2002 yılında "Bilişim savaşı, sanal terör ve toplumsal değerler" konulu yüksek lisans tezi hazırlamıştır. Çalışmada, bilişim savaşı ve sanal terör çeşitli yönleriyle ele alınmış ve bilişim savaşının, bilişim ve bilişim sistemlerinin hem silahlı çatışma sırasında hem de savaş dışı operasyonlarda giriştikleri saldırı ve savunma eylemlerinden oluştuğu ifade edilmiştir. Çalışmada, bilişim teknolojisinin bir yandan yeni türden daha az öldürücü askeri araçların sözünü verirken, bir yandan da gittikçe artan karmaşıklıktaki ve birbirine bağlı global yapıdaki bilişim altyapısına bağımlılıktan kaynaklanan zayıflıkları sergilediği ve bu zayıflıkların, siyasal amaçlı korku yaymak için sivilleri hedef alanlar tarafından kullanıldıklarında sanal terör diye adlandırılan durumun ortaya çıktığı vurgulanmıştır.

Bilişim savaşı teknikleri evrildikçe bu teknikleri kullananların normatif sevk için yararlı kimi kaynaklara bakmaları gerekmektedir. Yararlı olan ve uluslar arasında paylaşılan değerlerin uluslararası teamüllerde, BM Sözleşmesinde, "bilişim suçunu" konu alan anlaşmalarda, bilişim savaşçıları tarafından yararlanabilinecek iletişim araçlarını yönetenlerde, UNGA Kararlarında ve Silahlı Çatışma Yasası'nı oluşturan sözleşme ve teamül normlarında bulunabileceği tez kapsamında ifade edilmektedir.

Torosyan, 2003 yılında "Eyalet ve Yerel Yürütme Tarafından Siber Suç Programı:Ulusal Araştırmanın İlk Analizi" konulu yüksek lisans tezi hazırlamıştır. Çalışmanın amacı olarak, siber suçlarla mücadele için koyulmuş yerel ve devlet kanunlarındaki resmi politika ve prosedürlerin içeriğinin ve doğasının etkilerini araştırma belirlenmiştir. Eyalet ve yerel yürütmenin siber suçla mücadelede

resmi siber suç verilerini değerlendirerek ne derece etkin bir mücadele ortaya koydukları ölçülmüştür. Bunun için, siber suç olaylarını araştırma ve kovuşturmayla sorumlu eyalet ve yerel yürütme kurumlarının girdileriyle birlikte 49 ayrı yürütme organından, çapraz kesitlerle ulusal çapta veri toplanmıştır. Çalışma kapsamında, Ulusal Yürütme ve Düzeltmeler Teknoloji Merkezi (NLECTC) Batı Bölgesi, verilerin toplanma sürecini desteklemiştir. Ulusal tarama sonucu bu çalışmanın bulguları bir çok varsayıma % 95 güvenilirlik oranıyla destek olmuştur.

Henych, 2003 yılında "Bilişim suçu algılamaları ve Florida Eyaleti'nde sanal evrenle ilgili hazırlıklar, konuyla ilgili gelecekte izlenecek politikalar" konulu doktora tezi hazırlamıştır. Çalışmada, şu sonuçlar elde edilmiştir. Bilgisayar suçlarının Amerika Birleşik Devleti'nde artmakta olduğu açıkça görülmektedir. Geçen her yıl artan sayıda şirket, resmi kurum ve kişi İnternet ya da bilgisayarla işlenen suçların kurbanı olmaktadır. Florida eyaletinde yaşayanlar da bu kurbanların arasındadır. Sanal evren suçlarıyla en yakından ilgilenmesi gerekenler doğal olarak güvenlik güçleri, yargı organları ve bu tür suçlardan etkilenen halktır. Bunların bilişim suçlarının çok önemli bir toplumsal sorun olup olmadığı konusundaki algılamalarının kaynak aktarımı ve yasamada öncelik gibi konuları içeren kamu politikası oluşturma ve uygulaması üzerinde etkisi olabileceği düşünülmektedir.

Bilişim suçlarıyla ilgili günümüzdeki algılama düzeyini veya farkındalığını belirlemek için, bu gruplar arasında özellikle halka, güvenlik gücü elemanlarına ve savcılara odaklanan bu tür suçlarla ilgili bir artalan taraması yapılmıştır. Çalışmanın araştırma konusu bu grupların görüşlerine odaklanmış, ana sorun üzerinde uzlaşmaya varıp varmadıkları irdelenmiştir. Bu durum, anılan grupların görüşlerinin oluşturulacak politikalar, süreçler ve kaynak aktarımları üzerindeki etkisi göz önüne alındığında büyük önem taşımaktadır.

Taramada rastalanan eksiklikleri gidermek amacıyla, çalışmada daha once anılan üç grup üzerine odaklanan Florida eyaletindeki bilişim suçları algılamasına ilişkin görgül (amprik) araştırma yöntemi uygulanmıştır. Bu

aşamada araştırmacılar kendileri tarafından hazırlanan ve örnek olarak rastgele seçilen güvenlik gücü yöneticilerine/çalışanlarına (N=304), halktan kişilere (N=304) ve Florida eyaleti hukuk kuruluşları üyelerine (N=304) yönelttikleri sorulardan oluşan bir kamuoyu soruşturmasından yararlanmışlardır. Soruşturmayı 912 kişi yanıtlamıştır.

Soruşturmada sorulan sorular bilişim suçuna yönelik algılamaları ve yapılan hazırlıkları saptamaya yöneliktir. Bu yolla bilgisayara yakınlık, bilişim suçlarına maruz kalma, İnternet kullanımı ve güvenlik güçlerinin etkinliği gibi değişkenlerin yanı sıra suçluları adalet önüne çıkaran hukuk kuruluşları da incelenmiştir. Kapsam alanının genişletilmesi, kontrolün yapılabilmesi için diğer değişkenlerden de yararlanılmış ve bir istatistiksel veri çözümlemesi yapılmıştır. Çok değişkenli sapma çözümlemelerinden (MANOVA) yararlanan araştırmacılar oluşturulan varsayımı üç nüfus grubu arasındaki bilişim suçlarına ilişkin algılama farklılıkları üzerinde yoğunlaşarak testten geçirilmiştir.

Maat, 2004 yılında “Karşılaştırmalı bir yasa çözümlemesi” konulu yüksek lisans tezi hazırlamıştır. Çalışmada, çeşitli yasalar kıyaslanmış ve yasaların hükümlerinden bahsedilmiştir. Elektonik İletişim ve İşlem Yasası, bilgisayar korsanlığı(hacking) ve kötü amaçlı bilgisayar şifrelerinin oluşturulması gibi bilişim suçlarıyla ilgili çeşitli yasal boşlukları ortadan kaldırmıştır. İzinsiz erişimlerin, izinsiz veri değiştirmelerin yanı sıra bu suçların işlenmesini kolaylaştıran donanım gereçlerine ve yazılım programlarına sahip olma ve bunları dağıtma yasa dışı eylemlerden sayılmıştır. Bu türden yasa dışı ilan edilen eylemler sonucunda yasal kullanıcılara hizmet sunmama da, yasada suç sayılmakta ve yaptırıma bağlanmaktadır. Bilgisayarla ilişkili dolandırıcılıkla ilgili özel cezai hükümler, *spamlama* ve bilgisayar ilişkili irtikap da yasa kapsamında yer alan hususlardır. Verilerin yetki dışında engellenmesi, hem Elektonik İletişim ve İşlem Yasası’nın hem de İletişimin Engellenmesi Yönetmeliği’yle Bilişim İlişkili İletişim Hükümleri Yasası’nın kapsamına girmektedir. Benzer biçimde İnternet’te çocuk pornografisi konusu da Film ve Yayınlar Yasası kapsamına girmektedir. Bilgi gibi maddi olmayan şeylerin hırsızlığı yasalarda yer almakla birlikte, konunun mantıksal sonuçları henüz içtihat hukukunda yerini

almamıştır. Bütün bunlara karşın ne teamül hukukunun ne de yasa hükümlerinin uygulanabildiği veri kopyalama gibi konular hala yasama konusu olmayı beklemektedir. Söz konusu yasa yargı yetkisi, veri iletilerinin kabul edilebilirliği, elektronik imzaların kabul edilebilirliği ve şifreyazım düzenlemesi gibi konuları yeterli düzeyde ele almaktadır. Yasanın yaptırım kapsamına görevlerine İnternet'i izlemek ve yasa hükümlerine uyulup uyulmadığını saptamak olan sanal alan denetmenleri de eklenmiştir.

Gillen, 2005 yılında **"**Sanal Gerçekliğe Sahip Çıkmak. İnternet'le ilgili etkili düzenleme: Toplumsal değerlere dönüş**"** konulu doktora tezi hazırlamıştır. Çalışma, Internet düzenlemesi sorununu ele almakta ve var olan düzenlemeyi genişletmek, var olan yasal sistemle gün ışığına çıkan sorunlara çözüm bulmak için oluşturulan aydınlanmacı öz-düzenleme formuna itirazda bulunmaktadır. Sanal gerçekliğin (cyberspace) doğasını özetleyerek araştırma başlanmış ve "Vahşi Batı" mecazını kullanarak bu evrende etkin olan çıkar gurupları sınıflara ayrılmıştır. Ardından sanal gerçeklik düzenlemesinin üç ana alanına odaklanılmış ve şu sonuçlara varılmıştır:

Fikri Mülkiyet: Fikri mülkiyet, mülkiyetle kamu alanı arasındaki doğru dengeyi bozmamakta ve uluslararası denetimler, dünya halklarının aleyhindeki özel çıkarların yayılmasını sınırlamada pek az etkinlik göstermektedir.

Sanal gerçeklik Evreninde Haklar: Haklar, sınırlı da olsa, büyük önem taşırlar: Devlet tacizine karşı kalkandır onlar. Ancak, bunları gerçek haklar olarak adlandırmak bizi yanılgıya sürükler; çünkü, standart koymada ve onları uygulamada karşılaşılan güçlükler nedeniyle, vatandaşların ihlalci bireylerin tacizinden, kendi devletimizin yargı sınırlarının ötesinde, her zaman için korundukları söylenemez.

Bilgisayarın kötü kullanımı: Bilgisayar sistemlerine yasa dışı erişimler hak ihlalinin başlıca nedeni sayılabilir. Bunun kadar önemli bir konu da dijital itaatsızlığın sanal gerçeklikteki özgür ifade ve siyasi aktivizmin önemli bir parçası oluşudur.

Karmaşık nitelikteki bu özellikler makro düzeyde yasal çözümlerin sanal gerçeklik alanının yönetimine ve düzenlenmesine tam olarak uymadıkları anlamına gelir. Ancak, etkin bir şekilde kendi kendini düzenleyen bir toplumla birlikte bu sorunlar çözülebilir.

Maltais, 2005 yılında "Managing Cyber Crime: an Assessment of Canadian Law Enforcement Responses" konulu yüksek lisans tezi hazırlamıştır. Bu araştırmada, Kanada'nın siber suçlarla mücadelede yürütme organlarının yetersiz kaldığı bir çok alanı incelemek ve Kanada yürütme organlarının siber suçlar karşısında takındığı tavrın değerlendirilmesi amaçlanmıştır. Araştırmada, bilişim suçlarıyla mücadele eden Kanada güvenlik güçleri yapısındaki eksiklikler saptanmıştır. Araştırma şu hususları açıklığa kavuşturmayı amaçlamıştır:

- Bilişim suçlarına karşı mücadelede Kanada'daki son durum nedir?
- Kanada güvenlik güçlerinin bilişim suçlarıyla mücadelede sahip olduğu kaynaklar nelerdir? (insan kaynakları, eğitim, kanunlar bakımından)
- Kanada'daki güvenlik güçleri bünyesinde bilişim suçlarına verilen öncelik hangi düzeydedir?

Ayrıca, Kanada'daki siber suçlarla ilgili olarak bu konuda ilerleme kaydedilmesi için yeterli tavsiyelerin oluşturulmasını sağlamak bu araştırmanın hedefleri arasındadır. Araştırma kapsamında sunulan öneriler ise şu şekildedir.

- 2005 *Kanada'da Bilişim Suçlarına İlişkin İstatistiklerin Uygulanabilirliği* başlıklı tamamlayıcı araştırma, Kanada'da işlenen bilişim suçlarının diğer yönlerini de ortaya sermek açısından mükemmel bir ortam yaratabilir.
- Bilişim suçunun ulusal içeriğiyle tanımlanması ve terminoloji üzerinde uzlaşım, Kanada'da suç eğilimlerinin azaltılması ya da önlenmesi konusunda verilen çabaların birleştirilmesine büyük ölçüde katkı yapar ve tanımların UCR soruşturmalarında kullanılmasına olanak sağlar.
- Bilişim suçlarını araştırmada sorumlu sayılan kişilerin bilgi ve uzmanlık düzeyini yükseltmeye yönelik, gerek eyaletler düzeyinde örgütlü tüm polis kuruluşları gerekse federal yönetimler için, ek tahsisat çıkarılması gerekir.
- Kanada halkının suç bildirimi ve genelde, sanal suçlar konusunda bilinç düzeyinin yükseltilmesi gerekir.

- Halkın olduğu kadar tüm kuruluşlarıyla yönetimlerin de sorunların çözümlenebilmesinde baş vuracakları bir adres olmalıdır.

Lazarevich, 2005 yılında “Use of Ontologies and Probabilistic Relation Models to Aid in Cyber Crime Investigation Decision Support” konulu doktora tezi hazırlamıştır. Bu araştırmanın amacı, soruşturmacıların bir suçla ilgili bilgi edindiklerinde ortaya çıkan tutarsızlık sorununu çözme ve ardından otomatik olarak hangi suçun işlendiğine ve bu suçun hangi yargı alanına girdiğine ve arama izni çıkarmak için olası nedeni ve desteği göstermek için yeterli kanıtın olup olmadığına karar verme sürecini belirlemektir. Bu sürece kendiliğinden işlerlik kazandırılarak tutarsızlıklar, en aza indirilebilecektir.

Bu araştırma, iki kısımdan oluşmaktadır. Birinci kısımda, uygun yasa ve yargı yetkisinin belirlenmesi için bir araç oluşturulmuştur. Eyalet ve federal yasalarının hem yapılarını hem de aralarındaki ilişkiyi içeren bir ontoloji geliştirilmiştir. Güvenlik güçlerinin bu yapıya, yargı alanının da belirlenebileceği şekilde, nasıl katılabileceği araştırılmıştır. Bu katılmanın federal düzeyde gerçekleşebileceği, uygulanan özel yasalar üzerindeki yargı yetkilerinin yalnızca belirleme yoluyla saptanacağı gösterilmiştir. İkinci kısım, bir kere yasa ve yargı yetkisi belirlendiğinde ve olay verileriyle test edildiğinde, soruşturmacının bu noktada toplanmış olanlar temelinde “olası nedeni” gösterecek yeterli kanıt olup olmadığını belirlemesi gereğini ele almaktadır.

Özeren, 2005 yılında “Global Response to Cyberterrorism and Cybercrime” konulu doktora tezi hazırlamıştır. Araştırma, siber terörizmin çeşitlerinin netleştirilmesi ve bir ölçek oluşturulmasına yoğunlaşmıştır. Araştırma, bir ölçek oluşturmak için yapılan ilk denemedir ve zaafiyetler, işbirliği, özgürlük ve siber terörirzm gibi önemli konulara açıklık getirmektedir. Araştırma kapsamında da, zaafiyet-işbirliği-özgürlükten oluşan (vulnerability, comprehensive cooperation, and freedom) bir ölçek (Ozeren Ölçeği - Ozeren Scale) geliştirilmiştir. Araştırma kapsamında, “Freedom House Database” gibi, ölçeğin ülkelerin siber saldırılara ne kadar açık oldukları, hangi düzeyde işbirliği içinde bulundukları ve sivil ve politik özgürlüklerinden taviz vermeden

güvenliklerini nasıl sağlamlaştıracakları konusundaki derecelendirmeleri için kullanılabileceği belirtilmiştir.

Çalışma kapsamında, gelecek araştırmalar için göstergeler göz önüne alınarak ve ülkelerin karakteristiklerine dayandırılarak ölçeğin ülkelere uygulanmasına yoğunlaşılması gerektiği vurgulanmıştır. Ayrıca, Zaafiyet-İşbirliği-Özgürlük ölçeğinin, bir başka deyişle "Özeren Ölçeğinin" ülkelerin bireysel özelliklerine dayalı derecelenmesini değerlendiren bir alet olarak kullanılabileceği belirtilmiştir.

Araştırma, siber suç ve siber terörizme çare bulma konusunda birlikte çalışmanın son derece önemli olduğunu vurgulamaktadır. Araştırma siber terörizm olsun, siber suçlar ya da geleneksel terörizm olsun, konu uluslararası işbirliği olduğunda bir fark olmadığını göstermiştir. Araştırmanın sonuçlarına göre, dünyadaki en gelişmiş ve güçlü ülkeler, uluslararası işbirliğine en çok dayanan, önem veren ülkeler olmuştur. Sistemleri terörizme yanıt vermekte ne kadar gelişmiş olursa olsun, diğer ülkelerden iş birliği isteyen bu gelişmiş ülkeler en çok siber terörizm mağduru olanlardır. Araştırma, ayrıca yürütme organlarının işbirliğinin bir çok mağdur ülke için kesin çözüm olduğunu net bir biçimde ortaya koymuştur.

Internet Crime Complaint Center (İnternet Suçları Şikayet Merkezi), NW3C ve FBI'ın ortak hazırladığı 2006 İnternet Suçları raporunda, geçtiğimiz yılın önde gelen İnternet suçları açıklanmıştır. Elde edilen verilere göre; açık artırma dolandırıcılığı, % 44.9, gönderilmeyen mal, % 19, çek dolandırıcılığı, % 4.9, kredi kartı dolandırıcılığı, % 4.8, bilgisayar dolandırıcılığı, % 2.8, güven istismarı, kandırmaca, % 2.2, finansal kuruluş sahtekarlığı, % 1.6, kimlik hırsızlığı, %1.6, yatırım ortaklık dolandırıcılığı, % 1.3 ve çocuk pornografisi, % 1.0 olarak sıralanmıştır (Seven, 2008).

DÖRDÜNCÜ BÖLÜM

4. YÖNTEM

Bu bölümde araştırmanın modeli, evren ve örneklemi, verilerin toplanması, verilerin çözümü ve yorumlanması ele alınmıştır.

4.1. Araştırmanın Modeli

Bu araştırma, nitel ve nicel olmak üzere iki kısımdan oluşmuştur. Nitel araştırma için gözlem, görüşme, doküman incelemesi, nicel araştırma içinde "betimsel survey - betimsel tarama" yöntemi kullanılmıştır.

Araştırmada, Emniyet Teşkilatı'nda ilgili birimlere bilişim suçlarının çeşitli yönleri ile değerlendirildiği anket çalışması uygulanmıştır. Anket çalışmasının odak noktası, özellikle bilişim suçlarıyla mücadele ve bu kapsamda nasıl bir öğretim programı geliştirilmesi gerektiğini ortaya koymayı amaçlayan ihtiyaç analizidir. İlgili çevrelere uygulanan anket çalışması sonucunda e-posta, doküman incelemesi ve konu alanı uzmanları görüşme dönütlerinden elde edilen bulgular yorumlanmıştır.

4.2. Araştırmanın Evreni ve Örneklemi

Araştırma evrenini; konuya ilişkin tüm dokümanlar, bilişim suçları alanında emniyet teşkilatında çalışanların tamamı oluşturmaktadır.

Ancak, gerek araştırma kaynaklarının sınırlılığı, gerekse kullanılan bilgi toplama ve analiz yöntemlerinin özelliği nedeniyle çok sayıda bireyi araştırma örneklemine dahil etmek gerçekçi olmayabilir (Yıldırım ve Şimşek, 1999:54). Bu nedenle araştırmanın örneklemini,

a- Mevcut yerli ve yabancı dokümanlar,

b- 81 İl Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü (204 Personel), Kaçakçılık ve Organize Suçlar Şube Müdürlüğü (175 Personel) personelinden oluşan toplam 379 kişi oluşturmaktadır.

Bu şubelerin örnekleme alınmasının nedeni, Emniyet Teşkilatı'nda bilişim suçları konularında mahkemeden gelen veya polise intikal eden her türlü bilişim

suçlarının çözümü ve bilirkişiliğinin, yukarıda anılan ve bu konuda yetkin durumda olan 2 birimdeki görevli polisler tarafından yerine getirilmesidir.

4.3. Verilerin Toplanması

Araştırmada veri toplama aracı olarak anket geliştirilmiştir. Anket; 1. Kişisel bilgiler bölümü 2. Bilişim Suçları konusunda personelin görüş ve değerlendirmeleri 3. Bilişim suçlarına ilişkin personelin yeterlilik düzeylerini belirlemeye yönelik 47 maddeden oluşan ölçek olmak üzere üç bölümden oluşmaktadır.

4.4. Veri Toplama Aracı

Bu araştırmada kullanılan veri toplama aracı ve veri toplama aracındaki boyutlar araştırmacı tarafından geliştirilmiştir. Araştırma aracı, şu aşamalardan sonra oluşturulmuştur:

1. Aşama: Literatürü taraması ve Emniyet Teşkilatı'nda bilişim suçları alanında Bilgi İşlem Şube Müdürlüğü'nde ve Kaçakçılık Organize Suçlar Şube Müdürlüğü'nde görev yapan polis memurlarının sahip oldukları nitelikler belirlenmiştir. Bilişim suçları alanında görev yapan polislerin, bilişim suçlarındaki niteliklerine ilişkin olarak daha önce yapılan araştırmalar incelenmiştir. Ayrıca, buna ek olarak literatürde bilişim suçları ile mücadele ve bilişim suçlarında gerekli olan teknik donanım ve ünitelerin yeterlik durumlarına ilişkin yapılan araştırmalar da gözden geçirilmiştir.

2. Aşama: Bilişim suçları alanında konu alanı uzmanlarından, bilişim suçları, delillendirme, personelin eğitimi ve bilişim suçları ile etkin mücadele hakkında yarı yapılandırılmış görüşme formuyla bilgi toplanmıştır. Yapılandırılmış görüşme formlarında önceden yapılan ve ne tür soruların ne şekilde sorulup, hangi verilerin toplanacağını en ayrıntılı biçimde saptayan ve aynen uygulanan görüşme formlarıdır. Yapılandırılmamış görüşme formları ise görüşmeciye büyük yargı serbestliği vererek kişisel görüşlerin yoğun bir şekilde sonucu etkileyen formlardır. Yarı yapılandırılmış görüşme formu ise bu iki uç arasında olan bir görüşme formudur (Karasar, 2003: 167-168).

3. Aşama: Araştırmacı, açık uçlu soru anketi ve karşılıklı görüş alış-verişi için yapılan toplantılardan elde edilen verilere dayalı olarak; bilişim suçları konularında görev yapan polislere yönelik veri toplama aracını geliştirmiştir. Karasar (2003: 151) tarafından açıklandığı gibi veri toplama aracının içerik geçerliliği; veri toplama aracındaki maddelerin Ölçme amacına uygun olup olmadığı ile ve ölçülmek istenen alanı temsil edip etmediği ile ilgilidir. Bunun için uzman görüşüne başvurulur. Yani öncelikle bir grup uzman tarafından, ölçme amaçları ve bu amaçların gerektirdiği içerik çözümlemeleri yapılarak hazırlanmış soruların; bu amaçları ve içeriği temsil edip edemeyeceği tartışılmış. Buna göre: öneriler doğrultusunda veri toplama aracı yeniden düzenlenmiştir.

4. Aşama: Veri toplama aracı, Ankara Emniyet Genel Müdürlüğü Kaçakçılık Organize Suçlarla Mücadele Şube Müdürlüğü'nde görevli 22 bilişim suçları polisine uygulanmıştır. Böylelikle görevli polislerin görüşleri doğrultusunda, anketin kapsamı, ifadelerin anlaşılırlığı, maddelerin ulaşılmak istenen amaca hizmet etme boyutları gözden geçirilmiştir. Araştırmanın uygulandığı 379 kişiden elde edilen veriler dikkate alınarak bir fikir vermesi amacıyla Cronbach Alpha katsayısı hesaplanmış ve bu değer 0,9759 bulunmuştur.

Veri toplama aracı, üç bölümden oluşmaktadır. Birinci bölümde, polislerin kişisel bilgileri, İkinci bölümde bilişim suçları konusunda görüş ve değerlendirmeleri bulunmaktadır. Üçüncü bölümde, bilişim suçlarına ilişkin personelin sahip oldukları niteliklerin düzeylerini ilişkin görüşlerini içeren sorular bulunmaktadır. Bilişim suçlarında görev yapan personelin, bilişim suçları konularında kendi yeterlik düzeylerine ilişkin olarak görüşlerini bildirdikleri anket beşli likert türündedir. Bu ankette, bilişim suçları alanına yönelik olarak bilişim polislerinde olması gereken **bilme düzeyleri**, bilişim suçları polislerinin kendilerini ne ölçüde yeterli bilgi düzeyinde buldukları; " hiç bilmiyorum", "bilmiyorum", "kısmen biliyorum", "iyi biliyorum", "çok iyi biliyorum" seçenekleri ile ifade edilmektedir.

Aynı zamanda, ankette bilişim suçları polislerinin bilmesi gereken konuları ne derecede gerekli gördüklerinin ortaya çıkarılması amacıyla **gerekli görme düzeyleri**; “Çok Gerekli Görüyorum”, “Gerekli Görüyorum” “Kısmen gerekli görüyorum”, ”Az Gerekli Görüyorum” ”Hiç Gerekli Görmüyorum” seçenekleri ile belirlenmiştir. Buna göre maddeler şu şekilde sunulmuştur.

1= hiç bilmiyorum / hiç gerekli görmüyorum
2= bilmiyorum / az gerekli görüyorum
3= kısmen biliyorum / kısmen gerekli görüyorum
4= İyi biliyorum / gerekli görüyorum
5= çok iyi biliyorum / çok gerekli görüyorum

4.5. Verilerin Çözümü ve Yorumlanması

Anket sonucu ve doğal gözlem yoluyla elde edilen bulgular; frekans, yüzde, aritmetik ortalamalar, iki faktörlü varyans (two-way ANOVA for mixed mesures) analizi tekniklerinden yararlanarak çözümlenmiştir. Bunun yanında niteliksel veri olarak internet, bilişim, bilişim suçları ve eğitim konularında konuyla ilgili uzman kişilerin görüşlerine yer verilmiştir.

Araştırmada ölçme araçlarının geliştirilmesinde ve araştırma sonucunda elde edilen verilerin değerlendirilmesinde aşağıdaki analiz işlemleri kullanılmıştır.

İstatistiksel analiz işlemlerinde güven aralığı (anlamlılık düzeyi) .05 olarak belirlenmiştir. Anket çalışmasında, emniyet personelinin bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi düzeyleri ve bu bilgileri gerekli görme düzeylerine ilişkin verilerin çözümlenmesi ve yorumlanması için beşli ölçek aralıkları 0,80 (5-1= 4, 4/5= 0,80) oranında eşit aralıklar olarak aşağıdaki şekliyle belirlenmiştir.

Aritmetik ortalamalar sınır değerleri şu şekildedir:

1.00 1,80 hiç bilmiyorum / hiç gerekli görmüyorum
1,81 2,60 bilmiyorum / az gerekli görüyorum
2,61 3,40 kısmen biliyorum / kısmen gerekli görüyorum
3,41 4,20 İyi biliyorum / gerekli görüyorum
4,21 5.00 çok iyi biliyorum / çok gerekli görüyorum

İstatistiksel analiz işlemlerinde bilgisayar paket programlarından yararlanılmıştır. Verilerin analizi için SPSS for Windows 9.0 paket programı kullanılmıştır. Araştırma ile ilgili verilerin analizinde aşağıdaki tekniklerden yararlanılmıştır.

Araştırma kapsamında, bilişim suçları konusunda ilgililerce yapılan görüşmeye dayalı verilerin analizinde üç temel aşama esas alınmıştır. Bunlar sırası ile “betimleme”, “analiz” ve “yorumlama” aşamalarıdır.

Tez kapsamında, bilişim suçlarıyla etkin mücadele yapmak durumunda bulunan Emniyet Genel Müdürlüğü merkez ve taşra teşkilatında görevli polislere kişisel bilgilerin yanı sıra, bilgisayar ve İnternet kullanımı, bilgisayar-İnternet-bilişim suçları ve ilgili mevzuat, ayrıca bilişim suçlarında polisin eğitimi konularında bilgi seviyelerini tespit etmek ve ihtiyaç belirlemesi yapmak amacıyla bir anket oluşturulmuştur. Anket sonuçlarından, bilişim suçları konusunda bir öğretim programı geliştirmede yararlanılmıştır.

Öğretim programı, eğitim programı kapsamında yer almaktadır. Eğitim programına göre daha özel alanları kapsar. Öğretim programı, eğitim programının amaçlarını gerçekleştirmek üzere belli bir öğretim basamağında; genel amaçları, işlenecek konuları, derslerin sürelerini, derslerde kullanılacak araç-gereçleri, derslere uygun yöntem ve teknikleri ve değerlendirme durumlarını gösteren bir programdır (Gürol, 2006: 6). Anket ile elde edilen veriler sonucunda öğretim programı çalışması yapılmıştır. Bu program değerlendirilmek üzere alan uzmanı 8 kişiye gönderilmiştir. Bu uzmanlara yarı

yapılandırılmış bazı sorular yöneltilmiş ve görüşlerini belirtmeleri istenmiştir. Bunlar;

1. Hazırlanan modüllerin amaçları bilişim suçları eğitimi alacak polisin ihtiyaçlarını karşılayabilecek düzeyde midir?

2. Modüllerin içeriği bilişim suçları eğitimi açısından yeterince kapsamlı mıdır?

3. Modüllerin içeriği ile amaçları tutarlı mıdır?

4. İçerik yeterince açık, anlaşılır, ilgi çekici, güncel ve katılımcıların düzeylerine uygun mudur?

5. İçeriğin öğrenilmesi için önerilen süre yeterli midir?

6. Modüllerde yer alan değerlendirme programın amaçlarına ulaşma düzeyini belirleme, kapsam geçerliliği vb. açılardan yeterli midir?

7. Hazırlanan modülleri biçimsel özellikleri (görünüm, sayfa dizaynı, yazı karakteri, resim vb.) açılardan nasıl değerlendirirsiniz?

8. Bunların yanında belirtmek istediğiniz başka bir husus varsa lütfen yazınız? şeklindedir.

Uzmanlara sorulan yarı yapılandırılmış sorular neticesinde, temel ve uzmanlık seviyesinde modüller geliştirilmiştir.

BEŞİNCİ BÖLÜM

5. BULGULAR VE YORUMLAR

Bu bölümde araştırma kapsamında, bilişim suçları konusunda görev yapan personele yönelik düzenlenen ankete katılan kişilerle ilgili veriler aşağıdaki amaçlar doğrultusunda ele alınmış ve sunulmuştur.

5.1. Emniyet Teşkilatı Personelinin Kişisel Özelliklerine İlişkin Bulgu ve Yorumlar

Bu bölümde araştırma kapsamında, bilişim suçları konusunda görev yapan 81 İl Emniyet Müdürlüğü'ndeki Kaçakçılık Organize Suçlarla Mücadele ve Bilgi İşlem Şube Müdürlüklerindeki personelin kişisel özelliklerinin değerlendirilmesi ile ilgili veriler aşağıdaki amaçlar doğrultusunda ele alınmış ve sunulmuştur.

5.1.1. Görevli Olduğu İl'ler Nerelerdir?
5.1.2. Görevli Bulunduğu Birimler?
5.1.3. Eğitim Düzeyi Nasıldır?
5.1.4. Rütbe Durumu Nasıldır?
5.1.5. Emniyet Teşkilatı'ndaki Hizmet Süresi Ne Kadardır?
5.1.6. Bilişim Suçları Konularındaki Hizmet Süresi Ne Kadardır?

5.1.1. Emniyet Teşkilatı Personeli'nin Görev Yaptığı İl'ler?

Araştırma çerçevesinde, Emniyet Genel Müdürlüğü'ne bağlı bilişim suçları konusunda görev yapan 81 İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü personeli (175 Personel), ayrıca 81 İl Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü Sistem İletişim ve Bilişim Suçları Büro Amirliği personeline yönelik olarak (204 Personel) kişisel bilgiler ve "Bilişim Suçları" konusunda genel değerlendirmelerden oluşan bir anket çalışması ve "Bilişim Suçları" na ilişkin nitelik belirleme anketi uygulanmıştır.

Kısaca, tüm ülke genelinde bilişim suçlarıyla ilgili görev yapan personelden çeşitli veriler elde edilmiştir. Anket çalışması, tüm illerde Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü'nde görevli 2 şer personel, Bilgi İşlem Şube Müdürlüğü'nden ise 3 er personel belirlenerek gerçekleştirilmiştir.

Böylece, Emniyet Genel Müdürlüğü bünyesinde "Bilişim Suçları" konusunda görev yapan birimlerden olan 81 İl Emniyet Müdürlüğü Kaçakçılık Organize Suçlarla Mücadele ve Bilgi İşlem Şube Müdürlüğü personeli toplam 379 personele, anket uygulanarak Emniyet Teşkilatı'nın "Bilişim Suçları" konusundaki mevcut durumu, alt yapısı, eğitim faaliyetleri, gerekli organizasyonlar ve olması gerekenler hakkında veriler toplanmıştır.

5.1.2. Emniyet Teşkilatı Personeli'nin Görevli Olduğu Birim

Tablo 8: Bilişim Suçları Konusunda Görev Yapan Birimler

Seçenekler	f	%
Bilgi İşlem Şube Müdürlüğü	204	53,8
KOM Şb. Md.lüğü	175	46,2
Toplam	379	100,0

Tablo 8'de ülke genelinde, Emniyet Teşkilatı'nda bilişim suçları konusunda görev yapan emniyet personelinin görevli oldukları birimleri hakkında veriler yer almıştır. Tablo incelendiğinde Emniyet Genel Müdürlüğü'ne bağlı taşra teşkilatında yani 81 İl Emniyet Müdürlüğü'nde, "Bilişim Suçları" konusunda görev yapan birimlerden Bilgi İşlem Şube Müdürlüğü Sistem İletişim ve Bilişim Suçları Büro Amirliklerinden 204 personelin (% 53,8) oranında, ayrıca; 81 İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüklerinde görevli 175 personelin (% 46,2) oranında anket çalışması kapsamında görüşleri alınmıştır.

Ülke genelinde ise, Bilgi İşlem (204 personel) ve KOM (175 personel) birimlerinde "Bilişim Suçları" konusunda görev yapan 379 personelden toplanan verilerle anket çalışmasının analiz edildiği görülmektedir.

5.1.3. Emniyet Teşkilatı Personeli'nin Eğitim Durumu

Tablo 9: Emniyet Personelinin Eğitim Durumu

Seçenekler	f	%
Ortaokul ve Dengi	-	-
Lise ve Dengi	96	25,3
Meslek Yüksek Okulu	71	18,8
Üniversite veya Yüksek Okul	201	53,0
Yüksek Lisans, Doktora	11	2,9
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin eğitim durumu incelendiğinde, Tablo 9'da personelin en çok üniversite veya yüksek okul düzeyinde bulunduğu (% 53,0), bunu lise ve dengi okul düzeyinde bulunanların (% 25,3) takip ettiği görülmektedir. Meslek Yüksek Okulu mezunlarının oranı, % 18,8 olup, bunu % 2,9 ile yüksek lisans ve doktora düzeyinde bulunan personel takip etmektedir. Genel olarak bakıldığında, "Bilişim Suçları" konusunda görev yapan personelin eğitim düzeyinin yüksek eğitim düzeyinde olduğu görülmektedir.

Bu tür suçlarla ilgili görevli personelin eğitim düzeyinin, lise seviyesinin altında bulunmaması bilişim suçlarıyla mücadelede önemli bir unsur olarak ortaya çıkmaktadır. Yapılacak eğitim çalışmalarıyla da, personelin bilişim suçları alanındaki yetkinliğinin artırılması gerekmektedir. Ayrıca, her türlü eğitim düzeyinde elektrik, elektronik, bilgisayar vb. alanlardan mezun olan personelin "Bilişim Suçları" konusunda görev yapan birimlerde istihdam edilmeleri büyük önem taşımaktadır. Ayrıca, bilişim suçları alanındaki konular, cihazlar, yazılı dökümanlar, paket programlar genellikle İngilizce kaynaklı olduğundan, bilişim

suçlarında görev yapan personelin genellikle üniversite veya yüksek okul düzeyinde bulunması ve İngilizce seviyelerinin daha üst düzeyde olması bilişim suçlarında eğitim ortamı için önemli bir avantaj teşkil etmektedir.

5.1.4. Emniyet Teşkilatı Personeli'nin Rütbe Durumu

Tablo 10: Emniyet Personelinin Rütbe Durumu

Seçenekler	f	%
Polis Memuru	328	86,5
Kom.Yrd.	9	2,4
Komiser	17	4,5
Başkomiser	11	2,9
Emniyet Amiri	8	2,1
Şube Müdürü	3	,8
Diğer	3	,8
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin rütbe durumu incelendiğinde, büyük çoğunluğun Polis Memuru rütbesindeki personelden (% 86,5) oluştuğu Tablo 10'da görülmektedir. Amir seviyesindeki personelin oranı ise %13,5'tir.

Bu oranlara bakıldığında, özellikle bilişim suçları ile mücadelede 81 İl Emniyet Müdürlüğü'nde Bilgi İşlem Şube Müdürlüğü Sistem İletişim ve Bilişim Suçları Büro Amirliklerindeki ve Kaçakçılık Organize Suçlarla Mücadele Şube Müdürlüklerindeki Polis Memuru rütbesindeki personelin "Bilişim Suçları" konusunda daha yoğun olarak görev yaptığı ortaya çıkmaktadır. Polis Memuru rütbesindeki personel, Emniyet Genel Müdürlüğü Eğitim Daire Başkanlığı'nın hazırlamış olduğu hizmetiçi eğitim planları doğrultusunda bilişim suçları konularında eğitime tabi tutulması önemli faydalar getirecektir.

5.1.5. Emniyet Teşkilatı Personeli'nin Hizmet Süresi

Tablo 11: Emniyet Teşkilatı Personelinin Hizmet Süresi

Seçenekler	f	%
1-5 yıl	38	10,0
6-10 yıl	138	36,5
11-15 yıl	179	47,2
16-20 yıl arası	17	4,5
21 yıl ve üzeri	7	1,8
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin kaç yıldır Emniyet Teşkilatı'nda görev yaptığı incelendiğinde, 11-15 yıl arası görev yapanların % 47,2 ile ilk sırada yer aldığı Tablo 11'de görülmektedir. Bunu, % 36,5 ile 6-10 yıl arası görev yapanlar izlemektedir.

Dolayısıyla, 6-15 yıl arasında bilişim suçları konusunda görev yapanların oranı % 83,7 olarak karşımıza çıkmaktadır. 1-5 yıl arası Emniyet Teşkilatı'nda görev yapanların oranı ise % 10,0'dır. Bu oranın, artırılması yönünde çaba sarfedilmesi ve bu yönde ilgili alanlardan (elektrik, elektronik, bilgisayar vb.) personel istihdam edilmesi ile bilişim suçlarında başarının artacağı düşünülmektedir.

5.1.6. Emniyet Teşkilatı Personeli'nin "Bilişim Suçları" Konularındaki Hizmet Süresi

Tablo 12: Emniyet Teşkilatı Personelinin "Bilişim Suçları" Konularındaki Hizmet Süresi

Seçenekler	f	%
1-3 yıl arası	192	50,7
4-6 yıl arası	50	13,2
7-9 yıl arası	29	7,7
10 yıl ve üzeri	14	3,7
Boş	94	24,7
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin kaç yıldır "Bilişim Suçları" konularında görev yaptığı incelendiğinde, ağırlıklı olarak % 50,7 oranı ile 1-3 yıl arasında görev yaptıkları Tablo 12'den anlaşılmaktadır. "Bilişim Suçları" ülkemizde son yıllarda artan bir olgu olduğu için, konuyla ilgili birimler oluşturulmakta olup, ilgili personelin istihdam edilmesine gayret edilmektedir.

Bu bölümde, bilişim suçları alanında yapan emniyet personelinin iletişim teknolojisi ve bilgisayara ilişkin özellikleri hakkında çeşitli bulgu ve yorumlara yer verilmiştir. Emniyet personeli hakkında elde edilen veriler aşağıdaki maddelerden oluşmuştur.

5.2. Emniyet Teşkilatı Personeli'nin İletişim Teknolojisi ve Bilgisayara İlişkin Özellikleriyle İlgili Bulgu ve Yorumlar

Bu bölümde araştırma kapsamında, 81 İl Emniyet Müdürlüğü'ndeki Kaçakçılık ve Organize Suçlarla Mücadele ile Bilgi İşlem Şube Müdürlüklerindeki bilişim suçları konusunda görev yapan personelin iletişim teknolojisi ve bilgisayara ilişkin durumuyla ilgili veriler aşağıdaki amaçlar doğrultusunda ele alınmış ve sunulmuştur.

a) Evde Bilgisayar Bulunma Durumu Nedir?
b) Bilgisayar Kullanma Süresi Nedir?
c) Günlük Bilgisayar Kullanım Süresi Ne Kadardır?
d) İnternet Kullanma Süresi Ne Kadardır?
e) Günlük İnternet Kullanım Süresi Ne Kadardır?
f) Şahsa Ait Tescilli Web Sitesi Olma Durumu Nedir?
g) En Çok Yararlandığı Haberleşme Aracı Nedir?
h) İnternet Üzerinden Alışveriş veya Para Transferi **(sanal bankacılık)** Yapma Durumu Nedir?
i) İşletim Sistemlerindeki Güncellemeleri Takip Edebilme Durumu Nedir?
j) Meslek Öncesi, Polis Eğitim Kurumunda Bilgisayar ve İnternet Kullanımı ile İlgili Eğitim Alma Durumu Nedir?

5.2.1. Evde Bilgisayar Bulunma Durumu

Tablo 13: Personelin Evinde Bilgisayar Bulunma Durumu

Seçenekler	f	%
Evet	294	77,6
Hayır	85	22,4
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin evlerinde bilgisayar bulunup bulunmadığı incelendiğinde, personelin genel olarak (% 77,6) evinde bilgisayar bulunduğu görülmektedir. % 22,4 oranında ise "Bilişim Suçları" ile ilgili

görev yapan personelin evinde bilgisayar bulunmadığı görülmektedir. İlgili personelin evinde bilgisayar bulunması ve bu bilgisayarın İnternet bağlantısı olması, personelin bu suçlarla mücadelede sürekli bir aktivasyon içerisinde bulunması açısından önem taşımaktadır.

5.2.2. Bilgisayar Kullanma Süresi

Tablo 14: Yıllar İtibariyle Bilgisayar Kullanma Süresi

Seçenekler	f	%
1-5 yıl	51	13,5
6-10 yıl	181	47,8
11-15 yıl	112	29,6
16-20 yıl	31	8,2
21 yıl ve üzeri	4	1,1
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin ne kadar süreyle bilgisayar kullandığı incelendiğinde, % 47,8 oranında 6-10 yıl süre arasında bilgisayar kullandıkları Tablo 14'ten anlaşılmaktadır. Bunu, 11-15 yıl arasında bilgisayar kullananlar (% 29,6) izlemektedir. Avrupa Birliği ülkelerinde olduğu gibi, bilgisayarlaşma oranının ülkemiz koşullarında da artması ile bilgisayara karşı olar yetkinlik daha da artacaktır. Bu durum da, bilişim suçları ile mücadelede Emniyet Teşkilatı'na önemli katkı sağlayacaktır.

Ayrıca, Emniyet Teşkilatı imkanları ve Halk Eğitim Merkezleri aracılığıyla temel ve ileri düzeyde bilgisayar eğitimlerinin artırılması, zaman içerisinde bilişim suçlarıyla mücadeleye önemli katkılar sağlayacaktır.

5.2.3. Günlük Bilgisayar Kullanım Süresi Ne Kadardır?

Tablo 15: Personelin Günlük Bilgisayar Kullanım Süresi

Seçenekler	f	%
1-3 saat	48	12,7
4-6 saat	121	31,9
7-9 saat	124	32,7
10 saat ve üzeri	86	22,7
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, günlük olarak bilgisayar başında ne kadar süreyle bulunduğu incelendiğinde, Tablo 15'te de görüldüğü gibi 4-6 saat arasında (% 31,9) ve 7-9 saat arasında (% 32,7) yoğunlukla bilgisayar başında bulunuldukları ortaya çıkmaktadır. Günlük olarak 10 saat ve üzerinde, bilgisayar başında bulunan personelin oranı % 22,7 iken, 1-3 saat oranında bilgisayar başında bulunma oranı % 12,7 dir.

5.2.4. İnternet Kullanım Süresi

Tablo 16: İnternet Kullanım Süresi

Seçenekler	f	%
1-3 yıl arası	98	25,9
4-6 yıl	143	37,7
7-9 yıl	99	26,1
10 yıl ve üzeri	39	10,3
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, kaç yıldır İnternet kullandığı incelendiğinde, ağırlıklı olarak (% 37,7) 4-6 yıl arasında İnternet

kullandığı Tablo 16'da görülmektedir. Bunu, 7-9 yıl arası (% 26,1) ve 1-3 yıl arası (% 25,9) İnternet kullanımı takip etmektedir. 10 yıl ve üzerinde İnternet kullanan personelin oranı ise % 10,3'tür.

İnternet, doğası gereği suç ortamına açık bir alan olduğundan dolayı polisin, İnternet ortamında meydana gelebilecek tehdit, risk ve açıkları iyi bilmesi bilişim suçlarının çözümünde önemli rol oynayacaktır. Bu nedenle, İnternet ortamı ile ilgili olarak İnternet terimleri ve İnternet üzerinden işlenen suçlarla ilgili personelin uygulamalı eğitimler ile yetkinliği sağlanması büyük önem taşımaktadır.

5.2.5. Günlük Olarak İnternet Kullanım Süresi

Tablo 17: Günlük Olarak İnternet Kullanım Süresi

Seçenekler	f	%
1 saat'ten az	88	23,2
1-3 saat	175	46,2
4-6 saat	77	20,3
7 saat ve üzeri	39	10,3
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, günlük olarak İnternet'e ne kadar zaman ayırdığı incelendiğinde ağırlıklı olarak (% 46,2) oranında, 1-3 saat arasında İnternet'e zaman ayırdıkları Tablo 17'de görülmektedir. Bunu, bir saat'ten az (% 23,2) ve 4-6 saat arası (% 20,3) İnternet kullanımı takip etmektedir. 7 saat ve üzerinde günlük olarak İnternet'e zaman ayıran personelin oranı ise % 10,3'tür.

5.2.6. Şahsa Ait Tescilli Web Sitesinin Varlığı

Tablo 18: Şahsa Ait Tescilli Web Sitesinin Varlığı

Seçenekler	f	%
Evet	41	10,8
Hayır	338	89,2
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, kendilerine ait tescilli web sitesi bulunup bulunmadığı incelendiğinde, genel olarak web sitelerinin bulunmadığı (% 89,2) Tablo 18'den anlaşılmaktadır. Kendilerine ait tescilli web sitesi bulunanların oranı ise sadece % 10,8'dir. Personelin kendisine ait tescilli web sitesi bulunması, İnternet ortamına daha yakın olması ve böylece İnternet üzerindeki sorunlarla ilgili etkililiği için önem taşımaktadır. Personelin, kendilerine ait tescilli web sitesi oranının zaman içerisinde % 10,8'den daha yukarı seviyelere çıkarılması arzu edilmektedir.

5.2.7. En Çok Yararlanılan Haberleşme Aracı

Tablo 19: En Çok Yararlanılan Haberleşme Aracı

Seçenekler	f	%
E-mail	46	12,1
Anlık mesajlaşma sistemleri (ICQ, Messenger, IRC vb.)	43	11,4
Cep Tel	287	75,7
Diğer	3	,8
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, haberleşme aracı olarak en çok hangi ortamdan yararlandıkları incelendiğinde, çoğunlukla (% 75,7) cep

telefonundan yararlandıkları görülmektedir. E-mail aracılığıyla %12,1 oranında, anlık mesajlaşma sistemlerinden (ICQ, Messenger, IRC vb.) ise % 11,4 oranında yararlanıldığı görülmektedir. Görüldüğü gibi, haberleşme aracı olarak İnternet ortamının kullanılması, yanında bir takım sorumlulukları da beraberinde getirmektedir. Özellikle, günümüzde MSN şifresi ele geçirilmesi vb. konular sıklıkla yaşanmakta olup, bu durum gerekli önlemlerin alınmasını ve halk bazında Toplum Destekli Polislik hizmetleriyle bilinçlendirme faaliyetlerinin yapılmasını gerektirmektedir.

5.2.8. İnternet Üzerinden Alışveriş veya Para Transferi (Sanal Bankacılık) Yapma Tercihleri

Tablo 20: İnternet Üzerinden Alışveriş veya Para Transferi (Sanal Bankacılık) Yapma Tercihleri

Seçenekler	f	%
Evet	214	56,5
Kısmen	47	12,4
Hayır	118	31,1
Toplam	379	100,0

Araştırmaya katılan 379 personelin, İnternet üzerinden alışveriş veya para transferi **(Sanal Bankacılık)** yapma tercihleri incelendiğinde, personelin genel olarak (% 56,5) sanal bankacılık uygulamalarını kullandıkları Tablo 20'de görülmektedir. % 31,1 oranında ise personel, İnternet üzerinden alışveriş veya sanal bankacılık uygulamasını tercih etmemektedir. İnternet üzerinden alışveriş veya para transferi **(Sanal Bankacılık)** uygulaması, içinde bir takım riskleri içeren ve bilişim suçlarının işlenebileceği bir ortamı içermektedir. Güvenlik katmanlarının geliştirilerek bu tür uygulamaların yapılmasının, risk faktörünü minimuma indireceği düşünülmektedir. Tüm dünya üzerinde bu tür uygulamalar gerçekleştirilmekte olup, ev ve iş yerlerinde güvenli şifre kullanımı, antivürüs kullanımı, firewall kullanımı gibi tedbirler ve genel elektronik güvenlik yöntemleriyle ve vatandaşların duyarlı hale getirilmesiyle sanal bankacılık konusunda problem olmadan yol alınabilecektir.

Türkiye'de internet bankacılığı uygulaması 2000 yılında başlamasına karşın, uygulama 2003'ten itibaren yoğun olarak kullanılmıştır. Sanal Banka Mağdurları Derneği tarafından, ülkemizde geçen yıl internet ortamında dolandırıcılığa uğrayan sanal banka mağdurlarının sayısının bir önceki yıla göre yüzde 50 düştüğü bildirilmiştir. Dernek, 2006'da yapılan yaklaşık 4 bin olan mağdur başvuru sayısının, geçen yıl yaklaşık yüzde 50 azalarak 2 bin 200'e düştüğünü belirtmiştir. Sanal Banka Mağdurları Derneği mağdurlar arasında, kamu ve özel kuruluşların yanı sıra işadamları, turizmci ve sanatçıların bulunduğunu belirtmiş ve bankaların personellerinin yanı sıra müşterilerini eğitmeye başlamalarının mağdurların sayısını önemli ölçüde azalttığını ifade etmiştir (stargazete.com, 2008).

5.2.9. İşletim Sistemlerindeki Güncellemeleri Takip Edebilme Durumu

Tablo 21: İşletim Sistemlerindeki Güncellemeleri Takip Edebilme Durumu

Seçenekler	f	%
Evet	211	55,7
Kısmen	128	33,8
Hayır	40	10,6
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, işletim sistemlerindeki güncellemeleri takip edip edemedikleri incelendiğinde, Tablo 21'de görüldüğü gibi genel olarak personelin (% 55,7) işletim sistemlerindeki güncellemeleri takip edebildikleri görülmektedir. Kısmen takip edebilen personelin oranı % 33,8 iken, işletim sistemlerindeki güncellemeleri takip edemeyen personelin oranı ise %10,6'dır. İşletim sistemindeki güncellemelerin takip edilememesi, bilişim suçlarının çözümünde zorluklar ve sisteme yapılan saldırıların niteliğinde artma ve zafiyetler meydana getirecektir. Yapılacak temel ve uzmanlık seviyesinde düzenlenen bilişim suçları eğitimi ile hizmetiçi eğitim faaliyetleri düzenlenerek

personelin işletim sistemlerindeki güncellemeleri takip edebilmeleri mümkün olacaktır.

5.2.10. Meslek Öncesi, Polis Eğitim Kurumunda Bilgisayar ve İnternet Kullanımı ile İlgili Eğitim Alma Durumu

Araştırmaya katılan 379 personelin, meslek öncesi polis eğitim kurumlarında bilgisayar ve İnternet kullanımı ile ilgili eğitim alıp almadıkları incelenmiş ve elde edilen veriler Tablo 22'de sunulmuştur.

Tablo 22: Meslek Öncesi, Polis Eğitim Kurumunda Bilgisayar ve İnternet Kullanımı ile İlgili Eğitim Alma Durumu

Seçenekler	f	%
Evet	173	45,6
Hayır	206	54,3
Toplam	379	100,0

Tablo 22'de görüldüğü gibi personelin genel olarak (% 54,3) eğitim almadıkları ortaya çıkmaktadır. Eğitim alanların oranı ise % 45,6'dır. Meslek öncesi, polis eğitim kurumlarında bilgisayar ve İnternet kullanımı ile ilgili eğitim alınması bilişim suçlarıyla mücadelede görev alacak personelin istihdamı ve uzmanlaştırılmasında büyük önem taşımaktadır. Bu nedenle, polis memuru yetiştiren POMEM ve PMYO'nın eğitim müfredatlarında bilgisayar ile ilgili programın yeniden düzenlenmesi, bilgisayar uygulama laboratuarlarının sayısının artırılması, bilgisayar eğiticilerinin istihdamı ve bilişim suçları konularının bilgisayar eğitimi aşamasında program içerisinde yer alması gerekmektedir.

5.3. Emniyet Personelinin Bilişim Suçları ile İlgili Niteliklerine İlişkin Bulgu ve Yorumlar

Bu bölümde, emniyet personelinin bilişim suçları ile ilgili niteliklerinin nasıl olduğu konusunda bulgu ve yorumlara yer verilmiştir. Bu kapsamda bilişim suçları ile ilgili personelin bu alandaki eğitim durumu, karşılaştıkları bilişim

suçlarının neler olduğu ve bilişim suçlarıyla ilgili mevcut yapı ve diğer konular hakkındaki görüş ve önerileri alınmıştır. Emniyet personelinin bilişim suçları ile ilgili niteliklerinin neler olduğu 21 maddeden oluşan verilerle ortaya konmuştur.

5.3.1. İnternet ve Güvenliği ile İlgili Kaynakları Takip Edebilme Durumu Ne Düzeyderdir?

5.3.2. Meslek İçinde, "Bilişim Suçları" ile İlgili Kurs Görme Durumu Nedir?

5.3.3. Bilişim Suçları ile İlgili Düzenlenen Konferans veya Seminerlere Katılma Durumu Ne Düzeydedir?

5.3.4. Bilişim Suçları ile İlgili Eğitim İhtiyaç Durumu Nedir?

5.3.5. Bilişim Suçlarıyla Mücadelede, Personelin Gelişimine Etki Eden Faktörler Nelerdir?

5.3.6. Bilişim Suçlarıyla Mücadelede Yeterli Olunan Konular Nelerdir?

5.3.7. Bilişim Suçlarıyla Mücadelede Yetersiz Olunan Konular Nelerdir?

5.3.8. Bilişim Suçlarıyla Mücadele Kapsamında Yeterli Eğitim Alma Durumu Ne Düzeydidir?

5.3.9. Bilişim Suçlarıyla Mücadele Kapsamında Eğitim Alma İhtiyacı Olunan Konular Nelerdir?

5.3.10. Bilişim Suçları Konusunda Bilirkişi Olarak Görev Alma Durumu Nedir? ve Görev Alınan Konular Nelerdir?

5.3.11. En Çok Karşılaşılan Bilişim Suçları Nelerdir?

5.3.12. Bilişim Suçlarıyla Mücadelede İyi Bilinen Sistemler Nelerdir?

5.3.13. Bilişim Suçları Konusunda Yetersiz Kalma Durumu Ne Düzeydedir?

5.3.14. Bilişim Suçları Konusunda Yetersiz Kalındığında EGM Bünyesinde Destek Alınan Birimler Hangileridir?

5.3.15. Bilişim Suçları Konusunda Yetersiz Kalındığında Dışarıdan Destek Alınan Kurum ve Kuruluşlar Hangileridir?

5.3.16. İl Emniyet Müdürlüklerinde Bilişim Suçlarıyla Mücadelede En Yetkin Birim Hangisidir?

5.3.17. İl Emniyet Müdürlüklerinde Bilişim Suçlarıyla Mücadele Eden Birimlerin Daha Donanımlı Hale Getirilmesi Gerekli Midir?

5.3.18. Emniyet Genel Müdürlüğü Bünyesinde **"Bilişim Suçları"** İle İlgili Bir Ünite Kurulması Gerekli Midir?

5.3.19. Bilişim Suçları ile İlgili Görev Alınan İlginç Olaylar Nelerdir?

5.3.20. Bilişim Suçlarıyla Mücadelede, Personelin Eğitimi Konusunda Belirtmek İstediği Konular Nelerdir?

5.3.21. Bilişim Suçlarıyla Mücadele Kapsamında Belirtmek İstedikleri Diğer Konular Nelerdir?

5.3.1. İnternet ve Güvenliği ile İlgili Kaynakları Takip Edebilme Durumu

Tablo 23: İnternet ve Güvenliği ile İlgili Kaynakları Takip Edebilme Durumu

Seçenekler	f	%
Evet	146	38,5
Kısmen	171	45,1
Hayır	62	16,4
Toplam	379	100,0

İnternet güvenliği ile ilgili kaynakları (Kitap, Dergi, Online Ortam vs.) takip edebilme, bilişim suçlarıyla mücadelede önemli yarar ve katkılar sağlayacaktır. Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, İnternet güvenliği ile ilgili kaynakları (Kitap, Dergi, Online Ortam vs.) takip edip edemedikleri incelendiğinde, Tablo 23'ten de anlaşılacağı gibi, çoğunlukla kısmen takip edebildikleri (% 45,1) görülmektedir. İlgili kaynakları takip edebilenlerin oranı ise % 38,5'tir. İnternet güvenliği ile ilgili kaynakları (Kitap, Dergi, Online Ortam vs.) takip edemeyenlerin oranı % 16,4'tür. Bilişim suçları konusunda görev yapan personelin dizayn edilecek eğitim portallarıyla, İnternet güvenliği hakkındaki kaynakları takip edebilmeleri söz konusu olacaktır. Aynı zamanda, adli bilişim ve bilişim suçları alanında yabancı web site ortamlarından da personelin istifade etmesi, bilişim suçlarının çözümünde büyük yararlar getirecektir.

5.3.2. Meslek İçinde "Bilişim Suçları" ile İlgili Kurs Görme Durumu

Araştırmaya katılan 379 personelin meslek içinde "Bilişim Suçları" ile ilgili bir kurs görüp görmediği incelenmiş ve elde edilen veriler Tablo 24'de sunulmuştur.

Tablo 24: Meslek İçinde "Bilişim Suçları" ile İlgili Kurs Görme Durumu

Seçenekler	f	%
Evet	74	19,5
Hayır	305	80,5
Toplam	379	100,0

Görüldüğü gibi personelin genel olarak (% 80,5) bir kurs görmediği Tablo 24' te ortaya çıkmaktadır. Kurs görenlerin oranı ise % 19,5 oranındadır. Bilişim suçları konusunda görev yapan personelin, "Bilişim Suçları" ile ilgili konularda, kendini yenilemek ve yetkinliğini artırmak amacıyla uygulamalı olarak meslek içinde kurs görmesi, bu tip suç türleri ile mücadelede büyük önem taşımaktadır. Bilişim suçlarında; sürekli olarak çeşitlilik, değişiklik ve yenilikler gözlemlenmektedir. Bu nedenle, "Bilişim Suçları" alanındaki eğitim faaliyetlerinin temel ve uzmanlık seviyesinde meslek yaşamı boyunca sürekli olarak da devam etmesi ve bu tür eğitimlerin Eğitim Daire Başkanlığı Hizmetiçi eğitim planları içerisinde bulunmasının sağlanması gerekmektedir.

Polis teşkilatında, özellikle Kaçakçılık ve Organize Suçlarla Mücüdele Daire Başkanlığı bünyesinde, bilişim suçları alanında düzenlemiş olduğu faaliyetler dikkat çekici ve takdire şayandır. Daire Başkanlığına bağlı 13 İl Emniyet Müdürlüğü belirlenmesi ve buralarda adli bilişim, bilişim suçları alanında uzman görevlilerin bulundurularak eğitimlerin düzenlenmesi bunun en açık örneğidir. Bilişim suçları konusunda görev yapan personelin de belirttiği gibi, bilişim suçlarıyla etkin mücadele için meslek içindeki eğitim sadece merkez teşkilatı ile sınırlı kalmayarak, taşra teşkilatınında eğitimine ve uygun ortam oluşturulmasına önem verilmesi gerekmektedir. Aynı zamanda, amir sınıfı personelinde yetiştirilmesi için gerekli ortamın tesis edilmesi gerekmektedir.

5.3.3. Bilişim Suçları ile İlgili Düzenlenen Konferans veya Seminerlere Katılma Durumu

"Bilişim Suçları" ile ilgili herhangi bir konferans veya seminere katılıp katılmadığı incelenmiş ve sonuçlar Tablo 25'te özetlenmiştir.

Tablo 25: Bilişim Suçları ile İlgili Düzenlenen Konferans veya Seminerlere Katılma Durumu

Seçenekler	f	%
Evet	90	23,7
Hayır	289	76,3
Toplam	379	100,0

Buna göre personelin çoğunlukla (% 76,3) böyle bir eğitim faaliyetine katılmadığı görülmektedir. "Bilişim Suçları" ile ilgili eğitim faaliyetine katılan personelin oranı ise % 23,7 dir. Bilişim suçları ile mücadelede; yetkinliğin artırılması, güncel gelişmelerin yakından takibi ve bu tür faaliyetlere katılanların paylaşımcılığının sağlanması için ulusal ve uluslararası konferans, seminer ve sempozyumların organize edilmesi ve çeşitli kurum ve üniversitelerce düzenlenen bu tür etkinliklere katılım büyük önem taşımaktadır. Üst düzey yönetimin, bu tür etkinliklere personelin katılımını sağlaması ve merkez tarafından organizeli bir şekilde tüm İl Emniyet Müdürlükleri'nden uygun personelin katılımının sağlanması teşkilatın konuya bakış açısı ve güncel olarak bilişim suçlarının takip edilerek yetkinliğin artırılması açısından son derece önemlidir.

5.3.4. Bilişim Suçları ile İlgili Eğitim İhtiyaç Durumu

Tablo 26: Bilişim Suçları ile İlgili Eğitim İhtiyaç Durumu

Seçenekler	f	%
Evet	350	92,3
Hayır	29	7,7
Toplam	379	100,0

“Bilişim Suçları” ile ilgili eğitim alma ihtiyacı incelendiğinde, personelin büyük çoğunlukla (% 92,3) eğitime ihtiyaç duyduğu Tablo 26’da görülmektedir. Sadece % 1,6 oranında personel eğitim alma ihtiyacı hissetmemektedir. Bu sonuçlara göre, Emniyet Teşkilatı’nda eğitim ile ilgili çeşitli faaliyet ve organizasyonların yoğun olarak yerine getirilmesi gerçeği ortaya çıkmaktadır. Personelin eğitim eksikliğinin giderilmesi, Emniyet Teşkilatı’nın “Bilişim Suçları” ile ilgili yetkin hizmetler vermesinde önemli birr yere sahiptir. Türk polisinin, bilişim suçlarında temel eğitim ve uzmanlık eğitimi programlarıyla sürekli olarak eğitim faaliyetlerinde bulunması gerekmektedir.

Emniyet Genel Müdürlüğü Eğitim Daire Başkanlığı Hizmetiçi eğitim programları içerisine “Bilişim Suçları” konusu dahil edilerek tüm teşkilat personelinin bu alanda bilgi sahibi olması ve belli bir bilgi düzeyine ulaşmasının, bilişim suçlarıyla mücadelede önemli rol oynayacağı düşünülmektedir. Gerek yüz yüze eğitimler ile, gerekse on-line eğitim ortamlarıyla ve yazılı doküman (broşür, kitapçık, kitap) sağlanmasıyla, kısacası her türlü eğitim ortamı oluşturularak bilişim suçlarında görev yapan personelin eğitim seviyesinin artırılması gerekmektedir.

5.3.5. Bilişim Suçlarıyla Mücadelede, Personelin Gelişimine Etki Eden Faktörler

Tablo 27: Bilişim Suçlarıyla Mücadelede,Personelin Gelişimine Etki Eden Faktörler

Seçenekler	f	%
Bireysel Çabalarım, Kendi Kendimi Geliştirmem	232	61,2
Kurumumun Sağladığı Eğitim Olanakları	22	5,8
Hem Kendi Çabalarım, Hem de Teşkilatın Eğitim Olanakları	82	21,6
Bilişim Suçlarıyla İlgili Konularda Sürekli Görev Almamdan Dolayı	29	7,7
Diğer	14	3,7
Toplam	379	100,0

Araştırmaya katılan 379 personelin “Bilişim Suçları” ile mücadele kapsamında gelişiminde en çok hangi faktörün rol oynadığı incelendiğinde, personelin daha çok (% 61,2) bireysel çabaları ve kendi kendini geliştirmesinin bu konuda rol oynadığı görülmektedir (Tablo 27). Bunu, personelin kendi çabaları ve teşkilatın eğitim olanakları (% 21,6) izlemektedir. Bilişim suçları konularında eğitim maliyetinin yüksek olması nedeniyle, kurum olanaklarının artırılması ve eğitim ortamlarının tesis edilmesi büyük önem taşımaktadır. Teşkilat olarak bilişim suçları konusuna önem verilmesi ve genel farkındalık düzeyinin artırılmasıyla, ayrıca uygun personel seçimine önem verilmesi ve bilişim suçları eğitimi için gerekli bütçe imkanları temin edilmesiyle, bilişim suçları alanında ilerleme kaydedilebilecektir.

5.3.6. Bilişim Suçlarıyla Mücadelede Çok İyi Olunan Konular

Emniyet Genel Müdürlüğü’ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelden “Bilişim Suçları” ile mücadele kapsamında çok iyi olduklarını düşündükleri 3 konunun tespiti amacıyla görüşleri istenmiştir. “Bilişim Suçları” ile mücadele kapsamında personelin **çok iyi** olduklarını düşündükleri ilk 3 konu; veri kurtarma, IP tespiti ve firewall konularıdır.

“Bilişim Suçları” ile mücadele kapsamında personelin **çok iyi** olduklarını düşündükleri diğer konular Tablo 28’de görülmektedir.

Tablo 28: Bilişim Suçlarıyla Mücadelede Kapsamında Personelin Çok İyi Olduklarını Düşündükleri Konular

Personelin, "Bilişim Suçları" ile mücadele kapsamında çok iyi olduklarını düşündükleri konular	Personel Sayısı
Veri Kurtarma	31
IP Tespiti	26
Firewall	13
İnternet Üzerinden Para Transferi	12
Kredi Kartı Dolandırıcılığı	10
Forensic(Adli bilişim)	9
E-mail Takibi	9
Delil İnceleme	8
Network	8
Virüs Programları	8
Ip Tools	7
Bilgisayar İnceleme	6
Kredi Kartı Kopyalama	6
İnternet Güvenliği	5
Korsan Yazılım	5
Suç ve Suçlu Takibi	5
Bilgisayar Yoluyla Dolandırıcılık	5
Sahte Belge (Bilgisayarda)	4
Virüs Server	4
İnternet'ten Kişilik Haklarına Saldırı, Tehdit	3
Mevzuat	3

Düzenlenecek eğitim faaliyetleri ile, bilişim suçları konusunda görev yapan personelin "Bilişim Suçları" ile mücadele kapsamında çok iyi olduklarını düşündükleri konuların daha da artırılması gereklidir.

5.3.7. Bilişim Suçlarıyla Mücadelede Yetersiz Olunan Konular

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelden "Bilişim Suçları" ile mücadele kapsamında yetersiz olduklarını düşündükleri 3 konunun tespiti amacıyla görüşleri istenmiştir. "Bilişim Suçları" ile mücadele kapsamında personelin

yetersiz olduklarını düşündükleri ilk 3 konu; saldırı tespit sistemleri, kredi kartları kopyalama ve sanal ortamda para transferi konularıdır. "Bilişim Suçları" ile mücadele kapsamında personelin yetersiz olduklarını düşündükleri diğer konular Tablo 29'da görülmektedir.

Tablo 29: Bilişim Suçlarıyla Mücadelede Kapsamında Personelin Yetersiz Olduklarını Düşündüğü Konular

Personelin, "Bilişim Suçları" ile mücadele kapsamında yetersiz olduklarını düşündükleri konulardan bazıları	Personel Sayısı
Saldırı Tespit Sistemleri	23
Kredi Kartları Kopyalama	22
Sanal Ortamda Para Transferi	19
IP Tespiti	18
Firewall	11
Bilgisayar Yoluyla Dolandırıcılık	10
Donanım	10
IP Manager (port açıkları tespiti)	10
Linux İşletim Sistemi	10
Kredi Kartı Dolandırılıcığı	9
Yazılım	8
Veri Kurtarma	8
Etherial (ip trafik)	6
Kripto	6
Hacking Yöntemleri	5
Veri İnceleme	5

Personelin, hangi alanlarda yetersiz olduğunu bilmesi önemli bir husustur. Böylece, düzenlenecek eğitim faaliyetlerinde özellikle belli alanlarda eksikliği bulunan personellere yönelik olarak eğitim içeriği sağlanabilecektir. Düzenlenecek eğitim faaliyetleri ile, bilişim suçları konusunda görev yapan personelin "Bilişim Suçları" ile mücadele kapsamında yetersiz oldukları konularda güçlendirilmeleri ve uygulama ile yetkin hale getirilmeleri gerekmektedir.

5.3.8. Bilişim Suçlarıyla Mücadele Kapsamında Yeterli Eğitim Alma Durumu

Araştırmada yer alan 379 personelin, "Bilişim Suçları" ile mücadele kapsamında yeterli eğitim aldıkları 3 konunun tespiti amacıyla görüşleri istenmiştir. "Bilişim Suçları" ile mücadele kapsamında personelin yeterli eğitim aldıklarını düşündükleri ilk 3 konu; IP tespiti, veri inceleme ve veri kurtarma konularıdır. Personelin, "Bilişim Suçları" ile mücadele kapsamında yeterli eğitim aldığını düşündükleri diğer konular Tablo 30'da yer almaktadır.

Tablo 30: Bilişim Suçlarıyla Mücadele Kapsamında Personelin Yeterli Eğitim Aldıklarını Düşündüğü Konular

Personelin, "Bilişim Suçları" ile mücadele kapsamında **yeterli eğitim aldığını** düşündüğü bazı konular	Personel Sayısı
Veri İnceleme	8
IP Tespiti	8
Veri Kurtarma	5
Network	3
Donanım	3
Encase	3
Adli Bilişim	3
Mevzuat	3
Web Sitesi İnceleme	2
Kredi Kartı Dolandırıcılığı	2
Sahte Kredi Kartı	2
İnteraktif Bankacılık	2

Personelin, "Bilişim Suçları" ile mücadele kapsamında genel olarak yeterli eğitim aldıkları söylenebilir. Ancak, düzenlenecek eğitim faaliyetleri ile bilişim suçları konusunda görev yapan personelin "Bilişim Suçları" ile mücadele kapsamında özellikle yeni suç tipleri ve teknolojideki gelişmeleri de göz önüne alarak yeterli eğitim aldıkları konuların daha da artırılması gerekmektedir.

5.3.9. Bilişim Suçlarıyla Mücadele Kapsamında Eğitim Alma İhtiyacı Olunan Konular

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan eden 379 personelin, "Bilişim Suçları" ile mücadele kapsamında eğitim alma ihtiyacı olduğu 3 konunun tespiti amacıyla görüşleri istenmiştir. Personelin, "Bilişim Suçları" ile mücadele kapsamında **eğitim alma ihtiyacı olduğu** ilk 3 konu; IP manager, saldırı tespit sistemleri ve bilgisayar yoluyla dolandırıcılık konularıdır. Personelin, "Bilişim Suçları" ile mücadele kapsamında eğitim alma ihtiyacı olduğunu düşündükleri diğer konular Tablo 31'de yer almaktadır.

Tablo 31: Bilişim Suçlarıyla Mücadele Kapsamında Personelin Eğitim Alma İhtiyacı Olduğunu Düşündüğü Konular

Personelin, "Bilişim Suçları" ile mücadele kapsamında **eğitim alma ihtiyacı olduğunu** düşündüğü konulardan bazıları	Personel Sayısı
IP Manager	40
Saldırı Tespit Sistemleri	39
Bilgisayar Yoluyla Dolandırıcılık	23
Kredi Kartı Kopyalama	23
İnternet Üzerinden Para Transferi	22
Firewall	19
Veri Kurtarma	17
Hackerların Kullanıldığı Yöntemler	15
İnternet Üzerinden Dolandırıcılık	15
Linux	14
Kredi Kartı Dolandırıcılığı	13
Bilgisayar Yoluyla Sahtecilik	11
Kripto	11
Çocuk Pornorafisi	10

Personel ayrıca, her konuda eğitim almak isterim (61 Kişi) şeklinde görüş belirterek, genel olarak eğitim konusunda eksiklikler olduğunu vurgulamıştır. Tabloda'da görüldüğü gibi personelin, "Bilişim Suçları" ile mücadele kapsamında genel olarak eğitim alma ihtiyacı görülmektedir.

Personelin, düzenlenecek olan eğitim faaliyetleri ile özellikle eğitim alma ihtiyacı olduğu konularda uygulamalı olarak eğitime tabi tutulması “Bilişim Suçları” ile mücadele kapsamında büyük faydalar sağlayacaktır.

5.3.10. Bilişim Suçları Konusunda Bilirkişi Olarak Görev Alma Durumu ve Görev Alınan Konular

Emniyet Genel Müdürlüğü’ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin herhangi bir (İnternet suçu, Bilgisayar suçu, Bilişim suçu) suç konusuyla ilgili bilirkişi olarak görev alıp almadığı incelendiğinde, personelin genel olarak (% 70,5) bilirkişilik yapmadığı Tablo 32’de görülmektedir.

Tablo 32: Bilişim Suçları Konusunda Bilirkişi OlarakGörev Alma Durumu ve Görev Alınan Konular

Seçenekler	f	%
Bugüne Kadar (İnternet suçu, Bilgisayar suçu, Bilişim suçu) Bir Suç Konusuyla İlgili Bilirkişi Olarak Görev Aldınız mı?		
Evet	112	29,5
Hayır	267	70,5
Toplam	379	100,0
Bilirkişi Olarak, En Çok Hangi Bilişim Suçu Konusunda Görev Aldınız?		
Çocuk Pornografisi	34	9,0
Bilgisayar Yoluyla Dolandırıcılık	33	8,7
Bilgisayar Yoluyla Sahtecilik	18	4,7
İnternet Üzerinden Para Transferi	18	4,7
Kredi Kartı Kopyalama	3	,8
Diğer	24	6,3
Boş	249	64,8
Toplam	379	100,0

Bilirkişi olarak görev alanların oranı ise % 29,5 düzeyindedir. Personelin gerekli eğitim organizasyonları neticesinde sertifikalandırılması ve bilirkişilik vasıflarının temin edilmesi ile, bilişim suçlarıyla mücadelede Emniyet Teşkilatı'na önemli katkılar sağlanacağı düşünülmektedir.

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin bilirkişi olarak, en çok hangi bilişim suçu konusunda görev aldığı incelendiğinde, % 9,0 oranı ile çocuk pornografisi konusunda yapılan bilirkişilik ön plana çıkmaktadır. Bunu, % 8,7 oranı ile bilgisayar yoluyla dolandırıcılık izlemektedir. Ayrıca, personelin genel olarak bu tür suçlarda bilirkişi olarak görev almadığı görülmektedir. Adli makamların, polisten bilirkişi talebi hususlarında, daha çok amir sınıfı personelin görevlendirildiği görülmekte olup, bilirkişi seviyesinde personelin polis memuru rütbesinde de sağlanması gerekmektedir. Bilişim suçu konusunda polis teşkilatında ülke genelinde bilirkişi seviyesinde personelin sayı olarak yeterli düzeye kavuşturulması, adli makamlarında daha rahat çalışma ortamı yakalamasına neden olacaktır.

5.3.11. En Çok Karşılaşılan Bilişim Suçları

Günümüzde bilişim suçlarında çeşitlilik artmakta olup, aynı zamanda çeşitlilik gösteren bu bilişim suçları tüm dünyada hızlı bir şekilde yaygınlaşmaktadır. Ülkemizde de bir çok bilişim suçu işlenmekte olup, emniyet teşkilatı bu suçlarla ilgili sürekli uğraş vermekte ve suçların çözümü ile ilgili stratejiler geliştirmeye çalışmaktadır. Araştırmaya katılan 379 personelin en çok karşılaştıkları bilişim suçları hakkındaki görüşleri alınmış veriler Tablo 33'te sunulmuştur.

En çok karşılaştıkları bilişim suçları incelendiğinde, en çok karşılaştıkları suçların başında virüs (% 15,7) konusu, daha sonra spam mail (% 11,7) ve aynı oranlarda (% 8,3) İnternet üzerinden para transferi ve bilgisayar yoluyla dolandırıcılık konularının geldiği Tablo 33'ten anlaşılmaktadır.

Tablo 33: Polisin En Çok Karşılaştığı Bilişim Suçları

Seçenekler	f	%
Spam Mail	169	11,7
Virüs	227	15,7
Fishing (Aldatmaca)	90	6,1
İnternet Üzerinden Para Transferi	120	8,3
Kredi Kartı Kopyalama	61	4,1
Kredi Kartı Dolandırıcılığı	113	7,8
İnternet Yoluyla Kişilik Haklarına Saldırı	110	7,6
İnternet Üzerinden Tehdit	71	4,9
Telif Haklarının İhlali	58	3,9
Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim	93	6,6
Bilgisayar Sabotajı	21	1,4
Bilgisayar Yoluyla Dolandırıcılık	120	8,3
Bilgisayar Yoluyla Sahtecilik	59	4,0
Bilgisayar Yazılımının İzinsiz Kullanımı	100	6,3
Kopya Sayfa Dolandırıcılığı	26	1,7
Diğer	23	1,6
Toplam	1455*	100,0

* Birden fazla seçenek işaretlenebilmiştir.

Günlük hayatta tüm ev ve iş yerlerinde bulunan bilgisayarlara çeşitli yollarla virüs bulaştırmak suretiyle bilişim suçları işlenebildiği gibi, spam mail yöntemiyle de bu suçların işlenmesine zemin hazırlanmış olmaktadır. Yine günümüzde İnternet üzerinden para transferi yapılması yaygınlaşmakta olup, dolayısıyla İnternet güvenliği aşılarak suçlar işlenebilmektedir. Bunun için ev ve iş ortamında asgari düzeyde bilişim güvenliğinin sağlanması ve toplumun bilinç düzeyinin artırılması gerekmektedir. Bilgisayar yoluyla dolandırıcılık yapılması da günümüzde artan bilişim suçları türlerindendir. Bu tür suçların nasıl işlendiği konusunda personel, uygulamalı eğitimle bilgilendirilmeli ve vatandaşların bu konuda duyarlı olması için eğitim ortamları oluşturulmalıdır.

Personelin en az karşılaştıkları bilişim suçları incelendiğinde bu suç türleri, telif hakları ihlali (% 3,9), bilgisayar sabotajı (% 1,4) ve kopya sayfa dolandırıcılığı (% 1,7) olarak karşımıza çıkmaktadır.

5.3.12. Bilişim Suçlarıyla Mücadelede İyi Bilinen Sistemler

Bilişim suçlarının çözümünde, personelin yetkinliğinin üst düzeyde olması büyük önem taşımaktadır. Bu tür suçların çözümünde ve bu tür suçlarla mücadelede personelin yetkinliğinin üst düzeyde olması ile suç işlemek durumunda olanların bir adım önüne geçilmesi söz konusu olarak suçun işlenmemesi sağlanmış olacaktır. Ayrıca, suç işlenmiş olsa bile bu tür suçların çözümü için yetkinliğin üst düzeyde olması ile işlenen suçların kısa sürede çözümü sağlanmış olacak ve suçun yaygınlaşmasının önüne geçilmiş olacaktır.

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, bilişim suçları ile mücadelelerinde en iyi bildikleri sistemlerin neler olduğu incelenmiş ve Tablo 34'te belirtilmiştir. Buna göre en iyi bildikleri sistemlerin neler olduğu incelendiğinde, personelin en çok (% 21,6) veri kurtarma programları konusunda yeterli olduğu belirlenmiştir. Bunu, firewall (% 14,9) ve Dos komutları (% 10,5) konuları takip etmektedir. Özellikle, personelin veri kurtarma konusunda yetkin olması önem taşımaktadır. Çünkü disket, hard disk ve çeşitli dijital medyalardan veri kurtarma işleminin yapılabilmesi emniyet teşkilatının yetkinliğine önemli ölçüde katkı saglayacaktır.

Tablo 34: Bilişim Suçları İle Mücadelede İyi Bilinen Sistemler

Seçenekler	f	%
Firewall	112	14,9
Kripto	23	3,0
Linux	27	3,6
IP Cop, ENDIAN	18	2,3
Saldırı Tespit Sistemleri	45	5,9
Virüs Server	61	8,1
IP Tools	72	9,5
Veri Kurtarma Programları	163	21,6
Etherial (IP Trafik)	45	5,9
IP Manager (Port Açıkları Tesbiti)	65	8,6
Telnet	29	3,8
Dos Komutları	79	10,5
Diğer	18	2,3
Toplam	757*	100,0

* Birden fazla seçenek işaretlenebilmiştir.

Kripto, IP Cop, ENDIAN ve Linux konuları, personelin bilişim suçları ile mücadelelerinde diğer konulara göre, az bildikleri alanlardır. Bu alanlarda ve diğer ihtiyaç duyulan yeni konularda personelin, bilgi ve uygulama seviyesinin artırılması gerekmektedir.

Öte yandan araştırmaya katılan personelin bilişim suçlarının çözümü konusunda kendilerini yeterli görme durumları, yeterli hissetmiyorlarsa bu konuda destek aldıkları resmi ve özel kuruluşlar belirlenmeye çalışılmıştır. Aynı zamanda il emniyet müdürlüğünde bu konuda en donanımlı birimin hangisi olduğu, yine il emniyet müdürlükleri kapsamında bu suçlarla mücadele etmek için daha donanımlı bir yapılanmaya gerek olup olmadığı ve Emniyet Genel Müdürlüğü kapsamında bu konu ile ilgili bir ünite oluşturulmasının gereği konusunda da personelin görüşleri alınmıştır.

5.3.13. Bilişim Suçları Konusunda Yetersiz Kalma Durumu

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin bilişim suçlarının çözümü hususunda kendilerini yeterli durumları incelenmiştir. Elde edilen bulgular Tablo 35'te sunulmuştur.

Tablo 35: Bilişim Suçları Konusunda Yetersiz Kalma Durumu

Seçenekler	f	%
Evet	190	50,1
Kısmen	169	44,6
Hayır	20	5,3
Toplam	379	100,0

Buna görev personel çoğunlukla bu suçların çözümünde birim olarak yeterli olduklarını (% 50,1) düşünmektedir. Kısmen yeterli olduklarını düşünenlerin oranı ise % 44,6 dır. Bilişim suçlarının çözümünde birim olarak yetersiz olduklarını düşünen personelin oranı ise % 5,3'tür. Bu verilere göre, bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin birim olarak bilişim suçlarının çözümünde kendilerini genel olarak yeterli gördükleri ortaya çıkmaktadır. Yetersiz olunduğunu düşünen personelin oranının % 5,3 seviyesinde olması ise sevindiricidir. Emniyet Genel Müdürlüğü merkez teşkilatının bilişim suçlarında uzman personel ve teknik ortam yönüyle güçlü olduğu göz önüne alındığında, özellikle bilişim suçlarında görev yapan taşra teşkilatı personeli başta KOM Daire Başkanlığı olmak üzere, ilgili daire başkanlıklarından yardım alabilecektir. Ayrıca KOM Daire Başkanlığı, taşra teşkilatı için bilişim suçlar konularında yetersiz kaldıklarında başvuru yapacakları 16 İl Emniyet Müdürlüğü belirlemiştir. Bu iller, bölge merkezi hükmünde olup, çözüm üretme konusunda yetkin personel ve teknik ortam barındırmaktadır.

5.3.14. Bilişim Suçları Konusunda Yetersiz Kalındığında EGM Bünyesinde Destek Alınan Birimler

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, meydana gelen bir bilişim suçu karşısında yetersiz kalındığında Emniyet Genel Müdürlüğü bünyesinde öncelikle hangi birimden teknik destek aldığı incelenmiştir (Tablo 36).

Tablo 36: Bilişim Suçları Konusunda Yetersiz Kalındığında EGM Bünyesinde Destek Alınan Birimler

Seçenekler	f	%
Bilgi İşlem Daire Başkanlığı	169	44,5
Asayiş Daire Başkanlığı	9	2,4
KOM Daire Başkanlığı	178	47,0
Kriminal Polis Lab. Daire Başk.	6	1,6
İstihbarat Daire Başkanlığı	11	2,9
Diğer	6	1,6
Toplam	379	100,0

Tablo 36'da görüldüğü gibi, % 47,0 sinin KOM Daire Başkanlığı'na başvurmayı düşündüğü ortaya çıkmaktadır. Bunu, % 44,5 oranı ile Bilgi İşlem Daire Başkanlığı'ndan teknik destek alırım fikri takip etmektedir. Diğer daire başkanlıklarından teknik destek alma düşüncesi oldukça az bir ihtimal olarak görülmektedir. EGM bünyesinde KOM Daire Başkanlığı ve Bilgi İşlem Daire Başkanlığı çarpıcı bir şekilde teknik destek konusunda ön plana çıkmaktadır.

5.3.15. Bilişim Suçları Konusunda Yetersiz Kalındığında Dışarıdan Destek Alınan Kurum ve Kuruluşlar

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, meydana gelen bir bilişim suçu karşısında yetersiz kalındığında dışarıdan yardım ve destek aldıkları kurum veya kuruluşlar incelenmiş ve veriler Tablo 37'de sunulmuştur.

Tablo 37: Bilişim Suçları Konusunda Yetersiz Kalındığında Dışarıdan Destek Alınan Kurum ve Kuruluşlar

Seçenekler	f	%
Özel Firma ve Şirketler	96	15,7
Üniversite	42	6,9
Türk Telekom	213	34,8
Servis Sağlayıcılar	97	15,9
GSM Şirketleri	56	9,2
Kamu Kuruluşları	67	10,9
Diğer	41	6,6
Toplam	612*	100,0

* Birden fazla seçenek işaretlenebilmiştir.

Buna göre personelin öncelikle (% 34,8) Türk Telekom'dan destek aldığı ortaya çıkmaktadır. Bu kurumu, servis sağlayıcılar (%15,9) ile özel firma ve şirketler (%15,7) izlemektedir. Tablo 37'de de görüldüğü gibi, kamu kuruluşları (% 10,9) ve GSM şirketleri (% 9,2) destek alınan diğer birimlerdir. Bilişim suçları konusunda, ortak paydada sorumluluğu olan özellikle Telekomünikasyon Kurumu, olayların çözümü aşamasında en çok bilgisine başvurulan bir mercidir.

5.3.16. İl Emniyet Müdürlükleri'nde Bilişim Suçlarıyla Mücadelede En Yetkin Birim

Araştırmaya katılan bilişim suçları konusunda görev yapan 379 personelin, İl Emniyet Müdürlükleri bünyesinde bilişim suçlarıyla mücadelede, **en yeterli - donanımlı** birimin hangisi olduğu konusundaki düşünceleri incelenmiş ve sonuçlar Tablo 38'de sunulmuştur.

Tablo 38: İl Emniyet Müdürlükleri'nde Bilişim Suçlarıyla Mücadelede En Yetkin Birim

Seçenekler	f	%
Mali Şube Müdürlüğü	19	5,0
Bilgi İşlem Şube Müdürlüğü	141	37,3
KOM Şube Müdürlüğü	174	45,9
Asayiş Şube Müdürlüğü	2	,5
İstihbarat Şube Müdürlüğü	38	10,0
Olay Yeri İnc. Şb.Md.lüğü	-	-
Diğer	5	1,3
Toplam	379	100,0

Tablo 38'de görüldüğü gibi personel öncelikle (% 45,9) KOM Şube Müdürlüğü'nü en yeterli-donanımlı birim olarak görmektedir. Bunu, % 37,3 oranı ile Bilgi İşlem Şube Müdürlüğü takip etmektedir. İstihbarat Şube Müdürlüğü'nü bilişim suçlarıyla mücadelede **en yeterli - donanımlı** birim olarak düşünenlerin oranı ise % 10,0 dır. Gerçekten de, KOM Daire Başkanlığı'na bağlı taşra teşkilatları (16 İl Emniyet Müdürlüğü KOM Şube Müdürlükleri) bölge merkezi hükmünde olup, kendi civarındaki illere eğitim yönüyle ve bilişim suçları vakalarının aydınlanması yönüyle destek vermektedir.

5.3.17. İl Emniyet Müdürlüklerinde Bilişim Suçlarıyla Mücadele Eden Birimlerin Daha Donanımlı Hale Getirilmesi Gerekliliği

Tablo 39: İl Emniyet Müdürlüklerinde Bilişim Suçlarıyla Mücadele Eden Birimlerin Daha Donanımlı Hale Getirilmesi Gerekliliği

Seçenekler	f	%
Evet	368	97,1
Hayır	11	2,9
Toplam	379	100,0

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personele, İl Emniyet Müdürlükleri bünyesinde bilişim suçlarıyla mücadele eden birimlerin bu konuda daha donanımlı hale getirilmesine gerek olup olmadığı sorulduğunda personelin neredeyse tamamına yakını Tablo 39'da görüldügü gibi (% 97,1) oranında ilgili birimlerin daha donanımlı hale getirilmesi gerekir şeklinde görüş belirtmiştir.

Maliyeti yüksek de olsa, bilişim suçlarının çözümünde gerekli teknolojik ortam ve labaratuarlar tesis edilebildiği takdirde, personelin motivasyonu artarak etkin görev yapması ve bilişim suçlarının çözülerek adli makamlara somut delil sunabilme imkanı artmış olacaktır.

Maltais (2005), bu konuda bilişim suçlarını araştırmada sorumlu sayılan kişilerin bilgi ve uzmanlık düzeyini yükseltmeye yönelik, gerek eyaletler düzeyinde örgütlü tüm polis kuruluşları gerekse federal yönetimler için, ek tahsisat çıkarılması gerekir şeklinde görüş belirtmektedir.

5.3.18. Emniyet Genel Müdürlüğü Bünyesinde "Bilişim Suçları" İle İlgili Bir Ünite Kurulması Gerekliliği

Tablo 40: Emniyet Genel Müdürlüğü Bünyesinde "Bilişim Suçları" İle İlgili Bir Ünite Kurulması Gerekliliği

Seçenekler	f	%
Evet	366	96,6
Hayır	13	3,4
Toplam	379	100,0

"Bilişim Suçları" ile mücadele eden ve konu alanı uzmanlarından oluşan **bir ünite kurulmasının** gerekliliği konusundaki düşünceler incelendiğinde, personelin büyük çoğunluğunun % 96,6 oranında böyle bir ünitenin kurulması gerektiği fikrine sahip olduğu Tablo 40'da görülmektedir. Emniyet Genel Müdürlüğü bünyesinde, bilişim suçları konusunda ilgili daire başkanlıkları kendi alanlarına giren konularda çalışma yürütmektedir. Bu durum

da; zaman, emek, işgücü kaybına neden olabilmektedir. Ayrıca, bilişim suçları alanında merkezi bir birimin olmaması koordinasyon sorununa, yeknesaklığın sağlanamamasına, bilişim suçları bilgi bankası ve sağlıklı istatistiki veriler tutulamamasına neden olmaktadır. ABD ve bazı Avrupa ülkeleri gibi, ülkemizde de sadece bilişim suçları konularında çalışma yapan bir merkez oluşturulmasının yararlı olacağı düşünülmektedir.

5.3.19. Bilişim Suçları ile İlgili Görev Alınan İlginç Olaylar

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin görev almış olduğu bilişim suçu araştırma olaylarından kendilerine en ilginç gelen bir konuyu özetlemeleri istenmiştir. Bilişim suçları konusunda görev alınan ilginç olaylar ek-3'te belirtilmiştir.

5.3.20. Bilişim Suçlarıyla Mücadelede, Personelin Eğitimi Konusunda Belirtmek İstediği Konular

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin bilişim suçlarıyla mücadele edecek personelin eğitimi konusunda (meslek öncesi eğitim, hizmetiçi eğitim, yurtdışı eğitimi, uzmanlık eğitimi, online eğitim vb.) belirtmek istediği görüş ve önerilerini özetlemeleri istenmiştir. Bilişim suçlarıyla mücadelede personelin eğitim konusunda bahsetmek istediği konular ek-4'te belirtilmiştir.

5.3.21. Bilişim Suçlarıyla Mücadele Kapsamında Belirtmek İstedikleri Diğer Konular

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin bilişim suçlarıyla mücadele kapsamında belirtmek istedikleri (Mevzuat, İdari Yapılanma, Teknik Ünite, Uluslararası İşbirliği vb.) görüş ve önerileri özetlemeleri istenmiştir. Bilişim suçlarıyla mücadele kapsamında personelin belirtmek istediği diğer konular ek-5'te sıralanmıştır.

5.4. Emniyet Personelinin Bilişim Suçları ile İlgili Sahip Olması Gereken Yeterlikler Konusundaki Bilgi Düzeyleri ve Bu Bilgileri Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Emniyet personelinin bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi düzeyleri ve bu bilgileri gerekli görme düzeyleri arasında anlamlı bir fark olup olmadığı konusunda görüşleri alınmıştır. Elde edilen görüşler Tablo 41'de görülmektedir.

Tablo 41: Emniyet Personelinin Bilişim Suçları ile İlgili Sahip Olması Gereken Yeterlikler Konusundaki Bilgi Düzeyleri ve Bu Bilgileri Gerekli Görme Düzeyleri Arasındaki İlişki

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
1. Bilgisayar ve İnternet Terimlerini								
Bilme Düzeyi	379	3,66	0,83	378	0,230	0,000	-20,655	0,000*
Gerekli Bulma Düzeyi		4,63	0,60					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilgisayar ve internet terimlerini iyi bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
2. Bilişim Suçları Terimlerini (fake, mail, spammer, stenografi, cracker vb.)								
Bilme Düzeyi	379	3,01	0,95	378	0,175	0,001	-27,891	0,000*
Gerekli Bulma Düzeyi		4,54	0,67					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilişim suçları terimlerini kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
3. Bilişim Suçlarının Kapsamını								
Bilme Düzeyi	379	3,28	0,90	378	0,253	0,000	-26,141	0,000*
Gerekli Bulma Düzeyi		4,58	0,63					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilişim suçlarının kapsamını kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
4. Bilişim Suçlarının İşleniş Yöntemlerini								
Bilme Düzeyi	379	3,17	0,89	378	0,185	0,000	-27,311	0,000*
Gerekli Bulma Düzeyi		4,59	0,66					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilişim suçlarının işleniş yöntemlerini kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

Tablo 41'den devam

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
5. Bilişim Suçlarında Delillendirmeyi								
Bilme Düzeyi	379	2,85	0,89	378	0,116	0,024	-33,734	0,000*
Gerekli Bulma Düzeyi		4,64	0,63					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilişim suçlarını delillendirmeyi kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
6. Bilişim Suçları Konusunda Yasal Mevzuatı								
Bilme Düzeyi	379	2,95	0,92	378	0,183	0,000	-31,370	0,000*
Gerekli Bulma Düzeyi		4,60	0,63					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilişim suçlarının konusunda yasal mevzuatı kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
7. Bilişim Suçlarıyla İlgili Uluslararası Hukuki Düzenlemeleri								
Bilme Düzeyi	379	2,53	0,85	378	0,138	0,007	-39,671	0,000*
Gerekli Bulma Düzeyi		4,54	0,63					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilişim suçlarıyla ilgili uluslararası hukuki düzenlemeleri bilmediklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
8. Wireless Güvenliğini								
Bilme Düzeyi	379	2,70	1,01	378	0,136	0,008	-30,888	0,000*
Gerekli Bulma Düzeyi		4,53	0,68					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Wireless Güvenliğini" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
9. Windows Güvenliğini								
Bilme Düzeyi	379	3,26	0,94	378	0,198	0,000	-25,644	0,000*
Gerekli Bulma Düzeyi		4,61	0,62					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Windows Güvenliğini" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
10. Ağ Trafiğini Analiz Etmeyi								
Bilme Düzeyi	379	2,80	1,00	378	0,091	0,078	-27,570	0,000*
Gerekli Bulma Düzeyi		4,47	0,71					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Ağ Trafiğini Analiz Etmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

Tablo 41'den devam

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
11. TCP/IP Konusunu								
Bilme Düzeyi	379	3,22	0,98	378	0,103	0,044	-21,776	0,000*
Gerekli Bulma Düzeyi		4,50	0,70					
Bilişim suçları ile mücadelede görev yapan 379 personel, "TCP/IP Konusunu" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
12. Dinleme Sistemlerini (Sniffer)								
Bilme Düzeyi	379	2,54	1,02	378	0,088	0,086	-28,664	0,000*
Gerekli Bulma Düzeyi		4,41	0,85					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Dinleme Sistemlerini (Sniffer)" bilmediklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
13. Kayıp Alanlardan Kurtarılmış Veriler Konusunu								
Bilme Düzeyi	379	3,06	1,04	378	0,088	0,088	-23,585	0,000*
Gerekli Bulma Düzeyi		4,52	0,69					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Kayıp Alanlardan Kurtarılmış Veriler Konusunu" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
14. Anlık Mesajlaşma Sistemlerini (ICQ, Messenger, IRC vb.)								
Bilme Düzeyi	379	3,52	0,95	378	0,062	0,227	-13,524	0,000*
Gerekli Bulma Düzeyi		4,36	0,78					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Anlık Mesajlaşma Sistemlerini (ICQ, Messenger, IRC vb.) " iyi bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
15. İnternet Geçmisi ve Firewall Kayıtlarını								
Bilme Düzeyi	379	3,06	1,06	378	0,138	0,007	-22,142	0,000*
Gerekli Bulma Düzeyi		4,43	0,71					
Bilişim suçları ile mücadelede görev yapan 379 personel, bilişim suçlarının kapsamını kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
16. Sistem Kayıt Log'larını Analizi Etmeyi								
Bilme Düzeyi	379	2,77	1,00	378	0,068	0,187	-27,416	0,000*
Gerekli Bulma Düzeyi		4,45	0,70					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Sistem Kayıt Log'larını Analizi Etmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

Tablo 41'den devam

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
17.İşletim Sistemi Kayıtlarını (Registry)								
Bilme Düzeyi	379	3,03	1,00	378	0,056	0,279	-22,709	0,000*
Gerekli Bulma Düzeyi		4,44	0,71					
Bilişim suçları ile mücadelede görev yapan 379 personel, "İşletim Sistemi Kayıtlarını (Registry)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
18. Güvenlik Duvarı Sistemlerini (Firewall)								
Bilme Düzeyi	379	2,96	1,01	378	0,108	0,036	-24,709	0,000*
Gerekli Bulma Düzeyi		4,46	0,72					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Güvenlik Duvarı Sistemlerini (Firewall)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
19. Saldırı Tespit Sistemlerini								
Bilme Düzeyi	379	2,63	0,92	378	0,056	0,276	-33,712	0,000*
Gerekli Bulma Düzeyi		4,56	0,67					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Saldırı Tespit Sistemlerini" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
20. Spamming ve Fishing (Aldatmaca) Konularını								
Bilme Düzeyi	379	2,65	0,94	378	0,051	0,318	-30,583	0,000*
Gerekli Bulma Düzeyi		4,48	0,72					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Spamming ve Fishing (Aldatmaca) Konularını" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
21. Elektronik Olaylara İlk Müdahale Yapabilmeyi								
Bilme Düzeyi	379	2,67	0,98	378	0,035	0,499	-30,906	0,000*
Gerekli Bulma Düzeyi		4,54	0,68					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Elektronik Olaylara İlk Müdahale Yapabilmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir..								
22. E-Posta Haberleşme Trafiğini Tespit Edebilmeyi								
Bilme Düzeyi	379	2,64	0,94	378	0,073	0,155	-31,645	0,000*
Gerekli Bulma Düzeyi		4,51	0,73					
Bilişim suçları ile mücadelede görev yapan 379 personel, "E-Posta Haberleşme Trafiğini Tespit Edebilmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

Tablo 41'den devam

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
23. Bir Bilgisayarı Rahatlıkla -usulüne uygun- İnceleyebilmeyi, Tanımlayabilmeyi ve Teknik Rapor Hazırlayabilmeyi								
Bilme Düzeyi	379	2,94	1,13	378	0,119	0,021	-24,686	0,000*
Gerekli Bulma Düzeyi		4,54	0,69					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Bir Bilgisayarı Rahatlıkla -usulüne uygun- İnceleyebilmeyi, Tanımlayabilmeyi ve Teknik Rapor Hazırlayabilmeyi kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
24. Network Elemanları ve Cihazlarını								
Bilme Düzeyi	379	3,16	1,11	378	0,070	0,173	-20,382	0,000*
Gerekli Bulma Düzeyi		4,48	0,68					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Network Elemanları ve Cihazlarını" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
25. Dosya Sistemlerini (FAT, NTFS, EXT3)								
Bilme Düzeyi	379	3,18	1,11	378	0,010	0,846	-18,788	0,000*
Gerekli Bulma Düzeyi		4,46	0,71					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Dosya Sistemlerini (FAT, NTFS, EXT3)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
26. Kredi Kartı Dolandırıcılığını								
Bilme Düzeyi	379	2,89	0,97	378	0,130	0,011	-29,803	0,000*
Gerekli Bulma Düzeyi		4,59	0,67					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Kredi Kartı Dolandırıcılığını" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
27. Saldırılardan Korunmak İçin Alınacak Önlemleri								
Bilme Düzeyi	379	3,13	0,99	378	0,170	0,001	-25,942	0,000*
Gerekli Bulma Düzeyi		4,59	0,65					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Saldırılardan Korunmak İçin Alınacak Önlemleri" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
28. Depolama Aygıtlarının Güvenli Yedeğini Almayı (İmaj Alma İşlemi)								
Bilme Düzeyi	379	3,32	1,14	378	0,104	0,043	-19,113	0,000*
Gerekli Bulma Düzeyi		4,57	0,67					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Depolama Aygıtlarının Güvenli Yedeğini Almayı (İmaj Alma İşlemi)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

Tablo 41'den devam

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
29. Sanal Özel Ağ (VPN) Konusunu								
Bilme Düzeyi	379	2,74	0,95	378	0,017	0,735	-27,949	0,000*
Gerekli Bulma Düzeyi		4,45	0,72					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Sanal Özel Ağ (VPN) Konusunu" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
30. Güçlü Password Oluşturmayı								
Bilme Düzeyi	379	3,12	1,13	378	0,081	0,117	-21,787	0,000*
Gerekli Bulma Düzeyi		4,55	0,66					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Güçlü Password Oluşturmayı" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
31. Görüntü İçinde Metin Taşımayı (Steganography)								
Bilme Düzeyi	379	2,64	1,03	378	0,103	0,045	-26,754	0,000*
Gerekli Bulma Düzeyi		4,36	0,82					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Görüntü İçinde Metin Taşımayı (Steganography)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
32. Şifreleme Konusunu (Kriptoloji)								
Bilme Düzeyi	379	2,64	0,97	378	0,172	0,001	-31,341	0,000*
Gerekli Bulma Düzeyi		4,48	0,78					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Şifreleme Konusunu (Kriptoloji)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
33. Güvenlik Taraması Yapmayı (Security Testing)								
Bilme Düzeyi	379	2,87	0,99	378	0,107	0,038	-28,332	0,000*
Gerekli Bulma Düzeyi		4,54	0,68					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Güvenlik Taraması Yapmayı (Security Testing)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
34. İnternet Üzerinden Alışveriş ve Para Transferi Yapmayı								
Bilme Düzeyi	379	3,66	1,02	378	0,191	0,000	-11,747	0,000*
Gerekli Bulma Düzeyi		4,39	0,86					
Bilişim suçları ile mücadelede görev yapan 379 personel, "İnternet Üzerinden Alışveriş ve Para Transferi Yapmayı" iyi bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

Tablo 41'den devam

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
35. Virus, Worm ve Spyware Taramasını								
Bilme Düzeyi	379	3,59	1,02	378	0,183	0,000	-16,717	0,000*
Gerekli Bulma Düzeyi		4,55	0,68					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Virus, Worm ve Spyware Taramasını" iyi bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
36. Linux ve Unix İşletim Sistemlerini								
Bilme Düzeyi	379	2,31	0,92	378	0,162	0,002	-32,789	0,000*
Gerekli Bulma Düzeyi		4,29	0,88					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Linux ve Unix İşletim Sistemlerini" bilmediklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
37. Tuzak Sistemler (Honey Pots) Konusunu								
Bilme Düzeyi	379	2,33	0,90	378	0,104	0,043	-37,986	0,000*
Gerekli Bulma Düzeyi		4,49	0,73					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Tuzak Sistemler (Honey Pots) Konusunu" bilmediklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
38. Hacking Yöntemlerini								
Bilme Düzeyi	379	2,45	0,95	378	0,125	0,015	-35,270	0,000*
Gerekli Bulma Düzeyi		4,50	0,73					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Hacking Yöntemlerini" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
39. Keylogger Konusunu								
Bilme Düzeyi	379	2,51	1,03	378	0,142	0,006	-31,125	0,000*
Gerekli Bulma Düzeyi		4,44	0,77					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Keylogger Konusunu" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
40. Güvenlik Tarama Sonuçlarını Raporlayıp, Yorumlayabilmeyi								
Bilme Düzeyi	379	2,53	0,98	378	0,002	0,973	-30,154	0,000*
Gerekli Bulma Düzeyi		4,44	0,74					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Güvenlik Tarama Sonuçlarını Raporlayıp, Yorumlayabilmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

Tablo 41'den devam

GRUPLAR	N	$\overline{X}$	SS	sd	r	Anl. Düzeyi	t	Anl. Düzeyi
41. Bilgisayarlardaki Port'lar Konusunu (Sanal Kapılar)								
Bilme Düzeyi	379	2,69	1,02	378	0,080	0,122	-29,364	0,000*
Gerekli Bulma Düzeyi		4,50	0,71					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Bilgisayarlardaki Port'lar Konusunu (Sanal Kapılar)" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
42. Silinmiş Bir Veriyi Kurtarabilmeyi								
Bilme Düzeyi	379	3,29	1,09	378	0,075	0,144	-20,524	0,000*
Gerekli Bulma Düzeyi		4,58	0,64					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Silinmiş Bir Veriyi Kurtarabilmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
43. Bir Veriyi İz Bırakmadan Silebilmeyi								
Bilme Düzeyi	379	3,05	1,11	378	0,097	0,060	-22,865	0,000*
Gerekli Bulma Düzeyi		4,53	0,71					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Bir Veriyi İz Bırakmadan Silebilmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
44. Sistemin Çalışması İçin Gerekli Temel Donanım Bilgisini								
Bilme Düzeyi	379	3,59	1,13	378	0,128	0,013	-14,928	0,000*
Gerekli Bulma Düzeyi		4,54	0,67					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Sistemin Çalışması İçin Gerekli Temel Donanım Bilgisini" iyi bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
45. Uzaktan Erişim ve Yönetim Sistemlerini								
Bilme Düzeyi	379	3,23	1,06	378	0,151	0,003	-21,801	0,000*
Gerekli Bulma Düzeyi		4,55	0,69					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Uzaktan Erişim ve Yönetim Sistemlerini" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
46. Kurulmuş Bir Network'ün Yazılım ve Donanım Bileşenlerini Raporlayabilmeyi								
Bilme Düzeyi	379	2,87	1,06	378	0,126	0,014	-24,776	0,000*
Gerekli Bulma Düzeyi		4,42	0,73					
Bilişim suçları ile mücadelede görev yapan 379 personel, "Kurulmuş Bir Network'ün Yazılım ve Donanım Bileşenlerini Raporlaya bilmeyi" kısmen bildiklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								
47. PARDUS Açık Kaynak Kodlu İşletim Sistemini								
Bilme Düzeyi	379	2,19	0,91	378	0,185	0,000	-35,013	0,000*
Gerekli Bulma Düzeyi		4,27	0,90					
Bilişim suçları ile mücadelede görev yapan 379 personel, "PARDUS Açık Kaynak Kodlu İşletim Sistemini" bilmediklerini ve bunları öğrenmenin de çok gerekli olduğunu belirtmiştir.								

* $p < 0,05$ anlamlı

Tablo 41'de görüldüğü gibi araştırmaya katılan emniyet personelinin Bilişim Suçları ile ilgili sahip Olması gereken nitelikler konusundaki bilgi düzeyleri ve bu bilgileri gerekli görme düzeyleri arasında bütün boyutlar açısındananlamlı farklılık olduğu gözlenmiştir. Bütün maddeler incelendiğinde görülebilecek ortak nokta, tüm nitelikler açısından, grup kendisini genel olarak kısmen yeterli görmektedir. Buna karşın bu konularda mutlaka eğitim almaları gerektiğini vurgulamaktadırlar. Bu durum bilişim suçları konusunda eğitim verilmesinin önemini ortaya koymaktadır.

Emniyet Personelinin Bilişim Suçları ile İlgili Sahip Olması Gereken Yeterlikler Konusundaki Bilgi Düzeyleri ve Bu Bilgileri Gerekli Görme Düzeyleri ile İlgili Genel Profil:

Emniyet personelinin bilişim suçları ile ilgili konulardan **iyi** bildikleri ve bunları öğrenmenin de **çok gerekli** olduğunu belirttikleri konular şu şekildedir:

Tablo 42: Emniyet Personelinin Bilişim Suçları ile İlgili Konulardan İyi Bildikleri ve Bunları Öğrenmenin de Çok Gerekli Olduğunu Belirttikleri Maddeler

1. Madde	Bilgisayar ve İnternet terimleri
14. Madde	Anlık mesajlaşma sistemleri (ICQ, Messenger, IRC vb.)
34. Madde	İnternet üzerinden alışveriş ve para transferi yapma
35. Madde	Virus, Worm ve Spyware taraması
44. Madde	Sistemin çalışması için gerekli temel donanım bilgisi

Emniyet personelinin bilişim suçları ile ilgili konulardan **bilmedikleri**, ancak bunları öğrenmenin de çok gerekli olduğunu belirttikleri konular şu şekildedir:

Tablo 43: Emniyet Personelinin Bilişim Suçları ile İlgili Konulardan Bilmedikleri Ancak Bunları Öğrenmenin de Çok Gerekli Olduğunu Belirttikleri Maddeler

7. Madde	Bilişim suçlarıyla ilgili uluslararası hukuki düzenlemeler
12. Madde	Dinleme Sistemleri (Sniffer)
36. Madde	Linux ve Unix işletim sistemleri
37. Madde	Tuzak sistemler (Honey Pots) konusu
47. Madde	PARDUS açık kaynak kodlu işletim sistemi

Emniyet personelinin bilişim suçları ile ilgili konulardan **kısmen** bildikleri ve bunları öğrenmenin de **çok gerekli** olduğunu belirttikleri maddeler Tablo 44'te belirtildiği gibidir :

Tablo 44: Emniyet Personelinin Bilişim Suçları ile İlgili Konulardan Kısmen Bildikleri ve Bunları Öğrenmenin de Çok Gerekli Olduğunu Belirttikleri Maddeler

2. Madde: Bilişim suçları terimleri (fake, mail, spammer, stenografi, cracker vb.)
3. Madde: Bilişim suçlarının kapsamı
4. Madde: Bilişim suçlarının işleniş yöntemleri
5. Madde: Bilişim suçlarında delillendirme
6. Madde: Bilişim suçları konusunda yasal mevzuat
7. Madde: Bilişim suçlarıyla ilgili uluslararası hukuki düzenlemeler
8. Madde: Wireless güvenliği
9. Madde: Windows güvenliği
10. Madde: Ağ trafiğini analiz etme
11. Madde: TCP/IP konusu
12. Madde: Dinleme Sistemleri (Sniffer)
13. Madde: Kayıp alanlardan kurtarılmış veriler konusu
15. Madde: İnternet geçmisi ve firewall kayıtları
16. Madde: Sistem kayıt log'larını analiz etme
17. Madde: İşletim sistemi kayıtları (Registry)
18. Madde: Güvenlik duvarı sistemleri (Firewall)
19. Madde: Saldırı tespit sistemleri
20. Madde: Spamming ve Fishing (Aldatmaca) konuları
21. Madde: Elektronik olaylara ilk müdahale yapabilme

Tablo 44'den devam

22. Madde: E-Posta haberleşme trafiğini tespit edebilme
23. Madde: Bir bilgisayarı usulüne uygun inceleyebilme, tanımlayabilme ve teknik rapor hazırlayabilme
24. Madde: Network elemanları ve cihazları
25. Madde: Dosya sistemlerini (FAT, NTFS, EXT3)
26. Madde: Kredi kartı dolandırıcılığı
27. Madde: Saldırılardan korunmak için alınacak önlemler
28. Madde: Depolama aygıtlarının güvenli yedeğini alma (İmaj Alma İşlemi)
29. Madde: Sanal özel ağ (VPN) konusu
30. Madde: Güçlü password oluşturma
31. Madde: Görüntü içinde metin taşıma (Steganography)
32. Madde: Şifreleme konusu (Kriptoloji)
33. Madde: Güvenlik taraması yapma (Security Testing)
36. Madde: Linux ve Unix işletim sistemleri
37. Madde: Tuzak sistemler (Honey Pots) konusu
38. Madde: Hacking yöntemleri
39. Madde: KEYLOGGER konusu
40. Madde: Güvenlik tarama sonuçlarını raporlayıp, yorumlayabilme
41. Madde: Bilgisayarlardaki port'lar konusu (Sanal Kapılar)
42. Madde: Silinmiş bir veriyi kurtarabilme
43. Madde: Bir veriyi iz bırakmadan silebilme
45. Madde: Uzaktan erişim ve yönetim sistemleri
46. Madde: Kurulmuş bir network'ün yazılım ve donanım bileşenlerini raporlayabilme
47. Madde: PARDUS açık kaynak kodlu işletim sistemi

5.5. Emniyet Personelinin Görev Yaptığı Birime Göre, Bilişim Suçları İle İlgili Sahip Olması Gereken Yeterlikler Konusundaki Bilgi ve Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Bu konuya ilişkin olarak verilerin çözümlenmesinde İlişkili-tekrarlı ölçümler için "İki Faktörlü Varyans Analizi" tekniği (two-way ANOVA for mixed mesures) uygulanmıştır. Bu analizde farklı gruplardan oluşan bağımsız değişkenin ilişkili ya da tekrarlı ölçümler üzerindeki etkisi araştırılmaktadır (Büyüköztürk, 2003: 76; Ural ve Kılıç, 2005: 207). Bu çözümleme sonucunda elde edilen bulgular Tablo 45'te görülmektedir.

Tablo 45: Emniyet Personelinin Bilişim Suçlarına İlişkin Görev Yaptığı Birime Göre, Bilişim Suçlarıyla İlgili Bilgilere Sahip Olma ve Bu Bilgileri Gerekli Görme Durumlarının Karşılaştırıldığı İki Faktörlü Varyans Analizi Sonuçları

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
1. Bilgisayar ve İnternet Terimlerini							
Bilgi İş. Şb.Md.	204	3,87	0,762	4,61	0,637	29,944	0,000*
KOM Şb.M.	175	3,42	0,846	4,65	0,555		
Toplam	379	3,66	0,832	4,63	0,600		
2. Bilişim Suçları Terimlerini (fake, mail, spammer, stenografi, cracker vb.)							
Bilgi İş. Şb.Md.	204	3,15	0,947	4,52	0,711	10,483	0,001*
KOM Şb. M.	175	2,84	0,943	4,57	0,638		
Toplam	379	3,01	0,956	4,54	0,678		
3. Bilişim Suçlarının Kapsamını							
Bilgi İş. Şb.Md.	204	3,18	0,906	4,54	0,689	1,687	0,195
KOM Şb. M.	175	3,40	0,897	4,62	0,561		
Toplam	379	3,28	0,907	4,58	0,634		
4. Bilişim Suçlarının İşleniş Yöntemlerini							
Bilgi İş. Şb.Md.	204	3,12	0,904	4,56	0,694	0,245	0,621
KOM Şb. M.	175	3,24	0,890	4,63	0,627		
Toplam	379	3,17	0,898	4,59	0,664		
5. Bilişim Suçlarında Delillendirmeyi							
Bilgi İş. Şb.Md.	204	2,75	0,894	4,65	0,643	6,127	0,014*
KOM Şb. M.	175	2,98	0,874	4,62	0,619		
Toplam	379	2,85	0,891	4,64	0,631		
6. Bilişim Suçları Konusunda Yasal Mevzuatı							
Bilgi İş. Şb.Md.	204	2,74	0,913	4,59	0,648	18,901	0,000*
KOM Şb. M.	175	3,21	0,874	4,61	0,622		
Toplam	379	2,95	0,924	4,60	0,635		
7. Bilişim Suçlarıyla İlgili Uluslararası Hukuki Düzenlemeleri							
Bilgi İş. Şb.Md.	204	2,50	0,850	4,53	0,645	0,154	0,695
KOM Şb. M.	175	2,56	0,854	4,55	0,621		
Toplam	379	2,53	0,852	4,54	0,634		

Tablo 45'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
8. Wireless Güvenliğini							
Bilgi İş. Şb.Md.	204	2,89	1,023	4,55	0,730	9,466	0,002*
KOM Şb. M.	175	2,48	0,970	4,50	0,633		
Toplam	379	2,70	1,019	4,53	0,687		
9. Windows Güvenliğini							
Bilgi İş. Şb.Md.	204	3,53	0,844	4,62	0,657	30,763	0,000*
KOM Şb. M.	175	2,95	0,957	4,60	0,586		
Toplam	379	3,26	0,943	4,61	0,624		
10. Ağ Trafiğini Analiz Etmeyi							
Bilgi İş. Şb.Md.	204	3,08	0,940	4,42	0,742	36,176	0,000*
KOM Şb. M.	175	2,48	0,975	4,52	0,676		
Toplam	379	2,80	1,001	4,47	0,713		
11. TCP/IP Konusunu							
Bilgi İş. Şb.Md.	204	3,50	0,890	4,50	0,712	29,849	0,000*
KOM Şb. M.	175	2,89	0,979	4,50	0,693		
Toplam	379	3,22	0,981	4,50	0,702		
12. Dinleme Sistemlerini (Sniffer)							
Bilgi İş. Şb.Md.	204	2,43	0,993	4,35	0,948	0,511	0,475
KOM Şb. M.	175	2,66	1,048	4,48	0,718		
Toplam	379	2,54	1,023	4,41	0,851		
13. Kayıp Alanlardan Kurtarılmış Veriler Konusunu							
Bilgi İş. Şb.Md.	204	3,20	1,004	4,51	0,712	6,518	0,011*
KOM Şb. M.	175	2,90	1,081	4,53	0,684		
Toplam	379	3,06	1,049	4,52	0,698		
14. Anlık Mesajlaşma Sistemlerini (ICQ, Messenger, IRC vb.)							
Bilgi İş. Şb.Md.	204	3,69	0,902	4,34	0,812	10,974	0,001*
KOM Şb. M.	175	3,33	0,979	4,38	0,763		
Toplam	379	3,52	0,954	4,36	0,789		

Tablo 45'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
15. İnternet Geçmisi ve Firewall Kayıtlarını							
Bilgi İş. Şb.Md.	204	3,34	1,012	4,45	0,724	21,252	0,000*
KOM Şb. M.	175	2,74	1,047	4,41	0,696		
Toplam	379	3,06	1,069	4,43	0,710		
16. Sistem Kayıt Log'larını Analizi Etmeyi							
Bilgi İş. Şb.Md.	204	3,00	1,007	4,45	0,737	16,718	0,000*
KOM Şb. M.	175	2,52	0,945	4,46	0,676		
Toplam	379	2,77	1,007	4,45	0,709		
17. İşletim Sistemi Kayıtlarını (Registry)							
Bilgi İş. Şb.Md.	204	3,32	0,906	4,44	0,744	26,104	0,000*
KOM Şb. M.	175	2,69	1,019	4,43	0,690		
Toplam	379	3,03	1,008	4,44	0,719		
18. Güvenlik Duvarı Sistemlerini (Firewall)							
Bilgi İş. Şb.Md.	204	3,25	0,999	4,43	0,769	35,754	0,000*
KOM Şb. M.	175	2,62	0,937	4,50	0,668		
Toplam	379	2,96	1,019	4,46	0,724		
19. Saldırı Tespit Sistemlerini							
Bilgi İş. Şb.Md.	204	2,77	0,949	4,59	0,654	4,559	0,033*
KOM Şb. M.	175	2,46	0,869	4,53	0,701		
Toplam	379	2,63	0,925	4,56	0,676		
20. Spamming ve Fishing (Aldatmaca) Konularını							
Bilgi İş. Şb.Md.	204	2,77	0,928	4,46	0,732	6,236	0,013*
KOM Şb. M.	175	2,52	0,951	4,50	0,710		
Toplam	379	2,65	0,947	4,48	0,721		
21. Elektronik Olaylara İlk Müdahale Yapabilmeyi							
Bilgi İş. Şb.Md.	204	2,77	0,945	4,54	0,667	2,807	0,095
KOM Şb. M.	175	2,56	1,008	4,53	0,709		
Toplam	379	2,67	0,980	4,54	0,686		
22. E-Posta Haberleşme Trafiğini Tespit Edebilmeyi							
Bilgi İş. Şb.Md.	204	2,76	0,922	4,52	0,758	3,776	0,053
KOM Şb. M.	175	2,51	0,946	4,50	0,710		
Toplam	379	2,64	0,940	4,51	0,735		

Tablo 45'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
23. Bir Bilgisayarı Rahatlıkla -usulüne uygun- İnceleyebilmeyi, Tanımlayabilmeyi ve Teknik Rapor Hazırlayabilmeyi							
Bilgi İş. Şb.Md.	204	3,29	1,018	4,54	0,724	38,215	0,000*
KOM Şb. M.	175	2,54	1,138	4,55	0,657		
Toplam	379	2,94	1,138	4,54	0,693		
24. Network Elemanları ve Cihazlarını							
Bilgi İş. Şb.Md.	204	3,53	0,969	4,45	0,717	52,664	0,000*
KOM Şb. M.	175	2,72	1,121	4,53	0,641		
Toplam	379	3,16	1,116	4,48	0,683		
25. Dosya Sistemlerini (FAT, NTFS, EXT3)							
Bilgi İş. Şb.Md.	204	3,56	0,997	4,41	0,773	52,799	0,000*
KOM Şb. M.	175	2,74	1,091	4,52	0,641		
Toplam	379	3,18	1,119	4,46	0,716		
26. Kredi Kartı Dolandırıcılığını							
Bilgi İş. Şb.Md.	204	2,66	0,880	4,59	0,713	19,424	0,000*
KOM Şb. M.	175	3,16	1,006	4,60	0,634		
Toplam	379	2,89	0,971	4,59	0,677		
27. Saldırılardan Korunmak İçin Alınacak Önlemleri							
Bilgi İş. Şb.Md.	204	3,34	0,871	4,58	0,664	18,548	0,000*
KOM Şb. M.	175	2,89	1,067	4,60	0,642		
Toplam	379	3,13	0,991	4,59	0,653		
28. Depolama Aygıtlarının Güvenli Yedeğini Almayı (İmaj Alma İşlemi)							
Bilgi İş. Şb.Md.	204	3,66	0,951	4,52	0,738	43,118	0,000*
KOM Şb. M.	175	2,94	1,221	4,62	0,602		
Toplam	379	3,32	1,140	4,57	0,679		
29. Sanal Özel Ağ (VPN) Konusunu							
Bilgi İş. Şb.Md.	204	2,96	0,948	4,39	0,770	26,255	0,000*
KOM Şb. M.	175	2,49	0,896	4,52	0,668		
Toplam	379	2,74	0,953	4,45	0,727		

Tablo 45'ten devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
30. Güçlü Password Oluşturmayı							
Bilgi İş. Şb.Md.	204	3,42	1,087	4,51	0,725	33,096	0,000*
KOM Şb. M.	175	2,78	1,103	4,59	0,578		
Toplam	379	3,12	1,139	4,55	0,662		
31. Görüntü İçinde Metin Taşımayı (Steganography)							
Bilgi İş. Şb.Md.	204	2,77	1,063	4,32	0,862	7,949	0,005*
KOM Şb. M.	175	2,50	0,976	4,41	0,775		
Toplam	379	2,64	1,031	4,36	0,823		
32. Şifreleme Konusunu (Kriptoloji)							
Bilgi İş. Şb.Md.	204	2,71	1,001	4,45	0,855	3,495	0,062
KOM Şb. M.	175	2,56	0,937	4,52	0,693		
Toplam	379	2,64	0,974	4,48	0,784		
33. Güvenlik Taraması Yapmayı (Security Testing)							
Bilgi İş. Şb.Md.	204	3,03	0,981	4,51	0,725	12,768	0,000*
KOM Şb. M.	175	2,67	0,983	4,57	0,638		
Toplam	379	2,87	0,998	4,54	0,686		
34. İnternet Üzerinden Alışveriş ve Para Transferi Yapmayı							
Bilgi İş. Şb.Md.	204	3,86	0,940	4,30	0,935	27,013	0,000*
KOM Şb. M.	175	3,42	1,079	4,49	0,764		
Toplam	379	3,66	1,029	4,39	0,864		
35. Virus, Worm ve Spyware Taramasını							
Bilgi İş. Şb.Md.	204	3,86	0,882	4,53	0,690	32,315	0,000*
KOM Şb. M.	175	3,28	1,080	4,58	0,688		
Toplam	379	3,59	1,020	4,55	0,689		
36. Linux ve Unix İşletim Sistemlerini							
Bilgi İş. Şb.Md.	204	2,38	0,958	4,25	0,938	3,992	0,046*
KOM Şb. M.	175	2,23	0,882	4,34	0,828		
Toplam	379	2,31	0,925	4,29	0,889		
37. Tuzak Sistemler (Honey Pots) Konusunu							
Bilgi İş. Şb.Md.	204	2,35	0,917	4,41	0,792	3,599	0,059
KOM Şb. M.	175	2,30	0,893	4,57	0,655		
Toplam	379	2,33	0,905	4,49	0,735		

Tablo 45'ten devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
38. Hacking Yöntemlerini							
Bilgi İş. Şb.Md.	204	2,53	0,948	4,47	0,802	4,514	0,034*
KOM Şb. M.	175	2,36	0,953	4,54	0,658		
Toplam	379	2,45	0,953	4,50	0,739		
39. KEYLOGGER Konusunu							
Bilgi İş. Şb.Md.	204	2,61	1,008	4,38	0,842	7,114	0,008*
KOM Şb. M.	175	2,41	1,051	4,50	0,693		
Toplam	379	2,51	1,032	4,44	0,779		
40. Güvenlik Tarama Sonuçlarını Raporlayıp, Yorumlayabilmeyi							
Bilgi İş. Şb.Md.	204	2,76	0,994	4,41	0,780	20,378	0,000*
KOM Şb. M.	175	2,26	0,898	4,48	0,709		
Toplam	379	2,53	0,981	4,44	0,748		
41. Bilgisayarlardaki Port'lar Konusunu (Sanal Kapılar)							
Bilgi İş. Şb.Md.	204	2,88	1,008	4,49	0,752	12,938	0,000*
KOM Şb. M.	175	2,48	0,993	4,52	0,676		
Toplam	379	2,69	1,020	4,50	0,717		
42. Silinmiş Bir Veriyi Kurtarabilmeyi							
Bilgi İş. Şb.Md.	204	3,68	0,942	4,57	0,672	53,755	0,000*
KOM Şb. M.	175	2,84	1,086	4,60	0,606		
Toplam	379	3,29	1,094	4,58	0,642		
43. Bir Veriyi İz Bırakmadan Silebilmeyi							
Bilgi İş. Şb.Md.	204	3,32	1,038	4,55	0,702	18,820	0,000*
KOM Şb. M.	175	2,73	1,115	4,51	0,733		
Toplam	379	3,05	1,113	4,53	0,716		
44. Sistemin Çalışması İçin Gerekli Temel Donanım Bilgisini							
Bilgi İş. Şb.Md.	204	4,01	0,893	4,52	0,683	66,951	0,000*
KOM Şb. M.	175	3,09	1,177	4,56	0,656		
Toplam	379	3,59	1,130	4,54	0,670		
45. Uzaktan Erişim ve Yönetim Sistemlerini							
Bilgi İş. Şb.Md.	204	3,64	0,928	4,58	0,685	50,665	0,000*
KOM Şb. M.	175	2,75	1,012	4,51	0,710		
Toplam	379	3,23	1,063	4,55	0,697		

Tablo 45'ten devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
46. Kurulmuş Bir Network'ün Yazılım ve Donanım Bileşenlerini Raporlayabilmeyi							
Bilgi İş. Şb.Md.	204	3,24	1,048	4,41	0,754		
KOM Şb. M.	175	2,44	0,926	4,43	0,707	47,696	0,000*
Toplam	379	2,87	1,068	4,42	0,731		
47. PARDUS Açık Kaynak Kodlu İşletim Sistemini							
Bilgi İş. Şb.Md.	204	2,32	0,979	4,25	0,913		
KOM Şb. M.	175	2,04	0,801	4,29	0,892	7,095	0,008*
Toplam	379	2,19	0,910	4,27	0,902		

* p < 0,05 anlamlı

Elde edilen verilere göre üç boyutlu bir sonuç ortaya çıkmıştır. Bunlar şöyle özetlenebilir: Personelin görev aldıkları yer değişkenine bakılmaksızın tek grup olarak ele alındığında, söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir. Diğer bir boyut ise gruplar dikkate alındığında, hem Bilgi İşlem Şube Müdürlüğü personeli hem de KOM Şube Müdürlüğü personelinin söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir. Ancak bilindiği gibi grup ve ölçüm temel etki testlerinin anlamlı çıkması durumunu, araştırmacının oluşturduğu düzeneğin bağımlı değişken değişim miktarı üzerinde etkili olduğu biçiminde yorumlamak güçtür. Bu yorum ancak grup ve ölçüm ortak etkisinin anlamlı çıkması ile söylenebilir ve ilişkili-tekrarlı ölçümler için "İki Faktörlü Varyans Analizi" tekniğinde daha çok bu ortak etkiye odaklanılmaktadır (Büyüköztürk, 2003: 78). Bir başka deyişle, farklı birimlerde çalışıyor olmak acaba bilişim suçları ile ilgili bilgileri bilme ve gerekli görme düzeyleri açısından anlamlı bir farklılık oluşturmakta mıdır? sorusu ortak etki sorusu olarak araştırılmaktadır. Üçüncü boyut olarak değerlendirilebilecek bu açıdan bakıldığında ise 3, 4, 7, 12, 21, 22, 32, 37. maddelerde farklı birimlerde çalışıyor olmanın bilgileri bilme ve gerekli görme düzeyleri açısından bir faktör olmadığı sonucuna varılmıştır.

Bunun dışında kalan tüm maddelerde, farklı birimlerde çalışmak, söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı bir farklılığa yol açmıştır. Maddeler bazında bulgular genel olarak şöyle özetlenebilir.

Her iki grubun da 1.madde bilgisayar ve internet terimlerini ve 34.madde internet üzerinden alışveriş ve para transferi yapmayı iyi bildikleri gözlenirken, 36.madde linux ve unix işletim sistemleri ile 47.madde PARDUS açık kaynak kodlu işletim sistemleri konusunu hiç bilmedikleri belirlenmiştir. Bu maddelerin dışında kalan maddelerde göre daha iyi bilgi düzeyine sahip olmakla birlikte çoğunlukla kısmen bilme düzeyinde bilgiye sahip olunduğu görülmektedir. Bilgi İşlem Şb. Md personeli 9, 11, 14, 24, 25, 28, 30, 35, 42, 44 ve 45. maddelerde iyi bir bilgi düzeyine sahip olduğunu belirtirken KOM Şb. Md. personeli kısmen bilgi sahibidir. KOM Şb. Md. personeli sadece 8. ve 10 maddelerde iyi bilgi düzeyine sahip olduğunu ifade etmekte iken bu maddelerde Bilgi İşlem Şb. Md personeli kısmen düzeyinde bilgi sahibidir. Buna göre Bilgi İşlem Şb. Md personelinin söz konusu maddeler açısından KOM Şb. Md. personeline göre biraz daha iyi bir bilgi düzeyine sahip oldukları söylenebilir.

Öte yandan her iki grup ta tüm maddelerde bilgi düzeyleri ne olursa olsun hepsini çok iyi bilmeleri gerektiğini ifade etmektedirler. Bu durum bilişim suçları konusunda personelin görev yeri neresi olursa olsun, böyle bir eğitimi alması gerektiği sonucunu ortaya çıkarmaktadır.

5.6. Bilişim Suçları İle İlgili Görev Süresi Açısından, Personelin Sahip Olması Gereken Nitelikler Konusundaki Bilgi ve Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Bu konuya ilişkin verilerin çözümlenmesinde İlişkili ölçümler için İki faktörlü varyans analizi tekniği (two-way ANOVA for mixed mesures) kullanılmıştır. Bu analizde Farklı gruplardan oluşan bağımsız değişkenin ilişkili ya da tekrarlı ölçümler üzerindeki etkisi araştırılmaktadır (Büyüköztürk, 2003: 76; Ural ve Kılıç, 2005: 207). Elde edilen bulgular Tablo 46'da görülmektedir.

Tablo 46: Emniyet Personelinin Görev Süresine Göre, Bilişim Suçlarıyla İlgili Bilgilere Sahip Olma ve Bu Bilgileri Gerekli Görme Durumlarının Karşılaştırıldığı İki Faktörlü Varyans Analizi Sonuçları

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
1. Bilgisayar ve İnternet Terimlerini							
1-10 yıl arası	176	3,78	0,799	4,63	0,635	4,945	0,027*
11 yıl ve fazla	203	3,56	0,849	4,62	0,569		
Toplam	379	3,66	0,832	4,63	0,600		
2. Bilişim Suçları Terimlerini (fake, mail, spammer, stenografi, cracker vb.)							
1-10 yıl arası	176	3,03	0,946	4,53	0,708	0,487	0,486
11 yıl ve fazla	203	2,98	0,967	4,55	0,652		
Toplam	379	3,01	0,956	4,54	0,678		
3. Bilişim Suçlarının Kapsamını							
1-10 yıl arası	176	3,33	0,910	4,59	0,634	0,475	0,491
11 yıl ve fazla	203	3,24	0,904	4,57	0,636		
Toplam	379	3,28	0,907	4,58	0,634		
4. Bilişim Suçlarının İşleniş Yöntemlerini							
1-10 yıl arası	176	3,19	0,919	3,19	0,919	0,017	0,895
11 yıl ve fazla	203	3,15	0,881	3,15	0,881		
Toplam	379	3,17	0,898	3,17	0,898		
5. Bilişim Suçlarında Delillendirmeyi							
1-10 yıl arası	176	2,87	0,911	4,67	0,627	0,026	0,872
11 yıl ve fazla	203	2,84	0,875	4,62	0,636		
Toplam	379	2,85	0,891	4,64	0,631		
6. Bilişim Suçları Konusunda Yasal Mevzuatı							
1-10 yıl arası	176	3,01	0,903	4,63	0,635	0,231	0,631
11 yıl ve fazla	203	2,90	0,941	4,57	0,635		
Toplam	379	2,95	0,924	4,60	0,635		
7. Bilişim Suçlarıyla İlgili Uluslararası Hukuki Düzenlemeleri							
1-10 yıl arası	176	2,62	0,866	4,56	0,646	1,776	0,183
11 yıl ve fazla	203	2,44	0,833	4,52	0,623		
Toplam	379	2,53	0,852	4,54	0,634		

Tablo 46'dan devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
8. Wireless Güvenliğini							
1-10 yıl arası	176	2,78	0,990	4,54	0,666		
11 yıl ve fazla	203	2,64	1,040	4,51	0,706	0,952	0,330
Toplam	379	2,70	1,018	4,53	0,686		
9. Windows Güvenliğini							
1-10 yıl arası	176	3,36	0,928	4,63	0,654		
11 yıl ve fazla	203	3,18	0,949	4,60	0,598	2,378	0,124
Toplam	379	3,26	0,943	4,61	0,624		
10. Ağ Trafiğini Analiz Etmeyi							
1-10 yıl arası	176	2,86	0,991	4,48	0,740		
11 yıl ve fazla	203	2,75	1,009	4,46	0,691	0,624	0,430
Toplam	379	2,80	1,001	4,47	0,713		
11. TCP/IP Konusunu							
1-10 yıl arası	176	3,30	0,972	4,52	0,683		
11 yıl ve fazla	203	3,15	0,985	4,48	0,720	0,922	0,338
Toplam	379	3,22	0,981	4,50	0,702		
12. Dinleme Sistemlerini (Sniffer)							
1-10 yıl arası	176	2,61	1,089	4,46	0,827		
11 yıl ve fazla	203	2,47	0,961	4,37	0,871	0,145	0,704
Toplam	379	2,54	1,023	4,41	0,851		
13. Kayıp Alanlardan Kurtarılmış Veriler Konusunu							
1-10 yıl arası	176	3,13	1,063	4,56	0,689		
11 yıl ve fazla	203	3,00	1,036	4,49	0,706	0,238	0,626
Toplam	379	3,06	1,049	4,52	0,698		
14. Anlık Mesajlaşma Sistemlerini (ICQ, Messenger, IRC vb.)							
1-10 yıl arası	176	3,64	0,914	4,36	0,816		
11 yıl ve fazla	203	3,42	0,979	4,35	0,766	2,885	0,090
Toplam	379	3,52	0,954	4,36	0,789		
15. İnternet Geçmisi ve Firewall Kayıtlarını							
1-10 yıl arası	176	3,13	1,049	4,44	0,715		
11 yıl ve fazla	203	3,00	1,085	4,41	0,708	0,608	0,436
Toplam	379	3,06	1,069	4,43	0,710		

Tablo 46'dan devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
16. Sistem Kayıt Log'larını Analizi Etmeyi							
1-10 yıl arası	176	2,83	0,980	4,48	0,717		
11 yıl ve fazla	203	2,72	1,029	4,42	0,702	0,141	0,708
Toplam	379	2,77	1,007	4,45	0,709		
17. İşletim Sistemi Kayıtlarını (Registry)							
1-10 yıl arası	176	3,10	1,003	4,48	0,724		
11 yıl ve fazla	203	2,97	1,012	4,40	0,713	0,148	0,700
Toplam	379	3,03	1,008	4,44	0,719		
18. Güvenlik Duvarı Sistemlerini (Firewall)							
1-10 yıl arası	176	3,07	1,008	4,48	0,755		
11 yıl ve fazla	203	2,87	1,021	4,45	0,697	2,112	0,147
Toplam	379	2,96	1,019	4,46	0,724		
19. Saldırı Tespit Sistemlerini							
1-10 yıl arası	176	2,73	0,927	4,61	0,656		
11 yıl ve fazla	203	2,55	0,917	4,52	0,691	0,535	0,465
Toplam	379	2,63	0,925	4,56	0,676		
20. Spamming ve Fishing (Aldatmaca) Konularını							
1-10 yıl arası	176	2,80	0,995	4,55	0,690		
11 yıl ve fazla	203	2,53	0,885	4,42	0,743	1,521	0,218
Toplam	379	2,65	0,947	4,48	0,721		
21. Elektronik Olaylara İlk Müdahale Yapabilmeyi							
1-10 yıl arası	176	2,76	1,001	4,59	0,686		
11 yıl ve fazla	203	2,59	0,956	4,49	0,684	0,352	0,554
Toplam	379	2,67	0,980	4,54	0,686		
22. E-Posta Haberleşme Trafiğini Tespit Edebilmeyi							
1-10 yıl arası	176	2,76	0,942	4,56	0,745		
11 yıl ve fazla	203	2,54	0,928	4,48	0,726	1,407	0,236
Toplam	379	2,64	0,940	4,51	0,735		
23. Bir Bilgisayarı Rahatlıkla -usulüne uygun- İnceleyebilmeyi, Tanımlayabilmeyi ve Teknik Rapor Hazırlayabilmeyi							
1-10 yıl arası	176	3,03	1,125	4,61	0,649		
11 yıl ve fazla	203	2,87	1,147	4,49	0,726	0,078	0,781
Toplam	379	2,94	1,138	4,54	0,693		

Tablo 46'dan devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
24. Network Elemanları ve Cihazlarını							
1-10 yıl arası	176	3,25	1,118	4,49	0,684	1,405	0,237
11 yıl ve fazla	203	3,08	1,111	4,48	0,684		
Toplam	379	3,16	1,116	4,48	0,683		
25. Dosya Sistemlerini (FAT, NTFS, EXT3)							
1-10 yıl arası	176	3,29	1,060	4,47	0,763	1,705	0,192
11 yıl ve fazla	203	3,09	1,163	4,45	0,675		
Toplam	379	3,18	1,119	4,46	0,716		
26. Kredi Kartı Dolandırıcılığını							
1-10 yıl arası	176	2,89	0,980	4,60	0,709	0,008	0,931
11 yıl ve fazla	203	2,89	0,966	4,59	0,648		
Toplam	379	2,89	0,971	4,59	0,676		
27. Saldırılardan Korunmak İçin Alınacak Önlemleri							
1-10 yıl arası	176	3,26	0,981	4,65	0,631	1,257	0,263
11 yıl ve fazla	203	3,02	0,989	4,54	0,668		
Toplam	379	3,13	0,991	4,59	0,653		
28. Depolama Aygıtlarının Güvenli Yedeğini Almayı (İmaj Alma İşlemi)							
1-10 yıl arası	176	3,42	1,097	4,59	0,678	1,072	0,301
11 yıl ve fazla	203	3,25	1,173	4,55	0,682		
Toplam	379	3,32	1,140	4,57	0,679		
29. Sanal Özel Ağ (VPN) Konusunu							
1-10 yıl arası	176	2,80	0,932	4,48	0,732	0,148	0,700
11 yıl ve fazla	203	2,69	0,971	4,42	0,723		
Toplam	379	2,74	0,953	4,45	0,727		
30. Güçlü Password Oluşturmayı							
1-10 yıl arası	176	3,19	1,161	4,58	0,679	0,260	0,610
11 yıl ve fazla	203	3,06	1,119	4,52	0,647		
Toplam	379	3,12	1,139	4,55	0,662		
31. Görüntü İçinde Metin Taşımayı (Steganography)							
1-10 yıl arası	176	2,73	1,043	4,37	0,846	1,286	0,258
11 yıl ve fazla	203	2,57	1,018	4,36	0,805		
Toplam	379	2,64	1,031	4,36	0,823		

Tablo 46'dan devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
32. Şifreleme Konusunu (Kriptoloji)							
1-10 yıl arası	176	2,72	0,954	4,52	0,747		
11 yıl ve fazla	203	2,58	0,988	4,44	0,815	0,314	0,576
Toplam	379	2,64	0,974	4,48	0,784		
33. Güvenlik Taraması Yapmayı (Security Testing)							
1-10 yıl arası	176	2,94	0,954	4,56	0,672		
11 yıl ve fazla	203	2,80	1,032	4,52	0,698	0,568	0,451
Toplam	379	2,87	0,998	4,54	0,686		
34. İnternet Üzerinden Alışveriş ve Para Transferi Yapmayı							
1-10 yıl arası	176	3,73	1,015	4,38	0,906		
11 yıl ve fazla	203	3,60	1,039	4,40	0,829	1,345	0,247
Toplam	379	3,66	1,029	4,39	0,864		
35. Virus, Worm ve Spyware Taramasını							
1-10 yıl arası	176	3,65	0,990	4,57	0,688		
11 yıl ve fazla	203	3,53	1,044	4,54	0,690	0,608	0,436
Toplam	379	3,59	1,020	4,55	0,689		
36. Linux ve Unix İşletim Sistemlerini							
1-10 yıl arası	176	2,38	0,924	4,38	0,846		
11 yıl ve fazla	203	2,25	0,924	4,22	0,920	0,057	0,812
Toplam	379	2,31	0,925	4,29	0,889		
37. Tuzak Sistemler (Honey Pots) Konusunu							
1-10 yıl arası	176	2,43	0,923	4,53	0,739		
11 yıl ve fazla	203	2,24	0,883	4,45	0,732	0,843	0,539
Toplam	379	2,33	0,905	4,49	0,735		
38. Hacking Yöntemlerini							
1-10 yıl arası	176	2,53	0,979	4,56	0,753		
11 yıl ve fazla	203	2,38	0,928	4,45	0,725	0,121	0,728
Toplam	379	2,45	0,953	4,50	0,739		
39. KEYLOGGER Konusunu							
1-10 yıl arası	176	2,65	1,052	4,50	0,770		
11 yıl ve fazla	203	2,40	1,002	4,38	0,783	1,071	0,301
Toplam	379	2,51	1,032	4,44	0,779		

Tablo 46'dan devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
40. Güvenlik Tarama Sonuçlarını Raporlayıp, Yorumlayabilmeyi							
1-10 yıl arası	176	2,61	0,984	4,50	0,740	0,123	0,726
11 yıl ve fazla	203	2,46	0,976	4,39	0,752		
Toplam	379	2,53	0,981	4,44	0,748		
41. Bilgisayarlardaki Port'lar Konusunu (Sanal Kapılar)							
1-10 yıl arası	176	2,75	1,043	4,52	0,770	0,317	0,574
11 yıl ve fazla	203	2,65	1,000	4,49	0,670		
Toplam	379	2,69	1,020	4,50	0,717		
42. Silinmiş Bir Veriyi Kurtarabilmeyi							
1-10 yıl arası	176	3,39	1,064	4,64	0,643	0,514	0,474
11 yıl ve fazla	203	3,20	1,114	4,53	0,638		
Toplam	379	3,29	1,094	4,58	0,642		
43. Bir Veriyi İz Bırakmadan Silebilmeyi							
1-10 yıl arası	176	3,11	1,107	4,57	0,729	0,196	0,658
11 yıl ve fazla	203	2,99	1,119	4,50	0,706		
Toplam	379	3,05	1,113	4,53	0,716		
44. Sistemin Çalışması İçin Gerekli Temel Donanım Bilgisini							
1-10 yıl arası	176	3,67	1,108	4,60	0,659	0,070	0,792
11 yıl ve fazla	203	3,52	1,148	4,49	0,677		
Toplam	379	3,59	1,130	4,54	0,670		
45. Uzaktan Erişim ve Yönetim Sistemlerini							
1-10 yıl arası	176	3,34	1,018	4,59	0,710	1,034	0,310
11 yıl ve fazla	203	3,13	1,094	4,51	0,684		
Toplam	379	3,23	1,063	4,55	0,697		
46. Kurulmuş Bir Network'ün Yazılım ve Donanım Bileşenlerini Raporlayabilmeyi							
1-10 yıl arası	176	2,96	1,092	4,49	0,740	0,048	0,827
11 yıl ve fazla	203	2,79	1,045	4,35	0,720		
Toplam	379	2,87	1,068	4,42	0,731		
47. PARDUS Açık Kaynak Kodlu İşletim Sistemini							
1-10 yıl arası	176	2,27	0,934	4,29	0,940	0,855	0,356
11 yıl ve fazla	203	2,12	0,886	4,26	0,870		
Toplam	379	2,19	0,910	4,27	0,902		

* $p < 0,05$ anlamlı

Elde edilen verilere göre üç boyutlu bir sonuç ortaya çıkmıştır. Bunlar şöyle özetlenebilir. Personelin kıdemine bakılmaksızın tek grup olarak ele alındığında söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında tüm maddelerde anlamlı farklılık belirlenmiştir. Bir başka deyişle tüm personel maddelerde yer alan konuların büyük çoğunluğunda kısmen bilgili olduklarını, ancak hepsinde bu bilgileri kesinlikle bilmeleri gerektiğini belirtmişlerdir.

Diğer bir boyut ise kıdemler dikkate alındığında hem 1-10 yıl deneyime sahip olanlar, hem de 11 yıl ve üzeri deneyime sahip olanların söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir. Ancak bilindiği gibi grup ve ölçüm temel etki testlerinin anlamlı çıkması durumunu, araştırmacının oluşturduğu düzeneğin bağımlı değişken değişim miktarı üzerinde etkili olduğu biçiminde yorumlamak güçtür. Bu yorum ancak grup ve ölçüm ortak etkisinin anlamlı çıkması ile söylenebilir ve ilişkili-tekrarlı ölçümler için iki faktörlü varyans analizi tekniğinde daha çok bu ortak etkiye odaklanılmaktadır (Büyüköztürk, 2003: 78).

Bir başka ifadeyle, farklı kıdemlerde olmak “acaba bilişim suçları ile ilgili bilgileri bilme ve gerekli görme düzeyleri açısından anlamlı bir farklılık oluşturmakta mıdır?” sorusu ortak etki sorusu olarak araştırılmaktadır. Üçüncü boyut olarak değerlendirilebilecek bu açıdan bakıldığında ise sadece 1. madde açısından farklı mesleki kıdemde olmak bilgileri bilme ve gerekli görme düzeyleri açısından bir farklılık oluştururken, diğer tüm maddelerde bir faktör olmadığı sonucuna varılmıştır. Maddeler bazında bulgular genel olarak şöyle özetlenebilir. Buna göre kıdemleri ne olursa olsun tüm personelin genel olarak bilişim suçları ile ilgili bilgileri büyük ölçüde kısmen bildikleri, ancak hepsini kesinlikle bilmeleri gerektiği görüşünde oldukları söylenebilir.

5.7. Bilişim Suçları Kursuna Katılma Durumuna Göre Sahip Olması Gereken Nitelikler Konusundaki Bilgi ve Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Bu konuya ilişkin verilerin çözümlenmesinde İlişkili ölçümler için İki faktörlü varyans analizi tekniği (two-way ANOVA for mixed mesures) kullanılmıştır. Farklı gruplardan oluşan bağımsız değişkenin ilişkili ya da tekrarlı ölçümler üzerindeki etkisinin araştırıldığı (Büyüköztürk, 2003: 76; Ural ve Kılıç, 2005: 207) bu çözümleme sonucunda elde edilen bulgular Tablo 47'de görülmektedir.

Tablo 47: Emniyet Personelinin Bilişim Suçlarına İlişkin Kurs Alma Durumuna Göre, Bilişim Suçlarıyla İlgili Bilgilere Sahip Olma ve Bu Bilgileri Gerekli Görme Durumlarının Karşılaştırıldığı İki Faktörlü Varyans Analizi Sonuçları

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
1. Bilgisayar ve İnternet Terimlerini							
Kurs alan	74	4,04	0,766	4,64	0,508	14,564	0,000*
Kurs almayan	305	3,57	0,824	4,62	0,621		
Toplam	379	3,66	0,832	4,63	0,600		
2. Bilişim Suçları Terimlerini (fake, mail, spammer, stenografi, cracker vb.)							
Kurs alan	74	3,63	0,959	4,60	0,518	27,087	0,000*
Kurs almayan	305	2,85	0,893	4,53	0,711		
Toplam	379	3,01	0,056	4,54	0,678		
3. Bilişim Suçlarının Kapsamını							
Kurs alan	74	3,54	0,909	4,62	0,515	4,681	0,031*
Kurs almayan	305	3,22	0,897	4,57	0,660		
Toplam	379	3,28	0,907	4,58	0,634		
4. Bilişim Suçlarının İşleniş Yöntemlerini							
Kurs alan	74	3,68	0,660	4,68	0,494	16,606	0,000*
Kurs almayan	305	3,05	0,905	4,57	0,698		
Toplam	379	3,17	0,898	4,59	0,664		

Tablo 47'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
6. Bilişim Suçları Konusunda Yasal Mevzuatı							
Kurs alan	74	3,37	0,917	4,72	0,476	7,808	0,005*
Kurs almayan	305	2,85	0,898	4,57	0,665		
Toplam	379	2,95	0,924	4,60	0,635		
7. Bilişim Suçlarıyla İlgili Uluslararası Hukuki Düzenlemeleri							
Kurs alan	74	2,91	0,975	4,62	0,515	9,419	0,002*
Kurs almayan	305	2,43	0,792	4,52	0,659		
Toplam	379	2,53	0,852	4,54	0,634		
8. Wireless Güvenliğini							
Kurs alan	74	3,20	0,992	4,54	0,553	17,105	0,000*
Kurs almayan	305	2,58	0,990	4,52	0,716		
Toplam	379	2,70	1,019	4,53	0,687		
9. Windows Güvenliğini							
Kurs alan	74	3,67	0,795	4,59	0,546	16,859	0,000*
Kurs almayan	305	3,17	0,951	4,62	0,642		
Toplam	379	3,26	0,943	4,61	0,624		
10. Ağ Trafiğini Analiz Etmeyi							
Kurs alan	74	3,31	0,992	4,50	0,555	15,640	0,000*
Kurs almayan	305	2,68	0,966	4,46	0,747		
Toplam	379	2,80	1,001	4,47	0,713		
11. TCP/IP Konusunu							
Kurs alan	74	3,67	0,893	4,52	0,624	13,422	0,000*
Kurs almayan	305	3,11	0,971	4,50	0,721		
Toplam	379	3,22	0,981	4,50	0,702		
12. Dinleme Sistemlerini (Sniffer)							
Kurs alan	74	3,09	1,062	4,48	0,646	13,606	0,000*
Kurs almayan	305	2,40	0,969	4,39	0,894		
Toplam	379	2,54	1,023	4,41	0,851		
13. Kayıp Alanlardan Kurtarılmış Veriler Konusunu							
Kurs alan	74	3,66	0,996	4,58	0,549	19,650	0,000*
Kurs almayan	305	2,91	1,011	4,51	0,730		
Toplam	379	3,06	1,049	4,52	0,698		

Tablo 47'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
14. Anlık Mesajlaşma Sistemlerini (ICQ, Messenger, IRC vb.)							
Kurs alan	74	3,71	0,914	4,32	0,795	3,270	0,071
Kurs almayan	305	3,48	0,960	4,37	0,788		
Toplam	379	3,52	0,954	4,36	0,789		
15. İnternet Geçmisi ve Firewall Kayıtlarını							
Kurs alan	74	3,60	0,990	4,50	0,646	14,774	0,000*
Kurs almayan	305	2,93	1,047	4,41	0,725		
Toplam	379	3,06	1,069	4,43	0,710		
16. Sistem Kayıt Log'larını Analizi Etmeyi							
Kurs alan	74	3,39	0,918	4,51	0,646	21,122	0,000*
Kurs almayan	305	2,62	0,971	4,44	0,723		
Toplam	379	2,77	1,007	4,45	0,709		
17. İşletim Sistemi Kayıtlarını (Registry)							
Kurs alan	74	3,67	0,908	4,47	0,645	24,953	0,000*
Kurs almayan	305	2,87	0,970	4,43	0,736		
Toplam	379	3,03	1,008	4,44	0,719		
18. Güvenlik Duvarı Sistemlerini (Firewall)							
Kurs alan	74	3,50	0,940	4,55	0,576	13,702	0,000*
Kurs almayan	305	2,83	0,996	4,44	0,755		
Toplam	379	2,96	1,019	4,46	0,724		
19. Saldırı Tespit Sistemlerini							
Kurs alan	74	3,08	0,823	4,54	0,645	17,168	0,000*
Kurs almayan	305	2,52	0,917	4,57	0,684		
Toplam	379	2,63	0,925	4,56	0,676		
20. Spamming ve Fishing (Aldatmaca) Konularını							
Kurs alan	74	3,18	0,916	4,56	0,642	13,973	0,000*
Kurs almayan	305	2,53	0,910	4,46	0,738		
Toplam	379	2,65	0,947	4,48	0,721		
21. Elektronik Olaylara İlk Müdahale Yapabilmeyi							
Kurs alan	74	3,13	0,997	4,66	0,530	7,864	0,005*
Kurs almayan	305	2,56	0,944	4,51	0,716		
Toplam	379	2,67	0,980	4,54	0,686		

Tablo 47'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
22. E-Posta Haberleşme Trafiğini Tespit Edebilmeyi							
Kurs alan	74	3,13	0,896	4,66	0,504	8,360	0,004*
Kurs almayan	305	2,53	0,914	4,48	0,778		
Toplam	379	2,64	0,940	4,51	0,735		
23. Bir Bilgisayarı Rahatlıkla -usulüne uygun- İnceleyebilmeyi, Tanımlayabilmeyi ve Teknik Rapor Hazırlayabilmeyi							
Kurs alan	74	3,63	1,092	4,64	0,559	20,862	0,000*
Kurs almayan	305	2,78	1,087	4,52	0,721		
Toplam	379	2,94	1,138	4,54	0,693		
24. Network Elemanları ve Cihazlarını							
Kurs alan	74	3,66	0,983	4,52	0,554	12,606	0,000*
Kurs almayan	305	3,03	1,114	4,47	0,712		
Toplam	379	3,16	1,116	4,48	0,683		
25. Dosya Sistemlerini (FAT, NTFS, EXT3)							
Kurs alan	74	3,68	1,005	4,51	0,579	11,049	0,001*
Kurs almayan	305	3,06	1,113	4,45	0,746		
Toplam	379	3,18	1,119	4,46	0,716		
26. Kredi Kartı Dolandırıcılığını							
Kurs alan	74	3,24	0,933	4,60	0,592	8,509	0,004*
Kurs almayan	305	2,81	0,963	4,59	0,696		
Toplam	379	2,89	0,971	4,59	0,677		
27. Saldırılardan Korunmak İçin Alınacak Önlemleri							
Kurs alan	74	3,59	0,792	4,60	0,569	15,554	0,000*
Kurs almayan	305	3,02	1,004	4,59	0,673		
Toplam	379	3,13	0,991	4,59	0,653		
28. Depolama Aygıtlarının Güvenli Yedeğini Almayı (İmaj Alma İşlemi)							
Kurs alan	74	3,93	0,969	4,63	0,563	17,466	0,000*
Kurs almayan	305	3,18	1,132	4,55	0,705		
Toplam	379	3,32	1,140	4,57	0,679		

Tablo 47'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
29. Sanal Özel Ağ (VPN) Konusunu							
Kurs alan	74	3,33	0,940	4,51	0,624	19,254	0,000*
Kurs almayan	305	2,60	0,901	4,43	0,750		
Toplam	379	2,74	0,953	4,45	0,727		
30. Güçlü Password Oluşturmayı							
Kurs alan	74	3,67	1,021	4,60	0,569	14,130	0,000*
Kurs almayan	305	2,99	1,128	4,53	0,683		
Toplam	379	3,12	1,139	4,55	0,662		
31. Görüntü İçinde Metin Taşımayı (Steganography)							
Kurs alan	74	3,09	1,035	4,48	0,646	6,420	0,012*
Kurs almayan	305	2,54	1,002	4,34	0,859		
Toplam	379	2,64	1,031	4,36	0,823		
32. Şifreleme Konusunu (Kriptoloji)							
Kurs alan	74	3,01	0,883	4,51	0,667	8,149	0,005*
Kurs almayan	305	2,55	0,975	4,47	0,811		
Toplam	379	2,64	0,974	4,48	0,784		
33. Güvenlik Taraması Yapmayı (Security Testing)							
Kurs alan	74	3,21	0,880	4,56	0,551	7,313	0,007*
Kurs almayan	305	2,78	1,008	4,53	0,715		
Toplam	379	2,87	0,998	4,54	0,686		
34. İnternet Üzerinden Alışveriş ve Para Transferi Yapmayı							
Kurs alan	74	3,91	0,932	4,39	0,773	4,204	0,041*
Kurs almayan	305	3,60	1,043	4,39	0,886		
Toplam	379	3,66	1,029	4,39	0,864		
35. Virus, Worm ve Spyware Taramasını							
Kurs alan	74	4,01	0,852	4,58	0,549	11,760	0,001*
Kurs almayan	305	3,49	1,032	4,55	0,719		
Toplam	379	3,59	1,020	4,55	0,689		

Tablo 47'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
36. Linux ve Unix İşletim Sistemlerini							
Kurs alan	74	2,63	1,041	4,44	0,622	1,886	0,170
Kurs almayan	305	2,23	0,880	4,25	0,939		
Toplam	379	2,31	0,925	4,29	0,889		
37. Tuzak Sistemler (Honey Pots) Konusunu							
Kurs alan	74	2,81	1,002	4,55	0,552	13,371	0,000*
Kurs almayan	305	2,21	0,842	4,47	0,773		
Toplam	379	2,33	0,905	4,49	0,735		
38. Hacking Yöntemlerini							
Kurs alan	74	2,90	1,009	4,63	0,538	7,498	0,006*
Kurs almayan	305	2,34	0,908	4,47	0,778		
Toplam	379	2,45	0,953	4,50	0,739		
39. KEYLOGGER Konusunu							
Kurs alan	74	3,17	0,998	4,59	0,617	16,716	0,000*
Kurs almayan	305	2,36	0,977	4,40	0,809		
Toplam	379	2,51	1,032	4,44	0,779		
40. Güvenlik Tarama Sonuçlarını Raporlayıp, Yorumlayabilmeyi							
Kurs alan	74	3,13	0,955	4,54	0,623	16,023	0,000*
Kurs almayan	305	2,39	0,932	4,42	0,774		
Toplam	379	2,53	0,981	4,44	0,748		
41. Bilgisayarlardaki Port'lar Konusunu (Sanal Kapılar)							
Kurs alan	74	3,20	0,992	4,62	0,541	10,000	0,002*
Kurs almayan	305	2,57	0,990	4,48	0,752		
Toplam	379	2,69	1,020	4,50	0,717		
42. Silinmiş Bir Veriyi Kurtarabilmeyi							
Kurs alan	74	3,78	0,969	4,64	0,559	11,512	0,001*
Kurs almayan	305	3,17	1,090	4,57	0,660		
Toplam	379	3,29	1,094	4,58	0,642		

Tablo 47'den devam

Gruplar	N	Bilme Durumu		Gerekli Görme Durumu		F	An.Düz.
		$\overline{X}$	SS	$\overline{X}$	SS		
43. Bir Veriyi İz Bırakmadan Silebilmeyi							
Kurs alan	74	3,56	1,073	4,62	0,676	10,982	0,001*
Kurs almayan	305	2,92	1,088	4,51	0,725		
Toplam	379	3,05	1,113	4,53	0,716		
44. Sistemin Çalışması İçin Gerekli Temel Donanım Bilgisini							
Kurs alan	74	3,94	0,889	4,54	0,553	7,698	0,006*
Kurs almayan	305	3,50	1,167	4,54	0,696		
Toplam	379	3,59	1,130	4,54	0,670		
45. Uzaktan Erişim ve Yönetim Sistemlerini							
Kurs alan	74	3,67	0,923	4,63	0,538	8,849	0,003*
Kurs almayan	305	3,12	1,068	4,53	0,729		
Toplam	379	3,23	1,063	4,55	0,697		
46. Kurulmuş Bir Network'ün Yazılım ve Donanım Bileşenlerini Raporlayabilmeyi							
Kurs alan	74	3,37	1,016	4,45	0,623	14,052	0,000*
Kurs almayan	305	2,75	1,046	4,41	0,756		
Toplam	379	2,87	1,068	4,42	0,731		
47. PARDUS Açık Kaynak Kodlu İşletim Sistemini							
Kurs alan	74	2,52	1,009	4,35	0,928	4,593	0,033*
Kurs almayan	305	2,11	0,867	4,25	0,896		
Toplam	379	2,19	0,910	4,27	0,902		

* p < 0,05 anlamlı

Elde edilen verilere göre üç boyutlu bir sonuç ortaya çıkmıştır. Bunlardan birincisi, hem bilişim kursu alanlar, hem de kurs almayanların bilişim suçları ile ilgili konuları bilme durumları ile gerekli görme durumları arasında anlamlı farklılık belirlenmiş olmasıdır. Bir başka deyişle her iki gruptaki bireyler ilgili maddelerdeki bilgi düzeyleri çeşitli düzeylerde olmakla beraber tüm konuları öğrenmeleri gerektiğini ifade etmişlerdir. Tüm toplam puan ortalamaları incelendiğinde de böyle bir kurs organizasyonu bilişim suçları ile ilgili bilgi düzeyi ve bu bilgileri gerekli görme düzeyleri arasında anlamlı fark ortaya çıkarmıştır. Üçüncü olarak da, tablodaki F değerleri dikkate alınarak elde edilen

sonuca göre ise kurs alanlarla almayanların. bilme ve gerekli görme düzeylerinin anlamlı biçimde farklılaştığı sonucudur. Tablodaki ortalamalar incelendiğinde kurs almayanların kurs alanlara oranla bilgileri daha fazla artan oranda gerekli gördükleri söylenebilir. Buna göre bilişim suçları konusunda bir eğitim almanın önemli bir değişken olduğu ve bilişim suçları ile ilgili personel açısından gerekli olduğu söylenebilir.

ALTINCI BÖLÜM

6. ÖZET, TARTIŞMA, SONUÇ ve ÖNERİLER

Bu bölümde araştırmanın özeti, tartışma, araştırmadan elde edilen sonuçlar ve bu sonuçlara dayalı öneriler ele alınmıştır.

6.1 Özet

Tüm dünyanın son asrımızda hızla bilgisayarlaşması ile beraber, bizlere hediye ettiği suç ortamlarından biriside çeşitliliği, kompleksliği ve sayısı hızla artan bilişim suçlarıdır. Yine, sürekli değişen dünyada özellikle 1990'lardan sonra günlük hayatın içerisine çok hızlı bir şekilde giren İnternet olgusu; bireylerin, toplumların, devletlerin hayatlarında önemli değişikliklere yol açmıştır ve açmaya da devam edecektir. İnternet olgusuyla birlikte, hayatın her alanında başta A.B.D. olmak üzere tüm dünyada olduğu gibi ülkemizde de bilişim suçları günlük hayata damgasını vurmakta ve ülkelerin yaka silktiği konuların başında yer almaktadır.

Devletlerin güvenliğini etkileyen, ayrıca ekonomi ve ticaret dünyasında da büyük maddi kayıplara yol açabilen, kişilerin günlük hayatını ihlal eden yapısıyla bilişim suçları, yediden yetmişe herkesi içine alan bir tehdit unsuru haline gelmiştir. Ne zaman, nerede, nasıl ortaya çıkacağı belli olmayan, ortaya çıkaracağı maddi külfeti kolayca hesaplanamayan, ayıca moral faktörleri de oldukça olumsuz etkileyen bu suç türü, çağın vebası olarak tüm dünyada başta kolluk güçleri olmak üzere, bilişim suçları ile mücadele eden tüm ortak paydaları sürekli olarak tedirgin eden ve önlemler almaya iten bir nitelik kazanmıştır. Türk polisi de, ülkemizde bilişim suçlarıyla mücadelede gecikmeden yerini alma çabasını göstererek, bu amaçla çeşitli idari yapılanma, organizasyonlar ve eğitim süreçleri geliştirme gayreti içerisine girmiştir. Bu araştırmada, bilişim suçları ve polisin bu suçlarla etkin mücadele etmesi için gerekli eğitim organizasyonları çeşitli boyutlarıyla incelenmiştir.

Öncelikle, bilişim suçları konusunda görev yapan polisin bilişim suçları konusundaki mevcut durumunu (eğitim seviyesi, teknik donanım ve ünite vb.) ortaya çıkarmak ve Türk polisinin bilişim suçları alanında genel bir profilinin çıkarılması amacıyla 81 İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlüklerindeki bilişim suçları konusunda görev yapan 379 personele yönelik anket uygulanarak çeşitli veriler elde edilmiş ve ihtiyaç belirlemesi yapılmıştır.

Anket çalışmasının odak noktası, özellikle bilişim suçlarıyla mücadele ve bu kapsamda nasıl bir öğretim programı geliştirilmesi gerektiğini ortaya koymayı amaçlayan ihtiyaç analizidir. İlgili çevrelere uygulanan anket çalışması, e-posta, doküman incelemesi ve görüşme dönütlerinden elde edilen bulgular yorumlanmıştır.

Araştırmanın genel amacı, dünyada ve ülkemizde farklı şekillerde işlenegelen ve sürekli bir artış seyri gösteren bilişim suçlarıyla mücadele aşamasında, öncelikle bilişim suçları sahasında görev yapan polislerle ilgili ihtiyaç tespiti yapmak, polisin bilişim suçlarında mevcut durumunun ortaya çıkarılması sağlanarak, bu alanda nasıl bir yapılanmaya geçilmesi ve bu suçlarla etkin mücadelede temel ve uzmanlık seviyesinde polisin nasıl eğitilmesi gerektiğini ortaya çıkarmak ve bu amaçla bir öğretim programı hazırlamaktır. Ayrıca, ülkemizde bilişim suçları konusunda izlenecek stratejiler için öneriler geliştirmekte bu araştırmanın amacıdır. Bu amaçları gerçekleştirmek üzere aşağıdaki sorulara cevap aranmıştır.

1. Emniyet Personel'nin Kişisel Özellikleri
2. Emniyet Personeli'nin İletişim Teknolojisi ve Bilgisayara İlişkin Özellikleri
3. Emniyet Personeli'nin Bilişim Suçları ile İlgili Nitelikleri
4. Emniyet personelinin bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi düzeyleri ve bu bilgileri gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?
5. Emniyet personelinin görev yaptığı birime göre, bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi ve gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?

6. Bilişim suçları ile ilgili görev süresi açısından, personelin sahip olması gereken nitelikler konusundaki bilgi ve gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?
7. Bilişim suçları kursuna katılma durumuna göre sahip olması gereken nitelikler konusundaki bilgi ve gerekli görme düzeyleri arasında anlamlı bir fark var mıdır?

Araştırma, nitel ve nicel olmak üzere iki kısımdan oluşmuştur. Nitel araştırma için gözlem, görüşme, doküman incelemesi, nicel araştırma içinde "betimsel survey - betimsel tarama" yöntemi kullanılmıştır.

Araştırmada, Emniyet Teşkilatı'nda Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlüklerine bilişim suçlarının çeşitli yönleri ile değerlendirileceği anket uygulanmıştır. Anketin odak noktası, özellikle bilişim suçlarıyla mücadele ve bu kapsamda nasıl bir öğretim programı geliştirilmesi gerektiğini ortaya koymayı amaçlayan ihtiyaç analizidir. İlgili çevrelere uygulanan anket çalışması sonucunda, e-posta, doküman incelemesi ve görüşme dönütlerinden elde edilen bulgular yorumlanmıştır.

Araştırma evrenini; konuya ilişkin tüm dokümanlar, bilişim suçları alanında emniyet teşkilatında çalışanların tamamı oluşturmaktadır.

Araştırmanın örneklemini;

a- Mevcut yerli ve yabancı dokümanlar,

b- 81 İl Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü (204 Kişi), Kaçakçılık ve Organize Suçlar Şube Müdürlüğü (175 Kişi) personelinden oluşan toplam 379 kişi oluşturmaktadır.

İstatistiksel analiz işlemlerinde bilgisayar paket programlarından yararlanılmıştır. Verilerin analizi için SPSS for Windows 9.0 paket programı kullanılmıştır. Araştırma ile ilgili verilerin analizinde aşağıdaki tekniklerden yararlanılmıştır.

Anket sonucu ve doğal gözlem yoluyla elde edilen bulgular; frekans, yüzde, aritmetik ortalamalar, t testi ve iki faktörlü varyans (two-way ANOVA for mixed mesures) analizi tekniklerinden yararlanarak çözümlenmiştir. Bunun yanında niteliksel veri olarak internet, bilişim, bilişim suçları ve eğitim konularında konuyla ilgili uzman kişilerin görüşlerine yer verilmiştir. Bu tür verileri toplamak içinse yarı yapılandırılmış görüşme formu oluşturulmuştur.

İstatistiksel analiz işlemlerinde güven aralığı (anlamlılık düzeyi) .05 olarak belirlenmiştir. Anket çalışmasında, emniyet personelinin bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi düzeyleri ve bu bilgileri gerekli görme düzeylerine ilişkin verilerin çözümlenmesi ve yorumlanması için beşli ölçek aralıkları 0,80 (5-1= 4, 4/5= 0,80) oranında eşit aralıklar olarak aşağıdaki şekliyle belirlenmiştir. Aritmetik ortalamalar sınır değerleri şu şekildedir:

1.00	1,80	hiç bilmiyorum / hiç gerekli görmüyorum
1,81	2,60	bilmiyorum / az gerekli görüyorum
2,61	3,40	kısmen biliyorum / kısmen gerekli görüyorum
3,41	4,20	İyi biliyorum / gerekli görüyorum
4,21	5.00	çok iyi biliyorum / çok gerekli görüyorum

Tez kapsamında, bilişim suçlarıyla etkin mücadele yapmak durumunda bulunan Emniyet Genel Müdürlüğü merkez ve taşra teşkilatında görevli polislere kişisel bilgilerin yanı sıra, bilgisayar ve İnternet kullanımı, bilgisayar-İnternet-bilişim suçları ve ilgili mevzuat, ayrıca bilişim suçlarında polisin eğitimi konularında bilgi seviyelerini tespit etmek ve ihtiyaç belirlemesi yapmak amacıyla bir anket oluşturulmuştur. Anket sonuçlarından, bilişim suçları konusunda bir öğretim programı geliştirmede yararlanılmıştır. Konu alanı uzmanlarından yararlanılarak bilişim suçları eğitimi için temel ve uzmanlık seviyesinde modüller geliştirilmiştir.

Araştırmadan elde edilen bulguların özeti şu şekildedir:

1. Kişisel Özelliklere İlişkin Bulgular

- Emniyet Genel Müdürlüğü bünyesinde "Bilişim Suçları" konusunda görev yapan birimlerden olan 81 İl Emniyet Müdürlüğü Kaçakçılık Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlüğü personeli toplam 379 personele "Bilişim Suçları"na ilişkin yeterlik ölçeği ve anket çalışması uygulanarak Emniyet Teşkilatı'nın "Bilişim Suçları" konusundaki mevcut durumu, alt yapısı, eğitim faaliyetleri, gerekli organizasyonlar ve olması gerekenler hakkında veriler toplanmıştır.

- Emniyet Genel Müdürlüğü'ne bağlı taşra teşkilatında yani 81 İl Emniyet Müdürlüğü'nde, "Bilişim Suçları" konusunda görev yapan birimlerden Bilgi İşlem Şube Müdürlüğü Sistem İletişim ve Bilişim Suçları Büro Amirliklerinden 204 personelin (% 53,8), Ayrıca, 81 İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüklerinde görevli 175 personelin (% 46,2) anket çalışması kapsamında görüşleri alınmıştır. Ülke genelinde ise, Bilgi İşlem (204 personel) ve KOM (175 personel) birimlerinde "Bilişim Suçları" konusunda görev yapan 379 personelden toplanan verilerle anket çalışmasının analiz edildiği görülmektedir.

- Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin eğitim durumu incelendiğinde, personelin en çok üniversite veya yüksek okul düzeyinde bulunduğu (% 53,0), bunu lise ve dengi okul düzeyinde bulunanların (% 25,3) takip ettiği görülmektedir.

- Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin rütbe durumu incelendiğinde, büyük çoğunluğun Polis Memuru rütbesindeki personelden (% 86,5) oluştuğu görülmektedir.

- Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin kaç yıldır Emniyet Teşkilatı'nda görev yaptığı incelendiğinde, 11-15 yıl arası görev yapanların % 47,2 ile ilk sırada yer aldığı görülmektedir.

- Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin kaç yıldır "Bilişim Suçları" konularında görev yaptığı incelendiğinde, ağırlıklı olarak % 50,7 oranı ile 1-3 yıl arasında görev yaptıkları görülmektedir

2. Emniyet Personelinin İletişim Teknolojisi ve Bilgisayara İlişkin Durumuyla İlgili Bulgu ve Yorumlar

- Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin evlerinde bilgisayar bulunup bulunmadığı incelendiğinde, personelin genel olarak (% 77,6) evinde bilgisayar bulunduğu görülmektedir. Personelin ne kadar süreyle bilgisayar kullandığı incelendiğinde, % 47,8 oranında 6-10 yıl süre arasında bilgisayar kullandıkları ortaya çıkmaktadır.

- 379 personelin, günlük olarak bilgisayar başında ne kadar süreyle bulunduğu incelendiğinde, 4-6 saat arasında (% 31,9) ve 7-9 saat arasında (% 32,7) yoğunlukla bilgisayar başında bulunulduğu görülmektedir. Günlük olarak 10 saat ve üzerinde, bilgisayar başında bulunan personelin oranı % 22,7 iken, 1-3 saat oranında bilgisayar başında bulunma oranı % 12,7 dir.

- Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, kaç yıldır İnternet kullandığı incelendiğinde, ağırlıklı olarak (% 37,7) 4-6 yıl arasında İnternet kullandığı görülmektedir. Bunu, 7-9 yıl arası (% 26,1) ve 1-3 yıl arası (% 25,9) İnternet kullanımı takip etmektedir. 10 yıl ve üzerinde İnternet kullanan personelin oranı ise % 10,3'tür.

- Bilişim suçları konusunda görev yapan yapan 379 personelin, İnternet üzerinden alışveriş veya para transferi (Sanal Bankacılık) yapma tercihleri incelendiğinde, personelin genel olarak (% 56,5) sanal bankacılığı kullandıkları görülmektedir. % 31,1 oranında ise personel, İnternet üzerinden alışveriş veya sanal bankacılık uygulamasını tercih etmemektedir. Personelin (% 55,7) işletim sistemlerindeki güncellemeleri takip edebildikleri görülmektedir.
- 379 personelin, meslek öncesi polis eğitim kurumlarında bilgisayar ve İnternet kullanımı ile ilgili eğitim alıp almadıkları incelendiğinde, personelin genel olarak (% 46,7) eğitim almadıkları ortaya çıkmaktadır. Eğitim alanların oranı ise % 38,8'dir.

3. Emniyet Personelinin Bilişim Suçları ile İlgili Niteliklerine İlişkin Bulgu ve Yorumlar

- Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, meslek içinde "Bilişim Suçları" ile ilgili bir kurs görüp görmediği incelendiğinde, personelin genel olarak (% 80,5) bir kurs görmediği ortaya çıkmaktadır. Kurs görenlerin oranı sadece % 11,1 oranındadır.

- Personelin, İnternet güvenliği ile ilgili kaynakları (Kitap, Dergi, Online Ortam vs.) takip edip edemedikleri incelendiğinde, öncelikli olarak kısmen takip edebildikleri (% 45,1) görülmektedir. İlgili kaynakları takip edebilenlerin oranı ise % 38,5'tir. İnternet güvenliği ile ilgili kaynakları (Kitap, Dergi, Online Ortam vs.) takip edemeyenlerin oranı % 16,4'tür. Personelin "Bilişim Suçları" ile ilgili herhangi bir konferans veya seminere katılıp katılmadığı incelendiğinde, personelin çoğunlukla (% 76,3) böyle bir eğitim faaliyetine katılmadığı görülmektedir. "Bilişim Suçları" ile ilgili eğitim faaliyetine katılan personelin oranı ise % 23,7 dir.

- Bilişim suçları konusunda görev yapan 379 personelin "Bilişim Suçları" ile ilgili eğitim alma ihtiyacı incelendiğinde, personelin büyük çoğunlukla (% 92,3) eğitime ihtiyaç duyduğu görülmektedir. Sadece % 1,6 oranında

personel eğitim alma ihtiyacı hissetmemektedir. Personelin “Bilişim Suçları” ile mücadele kapsamında gelişiminde en çok hangi faktörün rol oynadığı incelendiğinde, personelin daha çok (% 61,2) bireysel çabaları ve kendi kendini geliştirmesinin bu konuda rol oynadığı görülmektedir. Bunu, personelin kendi çabaları ve teşkilatın eğitim olanakları (% 21,6) izlemektedir.

- Personelin, “Bilişim Suçları” ile mücadele kapsamında çok iyi olduklarını düşündükleri ilk 3 konu sırasıyla 1-Veri kurtarma (31 Kişi), 2-IP tespiti (26 Kişi), 3-Firewall (13 Kişi) konularıdır. Personelin, “Bilişim Suçları” ile mücadele kapsamında yetersiz olduklarını düşündüğü ilk 3 konu, 1-Saldırı Tespit Sistemleri (23 Kişi), 2-Kredi Kartları Kopyalama (22 Kişi), 3- Sanal Ortamda Para Transferi (19 Kişi) olarak ortaya çıkmıştır.

- Personelin, “Bilişim Suçları” ile mücadele kapsamında yeterli eğitim aldıkları 3 konu, 1-Veri İnceleme (8 Kişi), 2-IP Tespiti (8 Kişi), 3- Veri Kurtarma (5 Kişi) konularıdır. Personelin, “Bilişim Suçları” ile mücadele kapsamında eğitim alma ihtiyacı olduğu ilk 3 konu ise, 1. IP Manager (40 Kişi),2. Saldırı Tespit Sistemleri (39 Kişi), ve 3. Bilgisayar Yoluyla Dolandırıcılık (23 Kişi) konularıdır.

- Emniyet Genel Müdürlüğü’ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin herhangi bir (İnternet suçu, Bilgisayar suçu, Bilişim suçu) suç konusuyla ilgili bilirkişi olarak görev alıp almadığı incelendiğinde, personelin genel olarak (% 64,7) bilirkişilik yapmadığı görülmektedir. Bilirkişi olarak görev alanların oranı ise % 23,7 düzeyindedir.

- 379 personelin en çok karşılaştıkları bilişim suçları incelendiğinde, en çok karşılaştıkları suçların başında virüs (% 15,7) konusu, daha sonra spam mail (% 11,7) ve aynı oranlarda (% 8,3) İnternet üzerinden para transferi ve bilgisayar yoluyla dolandırıcılık konuları gelmektedir.

- 379 personelin bilişim suçlarının çözümü hususunda yeterlilik durumu incelendiğinde, personel çoğunlukla bu suçların çözümünde birim olarak yeterli olduklarını (% 50,1) düşünmektedir. (% 44,6) oranında ise kısmen yeterli olduklarını düşünmektedirler. Bilişim suçlarının çözümünde birim olarak yetersiz olduklarını düşünen personelin oranı ise, % 5,3'tür.

- İl Emniyet Müdürlükleri bünyesinde bilişim suçlarıyla mücadelede, en yeterli - donanımlı birimin hangisi olduğu konusundaki düşünceleri incelendiğinde, personel öncelikle (% 45,9) KOM Şube Müdürlüğü'nü en yeterli-donanımlı birim olarak görmektedir. Bunu, % 37,3 oranı ile Bilgi İşlem Şube Müdürlüğü takip etmektedir.

- 379 personelin ABD ve bazı Avrupa ülkeleri gibi, Emniyet Genel Müdürlüğü bünyesinde sadece "Bilişim Suçları" ile mücadele eden ve konu alanı uzmanlarından oluşan bir ünite kurulmasının gerekliliği konusundaki düşünceleri incelendiğinde, personelin büyük çoğunluğunun (% 96,6) böyle bir ünitenin kurulması gerektiği fikrine sahip olduğu görülmektedir.

4. Emniyet Personelinin Bilişim Suçları ile İlgili Sahip Olması Gereken Yeterlikler Konusundaki Bilgi Düzeyleri ve Bu Bilgileri Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Emniyet personelinin bilişim suçları ile ilgili konulardan iyi bildikleri ve bunları öğrenmenin de çok gerekli olduğunu belirttikleri maddeler şu şekildedir:

1- Bilgisayar ve İnternet terimleri
14- Anlık mesajlaşma sistemleri (ICQ, Messenger, IRC vb.)
34- İnternet üzerinden alışveriş ve para transferi yapma
35- Virus, Worm ve Spyware taraması
44- Sistemin çalışması için gerekli temel donanım bilgisi

Emniyet personelinin bilişim suçları ile ilgili konulardan bilmedikleri, ancak bunları öğrenmenin de çok gerekli olduğunu belirttikleri maddeler şu şekildedir:

7- Bilişim suçlarıyla ilgili uluslararası hukuki düzenlemeler
12- Dinleme Sistemleri (Sniffer)
36- Linux ve Unix işletim sistemleri
37- Tuzak sistemler (Honey Pots) konusu
47-PARDUS açık kaynak kodlu işletim sistemi

5. Emniyet Personelinin Görev Yaptığı Birime Göre, Bilişim Suçları İle İlgili Sahip Olması Gereken Yeterlikler Konusundaki Bilgi ve Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Personelin görev aldıkları yer değişkenine bakılmaksızın tek grup olarak ele alındığında, söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir. Diğer bir boyut ise gruplar dikkate alındığında, hem Bilgi İşlem Şb. Md personeli hem de KOM Şb. Md. ve Daire Bşk.lığı personelinin söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir.

6. Bilişim Suçları İle İlgili Görev Süresi Açısından, Personelin Sahip Olması Gereken Nitelikler Konusundaki Bilgi ve Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Personelin kıdemine bakılmaksızın tek grup olarak ele alındığında söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında tüm maddelerde anlamlı farklılık belirlenmiştir. Bir başka deyişle tüm personel maddelerde yer alan konuların büyük çoğunluğunda kısmen bilgili olduklarını, ancak hepsinde bu bilgileri kesinlikle bilmeleri gerektiğini belirtmişlerdir. Diğer bir boyut ise kıdemler dikkate alındığında hem 1-10 yıl deneyime sahip olanlar, hem de 11 yıl ve üzeri deneyime sahip olanların söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir.

7. Bilişim Suçları Kursuna Katılma Durumuna Göre Sahip Olması Gereken Nitelikler Konusundaki Bilgi ve Gerekli Görme Düzeyleri ile İlgili Bulgu ve Yorumlar

Elde edilen verilere göre üç boyutlu bir sonuç ortaya çıkmıştır. Bunlardan birincisi, hem bilişim kursu alanlar hem de kurs almayanların bilişimi suçları ile ilgili konuları bilme durumları ile gerekli görme durumları arasında anlamlı farklılık belirlenmiş olmasıdır. Bir başka deyişle her iki gruptaki bireyler ilgili maddelerdeki bilgi düzeyleri çeşitli düzeylerde olmakla beraber tüm konuları öğrenmeleri gerektiğini ifade etmişlerdir. Tüm toplam puan ortalamaları incelendiğinde de böyle bir kurs organizasyonu bilişim suçları ile ilgili bilgi düzeyi ve bu bilgileri gerekli görme düzeyleri arasında anlamlı fark ortaya çıkarmıştır.

8. Bilişim Suçları Polis Öğretim Programı Konusunda Konu Alanı Uzmanlarının Görüşlerine İlişkin Bulgu ve Yorumlar

Anket bulgularında özellikle bilme ve gerekli görme düzeyi bulguları dikkate alınarak bir öğretim programı hazırlanmıştır. Bu program;

1. Hazırlanan modüllerin amaçları bilişim suçları eğitimi alacak polisin ihtiyaçlarını karşılayabilecek düzeyde midir?

2. Modüllerin içeriği bilişim suçları eğitimi açısından yeterince kapsamlı mıdır?

3. Modüllerin içeriği ile amaçları tutarlı mıdır?

4. İçerik yeterince açık, anlaşılır, ilgi çekici, güncel ve katılımcıların düzeylerine uygun mudur?

5. İçeriğin öğrenilmesi için önerilen süre yeterli midir?

6. Modüllerde yer alan değerlendirme programın amaçlarına ulaşma düzeyini belirleme, kapsam geçerliliği vb. açılardan yeterli midir?

7. Hazırlanan modülleri biçimsel özellikleri (görünüm, sayfa dizaynı, yazı karakteri, resim vb.) açılardan nasıl değerlendirirsiniz?

8. Bunların yanında belirtmek istediğiniz başka bir husus varsa lütfen yazınız?

soruları kapsamında 8 uzmanın görüşüne sunulmuştur. Bu uzmanlar polis akademisi öğretim elemanları ve eğitim programcıları ve eğitim teknologlarından oluşmaktadır. Buna göre elde edilen bulgular şunlardır. Uzmanlar programın amaçlarını yeterli bulmuşlardır. Amaçların, polisin bu konudaki niteliklerini geliştirici özellikler taşıdığı ölçülebilir, gözlenebilir açık seçik ifadelerden oluştuğunu belirtmişlerdir. Genel olarak amaçların, bilişim suçları eğitimi alacak polisin ihtiyaçlarını karşılayabilecek düzeyde olduğunu ifade etmişlerdir.

Konu alanı uzmanları, modüllerin içeriğinin bilişim suçları eğitimi açısından yeterli olduğunu ve mevcut içerik ile amaçların oluştuğunu belirtmişlerdir. Konu alanı uzmanları içeriğin, geniş kapsamlı, yeterince açık, anlaşılır, ilgi çekici, güncel ve katılımcıların düzeylerine uygun olduğunu, örnek uygulamalara yer verildiğini ve içeriğin öğrenilmesi için önerilen sürenin yeterli olduğunu, ancak uygulama aşamasına örnek olaylara biraz daha zaman ayrılması gerektiğini ifade etmişlerdir.

Konu alanı uzmanları, yaşanan örnek olaylara ve çözüm aşamalarına daha çok yer verilmesi ve eğitimlerde sesli, görsel materyallerden (projeksiyon) vb. belirtmişlerdir. Uzmanlar, hazırlanan modülleri biçimsel özelliklerini (görünüm, sayfa dizaynı, yazı karakteri, resim vb.) genel olarak yeterli bulmuştur.

6.2 Tartışma ve Sonuç

Emniyet Genel Müdürlüğü bünyesinde “Bilişim Suçları” konusunda görev yapan birimlerden olan 81 İl Emniyet Müdürlüğü Kaçakçılık Organize Suçlarla Mücadele ve Bilgi İşlem Şube Müdürlüğü personeli toplam 379 personelin; en çok üniversite veya yüksek okul düzeyinde bulunduğu (% 53,0), bunu lise ve dengi okul düzeyinde bulunanların (% 25,3) takip ettiği görülmektedir. Meslek Yüksek Okulu mezunlarının oranı, % 18,8 olup, bunu % 2,9 ile yüksek lisans ve doktora düzeyinde bulunan personel takip etmektedir. Personelin; büyük çoğunluğunun Polis Memuru rütbesindeki personelden (% 86,5) oluştuğu görülmektedir. Amir seviyesindeki personelin oranı ise %13,5’tir. Genel olarak

bakıldığında, "Bilişim Suçları" konusunda görev yapan personelin eğitim düzeyinin yüksek eğitim düzeyinde olduğu görülmektedir. Bu tür suçlarla ilgili görevli personelin eğitim düzeyinin, lise seviyesinin altında bulunmaması bilişim suçlarıyla mücadelede önemli bir unsur olarak ortaya çıkmaktadır.

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, kaç yıldır Emniyet Teşkilatı'nda görev yaptığı incelendiğinde, ağırlıklı olarak 11-15 yıl arası görev yaptığı (% 47,2) görülmektedir. Bunu, % 36,5 ile 6-10 yıl arası görev yapanlar izlemektedir. Dolayısıyla, 6-15 yıl arasında bilişim suçları konusunda görev yapanların oranı % 83,7 olarak karşımıza çıkmaktadır. 1-5 yıl arası Emniyet Teşkilatı'nda görev yapanların oranı ise % 10,0'dır. Bu oranın, artırılması yönünde çaba sarfedilmesi ve bu yönde ilgili alanlardan (elektrik, elektronik, bilgisayar vb.) personel istihdam edilmesi ile bilişim suçlarında başarının artacağı düşünülmektedir.

Personelin, "Bilişim Suçları" konularında ağırlıklı olarak % 50,7 oranında 1-3 yıl arasında görev yaptıkları görülmektedir.

Personel, % 47,8 oranında 6-10 yıl süre arasında bilgisayar kullanmaktadır. Bunu, 11-15 yıl arasında bilgisayar kullananlar (% 29,6) izlemektedir. Personelin, öncelikli olarak (% 37,7) 4-6 yıl arasında İnternet kullandığı görülmektedir. Bunu, 7-9 yıl arası (% 26,1) ve 1-3 yıl arası (% 25,9) İnternet kullanımı takip etmektedir. 10 yıl ve üzerinde İnternet kullanan personelin oranı ise % 10,3'tür.

Personel, 4-6 saat arasında (% 31,9) ve 7-9 saat arasında (% 32,7) yoğunlukla **günlük olarak** bilgisayar başında bulunmaktadır. Günlük olarak 10 saat ve üzerinde, bilgisayar başında bulunan personelin oranı % 22,7 iken, 1-3 saat oranında bilgisayar başında bulunma oranı % 12,7 dir.

Gürcan'ın (2007) belirttiğine göre, ASAGEM tarafından 26 il'de 4819 kişinin katıldığı 2007- "Türkiye'de Ailelerin İnternet Kullanım

Durumları" araştırması yapılmıştır. Araştırma bulguları, araştırmaya katılan her beş aileden dördünün evinde en az bir bilgisayar bulunduğu, araştırmaya katılan bireylerin yaklaşık %77'sinin İnternet kullandığı ve günlük 30 dakika ile 3 saat arasında % 53 oranında İnternet kullandıkları şeklindedir. Bu araştırmanın bulguları, Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin evlerinde genel olarak (% 77,6) evinde bilgisayar bulunması, günlük olarak (% 46,2) oranında, 1-3 saat arasında İnternet'e zaman ayırdıkları ve uzun zamandır İnternet kullandıkları bulgularıyla paralellik göstermektedir. Gerçekten de, ülkemizde bilgisayarlaşma oranı, İnternet bağlantı sayıları ve İnternet'e zaman ayırma konusunda önemli artışlar yaşanmaktadır. Ayrıca, bilişim suçlarında görevli polislerin evinde bilgisayar bulunması ve bu bilgisayarın İnternet bağlantısı olması, personelin bu suçlarla mücadelede sürekli bir aktivasyon içerisinde bulunması açısından önem taşımaktadır.

Personelin, genel olarak web sitelerinin bulunmadığı (% 89,2) görülmektedir. Kendilerine ait tescilli web sitesi bulunanların oranı ise sadece % 10,8'dir. Haberleşme aracı olarak en çok hangi ortamdan yararlandıkları incelendiğinde, öncelikle (% 75,7) cep telefonundan yararlandıkları görülmektedir. E-mail aracılığıyla % 12,1 oranında, anlık mesajlaşma sistemlerinden (ICQ, Messenger, IRC vb.) ise % 11,4 oranında yararlanılmaktadır.

Personelin, İnternet üzerinden alışveriş veya para transferi (Sanal Bankacılık) yapma tercihleri incelendiğinde, personelin genel olarak (% 56,5) sanal bankacılığı kullandıkları görülmektedir. % 31,1 oranında ise personel, İnternet üzerinden alışveriş veya sanal bankacılık uygulamasını tercih etmemektedir. Ülkemizde polisin genel olarak sanal bankacılık uygulamalarını kullandıkları görülmektedir. Bu durum, 8 ocak 2008 tarihli Star gazetesi "2007'de sanal banka mağdurları azaldı" konulu haberdeki, Türkiye'de İnternet bankacılığı uygulaması 2000 yılında başlamasına karşın, uygulama 2003'ten itibaren yoğun olarak kullanılmaktadır ifadesiyle paralellik arz etmektedir (stargazete.com, 2008). Gaziler, 2006 yılında "İnternet Bankacılığı ve

Kullanımının Etkinliği" konusunda yüksek lisans tezi'nde internet bankacılığı kullanımının etkinliğini ifade etmesi de bu bulguları desteklemektedir.

Sanal Banka Mağdurları Derneği, bankaların; personellerinin yanı sıra, müşterilerini eğitmeye başlamalarının mağdurların sayısını önemli ölçüde azalttığını ifade etmiştir (stargazete.com, 2008). Bu da tez kapsamında savunulan suç öncesinde bilişim suçları eğitim faaliyetlerini ve bu eğitimlerin Toplam Destekli Polislik uygulamaları ile vatandaş genelinde yaygınlaştırılarak bilinçlendirmenin arttırılması ve mağduriyetlerin bu şekilde önlenmesi uygulamasıyla paralellik taşımaktadır (Asayiş Daire Başkanlığı, 2008). Dilek (2007) de, kanunlarla birlikte toplumunda bilişim konusunda bilinçlenmesi ve eğitilmesi gerektiğini vurgulanmıştır.

Personelin genel olarak (% 54,3) meslek öncesi polis eğitim kurumlarında bilgisayar ve İnternet kullanımı ile ilgili konularda eğitim almadıkları ortaya çıkmaktadır. Eğitim alanların oranı ise % 45,6'dır. Meslek öncesi, polis eğitim kurumlarında bilgisayar ve İnternet kullanımı ile ilgili eğitim alınması bilişim suçlarıyla mücadelede görev alacak personelin istihdamı ve uzmanlaştırılmasında büyük önem taşımaktadır. İnternet güvenliği ile ilgili kaynakları (Kitap, Dergi, Online Ortam vs.) takip edip edemedikleri incelendiğinde, öncelikli olarak kısmen takip edebildikleri (% 45,1) görülmektedir. İlgili kaynakları takip edebilenlerin oranı ise % 38,5'tir. İnternet güvenliği ile ilgili kaynakları (Kitap, Dergi, Online Ortam vs.) takip edemeyenlerin oranı % 16,4'tür.

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, meslek içinde "Bilişim Suçları" ile ilgili bir kurs görüp görmediği incelendiğinde, personelin genel olarak (% 80,5) bir kurs görmediği ortaya çıkmaktadır. Kurs görenlerin oranı ise % 19,5 oranındadır.

Yine, personelin “Bilişim Suçları” ile ilgili herhangi bir konferans veya seminere katılıp katılmadığı incelendiğinde, personelin çoğunlukla (% 76,3) böyle bir eğitim faaliyetine katılmadığı görülmektedir. “Bilişim Suçları” ile ilgili eğitim faaliyetine katılan personelin oranı ise % 23,7 dir.

Bilişim suçları konusunda görev yapan 379 personelin “Bilişim Suçları” ile ilgili eğitim alma ihtiyacı incelendiğinde, personelin büyük çoğunlukla (% 92,3) eğitime ihtiyaç duyduğu görülmektedir. Yukarıdaki bulgular Dokurer’in (2007), ülkemizde “Adli Bilişim” konusunda yeterli uzman personel bulunmamaktadır. Özellikle suçla doğrudan ilgili olan ve hazırlık soruşturmasını takip eden kolluk görevlilerinin bu konuya eğilmesi, olay yeri ve Kriminal Laboratuarlarının geliştirilmesi gerekmektedir. Bilişim Suçlarının yaygınlaşması ile “Adli Bilişim” hizmeti gündeme gelmiştir. Ancak yetişmiş eleman ve teknoloji eksikliği bu hizmetin sağlıklı verilmesine büyük engel teşkil etmektedir (Dokurer, 2007) ve Şen’ in (2001) bilişim suçlarında başarıya ulaşmak için yürütme organlarının bilgisayar suçları incelemelerini yapabilecek düzeyde teknik ve analitik donanıma sahip çalışanları işe almaları gerektiği görüşleriyle paralellik göstermektedir. “Bilişim Suçları” ile ilgili konularda, personelin kendini yenilemesi ve yetkinliğini artırması amacıyla uygulamalı olarak meslek içinde kurs görmesi, bu tip suç türleri ile mücadele için önemlidir. Bu nedenle eğitim faaliyetlerinin teşkilat geneline yaygınlaştırılması gerekmektedir.

Personelin “Bilişim Suçları” ile mücadele kapsamında gelişiminde en çok hangi faktörün rol oynadığı incelendiğinde, personelin daha çok (% 61,2) bireysel çabaları ve kendi kendini geliştirmesinin bu konuda rol oynadığı görülmektedir.

“Bilişim Suçları” ile mücadele kapsamında yeterli eğitim aldıkları 3 konu; veri inceleme, IP tespiti ve veri kurtarma şeklindedir. Araştırmaya katılanların “Bilişim Suçları” ile mücadele kapsamında çok iyi olduklarını düşündüğü 3 konu; veri kurtarma, IP tespiti ve firewall (13 Kişi) şeklindedir. Bu iki bulgu birbirini desteklemektedir. Eğitim alındığı sürece personel, bilişim suçları ile mücadele kapsamında kendisini yetkin hissedecektir.

"Bilişim Suçları" ile mücadele kapsamında **yetersiz** olduklarını düşündüğü 3 konu; saldırı tespit sistemleri, IP tespiti ve sanal ortamda para transferi şeklindedir. "Bilişim Suçları" ile mücadele kapsamında **eğitim alma ihtiyacı olduğu** 3 konu ise şu şekildedir: IP manager, saldırı tespit sistemleri ve bilgisayar yoluyla dolandırıcılık.

379 personelin, herhangi bir (İnternet suçu, Bilgisayar suçu, Bilişim suçu) suç konusuyla ilgili bilirkişi olarak görev alıp almadığı incelendiğinde, personelin genel olarak (% 70,5) bilirkişilik yapmadığı görülmektedir. Bilirkişi olarak görev alanların oranı ise % 29,5 düzeyindedir. 379 personelin en çok hangi bilişim suçu konusunda görev aldığı incelendiğinde, % 9,0 oranı ile çocuk pornografisi konusunda yapılan bilirkişilik ön plana çıkmaktadır. Bunu, % 8,7 oranı ile bilgisayar yoluyla dolandırıcılık izlemektedir. Ayrıca, personelin genel olarak bu tür suçlarda bilirkişi olarak görev almadığı görülmektedir.

379 personelin en çok karşılaştıkları bilişim suçları incelendiğinde, en çok karşılaştıkları suçların başında virüs (% 15,7) konusu, daha sonra spam mail (% 11,7) ve aynı oranlarda (% 8,3) İnternet üzerinden para transferi ve bilgisayar yoluyla dolandırıcılık konuları gelmektedir. Bu bulgular, Doğan'ın (2008) kimlik bilgilerinin çalınması, hackerlık ve veri tabanı hırsızlığı, sahte web siteleri şifre hırsızlığı, virüs yazılımlarının kullanıcı hesaplarına yollanması, trojan yazılımların kullanılması, telekomünikasyon alanında, sistem konfigürasyonlarına yönelik saldırılar en çok karşılaşılan suç tipleridir bulgusuyla paralellik göstermektedir (masak.gov.tr, 2007). Ayrıca, Gürcan'ın da belirttiği gibi (2007) "Türkiye'de Ailelerin İnternet Kullanım Durumları" araştırmasına göre, aile bireylerinin İnternet'te en fazla karşılaştıkları sorunların virüs yazılımları ve Web sayfalarında gezinirken şiddet, terör ve pornografi gibi içeriklerle istek dışında karşılaşılması sorunları olduğu ortaya çıkmıştır. En çok karşılaşılan suçların başında gelen virüs konusunda, araştırma bulguları ile Doğan (2008) ve Gürcan (2007)'ın bulguları paralellik göstermektedir.

Tez kapsamında literatürde belirtilen, Türkiye'de de terör örgütleri İnternet ortamını öncelikle propaganda ve eğitim amaçlı olarak kullanmaktadırlar. Bölücü örgütlerin bu alanda kullandıkları en önemli platform İnternet'tir (Özcan, 2003) tespitiyle, Doğan (2007) ın, Siber Terörizm'de terörist grupların uluslar arası yapıya sahip olması, teknik olarak ehliyetli elemanları içinde barındırması, sanal ortamda planlama ve eğitim verebilmesi tespitiyle paralellik taşımaktadır.

Toplumsal bilincin arttırılması, sanal para birimleri ile ilgili düzenlemeler yapılması, sanal istihbarat faaliyetlerine ağırlık verilmesi sanal terörizm ile ilgili olarak alınabilecek tedbirlerin başında gelmektedir (Doğan, 2008). Doğan'ın bu tespiti, İnternet kafelerde siber suçların işlenmesini engellemek için alınabilecek bazı tedbirlerin geliştirilmesi kapsamında, İnternet kafeler üzerinden siber terör faaliyetlerinin yürütülmesine karşı olarak, güvenliği ve iletişimi sağlayan birimler başta olmak, internet kafe işletmecileri ve vatandaşlara yönelik olarak tüm ülke çapında bilinçlendirme eğitimleri düzenlenerek toplumsal bilincin arttırılması sağlanmalıdır (Elazığ Emniyet Müdürlüğü, 2002) tespitiyle paralellik göstermektedir.

379 personelin bilişim suçları ile mücadelelerinde en iyi bildikleri sistemlerin neler olduğu incelendiğinde, personelin en çok (% 21,6) veri kurtarma programları konusunda yeterli olduğu görülmektedir. Bunu, firewall (% 14,9) ve Dos komutları (% 10,5) konuları takip etmektedir. Kripto, IP Cop, ENDIAN ve Linux personelin, bilişim suçları ile mücadelelerinde en iyi bildikleri sistemlerin neler olduğu konusunda en az bildikleri sistemlerdendir.

Bilişim suçlarının çözümü hususunda personel çoğunlukla, birim olarak yeterli olduklarını (% 50,1) düşünmektedir. (% 44,6) oranında ise kısmen yeterli olduklarını düşünmektedirler. Bilişim suçlarının çözümünde birim olarak yetersiz olduklarını düşünen personelin oranı ise % 5,3'tür.

379 personelin, meydana gelen bir bilişim suçu karşısında yetersiz kalındığında Emniyet Genel Müdürlüğü bünyesinde **öncelikle** hangi birimden teknik destek aldığı incelendiğinde personelin % 47,0 sinin KOM Daire Başkanlığı'na başvurmayı düşündüğü görülmektedir. Bunu, % 44,5 oranı ile Bilgi İşlem Daire Başkanlığı'ndan teknik destek alırım fikri takip etmektedir. Meydana gelen bir bilişim suçu karşısında yetersiz kalındığında dışarıdan yardım ve destek aldıkları kurum veya kuruluşlar incelendiğinde personelin öncelikle (% 34,8) Türk Telekom'dan destek aldığı ortaya çıkmaktadır.

Personel, İl Emniyet Müdürlükleri bünyesinde bilişim suçlarıyla mücadelede öncelikle (% 45,9) KOM Şube Müdürlüğü'nü en yeterli-donanımlı birim olarak görmektedir. Bunu, % 37,3 oranı ile Bilgi İşlem Şube Müdürlüğü takip etmektedir. İl Emniyet Müdürlükleri için, gerekli mali kaynak oluşturularak bilişim suçlarının çözümünde gerekli teknolojik ortam ve laboratuarlar kurulması gerekmektedir.

Personel, İl Emniyet Müdürlükleri bünyesinde bilişim suçlarıyla mücadele eden birimlerin (% 97,1) daha donanımlı hale getirilmesi gerektiğini belirtmiştir. Genel olarak, ABD ve bazı Avrupa ülkeleri gibi Emniyet Genel Müdürlüğü bünyesinde sadece "Bilişim Suçları" ile mücadele eden ve konu alanı uzmanlarından oluşan bir ünitenin kurulması gerektiği fikrine (% 96,6) sahiptir.

Emniyet personelinin bilişim suçları ile ilgili konulardan iyi bildikleri ve bunları öğrenmenin de çok gerekli olduğunu belirttikleri konular; bilgisayar ve İnternet terimleri, anlık mesajlaşma sistemleri (ICQ, Messenger, IRC vb.), İnternet üzerinden alışveriş ve para transferi yapma, sistemin çalışması için gerekli temel donanım bilgisi ve virus, worm, spyware taramasıdır.

Emniyet personelinin bilişim suçları ile ilgili konulardan bilmedikleri, ancak bunları öğrenmenin de çok gerekli olduğunu belirttikleri konular; bilişim suçlarıyla ilgili uluslararası hukuki düzenlemeler, dinleme sistemleri (Sniffer), linux ve unix işletim sistemleri, tuzak sistemler (Honey Pots) konusu ve PARDUS açık kaynak kodlu işletim sistemidir.

National Center of Computer Crime Data'nın iki yıl süreyle Kaliforniya'da gerçekleştirdiği araştırmaya göre, bilişim suçlarına ilişkin mağdurların büyük bir çoğunluğunu sıra ile ticari kuruluşlar, bankalar, telekomünikasyon firmaları, kamu kurumları ve bilgisayar üreten firmalar oluşturmaktadır. Dokurer (2007), bu konuda çözüm için sadece kolluk görevlileri değil, diğer kamu kurum ve kuruluşları ile özel şirketlerin bilgi işlem departmanları da olay sonrası Adli Bilişim hizmeti verebilecek ekiplerini kurmalıdır şeklinde görüş belirtmiştir. Tulum (2006) bilişim suçları ile mücadelede, yasal tedbirlerin yanı sıra, her kurum ve kuruluşun kendi içerisinde özel tedbirler geliştirerek, güvenlik kurallarını önemsemelerini ifade etmiştir. Bu tespitler ile, tez kapsamında personelin bilişim suçlarının çözümünde "diğer kamu kurum kuruluşları ve diğer kolluk görevlileriyle ortak bir alanda buluşulamamaktadır" şeklinde belirttikleri görüşleri paralellik göstermektedir.

Önemli, 2005 yılında "İnternet suçlarıyla mücadele yöntemleri" konulu yüksek lisans tezi hazırlamıştır. Çalışmada, İnternet suçlarıyla mücadelede önemli bir yer tutan unsurun, uluslar arası işbirliği konusu olduğu vurgulanmıştır. Özeren (2005) ise siber suç ve siber terörizme çare bulma konusunda birlikte çalışmanın önemini vurgulamaktadır. Bu tespitler ile, tez kapsamında personelin bilişim suçlarının çözümünde "uluslar arası işbirliği sağlanmalıdır" şeklinde belirttikleri görüşleri paralellik göstermektedir.

Dijle (2006), bilişim suçları ile mücadele hakkında bilimsel çalışmaların yapılmasını önermiştir. Bu tespitler ile, tez kapsamında personelin bilişim suçlarının mücadelede" yurt içi ve yurt dışındaki üniversitelerde bilimsel çalışmalar yapılmalıdır" şeklinde belirttikleri görüşleri paralellik göstermektedir.

Maltais'in (2005), bilişim suçlarını araştırmada sorumlu sayılan kişilerin bilgi ve uzmanlık düzeyini yükseltmeye yönelik, gerek eyaletler düzeyinde örgütlü tüm polis kuruluşları gerekse federal yönetimler için, ek tahsisat çıkarılması gerekir görüşü ile tez kapsamında personelin bilişim suçlarının mücadelede "taşra teşkilatına teknik ünite için yeteri bütçe sağlanmalıdır" şeklinde belirttikleri görüşleri paralellik göstermektedir.

Gürcan'ın (2007), farkındalık oluşturmada öncelikle "güvenli internet" deniliyorsa kullanıcıların, denetleyicilerin, servis sağlayıcıların "güvensiz internet" de olduğunun farkına varmaları gereklidir, özellikle "farkındalık" (awerness) kavramına bu olgu çerçevesinde yer verilmelidir şeklindeki görüşü ve Şen'in (2008) bilişim suçlarıyla mücadelede farkındalık sorununun çözülmesi gerektiğini görüşü, tez kapsamında belirtilen bilişim suçları konuları ve internet kafeler genelgesi gibi hususlarda bilinçlendirme ve farkındalık düzeyinin artırılarak mağduriyetlerin önlenmesi görüşü ile paralellik göstermektedir.

Tez kapsamında personelin "Bilişim suçları'nda nereye müracaat edileceği bilinmelidir. Vatandaş bu konuda bilinçlendirilmelidir. Tek birim olursa işler, daha kolay olur. Vatandaşın tek bir muhatabı olur. Telekominikasyon birimi gibi tek birim olmalıdır" görüşleri ile Özdemir'in (2003), vatandaşların suçla karşılaştıklarında, nereye, nasıl başvurabilecekleri konusunda internet, medya vb. araçları kullanarak bilinçlendirilmesi gerekir ve Maltais'in (2005), Kanada halkının suç bildirimi ve genelde, sanal suçlar konusunda bilinç düzeyinin yükseltilmesi gerekir ve halkın olduğu kadar tüm kuruluşlarıyla yönetimlerin de sorunların çözümlenebilmesinde baş vuracakları bir adres olmalıdır görüşleriyle paralellik taşımaktadır.

Emniyet personelinin görev yaptığı birime göre, bilişim suçları ile ilgili sahip olması gereken yeterlikler konusundaki bilgi ve gerekli görme düzeyleri incelendiğinde, personelin görev aldıkları yer değişkenine bakılmaksızın tek grup olarak ele alındığında, söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir. Diğer bir boyut ise gruplar dikkate alındığında, hem Bilgi İşlem Şb. Md personeli hem de KOM Şb. Md. ve Daire Bşk.lığı personelinin söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir.

Bilişim suçları ile ilgili görev süresi açısından, personelin sahip olması gereken nitelikler konusundaki bilgi ve gerekli görme düzeyleri incelenerek kıdemler dikkate alındığında hem 1-10 yıl deneyime sahip olanlar, hem de 11 yıl ve üzeri deneyime sahip olanların söz konusu bilgileri bilme ve gerekli görme düzeyleri arasında anlamlı farklılık belirlenmiştir.

Bilişim suçları kursuna katılma durumuna göre sahip olması gereken nitelikler konusundaki bilgi ve gerekli görme düzeyleri incelendiğinde, elde edilen verilere göre üç boyutlu bir sonuç ortaya çıkmıştır. Bunlardan birincisi, hem bilişim kursu alanlar hem de kurs almayanların bilişimi suçları ile ilgili konuları bilme durumları ile gerekli görme durumları arasında anlamlı farklılık belirlenmiş olmasıdır. Bir başka deyişle her iki gruptaki bireyler ilgili maddelerdeki bilgi düzeyleri çeşitli düzeylerde olmakla beraber tüm konuları öğrenmeleri gerektiğini ifade etmişlerdir. Tüm toplam puan ortalamaları incelendiğinde de böyle bir kurs organizasyonu bilişim suçları ile ilgili bilgi düzeyi ve bu bilgileri gerekli görme düzeyleri arasında anlamlı fark ortaya çıkarmıştır.

Tez kapsamında, bilişim suçları konu alanı uzmanlarının görüşleri doğrultusunda temel ve uzmanlık seviyesinde öğretim programı ve modüller hazırlanmıştır. Bilişim suçları öğretim programı temel seviyede personel yetiştirme programı 10 modülden oluşmaktadır. Modüller, şu başlıklardan oluşmaktadır.

MODÜL NO:1 Bilişim Temel Terminolojisi (Bilgisayar, Bilişim ve İnternet'in Tanımları ve İlgili Kavramlar, Bilişim Aygıtları)

MODÜL NO: 2 Suç, Bilişim Suçları, Bilişim Suçluları ve Mağdurları

MODÜL NO: 3 Bilişim Dünyasında Güvenliğin (Security) Ana Esasları

MODÜL NO: 4 Bilgisayar Ağlarında (Network) Güvenliğinin Sağlanması

MODÜL NO: 5 Ülkemizde Sık Karşılaşılan Bilişim Suçları, Örnek Olaylar, İdari Yapılanma ve İlgili İstatistikler, Uluslar arası Platformda ve Bazı Ülkelerinde Bilişim Suçları

MODÜL NO: 6 Bilişim Suçlarının Çözümünde Temel Unsurlar ve Uygulamalar

MODÜL NO:7 Bilişim ve Hukuk, Türk Hukuk Sisteminde Bilişim Suçlarında İlgili Mevzuat

MODÜL NO: 8 Bilişim Yoluyla İşlenen Asayiş Suçları (B.Y.İ.A.) ve Soruşturma Şekilleri

MODÜL NO: 9 Suç Öncesi Polisin Bilişim Suçlarıyla Mücadelesi

MODÜL NO: 10 Bilişim Suçları İle Mücadelede Karşılaşılan Hukuki, Uluslararası, Teknik, İdari, Altyapı, Eğitim, Farkındalık Sorunları ve Çözüm Önerileri

Bilişim suçları öğretim programı uzman personel yetiştirme programı da, 10 modülden oluşmaktadır. Modüller, şu başlıklardan oluşmaktadır.

MODÜL NO:1 Suç, Bilişim Suçu, Adli Bilişim
MODÜL NO:2 Adli bilişim süreci ve Adli bilişim inceleme yöntemleri
MODÜL NO:3 Bilişim Suçlarında Olay Yeri İncelemesi
MODÜL NO:4 Bilişim Suçu Delilleri
MODÜL NO:5 Olay Yeri İncelemesinin Uygulama Yöntemi
MODÜL NO:6 Bilişim Suçlarında Laboratuvar İncelemeleri
MODÜL NO:7 Adli Bilişim Ekspertiz Raporu
MODÜL NO:8 Adli bilişim alanında kullanılan gereçler (Yazılımlar, Donanımlar)
MODÜL NO:9 Örnek Olay Çalışması ve Analizi
MODÜL NO:10 Encase İle Delil İnceleme

Geliştirilen modüllerden, Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı ve dairenin eğitim merkezi (TADOC) ve Asayiş Daire Başkanlığı ve dairenin bağlı eğitim merkezi (SASEM) olmak üzere, bu dairelere bağlı 81 İl Emniyet Müdürlüğü ilgili şube müdürlüklerinin bilişim suçları eğitimlerinde yararlanılabileceği değerlendirilmektedir. Tez kapsamında temel ve uzmanlık seviyesinde hazırlanan öğretim programı ve modüllerin, Eğitim Daire Başkanlığı'nıca hazırlanan yıllık eğitim planları doğrultusunda teşkilata uygulanacak hizmetiçi programlarında değerlendirilebileceği düşünülmektedir.

6.3. Öneriler

Bilişim suçlarıyla mücadelede polisin eğitimi konulu tez çalışmasından elde edilen sonuçlar doğrultusunda aşağıdaki öneriler geliştirilmiştir:

Emniyet Genel Müdürlüğü bünyesinde "Bilişim Suçları" konusunda görev yapan birimlerden olan 81 İl Emniyet Müdürlüğü Kaçakçılık Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlüğü personeli toplam 379 personelin; en çok üniversite veya yüksek okul düzeyinde bulunduğu (% 53,0), bunu lise ve dengi okul düzeyinde bulunanların (% 25,3) takip ettiği görülmektedir. Yapılacak eğitim çalışmalarıyla da, personelin bilişim suçları alanındaki yetkinliği artırılmalıdır.

Personelin; büyük çoğunluğunun Polis Memuru rütbesindeki personelden (% 86,5) oluştuğu ve amir seviyesindeki personelin oranının % 13,5 olduğu dikkate alındığında amir seviyesindeki personelin oranının artırılması için uygun personel istihdamı yapılmalı ve bu personele yönelik eğitim organizasyonları geliştirilmelidir. Ayrıca polis memuru rütbesindeki personel, Emniyet Genel Müdürlüğü Eğitim Daire Başkanlığı'nın hazırlamış olduğu hizmetiçi eğitim planları doğrultusunda bilişim suçları konularında eğitime tabi tutulmalıdır.

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelden, 1-5 yıl arası Emniyet Teşkilatı'nda görev yapanların oranı % 10,0'dır. Bilişim suçlarıyla etkin mücadele için bu oranın artırılması sağlanmalı, genç-dinamik personelin ilgili birimlerde istihdamı sağlanmalıdır. Bunun için, polis memuru yetiştiren kurumlardaki, daha öncesinde ilgili alanlardan (elektrik, elektronik, bilgisayar vb.) diploması olan personelin bilişim suçları için seçilmesine özen gösterilmelidir.

Personelin genel olarak (% 77,6) evinde bilgisayar bulunmaktadır. Bu oranın artması yönünde kurumun da çaba göstermesi gereklidir. Personel, % 47,8 oranında 6-10 yıl süre arasında bilgisayar kullanmaktadır. Emniyet Teşkilatı imkanları ve Halk Eğitim Merkezleri aracılığıyla temel ve ileri düzeyde bilgisayar eğitimlerinin artırılması sağlanmalıdır.

Emniyet Genel Müdürlüğü'ne bağlı merkez ve taşra teşkilatında bilişim suçları konusunda görev yapan 379 personelin, kaç yıldır İnternet kullandığı incelendiğinde, ağırlıklı olarak (% 37,7) 4-6 yıl arasında İnternet kullandığı görülmektedir. İnternet ortamı ile ilgili olarak, İnternet terimleri ve İnternet üzerinden işlenen suçlarla ilgili personelin uygulamalı eğitimler ile yetkinliği sağlanmalıdır.

Tüm dünya üzerinde İnternet üzerinden alışveriş veya para transferi **(Sanal Bankacılık)** uygulamaları gerçekleştirilmekte olup, ev ve iş yerlerinde güvenli şifre kullanımı, antivürüs kullanımı, firewall kullanımı gibi tedbirler ve

genel elektronik güvenlik yöntemleri hususlarında halk eğitim merkezleri eğitimler düzenlemelidir. Ayrıca, toplum destekli polis hizmetleri ile bu konularda vatandaşların duyarlı hale getirilmesi sağlanmalıdır.

Yapılacak temel ve uzmanlık seviyesinde düzenlenen bilişim suçları eğitimi ile hizmetiçi eğitim faaliyetleri düzenlenerek personelin işletim sistemlerindeki güncellemeleri takip edebilmeleri sağlanmalıdır.

Meslek öncesi polis eğitim kurumlarında, bilgisayar ve İnternet kullanımı, bilişim suçları konusunda eğitim içeriği zenginleştirilmelidir. POMEM ve PMYO'nın eğitim müfredatlarında bilgisayar dersleri ile ilgili program yeniden düzenlenmelidir.

Bilişim suçları konusunda görev yapan personelin, dizayn edilecek eğitim portalları ile İnternet güvenliği ile ilgili kaynakları takip edebilmeleri sağlanmalıdır.

Personel, genel olarak (% 80,5) meslek içinde bilişim suçları alanında bir kurs görmediği dikkate alındığında, "Bilişim Suçları" ile ilgili konularda, personelin kendini yenilemesi ve yetkinliğini artırması amacıyla uygulamalı olarak meslek içinde daha sık sayıda kurslar düzenlenmeli ve eğitim faaliyetlerinin teşkilat geneline yaygınlaştırılması sağlanmalıdır.

"Bilişim Suçları" ile ilgili herhangi bir konferans veya seminere personelin çoğunlukla (% 76,3) katılmadığı görüldüğünden, özellikle üst düzey yönetim bu tür etkinliklere personelinin katılımını sağlayıcı tedbirler geliştirmeli ve ayrıca merkez tarafından organizeli bir şekilde tüm İl Emniyet Müdürlükleri'nden uygun personelin bu tür faaliyetlere katılımı sağlanmalıdır.

Personelin "Bilişim Suçları" ile mücadelede daha çok (% 61,2) bireysel çabaları ve kendi kendini geliştirmesinin rol oynadığı görülmektedir. Personelin bilişim suçları konusundaki gelişiminde, kendi çabaları ve kendini geliştirme gayreti düzenlenecek organizasyonel eğitim faaliyetleri ile desteklenmelidir.

Bilişim suçları konularında eğitim maliyetinin yüksek olması nedeniyle, kurum olanaklarının artırılması ve eğitim ortamlarının dizayn edilmesi merkez teşkilatınca sağlanmalıdır.

Personelin gerekli eğitim organizasyonları neticesinde sertifikalandırılması ve böylece bilirkişilik vasıflarının güçlendirilmesi sağlanmalıdır.

Ev ve iş ortamında asgari düzeyde bilişim güvenliğinin sağlanması ve toplumun bilinç düzeyinin artırılması için eğitim faaliyetleri artırılmalıdır.

İl Emniyet Müdürlükleri için, gerekli mali kaynak oluşturulmalı ve bilişim suçlarının çözümünde gerekli teknolojik ortam ve laboratuarlar tesis edilmelidir.

Emniyet Genel Müdürlüğü bünyesinde, bilişim suçları alanında merkezi bir birim kurulmalıdır.

Emniyet personelinin bilişim suçları ile ilgili konulardan bilmedikleri, ancak bunları öğrenmenin de çok gerekli olduğunu belirttikleri,

- Bilişim suçlarıyla ilgili uluslararası hukuki düzenlemeler
- Dinleme sistemleri (Sniffer)
- Linux ve Unix işletim sistemleri
- Tuzak sistemler (Honey Pots) konusu
- PARDUS açık kaynak kodlu işletim sistemi konularında hizmetiçi eğitimler düzenlenmelidir.

Tez kapsamında, bilişim suçları konu alanı uzmanlarının görüşleri doğrultusunda temel ve uzmanlık seviyesinde hazırlanan öğretim programı ve modüllerden, başta Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı ve dairenin eğitim merkezi (TADOC) ve Asayiş Daire Başkanlığı ve dairenin bağlı eğitim merkezi (SASEM) olmak üzere, bu dairelere bağlı 81 İl Emniyet Müdürlüğü ilgili şube müdürlüklerinin bilişim suçları eğitimlerinde yararlanılabilir. Elbetteki öğretim programı ve modüller geliştirilmeye açıktır. Ancak, şu anki şekliyle ilgili birimler için yol gösterici bir

nitelik taşımaktadır. Aynı zamanda, öğretim programı içerisinde yer alan bazı modüller Olay Yeri İnceleme Şube Müdürlükleri ve Bilgi İşlem Şube Müdürlükleri için personelin adli bilişim konularında yetkinlik kazanması açısından uygulanabilecektir. Tez kapsamında konu alanı uzmanlarının görüşleri doğrultusunda temel ve uzmanlık seviyesinde hazırlanan öğretim programı ve modüllerin, Eğitim Daire Başkanlığı'nca hazırlanan yıllık eğitim planları doğrultusunda teşkilata uygulanacak hizmetiçi programlarında değerlendirilmesinin, teşkilatın; bilişim terimlerine ve bilişim suçlarına olan aşinalığını artırması, temel bilişim ve internet güvenliği konularına yetkinlik kazanması, bazı adli bilişim uygulamalarını (IP sorgulama, Domain- Network who is uygulamaları, e-posta tespiti, Mac adresi) rahatlıkla yapabilir hale gelmesi kapsamında önemli faydalar getireceği düşünülmektedir.

İnternet ve bilgisayar teknolojisi sürekli olarak bir gelişme göstermektedir. İnsan doğası gereği bu teknolojik gelişme içerisinde de suç işleme, tüm insanlığın başlıca sorunlarından biri haline gelmiştir. Bilişim suçları gibi bireyi, toplumu, kurumları, devletleri ve tüm hayatı etkileyen bu yeni suç türü için kesinlikle vakit geçirilmeksizin ciddi önlemler alınması ve bilincin artırılması gerekmektedir. Bunun için bireye, kurumlara, üniversitelere, devlete düşen görevler vardır. Uluslararası işbirliği, mali kaynak ayrılması ve uzman personel yetiştirilmesi şarttır. Toplumun bilinçlendirilmesi, veba gibi hızlı bir şekilde yaygınlaşan bilişim suçlarının önlenmesinde bu tür suçlara karşı en önemli unsur olarak görülmektedir. Bilişim suçlarıyla mücadele de teknolojik alt yapı, bilinçlendirmeden daha sonraki adımdır.

Bu suçların boyutları doğal olarak kolluk kuvvetlerini de düşündürmektedir. Teknik ve yasal zorlukların yanında operasyonel ve koordine zorlukları ve yine bu tür suçlarla ilgili uzman personel yetiştirme zorluğu, kolluğun bu suçlarla mücadelesi açısından engel teşkil etmektedir. Suçluların teknolojik gelişmeleri kullanarak kazandıkları hızı, kolluk kuvvetleri de yapacakları teknolojik yapılanma, işbirliği ve geliştirecekleri yeni çalışma sistemleri ile bir an önce kazanma yoluna gitmektedirler. Dünyanın neresinde olursa olsun her ülke, bilişim ortamında işlenen suçlar konusunda yüksek

teknolojiyi iyi takip eden, kendisini bilgisayar, internet ve iletişim konusuna adamış uzman görevlilere gereksinim duymaktadır. Kolluk, özellikle internet ortamında saldırı tespiti, bilgisayar delillendirme konularında yetiştirilmelidir.

Ülkemizde bilişim suçlarında gerek delillerin hukuki niteliği, gerekse de İnternet Servis Sağlayıcılardan delillerin elde edilmesi konusunda her türlü düzenleme yapılmış olsa da, uluslararası polis işbirliğine gidilmeden sağlıklı bir sonuç elde edilmesi mümkün olmayacaktır. Çünkü; özellikle internet üzerinde işlenen suçlarda birden fazla geçiş noktası bulunabilmektedir. Bu noktalarda genelde birden fazla ülke üzerinde bulunabilmektedir. Bir suç diğer ülkede suç niteliği teşkil etmiyorsa o ülkeden gerekli bilgiler alınamayacaktır. Bu amaçla İnterpol, Avrupa Birliği ve Avrupa Konseyinde uluslararası suçun tanımının yapılmasına dair çalışmalar bulunmaktadır. Bilişim suçları kapsamında ortak mevzuat uygulamalarının gerçekleştirildiği uluslar arası anlaşmalar ve protokoller düzenlenmelidir.

Ulusal yazılım güvenliği çerçevesinde, Linux işletim sistemi daha güvenlikli ve özgür bir işletim sistemi olduğundan Başbakanlık bünyesinde bir yazılım ve teknoloji geliştirme merkezi kurulmaladır. Ayrıca, tüm devlet bakanlıklarında kullanılmak üzere yeni bir işletim sistemi ve ofis programı yazılmalıdır. Mail güvenliği ve temel ağ güvenliği konusunda eğitimler düzenlenmelidir.

Ülkemizde, çağın en son bilişim mucizesi olan İnternet'in özellikle 1995 yılından sonra öncelikle kamu ve özel sektörde yaygın olarak kullanılmaya başlamasının ardından, sosyal hayatta İnternet hizmetlerinin verildiği yeni bir sektör ortaya çıkmıştır. Bu sektör, ülkenin ekonomik durumu da göz önüne alındığında sayıları hızla artan ve neredeyse her sokak başında hizmete giren internet kafeler biçiminde toplumsal hayatta yerini almıştır. Ancak, özellikle bu mekanlar bilişim suçlarının rahatlıkla işlenebileceği mekanlar durumundadır. Herhangi bir bilişim suçunun bir internet kafeden işlendiği teknik olarak tespit edilse dahi, o gün ve saatte bilgisayardan kimin işlem yaptığı belli değildir. Kanuni olarak bu konuda düzenlemeye gidilmelidir.

İnternet, geleneksel suçların işlenmesinde yeni bir araç haline gelmesinin yanısıra farklı suç tiplerinin ortaya çıkmasına neden olmuştur. Bu nedenle pek çok ülke mevzuatlarında düzenleme yaparak ya da yeni yasalar çıkarmak zorunda kalmıştır ve bu suçlarla mücadele edecek özel birimler oluşturmaktadır. Ülkemizde de, diğer dünya ülkelerinde olduğu gibi mutlaka bilişim suçları ile etkili bir şekilde kolluğun mücadele edebilmesi amacıyla, bilişim suçları yasası çıkarılmalı ve kurumlar koordinesinde çalışmalar yapılarak özellikle siber terör saldırılarına hazırlıklı olma ve müdahale edebilme gücü kazandırılmalıdır. Ayrıca, konu ile ilgili merkezi bir güvenlik birimi (TURKCERT) kurulmalı ve eğitim faaliyetlerinin yürütüleceği enstitüler açılmalıdır.

Polisin görevleri, günümüzün teknolojik ilerlemeleri ve dolayısıyla teknolojik yeni suç tiplerinin ortaya çıkmasıyla gün geçtikçe artmakta ve zorlaşmakta olup, gelecekte daha da artacaktır. Çağımız, bu durumlarda dikkate alındığında polisin en iyi şekilde eğitim görmesini gerektirmektedir. Polisler suçlulardan daha bilgili ve yetenekli olmak zorundadır. Geçmişte yaşanmış olan olaylar polisin eğitimine verilmesi gereken önemi daha da artırmıştır. Güvenlik hizmetlerinin kalitesinin artırılması polisin eğitim düzeyinin yüksek olmasına bağlıdır. Polisin özellikle toplumsal olaylarda ve bu nedenle ortaya çıkan yeni suç türlerine karşı son derece yetersiz kaldığı görülmektedir.

Polis, bilişim suçlarıyla mücadele kapsamında bilişim suçunu araştırma ve soruşturmasını öğrenmeli, konuyla ilgili kaynak araştırabilmelidir. Ayrıca, polise gerekli ekipmanları temin edilmelidir. Konusunda yetişmiş uzman polis, bilişim suçlarında ispatın zorluğu da göz önüne alındığında toplumsal adaletin yerine gelmesinde önemli bir işlev görmektedir.

Polis eğitim kurumlarının ve icracı birimlerin hizmet içi eğitim programlarının, bilişim suçları merkeze alınarak düzenlenmesi gerekmektedir. Çünkü yakın gelecekte, İnternet'i yoğun olarak kullanan gelişmiş ülkelerdeki gibi ülkemizin de bu tür suçlarla karşı karşıya kalma risk ve tehdidi bulunmaktadır. Kolluk kuvvetlerinin özellikle de polisin, ileride başını ağrıtacak en önemli suç

unsurları, bilişim suçları ve bu suçlarla mücadele olacaktır. Bu nedenle, yapılacak bilimsel çalışmalarla, gelişen çağın koşullarına uygun eğitim programları hazırlanması gerekmektedir.

Bilişim suçlarıyla mücadelede etkili olabilmek, başta kolluk ve adliye birimleri olmak üzere oldukça geniş bir çevreyi içine almaktadır. Devlet organları, sivil toplum kuruluşları, internet kafeler, evdeki anne ve tüm vatandaşların bilgisayar ve internet eğitimleri almaları ve bu konuda bilinçlenmeleri, bilişim suçları ile mücadelenin şüphesizki ana kaynağı olacaktır. Bilişim suçları ile mücadelede eğitim kapsamında halk eğitimi, kamunun eğitimi, internet kafe işletmecilerinin eğitimi, kolluk eğitimi ve adli birimlerinin eğitimi büyük önem taşımaktadır.

Ayrıca, temel internet güvenliği eğitimi Milli Eğitim Bakanlığı'na bağlı işletmenlik ve programcılık eğitimi veren özel eğitim kurslarında, bilgisayar eğitimi verilen okullarda, İnternet aracılığı ile iş yapan kamu ve özel sektör kurumlarında verilmeli ve yaygınlaştırılmalıdır. "Temel İnternet Güvenliği Eğiticilerin Eğitimi" organizasyonu gerçekleştirilmelidir. Toplumun bilinçlendirilmesi hususunda, bilgisayar satıcıları tarafından da asgari güvenlik ve kanuni bilgilerin müşterilere aktarılmasının sağlanması, bilinçlenme ve temel güvenlik önlemlerini alma konusundaki sorunları azaltacaktır.

Ülkemizde bilişim suçlarının yaygınlaşmaması amacıyla bazı tedbirler alınmalıdır. Bunlardan bazıları şu şekilde açıklanabilir. Müstehcen, pornografik ve özellikle de çocuk pornografisine ilişkin cezai müeyyideler caydırıcı bir yaptırıma bağlanmalıdır. İnternet üzerinden yapılan yayınların Basın Kanunda yapılacak değişiklikle açık bir şekilde bu kanuna dahil edilerek gerekli düzenlemeleri yapılmalıdır. İnternet'te yer alan verilere ve kişilere ilişkin özel bilgilerin deşifre edilmesi riskine karşı cezai önlem alınmalı ve özel hayatın korunması çerçevesinde tekrar düzenlenmelidir.

Uluslar arası alanda İnternet yolu ile işlenen suçların engellenmesini ve hatta faillerin iadesini düzenleyen uluslar arası anlaşma yapılmalıdır. İnternet

ortamında lisans ve düzenlemeler yoluyla sıkı ve istikrarlı bir denetim mekanizması oluşturulmalıdır. Terörizmin uluslar arası bir problem olduğu, mücadelenin de ancak uluslar arası işbirliğinden geçtiği bilinmeli, bu bağlamda terörizmle mücadele alanında mevcut bulunan uluslar arası anlaşma metinleri bilişim suçları çerçevesinde düzenlenmelidir. Adalet Bakanlığı koordinatörlüğünde, ilgili birimlerin katılımıyla oluşturulacak komisyon çalışmaları ile bilişim suçlarına yönelik yasal bir düzenleme yapılmalıdır.

Banka ve kredi kartları ile ilgili dolandırıcılık suçlarında bankalar ve kredi kartı merkezleri ile koordineli çalışmalar yapılmalıdır. Bilişim alanındaki suçlar konusunda KOM ve Bilgi İşlem Daire Başkanlığı, PMYO ve POMEM müdürlükleri ve Polis Akademisi'nce uluslararası sempozyum, panel ve konferanslar düzünlenmeli ve bu tür gerek yurt içi, gerek yurt dışında başka kurumlar tarafından düzenlenen etkinliklere personelin katılımı sağlanmalıdır.

Emniyet Genel Müdürlüğü'nce, sadece özel harekat polisi ve sadece trafik polisi yetiştirmek için özellikle ayrılan polis okulları örneğinde olduğu gibi, gerekli laboratuarları ve eğitim ortamı oluşturulmuş bilişim suçları polisi yetiştiren PMYO/POMEM kurumları açılmalıdır.

Bilişim alanındaki suçların önlenmesi için, bilişim seferberliği düzenlenmeli ve topyekün bilişim suçlarını önlemek amacıyla bilinçlendirme eğitimleri yapılarak, yaygınlaştırılmalıdır. Bilişim alanındaki suçlar konusunda on-line halk desteği için ortam oluşturulmalıdır.

6.4. Yeni Araştırmalar İçin Öneriler

1. Bilişim suçlarında başarı için, suç öncesinde Toplum Destekli Polis çalışmalarının değerlendirileceği bir çalışma yapılabilir.
2. Bilişim suçlarında farkındalık düzeyinin nasıl artırılabileceği yönünde çalışmalar yapılabilir.
3. Diğer ülke sistemleriyle karşılaştırmalı polisin bilişim suçlarında eğitimi konusunda çalışmalar yapılabilir.
4. Diğer ülke sistemleriyle karşılaştırmalı bilişim suçları istatistikleri

konusunda çalışmalar yapılabilir.

5. Bilişim suçlarında başarı için, sivil toplum kuruluşlarının rolü ve sorumlulukları hakkında çalışmalar yapılabilir.
6. Bilişim suçları eğitim programının uygulanması sonucunda program değerlendirme çalışmaları yapılabilir.
7. Bilişim teknolojisindeki hızlı gelişimden dolayı bilişim suçlarına ilişkin polisin eğitimi konusunda sürekli program geliştirme çalışmasına ihtiyaç vardır.
8. Tüm dünyadan bilişim suçlarında yaşanan örnek olayları ve bunların çözüm aşamalarını sistematik bir şekilde ele alan çalışmalar yapılabilir.

KAYNAKLAR

Akgül, M. (2002). **İnternet Üst Kurulu Üyesi ve Bilkent Üniversitesi Öğretim Üyesi Doç.Dr. Mustafa AKGÜL ile Yapılan Görüşme Notları**. 08 Kasım 2002. Ankara.

Akşam Gazetesi. (2000). **Avrupa Birliği İnternet Polisi Kuracak**. http://www.aksam.com.tr/arsiv/aksam/2000/04/12/dunya/dunya4.html. Erişim Tarihi: 12 Nisan 2000.

Akşam Gazetesi. (2004). **FBI Bile Bu Vurguna Şaştı**. 13 Haziran 2004.

Aktepe, B. (2003). **Emniyet Personelinin Bilgisayar ve Bilgisayar ilintili Suçlarla Mücadelede Dikkat Etmesi Gereken Hususlar (Adli Tip Esaslarına Uygun Olarak Delillendirme)**. 1.Polis Bilişim Sempozyumu. 21-22 Ekim 2003. Ankara.

Alkan, C. Şimşek, N. ve Deryakulu, D. (1995). **Eğitim Teknolojisine Giriş**. Ankara: Önder Matbaacılık.

Allee, V. (2000). **Bilgi Etiği**. Executive Excellence Dergisi. Yıl: 4 Sayı: 40. Temmuz 2000.

Andaç, Ş. (2003). **Oturdukları Yerden 4 Milyar Dolar Zarar Veriyorlar**. http://www.milliyet.com.tr/2003/09/10/business/abus.html. Erişim Tarihi: 10.09.2003

APK Dairesi Başkanlığı. (2002). **Polisle İlişkilerinizde Rehberiniz**. Ankara.

Asayiş Daire Başkanlığı. (2008). **Toplum Destekli Polis Büro Amirleri Toplantısı**. Ankara.

Aydın, E.D. (1992). **Bilişim Suçları ve Hukukuna Giriş**. Ankara.

Balcı, A. (1997). **Sosyal Bilimlerde Araştırma Yöntem, Kavram ve İlkeler**. (İkinci Baskı). Ankara:72 TDFO Bilgisayar-Yayıncılık San.Tic.Ltd.Şti.

Beceni, Y. (2002). **Siber Suçlar**. http://www.hukukcu.com./bilimsel/kitaplar/yasinbeceni/bolum5. Erişim Tarihi: 01 Aralık 2002

Berber, L.K. (2004). **Bilgi Üniversitesi ve İstanbul Emniyet Müdürlüğü İşbirliğiyle Hazırlanan Adli Bilişim El Kitapçığı**. İstanbul.

Beyhan, C. (2003). **Bilişim Suçları İle Etkin Mücadele Yöntemleri**. 1.Polis Bilişim Sempozyumu. 21-22 Ekim 2003. Ankara.

Boni, W. C. and Kovacich, G. L. (1999). **I-Way Robbery: Crime on the Internet**. Butterworth-Heinemann: United States of America.

Büyüköztürk, Ş. (2003). **Sosyal Bilimler İçin Veri Analizi El Kitabı**. Ankara: PegemA Yayıncılık

Carter, D. (1996). **Bilgisayar Suçları**. Strateji Dergisi. Sayı: 4 Yıl : 1996

Casey, E. (2000). **Digital Evidence and Computer Crime**. (İkinci Baskı). London: Academic Press. 2000

Cerrah, İ. ve Semiz, E. (2000). **2l. Yüzyılda Polis, Temel Sorunlar ve Çağdaş Yaklaşımlar**. Ankara: Sibel Matbaası.

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

Clarke, R. J., Liu, K, Andersen, P, B., Stamper, R. K. (2001)**. Information, Organization, and Technology: Studies in Organizaitonal Semiotics**. Kluwer ACADEMİC, Boston, MA.

Conway, M. (2002). **Reality Bytes: Cyberterrorism and Terrorist Use of the Internet**.http:www.firstmonday.org/issues/issue711/conway/index.htm. Erişim Tarihi: 14.12.2002

Çeken, H. (2001). **Amerika Birleşik Devletlerinde Siber Suçlar**. http://www.jura.uni-sb.de/turkish/HCeken.html. Erişim Tarihi: 10.11.2002

Çekiç, B. (2006). **İnternet Aracılığıyla İşlenen Suçlar**. Marmara Üniversitesi. Sosyal Bilimler Enstitüsü. İstanbul: Yayınlanmamış Yüksek Lisans Tezi.

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

Demirbaş, T. (2005). **Kriminoloji**. Seçkin Yayınları, Ankara.

Demirel, Ö. (2000). **Kuramdan Uygulamaya Eğitimde Program Geliştirme**. PegemA Yayıncılık, Ankara.

Denning, D. E. (2000). **Cyberterrorism. Testimony Before The Special Oversight Panel on Terrorism**. Committee on Armed Services. U.S. House of Representatives. May 2000.

Desouza, K. C., Hensgen, T. (2003). **Semiotic Emergent Framework to Address the Reality of Cyberterrorism. Technological Forecasting and Social Change.** Volume 70, Issue 4, May 2003, pp. 385-396

Dick, R. L. (2001). **Information Technology-Essential Yet Vulnerable: How Prepared are we for Attacks? Testimony Be on Government Efficiency, Financial Management and Intergovernmental Relations**. http://www.reform.house.gov/gefmir/hearings/2001hearings/0926_computer_security/0926_dick.htm. Erişim Tarihi: 26 Eylül 2001.

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

Dilek, H.İ. (2007). **Bilişim Suçları ve Türk Hukukundaki Yeri**. Dicle Üniversitesi. Sosyal Bilimler Enstitüsü. Diyarbakır: Yayınlanmamış Yüksek Lisans Tezi.

Doğan, A.C. (2007). TAIEX Semineri. **Bilişim Suçları ve Karapara**. Ankara. 19-20 Mart 2007. http://www.masak.gov.tr/Kurulumuz/egitim/ Erişim Tarihi: 18 Eylül 2007.

Dokurer, S. ve Kızılsu, H.Ö. (2001). **Adli Bakımdan İnternet'te Çocuk Pornografisiyle Mücadele Semineri Görev Dönüş Raporu**. 26-28 Mart 2001. Stockholm.

Dokurer, S. (2007). **Adli Bilişim**. http://www.tbd.org.tr/resimler/ekler/0008b9a5380fcac_ek.pdf Erişim Tarihi: 04 Şubat 2008.

Dönmezer, S. (1994). **Kriminoloji**. İstanbul. Beta Basım.

Dülger, M.V. (2004). **Türk Ceza Hukuku'nda Bilişim Suçları**. İstanbul Üniversitesi. Sosyal Bilimler Enstitüsü. Yayınlanmamış Yüksek Lisans Tezi.

Eğitim Daire Başkanlığı. (2008). **Eğitim Şube Müdürleri Toplantısı**.

Eğitim Daire Başkanlığı. (2008). **Eğitim Daire Başkanlığı Web Sitesi**. http://www.egm.gov.tr/egitim. Erişim Tarihi: 10 Temmuz 2008.

Ekizer, A.H. (2007). **Adli Bilişim Uzmanlığı Sertifikasyonları**. http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=136 Erişim Tarihi: 20 Ağustos 2008.

Elazığ Emniyet Müdürlüğü. (2000). **Sistem İletişim ve Bilişim Suçları Büro Amirliği E-Posta Servisi**. 11 Mayıs 2000. Elazığ

Elazığ Emniyet Müdürlüğü, (2002). **İnternet Kafe İşletmecileri ile Yapılan TSE Kalite Güvence Sistemi Eğitim Toplantısı Tutanağı**. Elazığ

Emniyet Genel Müdürlüğü. (1999). **Microsoft INTERNET**. Bilgi İşlem Daire Başkanlığı. Eğitim Şube Müdürlüğü Yayınları. Ankara.

Emniyet Genel Müdürlüğü. (1999). **Bilişim Suçları ve Bilgi Güvenliği Kurulu Çalışma Raporu**. Ankara.

Emniyet Genel Müdürlüğü. (2000). **Bilişim Suçları Raporu**. Ankara

Emniyet Genel Müdürlüğü. (2004). **Bilişim Suçlarıyla İlgili Resmi Yazı**. Ankara.

Erbschloe, M. (2001). **İnformation Warfare How to Survive Cyber Attacks**. Osborne.

Erdönmez, E. (2002). **Investigation Of Computer Crimes**. University of North Texas. Yüksek Lisans Tezi.

Ersanel, N. (2001). **Siber İstihbarat**. Ankara: ASAM Yayınları.

Ertürk, S. (1993). **Eğitimde Program Geliştirme**. Hacettepe Üniversitesi Basımevi, Ankara.

Forno, R. (2000). **Shredding the Paper Tiger of Cyberterrorism**. http://www.onlinesecurity.com/columnists/111. Erişim Tarihi: 27 Eylül 2000.

Gaziler, V. (2006). **İnternet Bankacılığı ve Kullanımının Etkinliği; Kullanım Etkinliği- Eğitim İlişkisini Ortaya Koymaya Yönelik Bir Araştırma**. Gazi Üniversitesi. Eğitim Bilimleri Enstitüsü. Ankara: Yayınlanmamış Yüksek Lisans Tezi.

Gillen, M.C. (2005). **Sanal Gerçekliğe Sahip Çıkmak. İnternet'le İlgili Etkili Düzenleme: Toplumsal Değerlere Dönüş**. Queen's University of Belfast. Doktora Tezi.

Göksu, T. (2000) **Toplumsal Psikoloji**. Ankara: Özen Yayımcılık, Şahin Matbaası, 2000.

Gümüş, Ç. (2003). **İnternet Kafelerin (Dijital Kütüphaneler) Denetlenmesi ve Eğitim Amaçlı Kullanımının Teşviki**. Fırat Üniversitesi. Sosyal Bilimler Enstitüsü. Elazığ: Yayınlanmamış Yüksek Lisans Tezi.

Gümüş, Ç. (2008). **Kocaeli Kentinde Toplum Destekli Polis Uygulamaları**. Kocaeli Yöresel Kültürler Fuarı ve Sempozyumu. 27 Haziran 2008. Kocaeli

Günay, B.(1999). **Siber Terörist Saldırı**. 12 Mayıs 1999 Tarihli Türkiye Gazetesi.

Gürcan, A. (2007). **Türkiye'de Ailelerin İnternet Kullanım Durumları Araştırması**. http://www.tbd.org.tr/resimler/ekler/8238e9ae2dd305d_ek.pps. Erişim Tarihi: 12 Ağustos 2008.

Gürol, M. (2006). **Öğretimde Planlama ve Öğretimde Değerlendirme**. Akış Yayıncılık. Ankara

Henych, (2003). **Bilişim Suçu Algılamaları ve Florida Eyaletinde Sanal Evrenle İlgili Hazırlıklar, Konuyla İlgili Gelecekte İzlenecek Politikalar**. University of Central Florida. Doktora Tezi.

İstanbul Emniyet Müdürlüğü. (2002) . **Bilişim Suçları Raporu**. İstanbul

İstanbul Emniyet Müdürlüğü. (2006). **Emniyet Müdürlüğü Web Sitesi.**

http://www.iem.gov.tr. Erişim Tarihi: 27 Kasım 2006.

İstanbul Emniyet Müdürlüğü. (2008) **Bilişim Suçları ve Sistemleri Şube Müdürlüğü Web Sitesi**. bilisimsuclari.iem.gov.tr. Erişim Tarihi: 11 Eylül 2008.

İzmir Emniyet Müdürlüğü (2008). **Bilişim Suçları.** http://bilisim.izmirpolis.gov.tr/bilisimsuclari/bilisimsuclari.htm. Erişim Tarihi: 08 Temmuz 2008.

Kalkandelen, H. (1979). **Hizmet İçi Eğitim El Kitabı**. Ankara: Ajans-Türk Matbaacılık ve Gazetecilik Sanayi.

Karaahmetoğlu, O. (2001). **İnternet Güvenliği Kavramları ve Teknolojileri**. İstanbul Üniversitesi. Fen Bilimleri Enstitüsü. İstanbul: Yayınlanmamış Yüksek Lisans Tezi.

Karaman, Ö. (2003). **Bilişim Suçları İle Mücadelede Polis Temel Eğitiminin Önemi**. 1.Polis Bilişim Sempozyumu. 21-22 Ekim 2003.Ankara.

Karakurt, Y. (2006). **Bilişim Suçları İle Mücadelenin Uluslararası Boyutu ve Türkiye'ye Yansıması**. TODAİE. Yayınlanmamış Yüksek Lisans Tezi.

Koch, E. ve Sperber, J. (1996). **Bilgi Mafyası**. Sarmal Yayınevi. İstanbul.

KOM Daire Başkanlığı. (2008). **Bilişim Suçları ile Mücadele Eğitimi Kurs Notları**. Antalya.

KOM Daire Başkanlığı (2008). **Bilişim Suçları ve Yükselen Trentler** http://www.kom.gov.tr/Tr/KonuDetay.asp?BKey=64&KKey=172 Erişim Tarihi: 16 Eylül 2008.

Kurt, E. (2003). **Hacker'lığın Kısa Tarihçesi**. http://www.olympos. org/article/articleview/283/1 /10.

Kurt, L. (2005). **Bilişim Suçları ve TCK'daki Uygulaması**. TODAİE. Yayınlanmamış Yüksek Lisans Tezi. Ankara

Küçükgörkey, A . (2002). **Siber Uzay, Siber Suç Ve Siber Polis**.

Lazarevich, A. (2005). **Use of Ontologies and Probabilistic Relation Models To Aid in Cyber Crime Investigation Decision Support**. George Mason of University. Doktora Tezi.

Maat, S.M. (2004). **Karşılaştırmalı Bir Yasa Çözümlemesi**. University of South Africa. Yüksek Lisans Tezi.

Maltais, C.F. (2005). **Managing Cyber Crime: an Assessment of Canadian Law Enforcement Responses**. Charles Sturt University, Australia. Yüksek Lisans Tezi.

Moore, J.W. (2002). **Bilişim Savaşı, Sanal Terör ve Toplumsal Değerler**. McGill University (Canada).

Mungo, P. ve Clough,B. (1999). **Sıfıra Doğru Veri Suçları ve Bilgisayar Yeraltı Dünyası**. Approaching Zero Data Crime and the Computer Underworld. İletişim Yayınevi. İstanbul.

Oliva, P. F. (1997). **Developing the Curriculum**. USA: Longman Inc.

Önemli, M. (2005). **İnternet Suçlarıyla Mücadele Yöntemleri**. TODAİE. Yayınlanmamış Yüksek Lisans Tezi. Ankara.

Özalp, S. (2002). **Hacker Olmak Her Zaman Kötü Mü?**. http://www.turk.internet.com/haber/yazigöster.php3?yaziid=3814 Erişim Tarihi: 10 Aralık 2002.

Özcan, M. ve Bal, İ. (2001). **Ulusal Güvenlik ve Bilişim Suçları. Türkiye'nin Güvenliği Sempozyumu**.17-19 Ekim 2001. Elazığ. s.587

Özcan, M. (2003).**Yeni Milenyumda Yeni Tehdit: Siber Terör**. Polis Dergisi Özel Sayı. 2003

Özcan, M. (2003). **Bilişim Suçlarının Ulusal Güvenlik Tehdidi. Bilişim Suçları ile Mücadele Semineri Bildiriler Kitabı**. Beytepe. 4.Sunum.

Özdemir, E. (2003). **Bilgi Savaşı Nedir? Bilgi Savaşlarının Türkiye'nin Bilim Teknoloji Politikaları ve Savunma Stratejilerine Etkileri**. Gebze İleri Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü. Gebze: Yayınlanmamış Yüksek Lisans Tezi.

Özdemir, M. (2003) **Bilişim Suçları ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler ve Çözüm Önerileri**. http://www.caginpolisi.com.tr/24/43-44-45-46.htm Erişim Tarihi: 18 Mart 2007.

Özel, C. (2002). **Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı.** http://www.hukukcu.com/bilimsem/kitaplar/bilisim suclari_TCKtasarisi.htm. Erişim Tarihi: 10 Ekim 2002.

Özeren, S. (2005). **Global Response to Cyberterrorism and Cybercrime". University of North Texas**. Doktora Tezi.

Pekgözlü, İ. (2008). **Küresel Tehdit: Bilişim Suçları.**

http://www.polis.gov.tr/egitim/dergi/eskisayi/41/web/kalite/Ilker_PEKGOZLU.htm

Erişim Tarihi: 25 Ekim 2008.

Pollitt, M. M. (2002). **Cyberterrorism. Fact or Fancy?**. http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Erişim Tarihi: 03 Kasım 2002.

Sağsan, M. (2002). **Bilgi Savaşı: Siperlerden Klavyelere Taşınan Harekatın Anatomisi**. Avrasya Dosyası İstihbarat Özel. Ankara.

Savaş, A. (2005). İnternet Ortamında Yapılan Hukuki Sözleşmeler ve Bunların Hukuki Sonuçları. Selçuk Üniversitesi. Sosyal Bilimler Enstitüsü. Konya: Yayınlanmamış Doktora Tezi.

Say, K. (2006). **Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuarlarda İncelenmesi.** Ankara Üniversitesi. Sağlık Bilimleri Enstitüsü. Ankara: Yayınlanmamış Yüksek Lisans Tezi.

Saylan, N. (1995). **Eğitimde Program Tasarısı**. Temeller-Prensipler-Kriterler. Balıkesir: İnce ofset.

Saylor, J. G., Alexander, W. M., & Lewis, A. J. (1981). **Curriculum Planning for Better Teaching and learning**. (4.Edition). USA: Holt, Rinehart and Winston Inc.

Seven, U. ve Seven O. (2008). **2006'da En Çok İşlenen İnternet Suçları**. http://www.chip.com.tr/konu/2006-da-En-Cok-islenen-internet-Suclari_3625.html Erişim Tarihi: 20 Temmuz 2007.

Shinder, D. L. (2002). **Scene of Cybercrime**. Computer Forensics Handbook. Syngress Publishing, USA, 2002

Star Gazetesi (2008). **2007'de Sanal Banka Mağdurları Azaldı**. http://www.stargazete.com/ekonomi/2007-8217-de-sanal-banka-magdurlari-azaldi-81713.htm. Erişim Tarihi: 8 Ocak 2008.

Şen, B. (2003). **İnternet Suçlarıyla Mücadelede Suç Önleme Anlayışı ve Bilinçli Kullanıcı**. 1.Polis Bilişim Sempozyumu. 21-22 Ekim 2003.Ankara.

Şen, B. (2008). **Bilişim Suçlarıyla Mücadelenin Stratejik Önemi-3**. http://turk.internet.com/haber/yazigoster.php3?yaziid=21067 Erişim Tarihi: 20 Haziran 2008.

Şen, O.N. (2001). **Criminal Justice Responses To Emerging Computer Crime Problems** . University of North Texas. Yüksek Lisans Tezi.

Şen, O.N. (2003). **Polisin Bilişim Suçlarıyla Mücadelede Yapması Gerekenler. 1.Polis Bilişim Sempozyumu**. 21-22 Ekim 2003.Ankara.

Şen, O.N. (2007). **Bilişim Şuuru**. bthukuku.bilgi.edu.tr/Documents/osman_nihat_sen_2.doc. Erişim Tarihi: 13 Mayıs 2008.

Tanşu, H.O. (2000). **21.Yüzyıl Çatışma Ortamı: Bilgi Savaşı**. Marmara Üniversitesi. Sosyal Bilimler Enstitüsü. İstanbul : Yayınlanmamış Doktora Tezi.

Taşpınar, M. (2007). **Kuramdan Uygulamaya Öğretim İlke ve Yöntemleri**. Üniversite Kitabevi. Elazığ

Taymaz, H. (1981) **Hizmet İçi Eğitim: Kavramlar, İlkeler, Yöntemler**. Ankara: A.Ü. Eğitim Fakültesi, Yayın No: 94.

Topçuoğlu, A. (2001). **Bilgisayarlar Artık Yalnızca Bizim Değil, Teröristlerinde Vazgeçilmezi**. Bilim ve Teknik Dergisi. Ekim 2001

Torosyan, A.. (2003). Eyalet ve Yerel Yürütme Tarafından Siber Suç Programı: Ulusal Araştırmanın İlk Analizi. California State University. Yüksek Lisans Tezi.

Türk Dil Kurumu (2008). **Güncel Türkçe Sözlük, Türk Dil Kurumu**. www.tdk.gov.tr. Erişim Tarihi: 5 Mayıs 2008

Tulum, İ. (2006). **Bilişim Suçları ile Mücadele**. Süleyman Demirel Üniversitesi. Kamu Yönetimi Bölümü. Isparta: Yayınlanmamış Yüksek Lisans Tezi.

Ural, A. ve Kılıç,İ. (2005). **Bilimsel Araştırma Süreci ve SPSS ile Veri Analizi**. (SPSS 12.0 for Windows). Ankara. Detay Yayıncılık.

Underwood, J. (2006). http://www-staff.it.uts.edu.au/~jim. Erişim Tarihi: 12.01.2008

Uzun, M. (1999). **Bilgisayar Ağlarında Firewall ile Güvenlik**. Gebze İleri Teknoloji Enstitüsü Mühendislik ve Fen Bilimleri Enstitüsü. Gebze: Yayınlanmamış Yüksek Lisans Tezi.

Uzunay, Y. ve Koçak, M. (2005). **Bilişim Suçları Kapsamında Dijital Deliller**. Akademik Bilisim Konferansı. Şubat 2005. Gaziantep http://www.ankara.pol.tr/yusufuzunay/documents/ab05.pdf Erişim Tarihi: 14 Temmuz 2008

Uzunay, Y. (2005). **Dijital Delil Araştırma Süreci**. 2. Polis Bilişim Sempozyumu. Nisan 2005. Ankara.

Wikipedia (2008). **Bilişim**. http://tr.wikipedia.org/wiki/Bili%C5%9Fim_bilimi. Erişim Tarihi: 22 Ağustos 2008

Varol, C. ve Varol, N. (2001). **Gençliğin İnternet Kullanımına Yaklaşımı ve İnternet Kafeler**. BTIE Konferansı. 3-5 Mayıs 2001. Ankara.

Yamaç, F. (2003). **Siber Terörizm**. Emniyet Genel Müdürlüğü. TEMÜH Daire Başkanlığı. Psikolojik Harekat Kurs Notları.

Yavuz, A.A. (2006). **Novel Methods For Security Mechanisms and Key Management Techniques in Wireless Networks Based On Signcryption and Hybrid Cryptography** . Boğaziçi Üniversitesi. İstanbul: Yayınlanmamış Yüksek Lisans Tezi.

Yazıcıoğlu, Y. (1997). **Bilgisayar Suçları**. İstanbul: Alfa Basım

Yıldırım, A. ve Şimşek, H. (1999) . **Sosyal Bilimlerde Nitel Araştırma Yöntemleri**. Ankara: Seçkin Yayınevi.

Yıldız, S. (2006). **Suç'ta Araç Olarak İnternet'in Teknik ve Hukuki Yönden İncelenmesi.** Selçuk Üniversitesi. Sosyal Bilimler Enstitüsü. Konya: Yayınlanmamış Doktora Tezi.

EKLER

EK-1 Ülkemizde, Bilişim ve Bilişim Suçları Alanındaki Yürürlükte Olan Mevzuat

3756 Sayılı Türk Ceza Kanunu

Ülkemizde, kanun koyucu bilgisayar suçlarına ilişkin ilki 1991 yılında, 3756 sayılı kanunla **Türk Ceza Kanunu'nun** ikinci kitabına bazı bilgisayar suçlarını öngören "Bilişim Alanında Suçlar" başlıklı 11. bölümü ilave etmiştir. Bundan sonra 1995 yılında, bilgisayar programlarının "eser" sayılacağını belirleyen bir değişiklik yapılmış ve bilgisayar programlarına karşı gerçekleştirilen bir takım eylemler de yaptırım altına alınmıştır.

3756 sayılı TCK. nun 2. Kitabına 11. bölümü olarak ilave olunan "Bilişim Alanında Suçlar", 525a, 525b, 525c ve 525d maddeleri olmak üzere dört maddeden oluşmaktadır. 525d maddesi hariç, 525a, b ve c maddelerinde feri cezalar yer almaktadır. 525a, b ve c maddesinde "bilgileri otomatik olarak işleme tabi tutmuş bir sistemden bahsetmek suretiyle bilgisayarlar kast edilmektedir. 525a/1 ve 2, 525b/1 maddelerinde bilgisayar, suçun konusunu oluşturmakta, 525b/2 ve 525c maddelerinde ise suçta araç vazifesini görmektedir.

TCK. Md 525 a/1' de, Bilgileri otomatik işleme tabi tutmuş bir sistemden "programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirmek" yaptırım altına alınmak suretiyle "Bilgisayar sistemlerinde bulunan programlar ve bilgiler" hukuki olarak koruma altına alınmıştır.

TCK md.525 a/2' de, "Bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanmak, nakletmek veya çoğaltmak" eylemleri yaptırım altına alınmaktadır.

TCK md.525 b/1' de, "Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen

tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan" kimselerin fiilleri yaptırım altına alınmak suretiyle bilgisayar ve sistemlerine veya bunlardaki veri, program ve diğer unsurlara karşı gerçekleştirilen ızrar eylemleri yaptırım altına alınmaktadır.

TCK. Md.525 b/2' de, " Bilgisayar kullanmak suretiyle kendisini veya başkasını lehine hukuka aykırı yarar sağlamak" suç olarak düzenlenmektedir.

TCK. Md.525 c'de ise, " Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme , verileri veya diğer unsurları yerleştiren veya var olan verileri veya diğer unsurları tahrif eden kimsenin fiili yaptırım altına alınmaktadır. Madde de ayrıca, "tahrif edilmiş olanları bilerek kullananlara ... hapis cezası verilir" denmek suretiyle de yukarıdaki suça ilaveten sahtecilik mahsulü bir belgenin bu niteliği bilinerek kullanılması da ayrıca kullanma suçu olarak düzenlenmektedir.

Ceza Hukukumuz açısından bir eylemin suç teşkil edebilmesi için esasa uygunluk, hukuka aykırılık ve kusurluluk unsurlarının bir arada olması gerekir.

5237 Sayılı Yeni Türk Ceza Kanunu

26.9.2004 tarihinde kabul edilen 5237 sayılı yeni Türk Ceza Kanunu'nda yer alan bilişim suçları ve yaptırımları şu şekildedir:

Kişisel Verilerin Kaydedilmesi
Madde 135
(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.
(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

Verileri Hukuka Aykırı Olarak Verme veya Elegeçirme

Madde 136

(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Nitelikli Hırsızlık

Madde 142

(2) Suçun;

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

Nitelikli Dolandırıcılık

Madde 158

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Karşılıksız Yararlanma

Madde 163

(2) Telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

Bilişim Alanında Suçlar: TCK'nın 243-244-245-246. maddeleri de, bilişim alanında işlenen suçları düzenlemektedir. Madde 243 Bilişim sistemine girme, Madde 244 Sistemi engelleme, bozma, verileri yok etme veya

değiştirme, Madde 245 Banka veya kredi kartlarının kötüye kullanılması ve Madde 246 ise Tüzel kişiler hakkında güvenlik tedbiri uygulamasıdır.

Bilişim Sistemine Girme

Madde 243

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

Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

Madde 244

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

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

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

Banka veya Kredi Kartlarının Kötüye Kullanılması

Madde 245

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

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

Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulaması

Madde 246

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

4077 Sayılı Tüketicinin Korunması Hakkında Kanundaki Düzenleme

23.02.1995 tarihli ve 4077 sayılı Tüketicinin Korunması Hakkında Kanunun 3'üncü maddesinde mal; *"… elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayrimaddi malları"* da içerecek şekilde tanımlanmış, 9/A maddesiyle de mesafeli sözleşmelerin *"…görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak"* gerçekleştirilebileceği, elektronik ortamda yapılan sözleşmelerin teyit işlemlerinin yeni elektronik ortamda yapılabileceği hüküm altına alınmıştır.

Adli ve Önleme Aramaları Yönetmeliği

Haziran 2005 tarihinde yürülüğe giren, Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde; bilişim ile ilgili delillere el konulması ve sonrasında incelenmesi konusunda "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlığı adı altında;

- Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından

kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

- Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
- Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.
- İstemesi hâlinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.
- Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir denilmektedir.

5070 Sayılı Elektronik İmza Kanunu (23.7.2004 YÜRÜRLÜK T.)

Amaç

MADDE 1 Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

Bu amaç doğrultusunda elektronik imzanın teknik yönlerini düzenlemek için Telekomünikasyon Kurumu tarafından 6.1.2005 tarihli ve 25692 sayılı Resmi Gazetede “Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ” yayımlanmıştır.

5070 sayılı Elektronik İmza Kanunu’nun 16’ncı maddesiyle imza oluşturma verilerinin izinsiz kullanımı ve 17’nci maddesiyle elektronik sertifikalarda sahte-karlık suç haline getirilmiş bulunmaktadır.

Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (06/01/2005 tarihli)

AMAÇ

Madde 1 Bu Yönetmeliğin amacı; elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin usul ve esasları düzenlemektir.

KAPSAM

Madde 2 Bu Yönetmelik; bildirim ve sertifikasyon süreçlerine, güvenli elektronik imza oluşturma ve doğrulama verileri ile araçlarına, elektronik sertifika hizmet sağlayıcısı, Kurum, nitelikli elektronik sertifika sahibi ve üçüncü kişilerin yükümlülüklerine, denetime, faaliyetin sona erme hallerine, zaman damgasına, yabancı elektronik sertifikalara, güvenliğe, teknik ve mali hususlara ilişkin usul ve esasları kapsar.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (04/05/2007 tarihli)

Amaç ve kapsam

MADDE 1

(1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik (01/11/2007 tarihli)

Amaç ve kapsam

Madde 1

(1) Bu Yönetmeliğin amacı; internet toplu kullanım sağlayıcıları ve ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri ve sorumlulukları ile denetimlerine ilişkin esas ve usulleri düzenlemektir.

Dayanak

Madde 2

(1) Bu Yönetmelik, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna dayanılarak hazırlanmıştır.

Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti Dinlenmesi Sinyal Bilgilerinin Değerlendirilmesive Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş görev ve Yetkileri Hakkında Yönetmelik (10/11/2005 tarihli)

Amaç

Madde 1 Bu Yönetmelik;

a) (Değişik bend : 04/07/2007 - 26572 S.R.G Yön\1.mad) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanununun ek 7 nci maddesi, 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun ek 5 inci maddesi, 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun 6 ncı maddesi ile 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 135 ilâ 138 inci maddeleri ile belirlenen çerçevede telekomünikasyon yoluyla yapılan iletişimin tespiti,

dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına ilişkin usul ve esasların belirlenmesi,

b) Telekomünikasyon İletişim Başkanlığı'nın kuruluş, görev ve yetkilerinin düzenlenmesi amacıyla hazırlanmıştır.

Hukukî dayanak

Madde 2 (Değişik madde : 04/07/2007 - 26572 S.R.G Yön\2.mad) Bu Yönetmelik, 4/7/1934 tarihli ve 2559 sayılı Kanunun ek 7 nci maddesi, 10/3/1983 tarihli ve 2803 sayılı Kanunun ek 5 inci maddesi, 1/11/1983 tarihli ve 2937 sayılı Kanunun 6 ncı maddesi ile 4/12/2004 tarihli ve 5271 sayılı Kanunun 135 ilâ 138 inci maddelerine dayanılarak hazırlanmıştır.

5846 sayılı Fikir ve Sanat Eserleri Kanunu

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun "Tanımlar" başlıklı 1/B maddesinin (g), (h), (ı) bentlerinde *"Bilgisayar programı", "Arayüz", "Ara işlerlik"* kavramlarının açıklamaları yapılmış, Fikir ve Sanat Eserlerinin Çeşitleri başlıklı bölümde yer alan 2' nci maddesinde *"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 fiiller de suç sayılmıştır.

EK 4/f.3: Dijital iletim de dahil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi içerik sağlayıcılar tarafından eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış haklarının ihlâli halinde, hak sahiplerinin başvuruları üzerine ihlâle konu eserler içerikten çıkarılır. Bunun için hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlâlin durdurulmasını ister. İhlâlin devamı halinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlâle devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir.

Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik *(Resmi Gazete Tarih / Sayı : 24.10.2007 / 26680)*

Bu yönetmeliğe göre; erişim sağlayıcı veya yer sağlayıcı olarak faaliyette bulunabilmek için Telekomünikasyon Kurumundan faaliyet belgesi almak gerekmektedir. Bu belgeyi almadan hizmet verenlerin faaliyetleri durdurulacaktır. Yönetmelik, erişim sağlayıcılara ve yer sağlayıcılara bazı yükümlülükler getirmektedir. Örneğin erişim sağlayıcılar, hukuka aykırı içerikten 5651 sayılı kanundaki usule göre; Telekomünikasyon Kurumu İletişim Başkanlığınca haberdar edilmeleri halinde söz konusu yayınlara erişimi engelleyeceklerdir.

Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik (06 Şubat 2004 Tarihli)

Bu Yönetmeliğin amacı, telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasları düzenlemektir. Yönetmelik, telekomünkasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri kapsamaktadır.

Madde 3 Tanımlar

Kişisel bilgiler/veriler: Tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgiyi,

Kişisel bilgilerin işlenmesi: Otomatik olsun olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütününü ifade eder.

Madde 8 Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır. İlgili trafik verilerinin ise işletmeci tarafından hizmet amaçları dışında kaydedilmesi, saklanması ve gözetimi yasaktır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik (30/11/2007 tarihli)

Amaç ve kapsam

Madde 1 (1) Bu Yönetmeliğin amacı; içerik sağlayıcıların, yer sağlayıcıların ve erişim sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir.

Birlikte Çalışabilirlik Esasları Rehberi ile İlgili 2005/20 Sayılı Başbakanlık Genelgesi (*Tarih: 04.08.2005)*

e-Dönüşüm Türkiye Projesi kapsamında başta kamu kurumları olmak üzere kamuya elektronik ortamda hizmet sunan tüm kurumlar arasında birlikte çalışılabilirliği sağlamak ve bu çerçevede yetki, sorumluluk, esas, prensip, yöntem ve kriterler ile teknik standartları belirlemek amacıyla hazırlanmıştır. Rehber'in ikinci bölümünde; bilginin sunumu, taşınması, değişimi, entegrasyonu, güvenliği ve geliştirilen çözümlerin yaşam döngülerine ilişkin teknik standartlar belirlenmiştir.

Kamu Kurumları İnternet Sitesi Kılavuzu ile İlgili 2007/4 Sayılı Başbakanlık Genelgesi (*Tarih: 27.01.2007)*

e-Dönüşüm Türkiye Projesi çalışmaları kapsamında 2003/48 sayılı Başbakanlık Genelgesi ile uygulamaya konulan Kısa Dönem Eylem Planı (KDEP) ve Yüksek Planlama Kurulu'nun 2005/5 sayılı Kararıyla hayata geçirilen 2005 Eylem Planı'nda, kamu kurum ve kuruluşlarının internet sitelerinde asgari

düzeyde içerik ve tasarım uyumunun sağlanmasına yönelik olarak "Kamu Kurumları İnternet Sitesi Kılavuzunun Hazırlanması" eylemine yer verilmiştir.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-Marmara Araştırma Merkezi (TÜBİTAK-MAM) sorumluluğunda yürütülen çalışmalar neticesinde "Kamu Kurumları İnternet Sitesi Kılavuzu " hazırlanmıştır.

Elektronik Haberleşme Güvenliği Yönetmeliği (24.07.2008 tarihli)

Elektronik haberleşme güvenliğine ilişkin usul ve esasları düzenlemek amacıyla yönetmelik çıkarılmıştır. Yönetmelik, işletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması için tehditlerden ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesi veya azaltılmasına ilişkin olarak alacakları tedbirlere yönelik usul ve esasları kapsamaktadır. Kişisel bilgilerin işlenmesi ve gizliliğinin korunması, yönetmeliğin kapsamı dışındadır.

Vergi Usul Kanunu

Mükerrer 242.madde:

Maliye Bakanlığı; elektronik defter, belge ve kayıtların oluşturulması, kaydedilmesi, iletilmesi, muhafaza ve ibrazı ile defter ve belgelerin elektronik ortamda tutulması ve düzenlenmesi uygulamasına ilişkin usul ve esasları belirlemeye, elektronik ortamda tutulmasına ve düzenlenmesine izin verilen defter ve belgelerde yer alması gereken bilgileri internet de dahil olmak üzere her türlü elektronik bilgi iletişim araç ve ortamında Maliye Bakanlığına veya belirleyeceği gerçek veya tüzel kişilere aktarma zorunluluğu getirmeye, ***bilgi aktarımında uyulacak format ve standartlar ile uygulamaya ilişkin usul ve esasları tespit etmeye,*** bu Kanun kapsamına giren işlemlerde elektronik imza kullanım usul ve esaslarını düzenlemeye ve denetlemeye yetkilidir.

İnternet Kafeler/Salonları ile İlgili İçişleri Bakanlığı Bakanlık Genelgesi. EGM Genelge No : 37 Bakanlık Genelge No : 2008/30 (14/04/2008 tarihli)

1/11/2007 tarihli ve 26687 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikle, ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri ve

sorumlulukları ile denetimlerine ilişkin esas ve usuller düzenlenerek, uygulamanın ne şekilde yapılması gerektiği belirlenmiştir.

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik uyarınca, ticari amaçlı toplu kullanım sağlayıcılara yapılacak işlemlere ilişkin yazılı ve sözlü tereddütlerle ilgili olarak İçişleri Bakanlığı genelgesi ile gerekli açıklamalar yapılmış ve valiliklere gönderilmiştir.

EK-2 Canadian Police College (CPC)'deki ve Atlantic Police Academy'de Düzenlenen Bazı Bilişim Suçları Alanında Kurslar

Canadian Internet Child Exploitation Course – 10 days

This course is designed to prepare investigators in their investigations andprosecutions of online offences related to the sexual exploitation of children.

This course covers topics such as how to:

. Identify the offence;

. Form an opinion on whether they believe the images viewed are child porn;

. Take a computer apart;

. Write a child exploitation related search warrant;

. Use both online tools and more traditional techniques to gather evidence;

. Execute a search warrant;

. Prepare a press release;

. Prepare a release and conditions;

. Testify in court;

. Update appropriate databases;

. Describe future challenges;

. Interview possible pedophiles;

. Describe the psychological impact this job has on them. (CPC, n.d.)

To be eligible to attend this course, the potential student must be currently working fulltime, investigating child exploitation crimes or be sanctioned to investigate child exploitation crimes and have completed the INTSTB course, or its equivalent.

Computer Forensic Examiner (CMPFOR) – 15 days

This course is for law enforcement officers who may be required to seize and analyze potential digital evidence found on computer hardware. During this course, the specialized forensic foundations and practical skills required to recognize, recover, examine and document findings when dealing with personal computer systems are covered.

This course covers topics such as:

. Computer hardware;
. Hard disk topology;
. Law and evidence;
. Forensic seizure of computer data;
. Modern computer file systems;
. Windows forensic software. (CPC n.d.e)

To be eligible to attend this course, the potential student mustobtain 75% on a preadmission exam.

Cybercrimes Investigative Techniques (CYBER) – 10 days

This course is designed to give students adequate skills to identify potential avenues of investigation when dealing with cyber crimes.

This course covers topics such as:

. Internet security issues and fraud concerns;
. Internet security problems and safeguards;
. World Wide Web and search engine technology;
. PGP (Pretty Good Privacy) encryption;
. Considerations in developing an effective research plan;
. Introduction of TCP/IP;
. Electronic Mail;
. Usenet (how to break down Usenet postings);
. IRC (Netmeeting, ICQ, Hotline);
. Telnet;
. Undercover investigations (CPC n.d.f).

To be eligible to attend this course, the student must be an experienced investigator with a requirement to do online investigations. Course applicants must also have successfully completed the CMPFOR course or demonstrate his/her proficiency using DOS commands. These requirements limit the potential intake of students because potential students whom do not have the DOS skills might still be interested in doing online investigations. The course prerequisites do not mirror the contents of the course. The CMPFOR course focuses on computer forensics whereas this one focuses on the Internet. One can investigate online crime without doing the forensics of the computers used in the commission of the crimes. It’s like saying that a homicide detective needs to be able to perform an autopsy in order to learn how to investigate a homicide.

Internet Searching Techniques Basic

(INTSTB) 1620
hours self directed
learning

This course serves as an introduction to the Web as a police intelligence tool. It takes students through many of the advanced features of both the better and lesser known search tools as well as resources of specific interest to the law enforcement community.

This course covers topics such as:

. Most popular search engines;
. Meta search sites, mega search site and advanced search queries;
. Newsgroups and web forums research;
. Web sites authoring. (CPC n.d.b)

There are no prerequisites to attend this course.

Internet Searching Techniques Intermediate

(INTSTI) 2535
hours, selfdirected
learning

Following through on the skills gained during the basic Internet Searching Techniques course (INTSTB), this course introduces students to the principals of Open Sources Research and the Intelligence Analysis process.

This course covers topics such as:

. The use of the Internet as an investigative tool;
. Search engine mechanics;
. Advanced browser functionality;
. Specialized databases and search tools. (CPC n.d.c)

To be eligible to attend this course, the student must be familiar with basic search engine use as outlined in the basic course (INTSTB). It is highly recommended that students complete the basic course before taking this course.

Internet Searching Techniques Advanced

(INTSTA) 3040
hours, selfdirected
learning

This course illustrates how an investigator may be exposed online and the techniques and tools that can be employed to effectively overcome this problem.

This course covers topics such as:

. Introduction to Internet Architecture and Network Analysis Tools;
. Introduction to online privacy and anonymity;
. Advanced anonymity tools;
. Maintaining online security. (CPC n.d.a)

To be eligible to attend this course, the student must have completed the INTSTI course and be able to install software applications such as VisualRoute, MultiProxy and ZoneAlarm.

Network Principles and Investigative Techniques (NPITC) – 10 days

This course provides investigators with the technical level of knowledge and skills necessary to complete common searches, seizures and investigations involving a network. To be eligible to attend this course, the student must be established as a hightech crime investigator, and have successfully completed the CMPFOR course, or have the equivalent knowledge.

Network Intrusion and Incident Investigation (NETINT) – 10 days

This course is designed to arm high tech crime investigators with the basic knowledge and skills necessary to evaluate a network intrusion complaint, determine the need to investigate the incident, and complete a successful investigation of the incident when warranted.

This course covers topics such as:

. InterNetworking concepts;
. The fundamentals of TCP/IP;
. Network security;
. How networkbased exploits operate;
. How a Network Incident is handled and investigated;
. Introduction to intrusion detection;

. Network traffic and logbased analysis. (CPC n.d.g)

To be eligible to attend this course, the student must be a Technological Crime Investigator assigned to investigate network intrusion cases, have successfully completed the CMPFOR, the NPITC and the Linux course. It is also highly recommended that students complete the INTSTB course before taking this course.

Using the Internet as an Intelligence tool (INTINT) – 5 days

This course was developed to assist investigative personnel in becoming more proficient in Internet based online research activities and as an introduction to Internet and computer related investigations.

This course covers topics such as:

. Using the Internet as an Effective Police Research Tool;
. Search Engine Fundamentals handson and indexing patterns;
. Introduction to USENET newsgroups, Web Forums and Blogs;
. Newsgroup search fundamentals (handson);
. Searching Exercise (handson);
. Web Browser advance features overview (book marking, monitoring and finding);
. Overview Open Source Intelligence and the Intelligence Analysis Process;
. Introduction to Web site mapping tools (handson);
. Introduction to Internet architecture;
. Introduction to Trace Route and associated tools;
. Desktop firewalls (handson);
. Introduction to Internet Relay Chat;
. Web site design basics;
. Introduction to Advanced Research Tools.

Students that have completed the online Internet searching basic, intermediate and advanced Course should not attend this course. (CPC n.d.d) This course is targeted at those with limited Internet experience and is open to various people, from administrative to enforcement.

Linux Forensic Techniques (LINUX) – 10 Days – online technological Course

This course is designed specifically for experienced technological crime

investigators who possess a basic knowledge of the Linux operating system and who may be required to seize and/or analyse computer hardware running Linux. This course takes an indepth look at some aspects of the Linux operating system and the Second Extended File System. The course addresses the forensic analysis of a Linux based system as well using Linux based system as an investigative / analysis tool.

This course covers topics such as:

. Linux basics review;
. Second Extended File System structure;
. Proper seizing procedure;
. Imaging;
. Searching;
. Data recovery;
. Linux tools and utilities;
. Linux forensics using Windows tools. (CPC n.d.h)

To be eligible to attend this course, the student must have passed the CMPFOR, completed an online general Linux course and have successfully passed the preadmission exam. In addition, the student must be an investigator with a mandate to perform forensic analysis of personalcomputers. The CPC also offers a Macintosh course titled “Macintosh Electronic Search and Seizure”. The CPC is also planning to introduce courses in ‘Advanced Cyber Crimes’.

ATLANTIC POLICE ACADEMY CYBER CRIME COURSE

Internet crime course 5
Days

This course is designed for Police Officers involved in investigative duties, which may be called upon to investigate Internet related offences. He/she is expected to have a working knowledge of Internet search engines and email prior to the start of the course.

This course covers topics such as:

. Introduction to PC Hardware;
. Networks;
. Internet (Introduction, history, configuration, bandwidth, IP addresses, PING, TRACEROUTE, SCANNING, Ports);
. Security (Passwords, encryption, virii, trojans, and firewalls);

. Hacking;
. ISP'S;
. Warrants and Charges;
. Tech Crime Units;
. Advanced Internet (Spam, Spoof, IRC, Chat, ICQ, FTP, WWW);
. Email;
. Child Pornography (Maltais, 2005).

EK-3 Bilişim Suçları ile İlgili Görev Alınan İlginç Olaylar

1. 2005 yılında ……. İl Emn. Md.lüğü, KOM Şb. Müdürlüğü'nce gerçekleştirilen operasyonda fishing yöntemi kullanılmak suretiyle Garanti Bankası, Yapı Kredi Bankası ve Akbank'a ait İnternet Bankacılığı web sitelerinin kopyası yapılarak müşterilerinin bilgileri çalmak suretiyle hesaplarının boşaltılması.
2. Çocuk pornosu olayına karışan avukatın olayı.
3. Kredi Kartı Kopyalama suretiyle haksız kazanç elde etmek ve sahtecilik suçu kapsamında şüpheli olarak ifadesine başvurulan şahıs polise verdiği ifadede; kopyaladığı kart bilgilerini Rus vatandaşı olarak bildiği bir şahsın kendisine vermiş olduğu bir internet sitesi vasıtasıyla elde ettiğini belirtmiştir. Şahsın vermiş olduğu bilgi doğrultusunda konuyla ilgili siteye girdiğimizde sitede yüzlerce kart bilgisi gördük. Ancak 16 rakamdan oluşan kart bilgisinin ekranda ya ilk 4 rakamı veya son 4 rakamı vardı. Diğerleri X şeklinde gizli idi. Şahıs ifadesinde beğendiği numarayı seçtiğini karşısında tutan miktarı Western Union aracılığı ile şahsa gönderdiğini belirtti. Track bilgilerini de bu şekilde aldığını ifadesinde belirterek, para karşılığında aldığı bilgilerin bazılarının boş çıktığını, bazılarının dolu çıktığını ifade etti. Bilgilerin %90 ının yabancı bankalara (özellikle Amerika) ait olduğunun söyledi.
4. Çok ünlü ve büyük bir alışveriş merkezinde kredi kartlarının kopyalandığı bir olayla karşılaşmıştım. İşin tuhaf yanı bunu yapan kişinin bu eylemi sadece 3 saat içerisinde gerçekleştirmesi idi.
5. Şüphelinin MSN yolu ile şahıslarla bağlantı kurarak, şahısları herhangi bir siteye yönelterek kişileri yöneltmiş olduğu siteden şahısların MSN şifrelerini çalarak, kişilerin diğer MSN arkadaşlarından telefon kontörü talep etmesi.
6. Bilişim suçları kapsamında gelen MSN şifre kırılma, tehdit edilme, menfaat talebi gibi konulara genellikle bayanların maruz kalması.
7. Bilişim suçları konusunda adli mercilerin emniyet birimleri kadar uzmanlaşmadıklarını müşahade ettim. Düzenlenen tahkikatlerin içeriğini adli mercilere teknik yönden anlatmada sıkıntı çekilmektedir. Adli mercilerin (C.savcıları , Hakimler) bilişim konusunda yetersiz olduğunu düşünüyorum.

8. Yapılan bir tahkikatta, müştekinin banka hesabına giren şahsın yabancı bir şahıs olması ve Türkiye'de suçu işletmiş olduğu kişilerin tamamını yüksekokul ve üniversite mezunu olan insanlardan seçmesi.
9. Rüşvet konusunda yapılan bilgisayar incelemesinde HTML sayfalarından hesap hareketlerine erişilmiştir.
10. Başkasının banka hesabına giren şahsın yabancı bir vatandaş olması ilginçti, ayrıca bu kişinin Türkiye'de Atom Mühendisliği'nde okuyan bir öğrencinin ve Makine Mühendisliği'ni bitirmiş bir şahsa belli bir yüzde (%) vermek suretiyle suça karıştırması olayı ilginçti.
11. Yaklaşık 3 ay kadar önce ilimizde meydana gelen bir olayda aynı büroda çalışmakta olan kişilerin birbirlerinin e-mail şifrelerini kırmak suretiyle bilişim suçu işlemeleri idi. İşlemler aynı ofis içerisinde yapıldığı için faili bulmak mümkün olmadı.
12. İnternet üzerinden kişilerin hesaplarını kullanarak, belirli yerlerde kendilerinin tanımadığı ancak aracı kullanarak işsiz kişilere sahte kimlik düzenleterek açılan banka hesaplarını havale yapmak suretiyle işlenen suç türü.
13. Esnaf bir kızın resmi ile İnternet'te bir arkadaşlık sitesine üye olunuyor. Bayanın resmi de olduğu için, kızın ağzıyla Balıkesir'deki görüştüğü kişilere kızın adına bazı vaatlerde bulunuluyor. Bu kişiler kızı rahatsız etmeye başlıyor. Bayan da, bahsi geçen siteye başka bir isimle üye olup kendi resmini kullanan kişiyle irtibata geçiyor. Tabi, polise şikayet edeceğim deyince şahıs ürküp kaçıyor ve yakalanamıyor. Bayan, sonra polise müracaat ediyor ama gerekli bilgiler alınamadığı için sonuca gidilemiyor.
14. 2002 yılında, ilkokul mezunu bir şahsın (ilimizde ikamet eder) yurt dışında yerleşik (Amerika-Kanada) şahısların kredi kartı hesaplarına yetkisiz giriş yaparak ilimizde açtığı bir hesaba 400 milyar para transferi yapması. Şahsın bilgisayar kullanımını internet kafelerde öğrenmesi bana çok ilginç geldi.
15. Bir bilgisayar incelemesinde, kasanın içinde 2 tane harddisk olduğu ve bir tanesinin takılı olduğu diğerinde suç unsurlarının bulunduğu ve bu dosyaları açacağı zaman hard disk'i bağladığını fark ettik.
16. Bilgisayar yoluyla yapılan bir sahtecilik olayında bilgisayar içinde aradığımız delillerin, bilgisayarların CD-Rom'unda takılı olan CD'de bulunması.

17. Bilgisayar Teknik Servisi, talep halinde porna CD'ler kopyalamaktadır. Ancak, bu işlemi yaparken CD'leri önceden hazırlayıp iş yerinde bulundurmamaktadır. İmaj olarak bilgisayarındaki dosyayı, müşteri ile ilgili sorgulama, araştırma yapıp emin olduktan sonra CD halinde şahzsa vermektedir.
18. İncelediğimiz bilgisayarda, grafik programı kullanarak pek çok resmi evrakın sahtesinin oluşturulmuş olması.
19. İlimizdeki ……. Üniversitesi'nde stajyer bir öğrencinin eğlence amaçlı olarak FBI'ın ABD'deki merkez binasına bomba koyduğunu bildiren bir e-mail atması ve FBI'ın bu mail'i dikkate alarak 1 hafta binayı baştan aşağı araması ve mail'in asılsız olduğu anlaşıldıktan sonra ABD makamlarının gelen mail'in nereden ve kim tarafından atıldığının tespiti yapıldıktan sonra, bize gelen resmi yazıyla adrese giderek mail'i atan öğrencinin bulunup ifadesini aldıktan sonra serbest bırakılması.
20. …….İl Emniyet Müdürlüğü kadrosunda çalışırken, uydu yayınlarının şifrelerini kıran bir cd 'nin satışa sunulduğunu ve internet üzerinden satışı yapılan bu cd ile pek çok kişinin mağdur edildiğini duyumunu almıştık. Bunun üzerine müracaatlarda gelince, olay tahkikata döndü ve bir erkek şahsın sırf bu iş için internet sitesi kurduğu, yurt dışından dahi mağdurlarının olduğu, içinde demo programlar olan bir cd'yi 2002-2003'de yüklü miktarlar karşılığı pazarladığı ve ismini sitede verdiği sahte şirketin hesap numaralarınında banka evrak sahteciliği usulü ile 80 yaşındaki sağır ve zor gören halasının adına açıldığı, şahsın ise çevre edinmek maksadı ile bir kitapcı dükkanını bir süre çalıştırıp vatandaşlarla diyalog sağladığı, böylece faaliyet alanını genişlettiği gibi ilginç bir konu ile bir sene uğraştık, ama sonunda şahıs yakalandı.
21. Dizüstü bilgisayarlara ait seri numaralarının takibini şirketler sosyal ortamda yapmıyorlar. Yani hangi seri nolu bilgisayarı, hangi müşterisine sattığını tespit edemiyor şirketler. Bu kayıtları sadece fatura üzerinde tutuyorlar. Bu yüzdende çalıntı cihazların gerçek sahiplerine ulaşmak güç oluyor. Bu konu ile ilgili yasal bir düzenlemenin yapılması uygun olur. Yani şirketler, muhakkak seri nolu takibi yapmalıdırlar.

22. 2004 yılında üniversitede görevli bayan profesöre tehdit ve porno mesajları gelmiş idi (rektörlük seçimleri ile ilgili). Ancak, maillerin gönderildiği bilgisayarı, Telekom ile yapılan işbirliğine rağmen tespit edememiştik.
23. Çocuk pornosunda tespitlerin genellikle, Almanya ve İtalya gibi yabancı ülkeler tarafından yapılması, ülkemizde bu tür konularda önleyici teknik çalışmaların bulunmaması.
24. Bir şahsa yapılan hakaret olayında gönderilen e-mail'in herhangi bir telefon sistemine bağlı olmayan direeway anten sisteminden gönderilmesi, mahkemenin adres tespitini Telekom kurumundan alamaması.
25. Genelde cd marketlerde ve internet cafelerde yaptığımız incelemelerde Doutad programların kullanıldığı, çocuk porno filmlerinin indirildiği, cd lerin çoğaltıldığını ve satıldığını gördüm.
26. İnternet banka dolandırıcılığı yapan şahısların genelde akrabalarının, arkadaşlarının hesaplarına transfer yaparak veya yaptırarak suç işlemesi.
27. Üzerinde 12 adet sahte kredi kartı bulunan şahsın, kredi kartlarıyla alışveriş yapması (tamamında kendi kimlik bilgilerin bulunması) ve hiç bir şeyden şüphelenilmeden alışverişine devam etmesi.
28. 2000 yıllarında üniversite öğrencisi bir kişinin FBI'a bomba atacağına dair mail göndermesi üzerine şahsın tespiti ve adli işlemlerin yapılması.
29. Belediye otobüsleri biletlerinin bilgisayar ortamında basılması, üniversitenin raporlarının bilgisayar ortamında çoğaltılıp haksız kazanç elde edilmesi.
30. Şüphelinin çalmış olduğu kredi kartı numaraları ile kendi kurduğu alışveriş sitesinden alışveriş yaparak, kredi kartlarındaki hesabı boşaltması.
31. İnteraktif banka dolandırıcılığı suçlarında mağdurların çok komik bahanelerle hesap bilgilerinin ele geçirilmesi, bilgisizlik seviyesini tespit etmek açısından bana çok ilginç gelmektedir.
32. …… ili konumu itibari ile pek bilişim suçlarıyla karşı karşıya kalmıyor. Ancak, bir mağdur bayanın msn kayıtlarını çalarak bilgi ve resimleri ile ilgili biz şüpheliyi ilimizde ararken şüpheli …….. ilinde çıkmıştı.
33. İlk yaptığım bilgisayar incelemesinde şüphelinin, çocuk pornografisi içeriğini değiştirmeyerek dosyanın bilgisayara indirilmesi, ancak daha sonra dosya uzantısının şifrelenerek gönderildiği, şahısların birbirlerine vermek süretiyle dağıtım yaptıklarının tespiti benim için yeni geldi. Bilgisayar incelemesinde,

normal bir bilgisayar kullanmasının, görünür incelemesinde ise standart uzantı dosyasının kontrol edileceği düşünüldüğünde bu olay benim için deneyim kazandırıcı oldu.

34. Haber merkezine bir ihbar gelir şu an bir online dolandırıcı var, şu an online adresi şu bağlanın ve tespit edin diye heyecanla ihbar gelir. Maalesef, ihbarı değerlendirebilecek eğitimli personel yoktur.
35. A ilinde ikamet eden bir şahsın banka hesabından, bilgisi dışında B ilinde ikamet eden başka bir şahsın hesabına para havalesi yapılır. B ilindeki bankadan parayı çeken şahıs yakalanır ve ifadesinde; İnternet'te tanıştığı Rus uyruklu bir şahsın bu parayı kendi hesabına gönderdiğini, bu paradan yüzde 10 komisyon aldıktan sonra kalan parayı western-union yöntimiyle Rusya'ya göndermesini istemesi üzerine hesabına gelen parayı çekerek yüzde 10 payını aldıktan sonra kalan parayı western-union yöntemiyle Rusya'ya gönderdiğini beyan eder. Bu olaydan sonra meydana gelen aynı mahiyetteki olaylar incelendiğinde genelde bu işlemin Rus kaynaklı olduğu anlaşılır ve suçun uluslurarası boyutta işlendiği tespit edilir. Sonuçta Rusya ile ilişkiler çerçevesinde hackerlerin tespitine çalışılır.
36. 2004 veya 2005 yılında KOM Şube'de görev yaparken, ….. ilinde Ziraat Fakültesi'nde bir öğretim elemanına yurt dışından gelen bir e-mail'de; yüklü miktarda para kazandığı bunun için bir miktar para yatırması gerektiği belirtilmiştir. Öğretim elemanı, olayın uluslararası dolandırıcılık olduğunu fark etmeyerek tam hatırlamıyorum 5-10 bin ABD doları yatırması sonucu dolandırılması olayı gerçekleşmişti.
37. Asayiş Şube Müdürlüğü görevlileri ile beraber gerçekleştirilen bir çocuk pornosu olayına inceleme yapmak üzere atandım. İncelemesini yaptığım bilgisayarda 32000 adet çocuk porno resmi 550 adet çocuk porno video görüntüsü elde etmiştim. Devam eden araştırmamda diğer resimlere bakarak şahsın, ilimizde küçük yaştaki erkek çocuklardan oluşan bir futbol kulübü çalıştırdığını fark ettim. Elde edilen çocuk porno resimlerinin tamamı erkek çocuklardan oluşmaktaydı. Çalıştırdığı çocukların büyük bir risk altında olduklarını fark ettim. Çünkü, resimlerin içeriklerine bakıldığında normal bir insanında bakabileceği resimler olmadığı görülmekteydi. Bu tespitler, ivedilikle adli mercilere rapor olarak iletildi.

EK-4 Bilişim Suçlarıyla Mücadelede Personelin Eğitim Konusunda Belirttiği Konular

1. Meslek öncesi eğitim kaçınılmazdır.
2. Meslek içindede değişen koşullar takip edilmeli, güncel eğitimler artırılmalıdır.
3. Bütün emniyet müdürlüklerinde, bilişim suçları konularında uzman eğitimli kişilerin olması gerekmektedir.
4. Teknoloji sürekli geliştiği için bir kere eğitim vermekle o kişi o dalda yeterli bilgiye sahip olmamaktadır. Sürekli, yeni gelişmelerle ilgili bilgilendirmeler yapılmalıdır. POL-NET gibi bir on-line ortamda, bir görüşme odası içerisinde tüm bilişim suçları personeli sürekli bilgi alış-verişinde bulunabilir. Eğitimlerde, bu sanal odalarda yapılabilir.
5. İlgili personelin yılda 2 kez seminer vb. düzenlenerek güncel konularda eğitimle kendisini geliştirmesi sağlanmalıdır.
6. Hizmet içi eğitim olarak Emniyet Genel Müdürlüğü, taşra teşkilatına daha fazla önem vermeli ve kapsamlı kurslar düzenlenmelidir.
7. Bilişim suçlarında görev alacak personelin sadece bu konular üzerinde görevlendirilmesi, personele bilişim suçları konularında güncelliği sürekli takip etmesi için kurslar verilmesi sağlanmalıdır.
8. Teknolojik eğitimin sürekliliği ve eğitim planlarının teknolojik gelişmelerle paralel tutularak yenilenmesi sağlanmalıdır.
9. Meslek öncesi eğitimin yanı sıra personelin verilecek olan kurslarla uzmanlaştırılması, her türlü donanımlarla donatılarak, hizmet içinde gerekli eğitimlerin verilerek branşlaşmalara gidilmesi gerekmektedir.
10. Bilişim suçlarıyla mücadelede görev alacak personel hizmet öncesi (Polis Meslek Yüksek Okulu, Polis Mesleki Eğitim Merkezi, Polis Koleji, Polis Akademisi) eğitim almalı, bu konu üzerinde uzmanlaşmalı ve devamlı olarak bu birimde çalışmalıdır. Sonradan verilecek kısa süreli (1-30 gün) aralıklı eğitimlerin fayda vermeyeceği kanaatindeyim.
11. Bilişim suçlarında çalışan personel, kesinlikle bu suçu işleyenlerden daha uzman olmalıdır. Bu personel; hem meslek öncesi ilgili eğitim alanlarından (elektrik, elektronik, bilgisayar vb. bölümleri) seçilmeli hem de meslek içinde

sürekli olarak eğitilmelidir. Ayrıca uzmanlık eğitimi de verilerek, yapacakları tüm işlerin mahkemelerde delil olarak problemsiz olarak sunulması sağlanmalıdır.

12. Özellikle taşra teşkilatı dikkate alınarak, daha çok sayıda personelin yurt dışında veya ülkemizde belli üniversiteler tarafından bilişim suçlarında yetiştirilmesi sağlanmalıdır.
13. Meslek öncesi eğitim (Polis Meslek Yüksek Okulu, Polis Mesleki Eğitim Merkezi, Polis Koleji, Polis Akademisi) elbette işe yarayacaktır. Ancak, bu personel aldıkları eğitim sonrası ya kendilerini artık uzmanlaştım diye geliştirmiyor, bilgilerini güncelleştirmiyor yada idari tasarruf sonucunda çok farklı bir görevde kullanılıyor. Mutlaka, meslek içerisinde güncelleştirme eğitimleri yapılmalıdır. Bilişim suçlarıyla mücadele edecek ve sadece bu konularla ilgilenecek eğitim görmüş ve sürekli bilgilerini gelişen teknolojiye uygun olarak yenileyen bir birim kurulmalıdır. Bilişim suçları konusunda, idari organizasyonda bir şubenin alt kuruluşu olarak değil, ayrı bir şube olarak kuruluşunun sağlanmasıyla hizmet verilmelidir.
14. Hiçbir eğitim görmedik. Eğitimlerin, çok faydası olacağına inanıyorum.
15. Bu birimlerde görev alacak personel bence Polis Meslek Yüksek Okulu, Polis Mesleki Eğitim Merkez'lerinden seçilerek, gerçekten istekli, becerikli, deneyimli ve de eğitilebilecek personel arasından değerlendirilmelidir.
16. Hackerler kadar İnternet'in ve bilgisayarın öğrenilebileceği bir kurs gerekmektedir. En az 1 ay süreli.
17. Devamlı gelişen teknolojiye ayak uydurabilmek için hizmet içi eğitime önem verilmelidir. Hizmet içi eğitim planlamalarında, tüm personele yönelik bilişim suçları eğitimine yer verilmelidir.
18. Bilişim suçlarında görevli personelin gelişen teknolojiye ayak uydurması için ve bilgilerin güncel olarak devam ettirebilmesi için üç ay süreli sürekli kurs gibi uzmanlık eğitimine tabi tutulması gerekmektedir. Bu personel bu görevinden başka herhangi bir ek görev veya hizmette kullanılmamalıdır.
19. Polis teşkilatında bilgisayar ve İnternet konusunda bilgisi olan personel azımsanmayacak kadar çok. Doğru bir personel istihdam sistemiyle bu tür suçla mücadelede başarının artacağı kanaatindeyim.
20. Teşkilatımız ve yargıda çok büyük eğitim eksikliği vardır. Bu tür olayların

altından teşkilat olarak kalkabilsek bile yargılama aşamasında emekler boşa gidebilmektedir. Yargılama sürecinde hakim ve savcıların da, bu konularda eksikleri olduğu için, dolayısıyla verilecek cezaların asgari düzeyde kaldığı görülmektedir. Teşkilatımızda üst düzey yöneticilere, özellikle bu konuların önemi, bilişim suçlarının ülkeye mali külfeti, hakkında bilgilendirme toplantısı yapılması gerekmektedir. Kanımca, bilişim suçlarına yeterli değer verilmemektedir.

21. Eğitimlerimizi bizzat kendi paramla aldım. Bu suçlarla mücadele etmede gerekli lisanslı bilgisayar yazılım ve donanım programlarına sahip değiliz. Zaten, bu tür lisanslı yazılımlar çok pahalı. Taşraya, gerekli desteğin sağlanması gerekmektedir.
22. Bilişim suçlarında, on-line eğitimin etkin bir şekilde uygulanmasının ve uygulamalı eğitimlere ağırlık verilmesinin personelin bu konularda uzmanlaşmasını hızlandıracağını düşünüyorum. Bu konularla ilgili Pol-Net ve KOM portalında bir forum sayfası açılabilir. Sıkça sorulan sorular, bilişim suçlarında sorunlar, yeni yöntemler ve mücadele teknikleri bu şekide hızlı bir şekilde paylaşılabilir ve de geliştirilebilir. KOM Daire Başkanlığı'nın bilişim suçları ile mücadele için tüm il KOM şubelerinde bilişim suçları bürosunu kurması gerekmektedir. Asayiş Şube Müdürlükleri'nde de, bilişim suçları büroları kurulmalı ve bu birimler kısa, orta, uzun vade de hedeflerini en kısa sürede belirleyerek uygulamaya başlamalıdır. Olay yeri İnceleme Şube Müdürlükleri de, fiziksel medyalar (hard disk, disket vb.) üzerinde dijital delil elde etme konusunda personel ve donanım konusunda güçlü hale getirilmelidir.
23. Bu suçla mücadele edecek personelin meslek öncesi olmasa dahi meslekte iken uzmanlık eğitimi alması gerekir. Şu an bu konuda, emniyet teşkilatında yeteri kadar uzman personel bulunmamaktadır.
24. Özellikle bilişim suçlarıyla mücadele etmek için mesleğin başında yani Polis Meslek Yüksek Okulu, Polis Mesleki Eğitim Merkez'lerinde uygun öğrenci seçilip, iyi eğitimle yetiştirilmesi gerekmektedir. Programların (seçmeli ders) şeklinde yeniden düzenlenmesi gerekmektedir.
25. Polis teşkilatındaki tüm adli personele, bilişim eğitimi verilmelidir.
26. Kurum içerisinde yeterli donanım ve teknik ekipman ayrıca gerekli olan

yazılımlar bulunmamaktadır. Gerekli donanım ve teknik desteğin sağlanamadığı bir yerde sağlıklı sonuçların elde edilemeyeceği düşüncesindeyim.

27. Bu konu üzerinde çalışacak personel, kullanılan araç gereçlere hakim olmalı eğitimi "TAM" olmalıdır.
28. Personel, İnternet kullanımında stndart kullanıcının üstünde olmalıdır. Bu konuda temel , uzmanlık ve hatta yurt dışı eğitimi almalıdır. Eğitimlerin uygulamalı olması büyük önem taşımaktadır.
29. Bilişim suçlarında eğitim almak isteyen istekli çok personel olduğunu düşünüyorum.
30. Görevli personeller eğitilmeli çağın suçu olarak daha ileriki zamanlarda daha da sorunlu bir suç olarak karşımıza çıkacak olan bilişim suçları konusunda mücadele edecek tüm personel en kısa zamanda eğitime tabi tutulmalıdır. Bilişim Suçları branşı kurulmalı, bilişim suçları üzerinde çok iyi durulmalı, genç, dinamik yabancı dil bilen, kavrama yeteneği iyi olan personeller seçilmeli, her personel yeterli düzeyde eğitime tabi tutulduktan sonra çalışma ortamları rahatlatılmalı ve İnternet üzerinden sürekli olarak suç önleme ve tespiti amacıyla denetleme sağlanmalıdır. Bilişim suçlarında görevli personel, bir bankacı kadar banka işlemlerinden anlamalı, karşılaştığı suçlarla ilgili sağlıklı yorum ya da çözüm geliştirebilmelidir.
31. Adli bilişim ile ilgili eğitim verilmeli, üniversiteler ile işbirliği yapılmalı, ortak çalışmalar yapılmalıdır. Personele akademik eğitim verilmeli, yurtdışındaki eğitim işbirliği araştırılmalı, AB projelerine bilişim suçları konularında teşkilat olarak ağırlık verilmelidir.
32. Bu konuda yetişen personelin özel olması, yetişen personelin KOM birimlerinde çalışmasının sürekliliğinin sağlanması, güncel olayları takip eden iyi eğitim almış, mücadeleci bir görev anlayışına sahip personelden seçim yapılmasının uygun olacağı düşünülmektedir.
33. Kurum dışındaki kurslardan, ilgili personelin yararlanması sağlanmalıdır.
34. Emniyet personelinin tamamına bu konular ile alakalı seminer verilerek, personel bilinçlendirilmelidir. (chat türü sohbet programları, program downloadları, banka hesabı kullanma vb.)
35. Çağımızın gereği olan İnternet kullanımı üzerinde yapılan dolandırıcılık çok

aşırı derecede yaygınlaşmıştır. Ancak, ne yazık ki ülkemizde bu konu ile ilgili çalışmalar minimum seviyesindedir. Bilişim suçları, alt birimden çıkartılarak şube müdürlüğü şeklinde faaliyet göstermesini temenni etmekteyim.

36. Computer Forensic konusunda bir personelin çalışması ve profesyonel olarak bu işin yapılması için; network (CCNA ,CCNP, Norte, Aktif Cihazlar), Microsoft Platformu, Linux Platformu, Database, Mail, Security vb. konularda eğitim organizasyonları düzenlenmelidir.
37. Bilgisayarla tanışma ilk öğretimde olmalı, ilk önce (bilgisayar ve kullanım) Türkiyede herkesçe bilinmeli, uzmanlık ile ilgili olarak öğrenciler kurulacak bilgisayar liselerine yönlendirilmeli oradan sonra kurulacak ileri teknoloji akademilerinde öğrenim görmek üzere yönlendirilmeli. Buradan mezun olanlar, ihtiyaca göre kamu kurumlarında ve devletin bizzat veya teşviki ile kurulacak silikon vadisi, araştırma geliştirme şirketlerinde görevlendirilmeli.
38. Her yaştan vatandaşa, suçların önlenmesi için Halk Eğitim Merkezleri'nde "Bilişim Suçları Farkındalık Eğitimi" verilmeli, değişik eğitim programları içeriğine "Bilişim Suçları'nda Farkındalık" konusu ilave edilmelidir.
39. Bilişim Suçları'nda başarı için yabancı dil eğitimi, yurtiçi eğitim, uzmanlık eğitimi tek ana merkezden olmalıdır. Karmaşıklık ve koordinasyon eksikliğinin önüne geçilmelidir.
40. Ben 10 yıllık Bilgi İşlem personeli olarak, bilişim suçları ile ilgili bir eğitim almadım. Benimle birlikte şube de çalışan hiç kimse bu eğitimi almadı. Ama, bize KOM ve Asayiş Şube Müdürlüğü'nden sürekli olarak incelememiz için bilgisayar ve unsurları konu olarak resmi yazıyla geliyor. Bu konuda çalışma olursa çok iyi olur.
41. Öncelikle Emniyet Genel Müdürlüğü bünyesinde bilişim suçları adı altında bir birim veya daire başkanlığı oluşturularak, bütün taşra teşkilatında bilişim suçları büro amirliği veya bilişim suçları şube müdürlüğü kurularak yeknesaklık sağlanmalıdır. İl Emniyet Müdürlükleri'nde Bilgi İşlem, KOM, Asayiş Şube Müdürlüğü'nün bu konulara ayrı ayrı bakmasından doğan çok başlılık ortadan kaldırılmalıdır.
42. Temel bilgisayar eğitimi alınmalıdır (meslek öncesi). Sistem iletişim, güvenlik, yazılım konularında hizmet içi eğitim düzenlenmelidir. Adli bilişim

ve etik hackerlik konularında yurtdışı eğitim ve uzmanlık eğitimi düzenlenmelidir. Online eğitim ortamında, genel geliştirme eğitimi düzenlenmelidir.

43. Eğitim konusunda meslek öncesi verilen eğitim için, polis okullarında konusuna hakim olan personelin bu eğitimi vermesinin yararlı olacağını düşünüyorum.
44. Bilişim suçlarıyla mücadele edecek personelin meslek öncesi eğitim almış , uzmanlık eğitimi almış kişilerden oluşması gerekir.
45. Mesleki eğitimlerde, üniversitelerden daha fazla yardım alınmalıdır.
45. Çağımız teknoloji olduğu için, koordineli olarak kurslar ve seminerler düzenlenerek personelin yeterliliği sağlanmalıdır. Eğitim konusunda meslek öncesi eğitim, hizmet içi eğitim ve on-line eğitim kesinlikle yeterli olmaz. Uygun personele “Uzmanlık Eğitimi” verilmelidir.
46. Teşkilatın bu konuda çağı yakalaması gerekmektedir. Bunun için hizmet içi eğitimler sıklaştırılarak konusunda bilgili personeller bu birimlerde istihdam edilmeli.
47. Eğitim konusunda özellikle taşra teşkilatımız, bilişim suçlarıyla mücadele noktasında yetersiz bulunmaktadır. Ayrıca, bilişim suçlarında hangi şubenin görevli olduğu konusunda belirsizlik bulunmaktadır. Bilgi İşlem Şube Müdürlüğü bünyesinde “Bilişim Suçları” ile ilgili herhangi bir birim bulunmamaktadır. Bu konuda çoğu İl Emniyet Müdürlüğü’nde bilişim suçları ile ilgili mücadeleye sahip bilgi birikimi olan ve bilirkişilik yapabilecek personele sahip birim, Bilgi İşlem Şb. Md. lüğüdür. Ancak gerekli teknik destek ve ünite yetersizliği nedeniyle delillendirme aşamasında zorluklar yaşanmaktadır. Bilgi İşlem Şube Müdürlüğü bünyesinde, Bilişim Suçları ile Mücadele büro amirliği oluşturulmalıdır.
48. Personele verilen eğitimlerde sadece yasal yollar değil yasa dışı yöntemlerde öğretilmelidir.
49. Personel her konuda uzmanlaşmalı, bizler Polis Akademisi mezunuyuz ve bu konularda temelimiz bulunmamaktadır. Eğitim programları yeniden düzenlenmelidir. Ayrıca, bilişim suçları konularında mühendis vs. kadroları bulunmalıdır. Bilişim suçları konularına üst düzey ve orta kademe yöneticiler maalesef gerektiği kadar önem vermemektedir.

50. Bilişim suçu ile mücadele edecek personel ve adli makamlar (cumhuriyet savcıları ve hakimler) birlikte zaman zaman eğitimlere tabi tutulmalıdır.
51. Verilen meslek içi eğitimleri yetersiz buluyorum.
52. Rutin zamanlarda bilişim suçları ile ilgili kurs verilmesi gerekmektedir.
53. Bu güne kadar bilişim suçları ile ilgili hiçbir eğitim almadım. Bu konuda eğitim ve araç ve gereç yönünden eksiklerimizin giderilmesine ihtiyaç duyuyorum.
54. Kesinlikle ciddi eğitimler alınmalıdır. Yurt içi, yurt dışı fark etmez. Yeter ki yararlı, verimli kurs olsun.
55. Bilişim suçları ile ilgili olarak, öncelikle bilgi işlem şubesinde çalışan bilgi işlem branşlı personele kurs verilmesini önermekteyim.
56. Bilişim suçları ile ilgili olarak daha çok çalışma yapılmalı. Özellikle daire başkanlıkları eğitim toplantılarını sıklaştırmalıdır.
57. Mesleğe ilk girişten itibaren bu konuda branşlaştırmaya gidilmelidir. Bilişim suçları branş olmalı ve hızlı bir gelişim sürecinde olan bilgisayar teknolojisi konusunda periyodik kurs verilmelidir.
58. Bilişim suçları ile ilgili konularda görev yapan personelin, sadece bu konular üzerine yoğunlaşması gerekmektedir. Teknolojiyi , gelişmeleri takip etmekte buna bağlıdır. Personelin de gelişmeleri takibi, hizmet içi eğitim vb. ile mümkün olabilecektir.
59. Bilişim suçları konularında personel temini için istekli personele eğitim verilmelidir.
60. Personel meslek öncesi eğitim durumuna göre bilişim suçları alanında işe başlamalı, daha sonra bu eğitim doğrultusunda branşlaşması sağlanmalı, hizmet içi eğitimlerle de gelişen teknoloji verilmelidir.
61. Çoğu İl Emniyet Müdürlüklerinde bilişim suçları konularında, fazla bilgili insanların olmaması önemli kayıp ve eksikliktir. Eğitim organizasyonları düzenlenmelidir.
62. İlk önce kurslarda, temel eğitim olarak bilişim suçlarının işleniş şekillerini herkese anlatmak gerekmektedir. Spy, Keylogger, Spam vb. suç yöntemleri ve tüm işletim sistemleri anlatılmalıdır.
63. Bilişim suçları ile ilgili birimde çalışıyorum, ancak bu zamana kadar konu hakkında hiçbir hizmet içi eğitim almadım. Suçlarla mücadeleyi mevcut

bilgilerle yürütmeye çalışıyoruz. İlgili personelin hem hizmet içi, hem de dışarıdan eğitim alarak uzmanlaştırılması gereklidir.

64. KOM Şb. Md. deki personele bilişim suçları konusunda eğitim verilmelidir. Personel seçimi, objektif yapılmalıdır. İlgili personele uzmanlık eğitimi, online eğitim gibi eğitimler verilmelidir. Yapılacak eğitim teorik de değil teknik ve uygulamalı olmalıdır.
65. Polis Meslek Yüksek Okulu, Polis Mesleki Eğitim Merkez'lerinde ve meslekte kurslar düzenlenmelidir.
66. Çalışacak personelin sadece bu konu üzerinde yoğunlaşması, gerekli eğitimi ve donanımı alarak çalışması, gerekirse tim olarak çalışması gerekmektedir. Bu personel başka konuda görevlendirilmemelidir.
67. Personele pratik yapma imkanı sağlanmalıdır. Her gün, yeni suç ve suç türü bilişim dünyasında karşımıza çıkmaktadır. Personel, kendini yenilemeli ve eğitilmeli, suçluların her zaman bir adım önünde olunmalıdır. Bu nedenle eğitime önem verilmelidir. Eğitim kalıcı ve öğretici olmalıdır.
68. Hizmet içi ve uluslararası eğitimlerle teknik personel yetiştirilmelidir. Ayrıca, hizmet içi eğitimle yetinilmeden uzmanlık eğitimi de verilmelidir. Emniyet Teşkilatı bu konuda yetersiz.
69. Bilişim suçları ile mücadelede görev alacak personelin zorunlu haller dışında görev yeri değiştirilmemelidir. Personele, uzmanlık seviyesinde eğitim verilmeli, belirli aralıklarla teknolojideki gelişmeleri aktaracak şekilde eğitim verilmelidir.
70. Sadece merkezde değil taşrada da bilişim suçları ile ilgili eğitimlerin verilmesini isterim.
71. Bilişim suçu ile mücadele edecek personele en azından bilişim suçu şüphelisi kadar bilgi sahibi olacak suç yöntemleri ve püf noktalarının öğretilmesi gerekmektedir. Ayrıca, bu suçlarla nasıl mücadele edeceği, hatta suç meydana gelmeden imkan var ise önleme yöntemlerinin bildirilmesi gereklidir.
72. Ben yeni polis memuruyum, eğitim almak için can atıyorum. Kendi çabamla bazı şeyleri yapmaya çalışıyorum. Her seviyeden personele yönelik gerekli kurslar açılırsa, bilişim suçlarında başarılı bir teşkilat olacağımız kanısındayım.

73. Bilişim suçları konularında ve bu suçlarla mücadele konusunda, eğitime gereken kadar önem verilmediğini düşünüyorum. Personel daima suçlulardan bir adım önde olmalı ki, tespit ve yakalama yapabilsin. Bunun da kesintisiz eğitimle mümkün olacağı kanısındayım.
74. Bilişim suçları konularındaki hizmet içi eğitimler hep kısa süreli tutulmaktadır. Aksine, önce online eğitim, ardından yüz yüze eğitim verilmelidir. Seçilecek personelin İngilizce bilmesi de gerekmektedir.
75. Eğitim her kademedeki personele yeterli düzeyde verilmelidir. Bu çerçevede yılda en az 2 eğitim verilmeli. On-line eğitimde organize edilebilir.
76. Teşkilatın diğer kurumlara ihtiyaç duymayacak düzeyde teknik donanımı bulunmalı, bu suçla mücadele eden bir birim oluşturulmalıdır.
77. Sürekli eğitim gereklidir. Değişim takip edilmeli, seminerler kendi İl Emniyet Müdürlüğümüzde ve düzenli olarak yapılmalıdır. Teşkilatta bütün polislere, bilişim suçlarında önemli noktalar öğretilmelidir.
78. Eğitimler, özellikle taşra teşkilatına verilmelidir. İstekli personel tespit edilip, özenle seçilerek eğitimi de aynı özende gerçekleştirilmelidir. Eğitimde hassasiyet gösteren personelin, uzmanlaşması sağlanmalıdır.
79. KOM ve Bilgi İşlem Şube Müdürlükleri'ndeki ilglili personele gelişen teknoloji kursları verilmelidir.
80. Sadece amirlerin katıldığı kurslar olmamalıdır. Alt birimlerdeki personelde bilişim suçları konularında eğitilmelidir.
81. Telekom tarafından yapılan tespitin, emniyet tarafından da kolaylıkla yapılabilmesinin çok yararlı olacağı kanaatindeyim.
82. Bilişim suçları konularında güncel bilgilendirme ve ev eğitimi çalışması yapılabilir.
83. Bilişim Suçları ile Mücadele şubesi kurularak, objektif alımlar yapılmalı, özel eğitimli personel istihdam edilmeli ve bu personele başka konularda görev verilmemelidir.
84. Özellikle taşra teşkilatları, bilişim suçları ile mücadele yetersiz bulunmaktadır. Teknik ortam ve eğitim açısından taşra teşkilatları desteklenmelidir. Eğitime süreklilik kazandırılmalıdır.
85. Eğitimler, İl Emniyet Müdürlükleri bazında yapılmalı, ancak bu eğitimleri merkez koordine etmelidir. En azından İl Emniyet Müdürlükleri belli bir

düzeye gelinceye kadar bu durum böyle olmalıdır. Çünkü, İl Emniyet Müdürlükleri bu konuda yetersiz kalmaktadır. En büyük eksiğimiz eğitimdir. Yapılacak işlemlerin bilinçli ve usulüne uygun yapılması, delillerin adliyede geçerliliği açısından eğitim çok gereklidir.

86. EGM bünyesinde merkezi bir bilişim birimi oluşturularak burada hem bu tür suçlarla mücadele teknikleri, hem mevzuat, hem de personelin bilişim suçları konusunda eğitilmesi sağlanmalıdır. Bilişim suçları ile mücadelede, illere de önem verilmelidir. Personel ihtiyacının giderilmesi sağlanmalıdır.
87. KOM ve Bilgi İşlem Şube Müdürlükleri ortaklaşa çalışabilmelidir. Koordinasyon iyi yapılabilmelidir.
88. Bilişim suçları konularında Savcılar bilgilendirilmelidir. Türk Telekom, servis sağlayıcılar, bankalar ile sıkı işbirliği kurulmalıdır.
89. Polnet üzerinden sürekli eğitimlerin olabileceği, gelişmelerin sürekli olarak duyurulduğu " BİLİŞİM SUÇLARI PORTALI" oluşturulmalıdır.
90. Bilişim Suçları uzmanları, sözleşmeli personel istihdam edilebilir.
91. KOM Şube Müdürlüğü'nde bulunan bu görev için, teknik donanım desteği sağlanmalı, ayrıca personel seçiminde belli kategorilerle değerlendirme yapılmalıdır. Mevcut durum her haliyle yetersiz bulunmaktadır.
92. Gelişen teknoloji ile artık suçlar, bilişim dünyasına kaymaktadır. Bu da personelin eğitiminde bu konuya önem verilmesi gerektiğini göstermektedir.
93. Taşra teşkilatı olarak eğitim eksiği büyüktür. Bu tür suçlara etkin müdahale edilememektedir. Sürekli diğer birimlerden yardım istemek zorunda kalıyoruz.

EK-5 Bilişim Suçlarıyla Mücadele Kapsamında Personelin Belirtmek İstediği Diğer Konular

1. Bu tür suçlarda kullanıcı IP adreslerini, kullanıcı kimlik ve adreslerini anında bulabilme ortamı oluşturulmalıdır.
2. İnternet bulunan işyerlerinde IP'yi kullanan kimlik bilgileri depolanmalıdır.
3. Microsoft Corporation ve hotmail gibi birimlere en seri şekilde ulaşılabilmelidir.
4. Bilişim suçları ile ilgili ayrı bir birim kurulmalı ve teknik bilgiye sahip personele uzmanlık eğitimi için ilgili kurslar verilmelidir.
5. Bilişim suçları ile ilgili, bağımsız bir daire başkanlığı/ünite kurulmalıdır.
6. Yurt içi ve dışı, tüm kurumlarla sürekli koordine sağlanmalıdır. Diğer ülkelerle işbirliğinde süreklilik ve anlık iletişim sağlanmalıdır.
7. Her İl Emniyet Müdürlüğü bünyesinde bilişim suçlarıyla ilgili şube bazında özel birimler kurulmalı ve özel eğitimler almaları sağlanmalıdır.
8. Bilişim suçları ile ilgili alanlarda, her türlü yasal düzenlemenin çıkartılması ve cezaların artırılması gerekmektedir.
9. Teknik cihazların temin edilmesi gereklidir.
10. Kurumlararası gerekli teknik alt yapının oluşturularak on-line izleme ve müdahaleye önem verilmesi gerekmektedir.
11. Bilişim suçları konusunda; öncelikle mevzuat tam olarak netleştirilmelidir. Yapılanma olarak çok başlılıktan kurtulup, merkezde bu konuda ayrı bir birim kurulmalı, taşrada da sadece bu konularla ilgilenecek ayrı bir birim kurulmalıdır. Ayrıca, bu birim her türlü teknik donanım olarak desteklenilmeli ve personel çok iyi eğitilmelidir.
12. Özellikle bilişim suçları konusunda Bilgi İşlem Şube Müdürlüğü personelinin eğitim alması sağlanmalıdır.
13. Merkez teşkilatında bir şekilde bilişim suçları konusunda gerekli destek bulunabilirken, taşrada mevcut imkanlar çok daha az ve sınırlı bulunmaktadır. Kolluk olarak Neyin? Nereye kadar? Nasıl? yapılacağı hususunda bir yapılanma bulunmamaktadır. Diğer kamu kurum kuruluşları ve diğer kolluk görevlileriyle ortak bir alanda buluşulamamaktadır. Özellikle merkez ve taşra yapılandırılmasında bilişim suçlarında görevli uzman

personel sıkıntısı çekilmektedir. Bu nedenle, ivedi olarak uzman personel yetiştirilmesi için eğitim organizasyonu yapılmalıdır.

14. İnternet bankacılığı kullanımı konusunda, bankaların müşteriyi bilgilendirmesi şeklinde zorlayıcı bir yaptırım oluşturulması gerekmektedir. Bankalarla ilgili, güvenlik yetersizliği ile meydana gelen zararların tanzimi yönünde mevzuat düzenlenmesi gerekmektedir.
15. C.Savcıları ve hakimlerde bilişim suçları ile ilgili alanlarda eğitilmeli ve sadece bu konulara bakan savcılar olmalıdır.
16. Bilişim suçları konusunda görevli personel, en az şüpheliler kadar eğitilmedikçe başarı sağlanamayacaktır.
17. MSN'lerin çalındığı ve adreste kayıtlı kişilerden kontör veya para istendiği durumlarda, IP adresleri belli olan kişilerin görüşme anında adres tespiti ivedilikle yapılamamaktadır. Çünkü, Telekom'dan savcı talimatı ile adres tespiti istenmesi prosedürü olayı geciktirmekte ve şahsa suçüstü yapılamamaktadır. Bilgisayarla iletişim halinde iken şüpheli adresinin ivedilikle tespiti bilişim suçlarında suçüstü yapılabilmesi için büyük önem taşımaktadır, bu yönde mevzuatta çalışmalar yapılması gerekmektedir.
18. Uzman birim sadece bilişim suçları ile uğraşmalı ve teknolojik-hukuki her türlü imkanı güçlü olmalıdır.
19. Bilişim suçları ile ilgili alanlardaki personel soruşturmalarında, resmi kurum ve kuruluşlar veya diğer özel şirketlerce genellikle resmi yazılara cevabi bilgi verilmemektedir. Cumhuriyet Savcılıkları kanalı ile gerekli bilgiler istenildiğinden, bu durum resmi yazışmaların uzun zaman almasına yol açmakta ve böylece tahkikat süresi uzamaktadır. Bilişim suçları konusunda uzman birime bilgi ve belge isteme konusunda yetki verilmelidir.
20. KOM Şube Müdürlüğü, bilişim suçları konusunda belirli iller ve merkez bazında eleman ve teknik donanım açısından yeterli bir konumda bulunmaktadır. 81 İl Emniyet Müdürlüğü, KOM Şube müdürlüklerinin eleman ve teknik donanım açısından yeterli bir konuma kavuşturulması gerekmektedir.
21. Mevzuata göre bilişim suçları konularında, servis sağlayıcı firmalar, Telekom veya bankalardan bilgi ve belge temininde savcılık talimatı veya

mahkeme kararı gerekmektedir. Ayrıca, savcılık talimatı ya da mahkeme kararına rağmen bu birimlerden IP numarası, MAC adresi ve Log'lar gibi istenilen bilgilerin teminin de gecikmeler olmaktadır. Bu konuda yasal süre zorunluluğu getirilmeli ve böylece emniyet yetkililerine etkin çalışma ortamı sağlanmalıdır.

22. Bilişim suçları, globalleşen dünyada baş döndürücü bir hızla gelişmektedir. Mücadelenin etkin bir şekilde yapılabilmesi için gelişen suç yöntemleri konusunda güncel olarak eğitimler düzenlenmeli ve teknolojik yapılanma günün şartlarına uygun olmalıdır. Ayrıca, uluslararası işbirliğide büyük önem arz etmektedir.
23. Zararlı içeriğin önüne geçilmesi amacıyla filtreleme programları yerine, ABD'deki gibi içeriği zararlı port'ların servis sağlayıcılar olarak kapatılması sağlanmalıdır.
24. Bilişim suçları konularında, yetişmiş deneyimli personel yanında teknik cihazlarla desteklenmiş sistemlerle online izleme yapılarak suç ve suçlularla daha verimli mücadele edilebileceği düşünülmektedir.
25. Emniyet Teşkilatı içinde, bilişim suçları ile mücadele için illerde şube müdürlüğü kurulmalı gerek eğitim, gerekse teknik donanım bakımından yeterli hale getirilmelidir. İnternet kafelerin denetimi bu birim tarafından yapılmalıdır. İnternetin suistimal edilerek, masum insanlara zarar vermek için kullanılması ve günümüzde mağdur kişilerin sayılarının artması konunun önemini ortaya çıkartmıştır. İnternet ortamındaki özgürlüğün kontrol altına alınması veya kısıtlanması çıkarılan kanunlarla ve gerektiğinde de cezai müeyyidelerle belirlenmelidir.
26. Bilişim suçlarıyla mücadelede en önemli unsurlardan birisi, kanun veya yasalarda neyin suç teşkil ettiğini iyi bilmektir. Bu konuda personelin eğitilmesi büyük önem taşımaktadır.
27. Emniyet Teşkilatı içinde, bir çok konuda kurslar düzenlenmektedir. Fakat, bilişim suçları konusu çok önemli olmasına rağmen bu konuda özellikle küçük illerde hiçbir kurs düzenlenmemekte veya bu konular hakkında konferans, seminer yoluyla bilgi verilmemektedir. Her geçen gün bu konuda olaylar artmakta olduğu için, olay türleri ve işleniş yöntemleri güncel olarak takip edilememekte ve çözümünde kişisel çabalar ile netice

alınmaya çalışılmaktadır. Bilişim suçları konularında görevli personelin, sadece bu konularda çalışması için ortam sağlanmalı ve görev alanı dışındaki iş yükünün azaltılması sağlanmalıdır.

28. Uluslararası işbirliği konusunda Rus hacker'ları ile etkin mücadele edilememesinin nedenleri ve çözüm yolları kesinlikle bulunmalıdır.
29. Tüm il birimlerinde bilirkişi yapabilecek seviyede bilgi sahibi olan personel olması için gelişen teknolojiye paralel olarak eğitim faaliyetleri düzenlenmeli ve bu suçlara hangi şubelerin hangi durumlarda bakacağı yönünde genelge veya tamim yayınlanması gerekmektedir.
30. Bilişim suçları konularında "Eğiticinin Eğitimi" türü kurslar düzenlenmeli ve böylece illerde bu alanda görev yapan personelin pratik ve uygulamalı olarak yerinde yetiştirilmesi sağlanmalıdır.
31. Bilişim suçları ile mücadele, özellikle günümüzde çok büyük önem arz etmektedir. Bu nedenle merkez ve taşra da bilişim suçları ile mücadele eden ayrı bir birimin kurulmasının faydalı olacağı düşünülmektedir.
32. Bilişim suçları ile mücadele en etkin şekilde olması için bu konu ile ilgili görev alan personelin en azından temel bir eğitimden geçirilmesi gerekmektedir. Bu temel eğitimi almış personelin bilişim suçları ile mücadele birimlerinde çalışabilmesi için gerekli düzenlemenin yapılması gerekmektedir.
33. Bilişim suçları ile mücadelede KOM Daire Başkanlığı'nca bölge olarak belirlenen illerde yeterli imkanlar oluşturulmuştur. Ancak, bu illerden bağlı bulunan illere yeterli destek verilmesi ve illerde bu konuda yetişmiş personel istihdam edilmesi gerekmektedir.
34. Bilişim suçları ile mücadelede, bütün alanlarda Microsoft ile koordine kurulmalıdır.
35. KOM Şube Müdürlüğü'nde çalışmama rağmen bilişim suçu ile karşılaştığımda nasıl bir yol izleyeceğim ve ne yapabileceğim konusunda hiçbir bilgim yok, bu eksikliğimi giderebilmek için bilişim suçu konusunda uzman olan kişiler tarafından eğitim almak isterim.
36. Bilişim suçları konularında mevzuat, idari yapılanma ve özellikle teknik ünite konusunda çalışmalar yapılmalı ve uluslararası işlenen suçun müdahele şekli konusunda personel örnek uygulamalar ile

bilgilendirilmelidir.

37. Günümüzde yeryüzü bilişim çılgınlığı yaşamaktadır, uluslararası bilgi casusluğu ülkelerin bağımsızlığını tehdit etmektedir. Bilgi güvenliği çerçevesinde kendi ülkemize ait milli yazılım ve işletim sistemleri geliştirilmelidir. Ayrıca, suç şüphesi altında bulunan bilgisayarların kayıtlarına daha kolay erişim için yasal mevzuat düzenlenmelidir.
38. Bilişim suçları kapsamında adli görevli şubeler haricindeki hiçbir birimin bilişim suçları kapsamında görev almamaları gerekmektedir. Örnek; ben Mali Suçlarla Müc. Şb. Müd.'de çalışıyorum, banka dolandırıcılığı konusundaki dijital delil inceleme ile ilgili görevleri iyi bir şekilde yapabilirim. Fakat Terörle Müc. Şb. Md ile ilgili gelen bir HDD incelemesi konusunda, ben ilgili birime küçükbir oranda yardım sağlayabilirim. Bu yüzden, adli polis olarak görev alan şubelerin (mesela Terör, KOM , Asayiş, Güvenlik Şb.) kendi personellerini yetiştirmeleri gerektiğini düşünüyorum.
39. Her birimin kendisine ait bilişim suçları biriminin olmasını gereksiz buluyorum. Her ilde bir tek adli bilişim uzmanlığı bulunmalıdır. Her birim kendisi (yakalama, el koyma gibi) adli işlemlerini takip etmelidir. Operasyon birimlerine, adli delil toplama eğitimi verilmelidir. Bilişim suçları ile mücadelede kurumsallık kazanılmalı ve mevzuat yeniden düzenlenmelidir. Bana göre dijital delil toplama, el koyma her birime anlatılmalıdır. Elde edilen delillerin bilirkişi uzmanlığı Bilgi İşlem Şb. Md. bünyesinde kurulacak dijital delil inceleme bürolarında yapılmalıdır. Sonuç raporu, ilgili birime verilerek yakalanması gereken şahısların yakalanması sağlanmalıdır. İnternet üzerinden suç talebi adli bilişim birimince yerine getirilmelidir.
40. Bilişim suçu olarak karşımıza en çok günümüzde, kredi kartı dolandırıcılığı ve mail hack'leme gelmektedir. Bu gibi durumlarda emniyete yansıyan şikayetlerde ilk yapılması gereken şeyin savcılığa şikayette bulunma olduğunu düşünüyorum.
41. Bilişim Suçları konularının yasal dayanağı ile birlikte meslek öncesi eğitim olan PMYO, POMEM ve Polis Akademi'sinde ders olarak verilmesi gereklidir. Bu dersi alan ve not ortalaması 90 ve üzeri olan personelin

bilişim suçları konusunda görev yapan birimlerde çalıştırılmasının uzmanlık gerektiren bu suç dalı için yararlı olacağını düşünüyorum.

42. Bilişim suçu ile bilişim cihazları kullanılarak işlenen suçlar kesin bir ifade ile ayrılmalıdır. Bilgisayar, mail vb. kullanılarak yapılan hakaret, şantajın bilişim suçu olmaması gibi.
43. Kurumlar arası gerekli teknik alt yapının oluşturularak online izleme ve müdahaleye önem verilmelidir.
44. Bilişim suçlarıyla ilgili mevzuatı çok yetersiz bulunmaktadır. Bilişim suçları kanunu çıkarılmalıdır. Ayrıca, internet cafeler teknik manada yeterince denetlenememektedir. İnternet cafelerde suç işlenmesini önlemek için kafe sahiplerine vatandaştan TC kimlik numaralarını kaydetmeleri kanunen sağlanmalıdır. Ayrıca kablosuz internet hizmeti veren büyük alışveriş merkezlerinde, otobüs terminellerinde şifre ile giriş yaptırılmalıdır.
45. İlk olarak bu konuya yakın olan personele php ve asp dilleri öğretilmeli yada öğrenmeleri için destek verilmelidir. Daha sonra korsan yazılımlarla yapılan sahtecilik olayları incelenerek, aynı yazılım metodları personele öğretilmelidir.
46. Bilişim suçlarıyla mücadele kapsamında görev alacak personelin geniş kapsamlı eğitim alması için pratik yapılarak eğitim verilmesinin faydalı olacağına inanıyorum. Personele kullanacağı gerekli materyallerin sağlanması ve kullanılacak olan gerekli araç, teknik malzemeler ve donanımla ilgili imkanların sağlanmasının faydalı olacağına inanıyorum.
47. Polisiye tedbirlerin bu konuda yeterli olmadığı gerçeğinden hareketle her kurum ve kuruluş bu konuda kendi tedbirini almalıdır. Meydana gelen suçları soruştururken polisin daha fazla veriye erişebilmesi gerekir. Bir takım veriler polise açık olmalıdır.
48. İl Emniyet Müdürlükleri bünyesinde en kısa zamanda bilişim suçları bürosu yada ayrı bir şube müdürlüğü kurulması gerekir. Bilgisayar sistemini kullanan banka ve iletişim şirketlerinin hem kendilerinin hem de müşterilerinin mağdur olmamaları için çok acele bu konuda tedbir almaları gerekmektedir. Bilişim suçlarıyla mücadele eden birimlerin diğer resmi kurumlar ile irtibatının sağlanması ve bu suçun çok kısa zaman aralığında işlendiğinide gözönünde bulundurularak, gereksiz yazışmalara meydan

vermeden istenilen yada gerekli bilgilere anında ulaşılmasının sağlanması gerekmektedir.

49. Bilişim suçları ile tek bir birim profesyonel olarak ilgilenmelidir. Çünkü, şu anda asayiş ve kaçakçılık şubeleri ayrı ayrı ilgilenmektedir. Birimlerin hangi konulara bakacağı belli değil. Bence, bilişim suçları bu konuya en yatkın birim olan bilgi işlem şubeye verilmelidir. Adli kısmı ile, ilgili şubeler ilgilenmelidir.
50. Bilişim suçları ile ilgili bir birimin kurulması gereklidir. Bilgi işlem Şube Müdürlüklerinde; mecburiyetten veya diğer şubelerin bilişim suçları bürolarının yetersizliğinden ya da yoğunluklarından dolayı bilişim suçları olayları araştırılmaktadır. İnceleme ve bilişim suçları ile ilgili konularda, genel müdürlüğe bağlı tek birim kurulmalıdır.
51. Bilişim suçları konusunu takip edecek merkezi bir kurum veya kuruluşun oluşturulması gerekmektedir. RTÜK gibi, İnternet'i gözden geçirecek resmi bir kurum oluşturulmalıdır.
52. IP tespiti ve diğer bir çok işlem için (Telekom'dan bilgi alma vb.) yetkili mahkemelerden izin almak zaman almaktadır. Bu nedenle araştırmayı genişletmek mümkün olamamaktadır. Kısacası, online olarak IP sorgulaması yapılabilmelidir. İstenilen belgeler çok geç gelmektedir.
53. Bilişim suçlarıyla mücadele kapsamında, idari yapılanma değiştirilmelidir. KOM Şube Müdürlüğü'nün Mali Büro Amirliği bünyesinde, bilişim suçlarla mücadele de iş yükünün ağır olması nedeniyle yeteri derecede başarı sağlanamamaktadır. Bilişim suçları için mutlaka ayrı bir birim oluşturulmalıdır.
54. Teknolojiyle birlikte suç çeşitleri artmaktadır. Bununla birlikte personelinde bu bağlamda sürekli değişim içinde olması gereklidir.
55. Kamuoyu bilgilendirilmesi yapılmalıdır.
56. En önemli sorun personel yetersizliğidir. Suçlu teknik açıdan bizden daha farklı cihazlar kullanmıyor. Bilgili ve donanımlı personel, çözüm için yeterlidir.
57. Meslek içi eğitim programları yapılmalı, ama mutlaka amirler içinde yapılmalıdır.
58. Bilişim suçları, bilgi işlem gibi tek bir birimde toplanmalıdır. Bu tür

suçlarda nereye müracaat edileceği bilinmelidir. Vatandaş bu konuda bilinçlendirilmelidir. Tek birim olursa işler, daha kolay olur. Vatandaşın tek bir muhatabı olur. Telekominikasyon birimi gibi tek birim olmalıdır.

59. Bilişim suçlarında önemli olan bence yetişmiş personeldir. Personel ne yapacağını bilmeli, hangi teknik gereksinimi olduğunu bilmeli ve buna göre kendini geliştirebilmeli.
60. Tek merkez ve güçlü birim kurulmalıdır. Görev karmaşası olmadan koordinasyon sağlanmalıdır.
61. Tüm emniyet teşkilatının bilişim suçları konusunda eğitilerek bilgi sahibi olmaları sağlanmalıdır. Özellikle internet kafelerde bir suçu işlemeye yönelik çalışmalar yapılmalıdır.
62. Bilişim suçlarında büyük ölçüde yetişmiş eleman ihtiyacı bulunmaktadır. İllerde 1 komiser en az 3 polis memuru olarak tim oluşturulmalıdır. Güncel olarak eğitilmeli ve yeterli donanım sağlanmalıdır.
63. Bilişim suçları alanında personel yetersiz bulunmaktadır. Var olan personel ise, kendi çabaları ile kendilerini yetiştirmeye çalışmaktadır. KOM, Asayiş ve Bilgi İşlem birimleri arasında konu ile ilgili çelişki bulunmaktadır. Bu karmaşa aşılmalıdır.
64. İnternet üzerinden işlem yapanları kayıt altına almak gereklidir. TC numarası ile İnternet'e giriş yapmalıdır.
65. Etkili ve verimli iş yapan personel azdır. Bu konuda yetişmiş kişilerde Ankara ve 3-4 büyük şehir de istihdam edilmektedir. Gerekirse, yurt dışına memur yollanarak uzman sayısının artırılması sağlanmalıdır.
66. Yazılım firmalarından eğitim sağlanmalıdır.
67. Bilgisayar sistemleri ve donanımları en üst düzeyde olmalıdır. Yurt dışındaki birimlerle koordine sağlayacak birimler oluşturulmalıdır.
68. Teknik alt yapı ve bilişim suçları hakkında ülkemizde yapılan çalışmaların sayısı yeterli değildir.
69. Bilişim suçları birimi kurulmalıdır. Telekom, kuruluşlar ve yurt dışı birimlerle bağlantı kurulmalıdır.
70. Bu işle uğraşacak personel çok ciddi eğitimden geçirilmelidir. Sadece merkezdeki personelin bu işleri bilmesi yeterli değildir. Her ilde bu işleri yapacak personel olması gerekmektedir. Her zaman ki gibi, personel önce

kendi çabasıyla öğreniyor, kurs ise daha sonra düzenlenmektedir.

71. KOM ve Bilgi İşlem (POLNET) web sitesinde soru-cevap şeklinde bir forum ortamı düzenlenmelidir. Personelin bu soru-cevaplarla kendini yenileyebilmesi sağlanmalıdır.
72. KOM ve Bilgi İşlem olarak her geçen gün bir yenisi çıkan bilişim suçları ile mücadele geri kaldığımızdan, çok acil olarak Microsoft Türkiye temsilcilerinin de desteği ile bu konular da eğitime alınmalıyız.
73. Mevzuat yetersiz durumdadır. Ne yapacağımız, suçlara karşı hangi prosedürü takip edeceğimiz konusunda eğitim almamız gerekmektedir.
74. Bilişim suçları birimi oluşturularak, bilgi ve belgelerine başvurulan kuruluşları da bu birime entegre ederek, daha hızlı ve bilinçli bir yapı oluşturulmalı ve en kısa sürede bu yapı işler hale getirilmelidir.
75. Bu suçlar TCK da yasal zemine oturtulmuştur. Ancak hem polis, hem de savcılar uygulamada yeterli tecrübeye sahip değildir. Büyük iller haricinde, personel ve teknik imkan yetersiz bulunmaktadır.
76. EGM bünyesinde bilişimle ilgili kuruluşlarla ortak çalışan bir birim oluşturulmalıdır. EGM de bilişim suçları birimi oluşturulmalıdır.
77. Bilişim konusu üzerine kurs almış personel az bulunmaktadır. Bu konuda uzmanlar yetiştirilmeli ve bu eğitim yaygınlaştırılarak tüm illerde yetişmiş personel bulundurulmalıdır. Bunun için gerekli mevzuat değişiklikleri yapılmalıdır.
78. Bilişim suçları, günlük suçlar arasına girebilmiş durumda değildir. Ne bu talepleri doğru alabilecek personel, ne de bu olaylara anında ve yeterli müdahaleyi yapabilecek kapasitede personel bulunmaktadır. Hatta vatandaşlar da nereye ve nasıl müracaat edeceklerini bilmemektedir.
79. Bilişim suçları artık organize bir olay olarak değerlendirilmeli, mevzuat bu doğrultuda düzeltilmelidir. Bilişim suçları, uluslararası bir suç olarak algılanmalı ve diğer devletlerle ortak çalışmalar yapılmalıdır.
80. İnternet kafeler de erişim adreslerini takip edebilecek teknik ve kanuni düzenleme yapılmalıdır. Bilişim suçları konusunda taşra da, her ilin kendine özgü bir yapılanması var. Örneğin, taşra asayiş şubelerinde yetişmiş personel çok azdır. Yetersiz sayıda kurs düzenlenmesiyle, bu suçlarla mücadelede başarılı olunamaz. Ancak, yeterli sayıda kursa

gitmekle bu suçlarla mücadelede başarılı olunabilir.

81. Özellikle Rus hackerlerin yaptığı dolandırıcılık olayları iyi incelenmeli ve çözümler geliştirilmelidir.
82. Bilişim suçlarını, yüksek teknolojik suçlar olarak değerlendiriyorum. Sürekli değişmektedir, kanımca biz polisler hep suçluların gerisinden takip ediyoruz, hiç onların önüne geçemedik.
83. Kanunları iyi uygulamak için, uzman kişilerin vereceği gerçek manada eğitime ihtiyaç vardır.
84. -Yasak siteler- Telekom, sakıncalı siteleri belirleyip ülke genelinde abonelerin erişimini engelleyebilir.
85. Bilişim suçları merkez ve İl Emniyet Müdürlüklerinde daha etkin ve daha verimli hizmet alınabilmesi için şube müdürlüğü şeklinde çalışmalıdır.
86. Bilişim suçlarında konular çok farklı olduğu için bu konularda bankalar, üniversiteler, emniyet kurumları ve Kültür Bakanlığı arasında koordinenin sağlanması gerekmektedir.
87. Bence çağın vebası “Bilişim Suçları” dır.
88. Suç öncesi kolluk çalışmaları yapılmalıdır. Bilişim teknolojileri (BT) ile ilgilenen ve polis olan bir şahıs olarak, geleceğin en önemli suç ve suçlu profilini bilişim sektöründe yaşayacağız diye düşünüyorum. Çünkü suçlular artık en yeni teknolojileri kullanarak karşımıza çıkmaktadır.
89. Bu konularda yapılan eğitim çalışmaları sınırlı ve yetersiz. Eğitim çalışmalarının hızlandırılması ve çoğaltılması gerekmektedir.
90. Bilişim ilerledikçe suçlar da ona orantılı olarak ilerleyeceğinden, bu suç ve suçluların önü kesilecek tedbirler alınmalıdır.
91. Bilişim suçları büro amirliğinde görevli personelin kullanmış olduğu bilgisayar ve diğer medyaların teknolojik olarak sürekli en yeni sistemler ile yenilenmesi, malzeme yazılım ihtiyacının temin edilmesi gerekmektedir.
92. Bu konuda mücadeleci personelin düzenli bir eğitimden geçirilmesi gerekmektedir. Bilişim suçları giderek büyüyen ve gelişen bir alan olduğundan bu birimlerde görev olacak personelin tamamen branşlaşarak uzmanlaşması gerekmektedir. Bu branşlaşmada kendini yetiştirmiş iyi niyetli hacker denilen şahıslardan faydalanılabileceğini düşünüyorum.
93. İl Emniyet Müdürlüklerinde, bilişim suçları ekibi kurulmuş değildir.

94. Personelin teknik açıdan da desteklenmesi ve eksiklerin giderilmesi gerekir.
95. İllerin birbirinden kopuk olduğunu düşünüyorum, bu konularda belirli birimlerin oluşturularak sadece bu konuya bakması ve diğer illerle koordinasyonun sağlanması amacı ile belirli aralıklarla kurslara çağırılması gerekmektedir. Bilişim suçları kursları ile, kişiler arasında ilişkilerin ve etkileşimlerin gelişeceğini düşünüyorum.
96. Bu suçla mücadele eden personelin eğitimi haricinde suçun önlenmesi açısından ülke genelinde insanlara eğitim verilmelidir. Bu eğitimle bu suçtan mağdur olanların sayısı azalacaktır. Ayrıca en çok karşımıza çıkan internet yoluyla banka dolandırıcılığı olaylarına karşı, bankaların gerkli güvenlik önlemlerini alması için yaptırım uygulanmalıdır.
97. Günümüz teknolojisinin çok hızlı gelişmesi ile meydana gelen olayların bir o kadar basit olaylardan daha karmaşık ve tespiti zor olan olaylara doğru gitmesinden bahisle, suç ve suça tevessül eden şahısların yakalanmasında gelişimin devamlı takibi ile etkin mücadele edilebilecektir.
98. Uygulanabilir ve caydırıcılığı üst seviyede olabilecek, etkili bir kanuni yapılanma ve mevzuata ihtiyaç vardır.
99. Yeterli eğitim verilmiş personel ve bu konu ile ilgili şube müdürlüğünün kurulması gereklidir.
100. Kapsamlı bir filtre programı tespit edilerek bu programın tanıtımı ve kullanımı personele gösterilmelidir. Çünkü, evinde bilgisayar olan personel sayısı her gün artmaktadır. Çocuklar da, bilişim suçları ile karşı karşıya kalmaktadır. Bu filtre programı, ülke genelinde düşük maliyet ile yaygınlaştırılmalıdır.
101. Bilişim suçları internet aracılığı ile yapılmakta, bu nedenle bilişim suçlarına ilişkin yeterlilikler konusunda gerek terimler, anlamları, özellikleri vb. konularda personel eğitilmelidir.
102. Terör, Güvenlik, Asayiş vb. kendi büro amirliklerini kurmalıdır. Sanal suçlarla ilgili şubelerin olay yerine gittikleri zaman dijital delil kapsamında toplanan materyaller ve dikkat edilecek hususları bilmeleri gereklidir. Sanal suçlular teknolojiyi her yönüyle kullandıkları için hukuki anlamda yeterli kanun çıkartılması gereklidir.

103. Bilişim suçları kapsamlarının, detaylı olarak savcı ve hakimlere tebliği gereklidir.
104. Bilişim suçları ile mücadele edecek seviyede polis teşkilatı mensuplarının (bilgi işlem, asayiş, KOM) eğitilmesi zaruret halini almıştır. Polis, sadece adli polis-idari polis olaraak değerlendirmemelidir. Bilişim alanında eğitilmemiş ve mücadele edecek personelin olmaması durumunda adli polisliğin ne kadar faydalı olacağı ortadadır.
105. Günümüzde her yerde bilgisayar ve internet kullanımı yaygınlaşmakta buna bağlı olarak, bilişim suçları da artmaktadır. Bunun önlemi şimdi alınmaz ise daha sonra geç olabilir. En yakın zamanda eğitim merkezleri oluşturulmalıdır.
106. Bu suç türünün narkotik veya mali suçlar kadar önemli olduğunun bilinmesi gereklidir. Bu tür suçların işlenmesi kimi zaman zor olsada, suçu işleyene getirisi çok fazla olmaktadır.
107. Bu konuda yeterli eğitim kurs ve teknik bilgiler olmadan, kurumlar arasında irtibatın kısa zamanda aşılması sağlanmadan, soruşturmayı yürütecek adli merciler bilgilendirilmeden, bankalar ile iletişim sistemi iyi kurulmadan, bilişim suçlarının önüne geçilmesi ve yapılan ya da yapılacak olan soruşturmaların yeterli bir şekilde sonuçlandırılması mümkün görünmemektedir.
108. Bilişim suçları ile ilgili yeni kanun düzenlemelerinin yapılması gereklidir.
109. İnternet kafe'lerden yapılan suçlarda suç işleyenlerin tespit edilebilmesi için gerekli çalışmanın yapılması gereklidir.
110. KOM Daire Başkanlığı, kendi mevzuatı ve görevleri açısından BİDEM salonlarında eğitim vermektedir. Bilgi İşlem Daire Başkanlığı, teknolojik gelişmeler ve bilişim suçları hakkında online eğitim vermelidir.
111. Bilişim suçları her geçen gün gelişerek artmakta, personelin de konuyla ilgili uzmanlaşarak sürekli gelişmesi gerekmektedir. Bilişim suçları ile mücadele kapsamında farklı birim kurulmasının faydalı olacağı düşüncesindeyim.
112. Bilişim suçları gelişerek her geçen gün artmaktadır. Bu nedenle çok önemlidir. Bu tür suçların bilinmesi ve önüne geçilmesi insanlarımız açısından çok önemlidir. Halk Eğitim Merkezleri'nde bilinçlendirme eğitimi

yapılmalıdır.

113. Teşkilatta her şey verilen imkanlara bağlıdır. Görev alacak personel istekli, iyi eğitim almış konusuna hakim kişilerden seçilmelidir. Bu işi severek yapacak personelin, amir-memur ayırmadan belirlenmesi gereklidir.
114. Bilişim suçları alanında mevzuat, suç çeşitleri, örnek olaylar, tedbirler vb. bilgilerin broşür olarak bastırılıp personel ve vatandaşların bilgilendirilmesi gereklidir.
115. Personel eğitimi kadar vatandaş eğitimi de önemlidir. Koruyucu hekimlik gibi, koruyucu polislik uygulamaları yapılmalıdır.
116. Personel bir çok konuya, aynı anda bakmaktadır. Bu nedenle uzmanlaşma olamamaktadır. Personelin kendini yetiştirmesine ve eğitimine imkan tanınmalıdır. Ülkemizde bilişim teknolojilerine gereken önem verilmemektedir. Konunun, karar mekanizmasında ki yetkililere anlatılması gerekmektedir.
117. Her ilin teknik alt yapısı düzenlenmeli, ileriye dönük çalışmalar yapılmalıdır.
118. Kurumlar arası irtibatların ivedilikle gerçekleşmesi için irtibat görevlilerinin bulundurulması gereklidir. Gerekli bilgilere ulaşılacak ortam sağlanmalı, direkt ilgili kuruluşlardan bilgi alınabilmeli ve bürokratik işlemler azaltılmalıdır.
119. Bilişim suçu ile uğraşan polisler, sayıca azdır. Teknik materyaller açısından da teşkilat yetersizdir. Aynı zaman da, bilişim dışında başka konularla da uğraştıkları için yetkin olunamamaktadır.
120. Eğitilmiş personele önem verilmeli, bilişim suçları ciddiye alınıp karakollardan başlayarak gerekli personelin en azından konu ile asgari düzeyde bilgilendirilmesi sağlanmalıdır. Ayrıca, ilgili kuruluşların bilinçlendirilerek müşterilerini de bilişim suçları konusunda uyarmaları gerekmektedir. Müracaatların nereye yapılacağının herkes tarafından bilinmesi, işlerin daha hızlı olmasını sağlayacaktır.
121. En az bu bilişim suçlarını işleyenler kadar bilgi seviyesine sahip yetişmiş personele ihtiyaç vardır. Ayrıca, emniyetin her birimindeki tüm personelin de bu konuda temel anlamda bilgisi olmalıdır.

EK-6 Basından 2007 Yılında Bilişim Suçlarına Yönelik Operasyonlar

İstanbul-KALE Operasyonu: İnteraktif Banka Dolandırıcılığı.

Yapılan ihbarlar ile KOM Daire Başkanlığı ve Niğde Emniyet Müdürlüğü tarafından gönderilen bilgiler ışığında örgüt kurmak ve teşekkül halinde interaktif banka dolandırıcılığı suçu işlendiği tespit edilmiş, şahıslar teknik takibe alınmış, yaklaşık 3 aylık teknik ve fiziki takip sonrasında tespit edilen 12 adreste 08.01.2007 tarihinde yapılan eşzamanlı operasyonla 7 şahıs yakalanmıştır.

Şahıslarla birlikte 48.485 ytl, 4.400 usd , 200 Euro , 1 Adet Dizüstü bilgisayar, 1 Adet Bilgisayar kasası, 30 Adet sahte nüfus cüzdanı, 4 Adet Sahte sürücü belgesi, 1 Adet Sıcak mühür makinesi, 3 Adet Bilgisayar harddiski, 1 Adet PVC makinesi, 2 Adet Em.Gnl.Müd. ait Mühür, 6 Adet İlçe Nüfus Müdürlüğüne ait Mühür, 2 Adet fotoğraf kesme makinesi, 20 Adet Bilgisayar Cd.si, 15 adet bankamatik kartı ele geçirilmiştir.

İzmir-PAPAĞAN Operasyonu: İnteraktif Banka Dolandırıcılığı.

Örgüt Kurmak Suretiyle İnternet Üzerinden Havale Dolandırıcılığı konulu Papağan (K) planlı operasyonU kapsamında elde edilen bilgiler neticesinde; MM liderliğinde İzmir ilinde kurulan ve faaliyet gösteren İnternet Üzerinden Havale Dolandırıcılığı yapan örgütün banka müşterilerinin hesaplarını ele geçirdikleri, bu hesaplardan üzerlerinde resimleri bulunan sahte kimliklerle açtırdıkları banka hesaplarına havaleler yaptıkları, elde ettikleri paraları Banka veya PTT aracılığı ile örgütün diğer üyelerine gönderildikleri, parayı alan örgüt üyelerinin bu paranın bir kısmını dövize çevirmek suretiyle Rusya da bulunan ve internet bankacılık şifresini kırdıkları değerlendirilen Rus uyruklu kişilere gönderdikleri, dolayısıyla hiyerarşik yapı içerisinde işleyen, lideri ve yöneticileri ile belirli bir ücrete karşılık çalışanları olduğu anlaşılan bir örgütün teşekkül etmiş olduğu anlaşılmıştır.

09-10.02.2007 tarihlerinde yapılan operasyonlarda 12 kişi yakalanmış, şahıslarla birlikte 3 adet dizüstü bilgisayar, 3 adet masaüstü bilgisayar, çok sayıda değişik kişilere ait sahte nüfus cüzdanı ve gerçek kişilere ait nüfus cüzdanı fotokopileri, bilgisayar cdleri ve flashbellekler, sahte ve gerçek nüfus cüzdanları ile bankalarda hesap açıldığını gösterir banka cüzdanları, manyetik şeritli kartlar, kredi kartları, suçtan kazanılan tahmini 45000 ytl ve 14550 usd para, çok miktarda altın bilezik, 2 adet otomobil ve bir miktar esrar ele geçirilmiştir.

İstanbul-SARIYILDIZ Operasyonu: İnteraktif Banka Dolandırıcılığı.

Yaklaşık üç aylık bir dinleme ve fiziki takipler sonucunda interaktif banka dolandırıcılığı yapan şahısların kaldığı toplam 7 adres tespit edilmiş,11.04.2007 günü eş zamanlı yapılan SARIYILDIZ operasyonunda toplam 13 şahıs yakalanmış, yakalanan şahısların iş,ikamet,araç ve üzerlerinde yapılan aramada 5 adet bilgisayar kasası ve harddiski, 30 adet çeşitli kurumlara ait mühür, çok sayıda boş lise diploması, 8 adet sahte nüfus cüzdanı, çok sayıda boş bayan ve erkek nüfus cüzdanı, 24 adet boş motorlu araç trafik belgesi, çeşitli firmalara ait kaşeler ele geçirilmiştir. Yakalanan şahısların 3'ü tutuksuz yargılanmak üzere serbest bırakılırken, 10'u tutuklanmıştır.

Ankara-MANYETİK Operasyonu: Banka ve Kredi Kartı Dolandırıcılığı.

Ankara Emniyet Müdürlüğünce yapılan istihbari çalışmalarda, örgüt kurmak, yönetmek, üye olmak, örgüt adına eylem ve faaliyette bulunmak, interaktif banka dolandırıcılığı, sahte kimlik ve sahte belgelerle kredi alarak kullanmak, sahte ve kopya kredi kartı imal ederek kullanmak, örgüt adına haksız kazanç sağlamak, rüşvet alıp vermek suçlarını işledikleri tespit edilen şahıslara yönelik olarak 12.04.2007 günü yapılan operasyonda 16 şahıs yakalanmış, şahıslarla birlikte 7 adet bilgisayar kasası,1 adet yazıcı, 1 adet kart kopyalama cihazı,1 adet pos cihazı, 1 adet pinpad cihazı, , kimlik fotokopileri, 290 adet cd, 4 adet disket,1 adet flashdisk, 13 adet değişik bankalara ait kredi kartı müracaat formu, 43 adet kredi kartı, 18 adet simkart, 1 adet kurusıkı tabanca , 1 adet kurusıkıdan bozma tabanca, boş ve şahıs adına tanzimli

manyetik şeritli kartlar, sahte sürücü belgesi ve sahte nüfus cüzdanları ele geçirilmiştir.

Şanlıurfa-VİRÜS Operasyonu: MSN Şifresi Kırma ve Kontör Dolandırıcılığı

Çeşitli illerde mağdurların şikayeti üzerine MSN dolandırıcılığı olaylarında Şanlıurfa ili Suruç ilçesindeki suç örgütlerinin yakalanmasına yönelik olarak 29.04.2007 tarihinde başlayan operasyonlarda 50 şahıs yakalanmış, şahıslarla birlikte 505 cd, 159 bilgisayar ele geçirilmiştir. Mahkemeye sevk edilen sanıklardan 11'i tutuklanırken 39'u tutuksuz yargılanmak üzere serbest bırakılmışlardır.

Malatya-KARGO Operasyonu: İnteraktif Kredi Kartı Dolandırıcılığı

Bilgisi haricinde kredi kartı hesabından 9 ayrı harcama yapılan bir şahsın şikayeti üzerine yapılan araştırmada alışveriş malzemesinin kargo ile Malatya ve Elazığ da bulunan kişilere teslim edileceğinin öğrenilmesi üzerine 26.05.2007 günü kargoyu almaya gelen 3 şahıs yakalanmıştır. Şahısların üzerlerinde ve sonrasında ikametlerinde yapılan aramalarda 1 adet sahte sürücü belgesi, 1 adet harddisk, 1 adet dizüstü bilgisayar, 4 adet cd , değişik şahıslara ait nüfus cüzdan fotokopileri elde edilmiştir. Yakalanan şahısların birisinin mail adresinde Rusya kaynaklı bir mail adresinden gelen kredi kartı numaraları, son kullanma tarihi ve CVV numaralarının bulunduğu tespit edilmiştir.

Kırklareli-PLASTİK Operasyonu: İnteraktif Banka Dolandırıcılığı

Bir organize suç çetesine yönelik yürütülen teknik takibe takılan bir görüşmede bir suç oluşumu içinde bulunduğu şüphesini uyandıran konuşmalar yapıldığı tespit edilince savcılık izniyle örgüt kurmak ve interaktif banka dolandırıcılığı suçlarını işleyen 6 şahıs hakkında iletişim dinlenmesi kararı alınmış, yapılan dinlemeler sonucu 2 kişinin hesabından sözkonusu örgüt üyesi şahısların hesaplarına havale yapıldığı öğrenilmiş ve hesaplara bloke konularak şahısların mağduriyeti önlenmiştir. 26.05.2007 tarihinde İstanbul Emniyeti ile yapılan eşzamanlı operasyonla 16 şahıs yakalanmıştır.

İstanbul-HORTUM Operasyonu: İnteraktif banka dolandırıcılığı

Yaklaşık üç aylık bir dinleme ve fiziki takipler sonucunda interaktif banka dolandırıcılığı yapan şahısların kaldığı toplam 13 adres tespit edilmiş, 29.05.2007 günü eş zamanlı yapılan HORTUM operasyonunda biri Ukrayna uyruklu olmak üzere 29 şahıs yakalanmıştır. Yakalanan şahısların iş,ikamet,araç ve üzerlerinde yapılan aramada 1 adet glock marka tabanca ve bu tabancaya ait 54 dolu fişek, 11700 usd, 50000 ruble,23000 ytl; 5 adet dizüstü bilgisayar, 1 adet bilgisayar kasası, 5 adet sahte kimlik, 1 adet encoder, çok sayıda Atm kartı ve başkalarına ait banka hesap cüzdanı ele geçirilmiştir.

Ankara-SONBAHAR Operasyonu: Banka ve Kredi Kartı Dolandırıcılığı.

Ankara Emniyet Müdürlüğünce yapılan istihbari çalışmalarda, örgüt kurmak, yönetmek, üye olmak, örgüt adına eylem ve faaliyette bulunmak, evrakta sahtecilik, interaktif banka dolandırıcılığı, kopya ve sahte kredi kartı yapmak, sahte ve kopya kredi kartları ile alışveriş yapmak, nitelikli dolandırıcılık ve silah kaçakçılığı suçlarını işledikleri tespit edilen şahıslara yönelik olarak 10.07.2007 günü yapılan operasyonda 9 şahıs yakalanmış, şahıslarla birlikte 3 adet bilgisayar kasası,2 adet dizüstü bilgisayar, 2 adet ruhsatsız silah, 12 adet Yargıtay Hakimi ve çalışanları kimlik kartı aslı, çok sayıda Yargıtay hakim, üye ve personeline ait preslenmeye hazır A4 kağıt üzerinde kurum kimlik bilgileri, çok sayıda CD , 2 adet flash disk, çok sayıda değişik şahıslara ait nüfus cüzdanı fotokopileri ele geçirilmiştir.

Antalya -ŞİFRE Operasyonu: İnteraktif Kredi Kartı Dolandırıcılığı

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı koordinesinde Bilişim Suçları ve Sistemleri Şube Müdürlüğü uzmanları ile Antalya Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü, Bilişim Suçları Büro Amirliği görevlilerinin yapmış oldukları analiz, değerlendirme ve istihbarı çalışmalar neticesinde, internet üzerinden elde ettiği kredi kartı bilgilerini 15 ile 150 ABD Doları arasında sahte kredi kartı dolandırıcılarına pazarlayan, 2006 ve 2007 yıllarında Ülkemizde yapılan kredi kartı sahteciliğine yönelik operasyonlarda kart bilgilerini temin ettiği tespit edilen ve uluslar arası

düzeyde aranan yabancı uyruklu bir şahsın ülkemize geleceğinin tespit edilmesi üzerine ŞİFRE kod adlı planlı çalışma başlatılmıştır.

Planlı çalışma çerçevesinde 26.07.2007 günü müştereken yapılan operasyonda yabancı uyruklu bir şahıs Kemer ilçesinde kalmakta olduğu otelde yakalanmış, şahıstan 2 adet Notebook bilgisayar ele geçirilmiş, bilgisayarların yapılan incelemesinde, değişik ülke vatandaşlarına ait çok sayıda kredi kartı bilgisinin bulunduğu tespit edilmiştir.

Şüpheli hakkında banka veya kredi kartlarının kötüye kullanılması suçundan işlem yapılmış, 29.07.2007 günü sevk edildiği adli makamlarca tutuklanmıştır.

Adana-HAVALE Operasyonu: İnteraktif Banka Dolandırıcılığı

20.06.2007 tarihli Havale Operasyonu kapsamında yapılan çalışmalarda, daha önce bilişim suçuna karışmış ve aranan bir şahıs ile suça iştirak eden diğer şahısların telefonları mahkeme kararı ile teknik takibe alınmış, bu teknik takip sonucu 4 şüpheli şahıs interaktif banka dolandırıcılığı suçu işlemek üzere 08.08.2007 günü bankaya gittiklerinde yakalanmışlardır. Olaylarla ilgili olarak 3 kişi de daha sonra gözaltına alınmıştır. Yakalanan şahısların 6'sı tutuklanmıştır.

İzmir - KARGA operasyonu: İnteraktif Kredi Kartı Dolandırıcılığı

S.D. liderliğindeki örgütün, internet yoluyla Rusya ve Ukrayna ülkelerinden temas kurduğu hacker tabir edilen kişilerden temin ettiği yurtdışı bankalarının müşterilerine ait kredi kartı bilgileri ile anlaşmalı işyerlerine kurdukları cihazlarla elde ettikleri kredi kartı bilgileriyle sahte kredi kartı oluşturdukları, bunları anlaşmalı işyerlerinde alışverişlerde kullandıkları ve sahte kimlikler kullanarak kargo aracılığı ile Antalya, İstanbul, Ankara, İzmit ve Mersin illerine gönderdiği belirlenmiş, 11.08.2007 günü örgüt lideri ve 3 şahıs yakalanmıştır. Yakalanan şahıslarla birlikte 711 adet sahte kredi kartı, 3 adet encoder cihazı, 1 adet emboss cihazı, 1 adet kart printer cihazı, 1 adet tiper cihazı,1 adet pos cihazı, 3 adet laptop, 1 adet bilgisayar ele geçirilmiştir.

İzmir-KELAYNAK Operasyonu: İnteraktif Kredi Kartı Dolandırıcılığı

Örgüt kurmak suretiyle uluslar arası kredi kartı dolandırıcılığı ve sahteciliği yaptıkları bilgisine ulaşılan şahısların 6 ay boyunca teknik takibe alınması sonrasında İzmir, Uşak ve Kocaeli illerinde 29.10.2007 tarihinde eşzamanlı yapılan Kelaynak Planlı operasyonu ile örgüt lideri ve biri aynı zamanda İsrail vatandaşı olmak üzere 12 kişi yakalanmış, şahıslarla birlikte sahte kredi kartı yapımında kullanılan 1 embosser, 3 encoder, 5 skimer,1 card printer, 2 takım smart card reader, 1 telefon call logar cihazı, 4 adet bankaların atm cihazlarına takılan card aparatları, aparatlara takılı kopyalama cihazları, 552 adet manyetik şeritli kart, 6 adet pos cihazı, 12 adet bilgisayar harddisk ve laptop, çok sayıda cd ve flash bellek, 4 adet sahte para, 3 adet boş pasaport, 19 adet banka cüzdanı, 6 sayfa bomba yapımını anlatan doküman ve bir miktar uyuşturucu madde ele geçirilmiştir.

EK-7 Basından 2008 Yılında Bilişim Suçlarına Yönelik Operasyonlar

1- Antalya: PARAVAN Operasyonu: Banka ve Kredi Kartı Dolandırıcılığı

Antalya KOM Şube Müdürlüğü Bilişim Suçları Büro Amirliğince C.S. liderliğindeki Haksız ekonomik çıkar amaçlı suç örgütünün Antalya, Ankara, İzmir, Bursa, Muğla-Marmaris, Osmaniye illerinde örgüt kurmak, örgüte üye olmak, örgüt adına faaliyette bulunmak, örgüt faaliyetleri çerçevesinde banka veya kredi kartlarının kötüye kullanılması, sahte kimlik kullanmak, suçtan elde edilen mal varlığı değerlerinin aklanması ve nitelikli dolandırıcılık suçlarını gerçekleştirdikleri tespit edilmiş; 15.01.2008 tarihinde sayılan illerde eşzamanlı yapılan operasyonlarla 13 şahıs yakalanmıştır. Yakalanan şahıslardan 12'si tutuklanmıştır. Olayla bağlantısı sonradan tespit edilen 1 şahıs ise firari olarak aranmaktadır.

Yakalanan şahıslarla birlikte 1 adet encoder, 5'sinde yabancı şahısların kart bilgilerinin yüklenmiş olduğu 175 adet manyetik şeritli kart, sahte kimliklerle ve farklı şahıslar adına alınmış banka kartları, 29 adet slip-çıktı, 3 adet ruhsatsız tabanca, bu tabancalara ait 10 adet fişek, 6 adet laptop, 5 adet PC bilgisayar,13 adet CD, 16 adet pos cihazı, 1 adet harici disk, 5 adet hafıza kartı ve suçtan elde edilen bir miktar para ve altın ele geçirilmiştir.

2- İstanbul: "İNTERNET ÜZERİNDEN ATM DOLANDIRICILIĞI" Operasyonu: Banka ve Kredi Kartı Dolandırıcılığı.

Çeşitli banka ve müşterilerinin şikâyetleri doğrultusunda İstanbul Emniyet Müdürlüğünce yapılan çalışmalarda; 2500 ayrı banka müşterisine ait hesaplara internet üzerinden yetkisiz erişim sağlanarak müşterilerin bilgisi dışında hesaplarının boşaltıldığı ve toplam zararın 3.580.000 YTL olduğu, bu boşaltma işleminde öncelikle müşteriye ait ATM kartının ikizinin üretildiği ve güvenlik kamerası bulunmayan bankamatiklerden çekilmek suretiyle müşteri ve bankaların zarara uğratıldığı tespit edilmiştir.

İstanbul Emniyet Müdürlüğünce 07.01.2008 günü başlatılan "İnternet Üzerinden ATM Dolandırıcılığı" operasyonu çerçevesinde; Sarıyer, Kadıköy, Beşiktaş ve Ümraniye ilçeleri ile Antalya ili ve Manavgat ilçesinde tespit edilen adreslerden toplam 7 şahıs yakalanmış olup, şahıslarla birlikte 2 adet dizüstü bilgisayar, 1 adet cep bilgisayarı, 1 adet uydu telefonu, 4 adet cep telefonu, 1 adet digital fotoğraf makinesi, 10 adet simkart, 50 adet banka kartı, yapılan işlemlere ait banka dekontları ele geçirilmiştir. Şahıslar haklarında düzenlenen soruşturma evrakı ile birlikte 10.01.2008 günü adli makamlara sevk edilmiştir.

3- Adana: SANAL TATİL Operasyonu: Banka ve Kredi Kartı Dolandırıcılığı.

Adana KOM Şube Müdürlüğü Bilişim Suçları Büro Amirliğince müşteki H.D.'nin bilgisi haricinde kredi kartlarından harcama yapıldığına dair şikayeti üzerine yapılan çalışmalar sonucunda internet üzerinden üye olduğu siteden 68 defa 23 adet farklı kredi kartı bilgileri girilerek kart güncelleme yapıldığı ve bu kredi kartları ile 51 adet farklı gsm operatörlerinden kontör alımı yaptıkları da tespit edilen 4'ü bayan 13 kişi 17.01.2008 günü yapılan Sanal Tatil Operasyonu ile yakalanmış; 1 bayan ise firari olarak aranmaktadır. Yakalanan şahıslardan 1'i tutuklanmış, diğerleri tutuksuz yargılanmaktadır. Yakalanan şahıslarla birlikte 2 adet bilgisayar kasası, 1 adet harici harddisk, 2 adet laptop, 37 adet gümrük kaçağı ve imei numaralarının kopyalandığından şüphe edilen cep telefonu ele geçirilmiştir.

4- İzmir: MARKAJ35 Operasyonu: Banka ve Kredi Kartı Dolandırıcılığı.

İzmir Kom Şube Müdürlüğü Bilişim Suçları Büro Amirliği görevlilerince yapılan istihbari çalışmalarda bazı şahısların sahte kimlik ve belgeler kullanarak bankalarda hesapları bulunan vatandaşların hesaplarını yasal olmayan yollardan elde ederek hesaplarında bulunan paraları çektiklerinin öğrenilmesi üzerine yapılan araştırmalar neticesinde tespit edilen şahıslar mahkeme kararıyla 4 ay teknik takibe alınmış, Şahısların A.Ş. liderliğinde çıkar amaçlı suç örgütü kurmak suretiyle nitelikli dolandırıcılık suçu işledikleri, örgüte hesabın

gerçek sahibine ait kimlik bilgilerinin vergi dairesinde memur olduğu değerlendirilen A.K. ve emlakçı K.A. isimli şahıslar tarafından verildiği, üretilen sahte kimliklere yapıştırılan fotoğraflarla bankalarda gerçek hesapları bulunan müşteriler adına değişik illerde aynı banka şubelerinde ikiz hesaplar açtırılarak paraların havale edildiği ve sahte kimliklerle çekildiği, örgütün bu yöntemlerle bugüne kadar 2.000.000 YTL civarında haksız gelir elde ettiği belirlenmiş, İzmir genelinde tespit edilen 17 adrese 22.01.2008 günü yapılan Markaj35 eşzamanlı operasyonu ile 10 şahıs yakalanmıştır. Kimlik tespiti yapılan 3 şahsı yakalama çalışmaları devam etmektedir. Yakalanan şahıslarla birlikte 6 adet bilgisayar,5 adet sahte sürücü belgesi, 2 adet sahte nüfus cüzdanı, 1 adet sahte çek, 7 adet senet, 4 adet kimlik bilgisi çıktıları, bankamatik makbuzları, hesap cüzdanları ele geçirilmiştir.

EK-8 Bilişim Suçları Çalışanlarına Yönelik Uygulanan Anket

A Ç I K L A M A

Bu çalışma, Fırat Üniversitesi Öğretim Üyesi Doç.Dr. Mehmet TAŞPINAR danışmanlığında yapılmaktadır. Yürütülmekte olan çalışmanın amacı; ülkemizde ve dünyada hızlı bir artış trendinde bulunan **"Bilişim Suçları"** ile mücadele etmek durumunda olan Emniyet Teşkilatımıza, akademik bir çalışma ile destek vermektir. Bu amaç doğrultusunda, bilişim suçları konusunda görev yapan ilgili personele yönelik olarak bir eğitim programı geliştirilmesi için, ihtiyaç belirlemesi yapılacaktır.

Bu amaçlar doğrultusunda, birey, toplum ve devlet üçgeninde ciddi mali, hukuksal ve güvenlik tehditlerine neden olan "**Bilişim Suçları"** konusunda görev ifa eden ve bu konuda ihtisas sahibi olan Emniyet Genel Müdürlüğü Bilgi İşlem ve KOM Daire Başkanlığı bünyesindeki personele yönelik olarak bir anket çalışması düzenlenmiştir.

Anket, iki bölümden oluşmaktadır. Anketin cevaplaması kolay ve az zaman alıcı olup, anketi doldurmak 10 dakikadan fazla zamanınızı almayacaktır. Maddelerin değerlendirmesini, sorularla birlikte verilen doldurma klavuzunu kullanarak yapınız.

Kişisel bilgileriniz ve cevaplarınız tamamen gizli tutulacaktır. Ankette sorulan kişisel (demografik) soruları cevaplandırmanız, araştırmanın güvenilirliğini artıracaktır. Çalışma sonucu elde edilen veriler, istatistiksel teknikler ile değerlendirilecektir.

Araştırmanın değeri ve başarısı için anket kapsamındaki soruları değerlendirerek araştırmamıza katıldığınız, zaman ayırdığınız, bilimsel bir çalışmaya katkıda bulunduğunuz ve bizi desteklediğiniz için teşekkür ederiz.

Doç. Dr. Mehmet TAŞPINAR
Fırat Üniversitesi
Teknik Eğitim Fakültesi
Eğitim Bilimleri Bölümü
ELAZIĞ

Emn. Amiri Çetin GÜMÜŞ
Kocaeli Emniyet Müdürlüğü
Saraybahçe Polis Merkez A.liği
KOCAELİ

Her türlü soru ve önerileriniz için, irtibat telefon numaraları ve elektronik posta adresleri:

Tel: 0.505.210 87 10
E-mail: mehmettaspinar@hotmail.com
cetingumus2003@msn.com

BİRİNCİ BÖLÜM

(KİŞİSEL BİLGİLER VE BİLİŞİM SUÇLARI KONUSUNDA GENEL DEĞERLENDİRMELER)

1- Görevli Olduğunuz İl?

……..

2- Görevli Bulunduğunuz Birim?

1. **( )** Bilgi İşlem Şube Müdürlüğü
2. **( )** KOM Şube Müdürlüğü

3- Eğitim Durumunuz?

1. **( )** Orta okul ve dengi
2. **( )** Lise ve dengi
3. **( )** Meslek Yüksek Okulu
4. **( )** Üniversite veya Yüksek Okul
5. **( )** Yüksek Lisans, Doktora

4- Rütbeniz?

1. **( )** Polis Memuru
2. **( )** Kom.Yrd.
3. **( )** Komiser
4. **( )** Başkomiser
5. **( )** Emniyet Amiri
6. **( )** Şube Müdürü
7. **( )** Diğer.....

5- Kaç yıldır Emniyet Teşkilatı'nda görev yapmaktasınız?

1. **( )** 1-5 yıl arası
2. **( )** 6-10 yıl arası
3. **( )** 11-15 yıl arası
4. **( )** 16-20 yıl arası
5. **( )** 21 yıl ve üzeri

6- Kaç yıldır "Bilişim Suçları" konularında görev yapmaktasınız?

1. **( )** 1-3 yıl arası
2. **( )** 4-6 yıl arası
3. **( )** 7-9 yıl arası
4. **( )** 10 yıl ve üzeri

7- Evinizde bilgisayarınız var mı?

1. **( )** Evet 2. **( )** Hayır

8- Ne kadar süredir Bilgisayar kullanmaktasınız?

1. **( )** 1-5 yıl arası
2. **( )** 6-10 yıl arası
3. **( )** 11-15 yıl arası
4. **( )** 16-20 yıl arası
5. **( )** 21 yıl ve üzeri

9- Günlük olarak Bilgisayar başında ne kadar süreyle bulunuyor sunuz?

1. **( )** 1-3 saat
2. **( )** 4-6 saat
3. **( )** 7-9 saat
4. **( )** 10 saat ve üzeri

10- Ne kadar süredir İnternet ortamını kullanmaktasınız?

1. **( )** 1-3 yıl arası
2. **( )** 4-6 yıl arası
3. **( )** 7-9 yıl arası
4. **( )** 10 yıl ve üzeri

11- Günlük olarak İnternet'e ne kadar zaman ayırıyorsunuz?

1. **( )** 1 saattaen az
2. **( )** 1-3 saat
3. **( )** 4-6 saat
4. **( )** 7 saat ve üzeri

12- Şahsınıza ait, tescilli web siteniz bulunmakta mıdır?
1. **( )** Evet 2. **( )** Hayır

13- Haberleşme aracı olarak **en çok** hangi ortamdan yararlanıyorsunuz?

1. **( )** E-mail
2. **( )** Anlık mesajlaşma sistemleri (ICQ, Messenger, IRC vb.)
3. **( )** Cep Tel
4. **( )** Diğer……

14- İnternet üzerinden alışveriş veya para transferi **(sanal bankacılık)** yapıyor musunuz?

1. **( )** Evet 2. **( )** Kısmen 3. **( )** Hayır

15- İşletim sistemlerindeki güncellemeler takip edebiliyor musunuz?
1. **( )** Evet 2. **( )** Kısmen 3. **( )** Hayır

16- İnternet ve güvenliği ile ilgili kaynakları (kitap, dergi, online ortam vs.) takip edebiliyor musunuz?

1. **( )** Evet 2. **( )** Kısmen 3. **( )** Hayır

17- En çok aşağıdaki bilişim suçlarından hangisi ile karşılaşıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz.)

1. **( )** Spam Mail
2. **( )** Virüs
3. **( )** Fishing (Aldatmaca)
4. **( )** İnternet Üzerinden Para Transferi
5. **( )** Fishing (Aldatmaca)
6. **( )** Kredi Kartı Kopyalama
7. **( )** Kredi Kartı Dolandırıcılığı
8. **( )** İnternet Yoluyla Kişilik Haklarına Saldırı
9. **( )** İnternet Üzerinden Tehdit
10. **( )** Telif Haklarının İhlali
11. **( )** Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim
12. **( )** Bilgisayar Sabotajı
13. **( )** Bilgisayar Yoluyla Dolandırıcılık
14. **( )** Bilgisayar Yoluyla Sahtecilik
15. **( )** Bilgisayar Yazılımının İzinsiz Kullanımı
16. **( )** Kopya Sayfa Dolandırıcılığı
17. **( )** Diğer……

18- Bilişim suçları ile mücadele kapsamında hangi sistemleri iyi bilmektesiniz? (Birden fazla seçenek işaretleyebilirsiniz.)

1. **( )** Firewall
2. **( )** Kripto
3. **( )** Linux
4. **( )** IP Cop, ENDIAN
5. **( )** Saldırı Tespit Sistemleri
6. **( )** Virüs Server
7. **( )** IP Tools
8. **( )** Veri Kurtarma Programları
9. **( )** Etherial (IP Trafik)
10. **( )** IP Manager (Port Açıkları Tesbiti)
11. **( )** Telnet
12. **( )** Dos Komutları
13. **( )** Diğer…….

19- Meydana gelen bir bilişim suçu karşısında yetersiz kaldığınızda, Emniyet Genel Müdürlüğü bünyesinde **öncelikle hangi birimden** teknik destek alırsınız?

1. **( )** Bilgi İşlem Daire Başkanlığı
2. **( )** Asayiş Daire Başkanlığı
3. **( )** KOM Daire Başkanlığı
4. **( )** Kriminal Polis Lab. Daire Başk.
5. **( )** İstihbarat Daire Başkanlığı
6. **( )** Diğer.....

20- Birim olarak bilişim suçlarının çözümü hususunda yetersiz kaldığınız oluyor mu?

1. **( )** Evet 2. **( )** Kısmen 3. **( )** Hayır

21- Meydana gelen bir bilişim suçu karşısında yetersiz kaldığınızda, dışarıdan yardım ve destek aldığınız kurum veya kuruluş hangisidir? (Birden fazla seçenek işaretleyebilirsiniz.)

1. **( )** Özel Firma ve Şirketler
2. **( )** Üniversite
3. **( )** Türk Telekom
4. **( )** Servis Sağlayıcılar
5. **( )** GSM Şirketleri
6. **( )** Kamu Kuruluşları
7. **( )** Diğer……

22- İl Emniyet Müdürlükleri bünyesinde bilişim suçlarıyla mücadelede, sizce **en yeterli - donanımlı** birim hangisidir?

1. **( )** Mali Şube Müdürlüğü
2. **( )** Bilgi İşlem Şube Müdürlüğü
3. **( )** KOM Şube Müdürlüğü
4. **( )** Asayiş Şube Müdürlüğü
5. **( )** İstihbarat Şube Müdürlüğü
6. **( )** Olay Yeri İnc. Şb.Md.lüğü
7. **( )** Diğer……

23- ABD ve bazı Avrupa ülkeleri gibi, Emniyet Genel Müdürlüğü bünyesinde sadece **"Bilişim Suçları"** ile mücadele eden ve konu alanı uzmanlarından oluşan bir ünite kurulması gerekli midir?

1. **( )** Evet 2. **( )** Hayır

24- İl Emniyet Müdürlükleri bünyesinde bilişim suçlarıyla mücadele eden birimlerin, bu konuda daha donanımlı hale getirilmesine gerek var mıdır?

1. **( )** Evet 2. **( )** Hayır

25- Meslek öncesi, polis eğitim kurumunda bilgisayar ve internet kullanımı ile ilgili eğitim aldınız mı?

1. **( )** Evet 2. **( )** Hayır

26- Meslek içinde, "Bilişim Suçlar ile ilgili bir **kurs** gördünüz mü?

1. **( )** Evet 2. **( )** Hayır

27- “Bilişim Suçları” ile ilgili bu güne kadar düzenlenen herhangi bir konferans veya seminere katıldınız mı?

1. **( )** Evet 2. **( )** Hayır

28- Bilişim suçları ile ilgili eğitim alma ihtiyacı hissediyor musunuz?

1. **( )** Evet 2. **( )** Hayır

29- Bilişim suçlarıyla mücadelede, sizin gelişiminizde en çok hangi faktör rol oynamıştır?

1. **( )** Bireysel çabalarım, kendi kendimi geliştirmem.
2. **( )** Kurumumun sağladığı eğitim olanakları
3. **( )** Her kendi çabalarım, hem de teşkilatın eğitim olanakları
4. **( )** Bilişim suçlarıyla ilgili konularda sürekli görev almam.
5. **( )** Diğer.....

30- Bilişim suçlarıyla mücadelede şu (3) konuda **çok iyi** olduğumu düşünüyorum.

1. ……
2. ……
3. ……

31- Bilişim suçlarıyla mücadele kapsamında özellikle şu (3) konuda **yetersiz** olduğumu düşünüyorum?

1. ……
2. ……
3. ……

32- Bilişim suçlarıyla mücadele kapsamında şu (3) konuda **yeterli** eğitim aldım.

1. ……
2. ……
3. ……

33- Bilişim suçlarıyla mücadele kapsamında özellikle şu (3) konuda **eğitim ve bilgi** almak isterim.

1. ……
2. ……
3. ……

34- Bugüne kadar (internet suçu, bilgisayar suçu, bilişim suçu) bir suç konusuyla ilgili bilirkişi olarak görev aldınız mı?

1. **( )** Evet 2. **( )** Hayır

35- Bilirkişi olarak, en çok hangi bilişim suçu konusunda görev aldınız?

1. **( )** Çocuk Pornografisi
2. **( )** Bilgisayar Yoluyla Dolandırıcılık
3. **( )** Bilgisayar Yoluyla Sahtecilik
4. **( )** İnternet Üzerinden Para Transferi
5. **( )** Kredi Kartı kopyalama
6. **( )** Diğer…….

Görev almış olduğunuz bilişim suçu araştırma olaylarından, **size en ilginç gelen bir konuyu** kısaca **<u>özetleyiniz.</u>**

……
……
……
……
……
……
……
……
……

Lütfen, bilişim suçlarıyla mücadele kapsamında belirtmek istediğiniz görüş ve önerilerinizi aşağıya yazınız. (Mevzuat, İdari Yapılanma, Teknik Ünite, Uluslararası İşbirliği vb.)

……
……
……
……
……
……
……
……
……

Lütfen, bilişim suçlarıyla mücadele edecek personelin **eğitimi** konusunda (meslek öncesi eğitim, hizmetiçi eğitim, yurtdışı eğitimi, uzmanlık eğitimi, online eğitim vb.) belirtmek istediğiniz görüş ve önerilerinizi aşağıya yazınız.

……
……
……
……
……
……
……
……
……

Lütfen, varsa "Bilişim Suçları" konusunda başkaca belirtmek istediğiniz diğer düşünce, görüş ve önerilerinizi aşağıya yazınız.

……
……
……
……
……
……
……
……
……

Nasıl Dolduracaksınız:

Açıklama: Aşağıda, bilişim suçlarına yönelik yeterlikler verilmiştir. Bunları ne düzeyde bildiğinizi ve ne düzeyde gerekli gördüğünüzü belirtiniz. Bunun için şu yolu izleyiniz.

1) "Çok İyi Biliyor" iseniz……(5)
2) "İyi Biliyor" iseniz ……....(4)
3) "Kararsız" iseniz……..…... (3)
4) "Bilmiyor" iseniz ……..….. (2)
5) "Hiç Bilmiyor" iseniz ……...(1)

1) "Çok Gerekli Görüyor" iseniz……..…(5)
2) "Gerekli Görüyor" iseniz …… ….(4)
3) "Kararsız" iseniz……..……..... .(3)
4) "Az Gerekli Görüyor" iseniz.……(2)
5) "Hiç Gerekli Değil" diyorsanız.……(1)'i

/ işareti ile seçiniz.

NOT: Kararsızım seçeneği % 50 Biliyor / Uyguluyor / Gerekli Görüyor,
% 50 Bilmiyor / Uygulamıyor / Gerekli Görmüyor anlamındadır.

Lütfen, kararsızım seçeneğini buna göre değerlendiriniz.

Örnek: Aşağıda "Bilişim Suçları" na ilişkin yeterliklerden,
1- Bilgisayar ve İnternet terimlerini,
"Çok İyi Biliyor" iseniz 5'in,
"Gerekli Görüyorsanız" 4'ün altına (*/*) işareti koyunuz.
2- Bilişim suçları terimlerini (fake, mail, spammer, stenografi, cracker vb.);
"Bilmiyorsanız" 2'nin,
ancak " Çok Gerekli Görüyorsanız" 5'in altına (*/*) işareti koyunuz.
(Altta, tablo da belirtildiği gibi)

BİLİŞİM SUÇLARINA İLİŞKİN YETERLİLİKLER	**Bilme Düzeyiniz**						**Gerekli Görme Düzeyiniz**				
	5	4	3	2	1		5	4	3	2	1
Bilgisayar ve İnternet terimlerini	/							/			
Bilişim suçları terimlerini (fake, mail, spammer, stenografi, cracker vb.)				/			/				

	Bilme Düzeyiniz						Gerekli Görme Düzeyiniz				
	Çok İyi Biliyorum	İyi Biliyorum	Kararsızım	Bilmiyorum	Hiç Bilmiyorum		Çok Gerekli Görüyorum	Gerekli Görüyorum	Kararsızım	Az Gerekli	Hiç Gerekli Değil
	5	**4**	**3**	**2**	**1**		**5**	**4**	**3**	**2**	**1**
1- Bilgisayar ve İnternet terimlerini											
2- Bilişim suçları terimlerini (fake, mail, spammer, stenografi, cracker vb.)											
3- Bilişim suçlarının kapsamını											
4- Bilişim suçlarının işleniş yöntemlerini											
5- Bilişim suçlarında delillendirmeyi											
6- Bilişim suçları konusunda yasal mevzuatı											
7- Bilişim suçlarıyla ilgili uluslararası hukuki düzenlemeleri											
8- Wireless güvenliğini											
9- Windows güvenliğini											
10- Ağ trafiğini analiz etmeyi											
11- TCP/IP konusunu											
12- Dinleme Sistemlerini (Sniffer)											
13- Kayıp alanlardan kurtarılmış veriler konusunu											
14- Anlık mesajlaşma sistemlerini (ICQ, Messenger,IRC)											
15- İnternet geçmisi ve firewall kayıtlarını											
16- Sistem kayıt log'larını analizi etmeyi											
17- İşletim sistemi kayıtlarını (Registry)											
18- Güvenlik duvarı sistemlerini (Firewall)											
19- Saldırı tespit sistemlerini											
20- Spamming ve Fishing (Aldatmaca) konularını											
21- Elektronik olaylara ilk müdahale yapabilmeyi											
22-E-Posta haberleşme trafiğini tespit edebilmeyi											
23- Bir bilgisayarı inceleyebilmeyi, tanımlayabilmeyi ve teknik rapor hazırlayabilmeyi											
24- Network elemanları ve cihazlarını											

25- Dosya sistemlerini (FAT, NTFS, EXT3)											
26- Kredi kartı dolandırıcılığını											
27- Saldırılardan korunmak için alınacak önlemleri											
28- Depolama aygıtlarının güvenli yedeğini almayı (İmaj Alma İşlemi)											
29- Sanal özel ağ (VPN) konusunu											
30- Güçlü password oluşturmayı											
31- Görüntü içinde metin taşımayı (Steganography)											
32- Şifreleme konusunu (Kriptoloji)											
33- Güvenlik taraması yapmayı (Security Testing)											
34- İnternet üzerinden alışveriş ve para transferi yapmayı											
35- Virus, Worm ve Spyware taramasını											
36- Linux ve Unix işletim sistemlerini											
37- Tuzak sistemler (Honey Pots) konusunu											
38- Hacking yöntemlerini											
39- KEYLOGGER konusunu											
40-Güvenlik tarama sonuçlarını raporlayıp, yorumlayabilmeyi											
41- Bilgisayarlardaki port'lar konusunu (Sanal Kapılar)											
42- Silinmiş bir veriyi kurtarabilmeyi											
43- Bir veriyi iz bırakmadan silebilmeyi											
44- Sistemin çalışması için gerekli temel donanım bilgisini											
45- Uzaktan erişim ve yönetim sistemlerini											
46- Kurulmuş bir network'ün yazılım ve donanım bileşenlerini raporlayabilmeyi											
47-PARDUS açık kaynak kodlu işletim sistemini											

EK-9 Bilişim Suçları Öğretim Programı Temel Seviyede Personel Yetiştirme Kursu Programı

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 1

MODÜLÜN ADI:	Bilişim Temel Terminolojisi (Bilgisayar, Bilişim ve İnternet'in Tanımları ve İlgili Kavramlar, Bilişim Aygıtları)
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Bilişim ile ilgili temel terimlerin tanımlarını yapabilir, 2. Bilişim aygıtlarını resimleriyle ve özellikleriyle tanır.
İÇERİK:	1.1. Bilgisayar'ın Tanımı, Temel Parçaları, Çevre Birimleri ve İlgili Terimler a. Bilgisayar ve Bilgisayarın temel parçaları (İşlemci, Harddisk, Kartlar, Network, İletişim, Elektronik veri) b. Bilgisayar çevre birimleri (Yazıcılar, USB cihazlar, Elektronik kartlar, CD, DVD yazıcılar, Dönüştürücüler, Programlar, Network donanımları) 1.2. İnternet'in Tanımı, İnternet Dünyasının Öğeleri, Özellikleri ve İlgili Terimler 1.3. Bilişim'in Tanımı ve Temel Bilişim Aygıtları a- Bilgisayar Sistemleri (Kullanıcı Tarafından Oluşturulan Dosyalar, Kullanıcı-Korumalı Dosyalar), b- Masaüstü ve Laptop Bilgisayarlar (Kapalı Durumda ve Açık Durumda Bulunan Bilgisayar Ekipmanları Üzerinde Yapılacak Elektronik Keşif, Nelere El Konulması Gerekir?) c- Bileşenler (Merkezi İşlem Birimi, Hafıza), d- Erişim Kontrol Araçları (Akıllı Kartlar, Konektörler, Biyometrik Tarayıcılar, Telesekreterler, Dijital

	Kameralar), e- Avuçiçi Aygıtlar (Elektronik Ajanda - PDA), f- Sabit Sürücüler, g- Bellek Kartları, h- Modemler, j- Ağ Bileşenleri (LAN/NIC Kartı, Routers, Hubs, Switches, Sunucular, Ağ Kabloları ve Konnektörler, Çağrı Cihazları, Yazıcılar, Taşınabilir Depolama Araçları ve Aygıtları (Flash Disk, CD-DVD-Disket, Sim Kart, Hafıza Kartı), Tarayıcılar, Telefonlar, Cep Telefonları), k- Çeşitli Elektronik Öğeler (Fotokopi Makineleri, Kredi Kartı Okuyucuları, Dijital Saatler, Faks Makineleri), l- Küresel Konum Sistemleri, m- Suçta Kullanılan Öğelerden Bazıları: Decoder-Encoder, Manyetik Şeritli Kart, Kredi Kartı-Banka Kartı, Slip-Dekont, Pinpad & Skimmer
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 2

MODÜLÜN ADI:	Suç, Bilişim Suçları, Bilişim Suçluları ve Mağdurları
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Bilişim ile ilgili temel terimlerin tanımlarını yapabilir, 2. Bilişim aygıtlarını resimleriyle ve özellikleriyle tanır. 3. Suç ve bilişim suçları ile ilgili kavramların tanımlarını yapabilir, 4. Bilişim suçlarının sınıflandırılması hakkında bilgi sahibi olur, 5. Bilişim suçluları ve mağdurları ile ilgili özelliklerin neler olduklarını bilir, bu suçların işlenme nedenleri ve önlenmesi için yapılması gerekli olan unsurları tanır, 6. Bilişim suçlarında başarı ve çözüm için rol üstlenen ilgili kurum ve kuruluşları tanır.
İÇERİK:	2.1. Suç Nedir? 2.2. Bilişim Suçları (Siber Suçlar, İnternet Suçları, Sanal Suçlar, Teknoloji Suçları, Bilgisayar Suçları), Tanımı, İlgili Terimler, Sınıflandırılması, Bilgisayarların Suçta Kullanımı (Suçun Unsuru Olarak Bilgisayar, Suçun Aracı Olarak Bilgisayar) 2.2. Bilişim Suçlarının Gelişimi ve Ortak Özellikleri, Bilişim Suçlarının İşlenme Nedenleri ve Önlenmesi İçin Yapılması Gerekenler? • Bilişim Suçlarının Gelişimi • Bilişim Suçlarının Ortak Özellikleri • Bilişim Suçlarının İşlenme

	Nedenleri • Bilişim Suçlarının Önlenmesi İçin Yapılması Gerekenler 2.3. Bilişim Suçluları ve Mağdurları • Suçlu Tipleri, Genel Özellikleri • Bilişim Suçlularının Suç İşleme Nedenleri • Mağdurların Genel Özellikleri 2.4. Bilişim Suçlarında Başarı ve Çözüm İçin İlgili Kurum ve Kuruluşlar, Servis Sağlayıcılar, Bankalar, Yer Sağlayıcılar, Microsoft, Telekom, Adliye, Emniyet TİB, MYNET, BKM vd.
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 3

MODÜLÜN ADI:	Bilişim Dünyasında Güvenliğin (Security) Ana Esasları
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Bilişim dünyasında güvenliğin ana esasları hakkında bilgi edinir, 2. Güvenliğin temellerini öğrenir, temel güvenlik prosedürleri hakkında bilgi sahibi olur, 3. Masaüstü güvenlik, windows güvenliği, İnternet erişim güvenliği hakkında bilgi sahibi olur, 4. Güvenlik tehditleri ve saldırılarının neler olduğu ve zararlı yazılımlar hakkında bilgi sahibi olur, 5. İnternet'te çalışma sistemi ve işleyişini kavrar, 6. Online ödeme sistemleri ve Incident Response hakkında bilgi sahibi olur.
İÇERİK:	3.1. Güvenliğin Temelleri • Temel Terminoloji • Güvenliğin Tanımı • Güvenlik için gerekenler • Güçlü Güvenlik Nasıl Olur? • Güvenlik Mitleri • Bilgi Güvenliği (Bilgi güvenliği ve bilgi güvenliği standartları, Örnek bilgi güvenliği yapılandırması, Vekil sunucular ve içerik filtreleme, Sistem kayıtlarının hukuka uygun olarak

	tutulması ve saklanması) 3.2. Temel Güvenlik Prosedürleri • Benim Bilgisayarımın Güvenliğinden Niçin Endişe Etmeliyim? • İşletim Sistemini Güçlendirme • Sistemi Güncelleştirme ve Güncellemenin Yapılandırması • Gereksiz Servislerin Kapatılması • Güçlü Şifre Oluşturulması (Şifre Seçimi ve Güvenliği) • Antivirüs ve Firewall'ın Kurulması • Kullanım hakkı verilmiş kullanıcıların erişimlerini kapatma • "Make Private" folders (kişiye özel dizin. Ağ ortamında paylaşım yapan diğer kullanıcıların erişemeyecekleri kişisel dizin). • MS Ofis Uygulamalarında Güvenlik Ayarları 3.3. Masaüstü Güvenlik • Dosya Paylaşımı Nedir? • Dosya Paylaşımının Tipleri • Dosya Paylaşımı Nasıl Yapılır? • Dosya Paylaşım İzinleri Yapılandırması • Gizli Dosya ve Klasörler • Dosya Paylaşım Tavsiyeleri • Dosya İndirme Tavsiyeleri • Yedek Veri ve Restoresi Nasıl Yapılır?

	• Dosyaların Şifrelenmesi ve Şifrenin Açılması Nasıl Yapılır? • Şüpheli İşlemler Nasıl Yok Edilir? 3.4. Windows Güvenliği • Olay Gösterici (event viewer) Nasıl Kullanılır? • Windows'ta Denetleyici Nasıl Çalıştırılır? • Sisteminizdeki Log'ları Nasıl Okursunuz? • Portlar Nasıl Kapatılır? • Windows Registry'nin (sistem kütüğü) • Gözden Geçirilmesi • Registry Nasıl Restore Edilir? • Dahili Komutlar • Portları ve Servisleri Nasıl Bulurum? 3.5. Güvenlik Tehditleri ve Saldırılar, Zararlı Yazılımlar • Phishing ve Koruyucu Önlemler • Trojan Horse • Worms • Spyware • Adware • Keylogger • Sosyal Mühendislik • Telefon çevirici (Dialer), • Denial of Service • Spamming • Port Scanning (Port Tarama) • Password Cracking (Parola Kırma) • Temel Güvenlik Önlemleri • Virüs

	Virüslerin Tarihsel Gelişimi Nasıl Bulaşır ve Yayılır? Virüs Çeşitleri Virüs Bulaşan Bilgisayarlarda Karşılaşılan Bazı Problemler Virüsten Korunma Yolları ve Öneriler Kişisel Olarak Virüslerden ve Bilişim Suçlarından Nasıl Korunulabilir? Kurumsal Olarak Virüslerden ve Bilişim Suçlarından Nasıl Korunulabilir? Virüslerin Finansal Etkileri 3.6. İnternet Erişim Güvenliği • Temel Güvenlik Ayarları Tarayıcısı • Site Erişimleri Nasıl Kısıtlanır? • Güvenli Bölgeden Site Silinmesi • Güvenli Website Algılaması • Güvenli Site ve Tarayıcı Özellikleri • Araçlar: Internet Filtreleme Yazılımı • İnternet Kullanım Hakkı İçeriğinin • Yapılandırılması • İçerik Haber Vericinin Aktive Edilmesi • Cookies'ler ile Nasıl Baş Edilir? • Uygun Tarayıcı Ayarlarının Seçimi • Kablosuz Network Güvenliği Özellikleri 3.7. İnternet'te Çalışma Sistemi ve İşleyiş • Güvenliğin Temel Prensipleri • Şifrelemenin Bilinmesi • Dijital Sertifika • Dijital İmza • e-mail ile çalışma (web ortamı)

	• e-mail ile çalışma (mail client) • File Transfer ile çalışma (FTP) • File Transfer ile çalışma (Web Folders) 3.8. Online Ödeme Sistemleri • Kredi Kartı İle Çalışma • Instant Messengers (Anlık İleti) İle Çalışma, Anlık Mesajlaşma Sistemleri (ICQ, MSN Messenger, Yahoo Messenger, Google Talk, IRC, Forum vb.) • Dosya Paylaşımlı Network'lerde Çalışma (Working across File sharing Networks • Taşınabilir Aygıtlar İle Çalışma • Dial-in Networklerde Çalışma • Wireless Aygıtlarla Çalışma • USB Aygıtlarla Çalışma • Media Dosyalarıyla Çalışma • Grup Yazılımla Çalışma 3.9. Incident Response • Incident Response Nedir? • Incidents and Responses • Trojan Saldırıları • Boot Sector Virüs Saldırıları • Bozulmuş Registry • CD-ROM'UN otomatik çalışması (autorun.inf)
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 4

MODÜLÜN ADI:	Bilgisayar Ağlarında (Network) Güvenliğinin Sağlanması
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Network Elemanları ve Cihazlarını tanır, 2. LAN ve WAN Teknolojileri hakkında bilgi edinir, 3. OSI İletişim Katmanları ve bu katmanlara göre güvenliğin nasıl sağlandığı ve Kullanıcı-Sunucu bilgisayarların güvenliğinin nasıl sağlandığı hakkında bilgi sahibi olur.
İÇERİK:	4.1. Network Elemanları ve Cihazları, LAN ve WAN Teknolojileri 4.2. OSI İletişim Katmanları ve Bu Katmanlara Göre Güvenlik • Fiziksel Altyapı Güvenliği (Donanım Güvenliği, Fiziksel Katman Güvenliği) • Data Link Katmanında Güvenlik • Network ve Transport Katmanında Güvenlik (Firewall, IDS -Intrudion Detection systems-, VPN - Virtual Private Network, Anti Spam, Honeypot - Bal Peteği) 4.3. Kullanıcı ve Sunucu Bilgisayarların Güvenliğinin Sağlanması
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 5

MODÜLÜN ADI:	Ülkemizde Sık Karşılaşılan Bilişim Suçları, Örnek Olaylar, İdari Yapılanma ve İlgili İstatistikler, Uluslar arası Platformda ve Bazı Ülkelerde Bilişim Suçları
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Ülkemizde sık karşılaşılan bilişim suçları konusunda bilgi sahibi olur, 2. Bu suçları örnek olaylarla ve istatistikler ile açıklayabilir, 3. Emniyet Teşkilatındaki bilişim suçlarındaki idari yapı hakkında bilgi sahibi olur, 4. Uluslar arası platformda bilişim suçları konusunda yapılan çalışmalar ile Avrupa Konseyi Siber Suç Sözleşmesi hakkında bilgi sahibi olur.
İÇERİK:	5.1. Ülkemizde Sık Karşılaşılan Bilişim Suçları • İnteraktif Banka Dolandırıcılığı • Kredi Kartı Dolandırıcılığı • ATM Dolandırıcılığı • Hacking • Çocuk pornografisi, • Bilgi hırsızlığı, sistemlere izinsiz erisim ve telif haklarının ihlali • Mali Konular • Organize Konular • Narkotik Konular 5.2. Bilişim Suçlarından Örnek Olaylar

	5.3. Bilişim Suçlarında Emniyet Teşkilatı İçerisindeki İdari Yapılanma Bilişim Suçlarıyla Mücadelede Daire Başkanlıkları ve TADOC, SASEM, 5.4. Ülkemizde İşlenen Bilişim Suçlarının İstatistikleri 5.5. Uluslar arası Platformda ve Bazı Ülkelerde Bilişim Suçları Konusunda Yapılan Çalışmalar ve İlgili İstatistikler ▪ AB Bünyesinde Bilişim Suçları Konusunda Yapılan Çalışmalar ▪ Ekonomik İşbirliği Ve Gelişme Teşkilatı (OECD) Bünyesinde Bilişim Suçları Konusunda Yapılan Çalışmalar ▪ Birleşmiş Milletler Bünyesinde Bilişim Suçları Konusunda Yapılan Çalışmalar ▪ Avrupa Konseyi Bünyesinde Bilişim Suçları Konusunda Yapılan Çalışmalar ▪ Avrupa Konseyi Siber Suç Sözleşmesi ▪ G8 Bünyesinde Bilişim Suçları Konusunda Yapılan Çalışmalar ▪ Bilişim Suçları ve Bazı Ülkelerde Yapılan Çalışmalar (Amerika Birleşik Devletleri, İsrail, Fransa, İtalya) 5.6. Bazı Ülkelerde Bilişim Suçları Konusundaki İstatistikler 5.7. Avrupa Konseyi Siber Suç Sözleşmesi
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 6

MODÜLÜN ADI:	Bilişim Suçlarının Çözümünde Temel Unsurlar ve Uygulamalar
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. IP Adresi, IP Sorgusu, Whois Uygulamaları (Kim Sorgusu) gibi uygulamaları gerçekleştirebilir, 2. Erişim Sağlayıcılar, Domain, Network hakkında genel bilgi sahibi olur.
İÇERİK:	• Bilgisayar Donanım ve Yazılımları • DOS komutları • Dosya isimleri ve Dosya sistemleri (FAT, NTFS, EXT3) • İşletim Sistemleri ve Güvenliği (Windows, Unix, Linux, Pardus) • Yazılım Güvenliği, Wireless Güvenliği, Web Güvenliği ve Mail Güvenliği • IP Adresi, IP Sorgusu, Erişim Sağlayıcılar • Domain, Network Whois Uygulamaları (Kim Sorgusu) • Gerçek Zaman Tespiti • BIOS kontrolü (Tarih, saat önemi, BIOS fonksiyonlar) • E-posta ve Header • Facebook

	• BOTNET • Veri saklama medya türleri (Manyetik, Optik, Silikon) • Phising Ailesi (Phising, Pharming, Smishing, Vishing) • İnternet Geçmisi, İnternet Aktiviteleri ve Geçici Yedekleme Dosyaları • Uzaktan Erişim ve yönetim sistemleri • Ağ trafiği analizi ve Posta haberleşme trafiği • TCP/IP konusu • KEYLOGGER • SQL • Güvenlik taraması yapma (Security Testing) • Dinleme Sistemleri (Sniffer) • Saldırı Tespit Sistemleri (Saldırılardan korunmak için alınacak önlemler, Saldırıların Sıklıkları, Tipleri, Kaynakları) • Görüntü içinde metin taşıma (Steganography) • Veri Kurtarma (Data Recovery and Analysis) • Siber Terör
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10
MODÜL NO: 7

MODÜLÜN ADI:	Bilişim ve Hukuk, Türk Hukuk Sistemi'nde Bilişim Suçlarında İlgili Mevzuat
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Hukuk sisteminde bilişim alanında suçların neler olduğunu kavrar, 2. Bilişimle İlgili Yasalarla Belirlenen Sorumluluklar ve Bilişim Suçlarında İlgili Mevzuat hakkında genel bilgi sahibi olur.
İÇERİK:	7.1. Türk Hukuku ve Bilişim Suçları 7.2. Polis ve Bilişim Hukuku 7.3. Ülkemizde Bilişim Suçları İle İlgili Hususlardaki Mevzuatlar (Türk Ceza Kanunu, Yönetmelik vb.) Hukuk'ta Bilişim Alanında Suçlar Nelerdir? 7.4. Yasalarda Yer Alan Bilişimle İlgili Kavramlar (Bilişim Sistemi, Veri, bilgi, enformasyon, kişisel veri, sır, ticari sır, İnternet, internet ortamı, yayın, internet ortamından yapılan yayın, İçerik sağlayıcı, Erişim, Erişim sağlayıcı, Toplu kullanım sağlayıcı, Yer sağlayıcı, Trafik bilgisi, Elektronik imza) 7.5. Bilişimle İlgili Yasalarla Belirlenen Sorumluluklar • Bilgilendirme yükümlülüğü • İçerik sağlayıcının sorumluluğu • Yer sağlayıcının yükümlülükleri • Erişim sağlayıcının yükümlülükleri • Toplu kullanım sağlayıcıların yükümlülükleri

	7.6. Kişisel Verilerin Korunması • E-posta hesapları ve teknik denetim • Özel hayatın gizliliğine giren durumlar • Kullanıcı ile yapılması gereken sözleşmeler • Hukuken kaydedilmesi gereken veriler (Trafik Verileri, Kullanım Verileri) • Sistem yedeklemesi ve kişisel veriler • Hukuka uygun veri saklama yöntemleri 7.7. İçerik ile ilgili suçlar ve hukuki yaptırımlar (Kişisel ve Kurumsal internet sayfaları, Bloglar, Bağlantı (link) vermek, İçeriği farklı bir çerçevede göstermek (Framing), Forum vb yapılarda içerik denetimi ve hukuki sorumluluk, İçerik nedeniyle verilen cezalar, Fikir ve Sanat eserlerine ilişkin esaslar) 7.8. İnternet üzerinden sözleşme kabul edilmesi • İnternet üzerinden sözleşme yapmak • E-imza almak ve kullanmak için gerekli teknik ve hukuki şartlar 7.9. Fikri Sınai Haklar (Telif hakkı Nedir? Tescili mümkün müdür? Veritabanlarının korunması söz konusu mu? İhlal olursa ne yapmalıyım? Yazılım lisansları ve lisans sözleşmeleri 7.10. Marka, Patent, Faydalı Model, Endüstriyel Tasarım ve Entegre Devre Topoğrafyaları (Nedir, Nasıl alınır? Neden alınmalıdır? Nerelerde geçerlidir?)
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 8

MODÜLÜN ADI:	Bilişim Yoluyla İşlenen Asayiş Suçları (B.Y.İ.A.) ve Soruşturma Şekilleri
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Bilişim Yoluyla İşlenen Asayiş Suçlarından (B.Y.İ.A.) olan, Kontür ve Kredi Kartı Dolandırıcılığı, Sanal Ortamda Dolandırıcılık işlemlerinin nasıl gerçekleştirildiğini kavrar, 2. Çocuk Pornografisi, Fuhuş, Kumar, Şantaj, Tehdit ve Hakaret Suçları gibi Bilişim Yoluyla İşlenen diğer Asayiş Suçları (B.Y.İ.A.) ve Soruşturma Şekilleri hakkında uygulamalı eğitimle genel bilgi sahibi olur.
İÇERİK:	8.1. Kontür ve Kredi Kartı Dolandırıcılığı, 8.2. Çocuk Pornografisi, 8.3. Sanal Ortamda Dolandırıcılık, Fuhuş, Kumar, Şantaj, Tehdit ve Hakaret Suçları
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10

MODÜL NO: 9

MODÜLÜN ADI:	Suç Öncesi Polisin Bilişim Suçlarıyla Mücadelesi
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Polisin Bilişim Suçlarıyla Mücadelesinde Suç Öncesi yapması gerekenler hakkında genel bilgi sahibi olur.
İÇERİK:	9.1. Bilişim Suçlarıyla Mücadelede Suç Önleme Anlayışı (Önleyici Hekimlik Modeli) 9.2. Toplum Destekli Polislik Faaliyetleri Kapsamında Bilişim Suçları Farkındalık Eğitimi Toplum Destekli Polislik Faaliyetleri ve MEB ile İşbirliğiyle Okullar Bazında Bilişim Suçları Farkındalık Eğitimi 9.3. Polisin Suç Öncesinde Bilişim Suçlarıyla Mücadelede Yapması Gerekenler • İhtiyaç Duyulan Nitelikte Personel Temin Etmek • Uygulamalı Bilişim Suçları Eğitimi ile

	Elektronik olaylara ilk müdahale Yapabilmek ve Bilişim Suçları Araştırma ve Soruşturmasını Öğrenmek, • Konuyla İlgili Kaynak Araştırmak • Polis Personeline Yeterli Eğitim (Sertifikasyon), Donanım ve Ünite Sağlamak • Bilişim Suçlarıyla Mücadelede Teşkilat Genelinde Farkındalık Eğitimleri 9.4. Bilişim Suçlarıyla Mücadelede Bazı Öneriler ve Alınabilecek Tedbirler • E-mail Adresine Tehdit ve Taciz İçerikle Mesaj Gönderildiğinde Nereye Müracaat Edilmelidir? • Kredi Kartı Kullanırken Dikkat Edilecek Hususlar? • Çocukların İnternet'te Zararlı Sitelere Girememeleri İçin Neler Yapılabilir? 9.5. Bilişim Suçlarıyla Etkin Mücadelede Ortak Paydada Yapılması Gerekenler ○ STK İşbirliği ile Bilişim Farkındalığını Geliştirmek ○ Ülkede Bilişim Etiği'nin Benimsenmesi ○ İnternet Kullanım Etiği ○ İnternet'te Başkalarına Karşı Saygı ○ İnternet'te Altyapı ve Zamanı Verimli Kullanma ○ İnternet'te Biçimsel Özen ○ İnternet'te İçerik İle İlgili Özen ○ İnternet'te Öteki Konular ○ HEM aracılığıyla Kurumlarda Çalışan

	Bilgisayar Operatörlerinin Eğitimleri o Bilgi İşlem Birimlerinin Etkinliklerinin Arttırılması ve Güvenlik o İnternet Servis Sağlayıcıları ve Cep Telefonu Servislerinin Yükümlülükleri o Bilişim Suçları ve İnternet Kafeler, İnternet Kafe İşletmecilerinin Sorumlulukları o İnternet Kafe Mantığında İnternet Kullanımının Olduğu Üniversiteler, Kamu Kurumları Ve Diğer Kuruluşlar o Banka Sistem Görevlilerinin Sorumlulukları
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
TEMEL SEVİYEDE PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 90 saat
Toplam Modül Sayısı: 10
MODÜL NO: 10

MODÜLÜN ADI:	Bilişim Suçları İle Mücadelede Karşılaşılan Hukuki, Uluslar arası, Teknik, İdari, Altyapı, Eğitim ve Farkındalık Sorunları ve Çözüm Önerileri
SÜRESİ:	6 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; Bilişim Suçları İle Mücadelede Karşılaşılan hukuki, uluslar arası, teknik, İdari, Altyapı, Eğitim ve Farkındalık Sorunları ile ilgili olarak genel bilgi sahibi olur ve gerekli çözüm yolları hakkında fikir sahibi olur.
İÇERİK:	Bilişim Suçları İle Mücadelede Hukuki Sorunlar Bilişim Suçları İle Mücadelede Uluslararası İşbirliği Sorunları Bilişim Suçları İle Mücadelede Teknik Sorunlar Bilişim Suçları İle Mücadelede İdari Sorunlar Bilişim Suçları İle Mücadelede Alt yapı Sorunları Bilişim Suçları İle Mücadelede Eğitim Sorunları Bilişim Suçları İle Mücadelede Farkındalık Sorunları Bilişim Suçları İle Mücadelede Sorunlara Çözüm Önerileri
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

EK-10 Bilişim Suçları Öğretim Programı Uzman Seviyede Personel Yetiştirme Kursu Programı

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı: 10

MODÜL NO: 1

MODÜLÜN ADI:	Suç, Bilişim Suçu, Adli Bilişim
SÜRESİ:	60 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Suç, Bilişim Suçu ve Adli Bilişimin ne olduğunu bilir ve neleri kapsadığı hakkında bilgi sahibi olur.
İÇERİK:	1.1 Suç, Bilişim Suçu ve Adli Bilişimin Tanımı 1.2 Bu suçlar neleri kapsar?
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 2

MODÜLÜN ADI:	Adli Bilişim Süreci ve Adli Bilişim İnceleme Yöntemleri
SÜRESİ:	60 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; Adli bilişim süreci ve Adli bilişim inceleme yöntemleri (eşzamanlı inceleme, eşzamansız inceleme) hakkında bilgi sahibi olur.
İÇERİK:	2.1 Adli bilişim süreci 2.2 Adli bilişim inceleme yöntemleri • eşzamanlı inceleme • eşzamansız inceleme
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı: 10

MODÜL NO: 3

MODÜLÜN ADI:	Bilişim Suçlarında Olay Yeri İncelemesi
SÜRESİ:	60 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Olay yeri incelemesinde amacın ne olduğunu ve bu incelemenin hukuki boyutunu kavrar, 2. Olay yeri incelemesi yürütülürken dikkat edilmesi gereken ana prensipler hakkında bilgi sahibi olur, 3. Olay yeri inceleme uzmanlarının genellikle karşılaştığı durumları öğrenir, 4. Olay yeri incelemesinde sık yapılan yanlışlar hakkında bilgi sahibi olur.
İÇERİK:	3.1 Olay yeri inceleme uzmanlarının genellikle karşılaştığı durumlar ve olay yeri incelemesinde sık yapılan yanlışlar 3.2 Olay Yeri İncelemesinin Hukuki Boyutu 3.3 Olay yeri incelemesinde amaç 3.4 Olay yeri incelemesi yürütülürken dikkat edilmesi gereken ana prensipler
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 4

MODÜLÜN ADI:	Bilişim Suçu Delilleri
SÜRESİ:	60 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Bilişim Suçu Delillerinin Neler olduğunu kavrar, 2. Elektronik deliller ile dijital delillerin özellikleri hakkında bilgi sahibi olur.
İÇERİK:	4.1 Kaça Ayrılır? Tanımları (Elektronik deliller, dijital deliller) 4.2. Elektronik delillerin, diğer delillerle ortak ve farklı özellikleri 4.3 Dijital delillerin yapısal özellikleri 4.4. Elektronik delillerin özellikleri
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 5

MODÜLÜN ADI:	Olay Yeri İncelemesinin Uygulama Yöntemi
SÜRESİ:	60 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Olay yerlerinde rastlanabilecek muhtemel bilişim delilleri hakkında bilgi sahibi olur, 2. Delillere uygulanacak prosedürlerin neler olduğunu öğrenir, 3. Delillerin data inceleme laboratuarına sevkinde dikkat edilecek hususlar hakkında bilgi sahibi olur. 4. Delillerin nasıl korunması gerektiğini öğrenir.
İÇERİK:	5.1 Olay yerlerinde rastlanabilecek muhtemel bilişim delilleri 5.2 Olay yerinde rastlanılması durumunda delillere uygulanacak prosedürler • Olay yerinde rastlanılan bilgisayarın kapalı olması durumunda • Olay yerinde rastlanılan bilgisayarın açık olması durumunda 5.3 Delillerin data inceleme laboratuarına sevkinde dikkat edilecek hususlar (Bilgisayar Kasası, Ekran, Sabit Disk, Disket ve Kaset, El Bilgisayarı, Klavye, Fare ve Kablolar, Piller) 5.4. Parmak izi alınacak delillerin korunması
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda

	yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 6

İSMİ	Bilişim Suçlarında Laboratuvar İncelemeleri
SÜRESİ	60 Saat
AMACI	Bu modülün sonunda eğitime katılan personel; 1. Dijital Sistemler ve Sayı Sistemler hakkında bilgi sahibi olur.
İÇERİĞİ	6.1. Dijital Sistemler • Adli Bilişimde Fiziksel Medya İncelemesi Sabit disk ve RAM • Veri Analiz Süreci • Dosya Sistemleri 6.2. Sayı Sistemleri
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 7

MODÜLÜN ADI:	Adli Bilişim Ekspertiz Raporu
SÜRESİ:	60 Saat
GENEL AMAÇ:	Bu modülün sonunda eğitime katılan personel; 1. Bilişim Suçlarında Laboratuvar İncelemelerinde dikkat edilmesi gereken hususları kavrar, 2. Adli Bilişim Ekspertiz Raporu Yazma aşamalarını öğrenir.
İÇERİK:	7.1 Adli Bilişim Ekspertiz Raporu Yazmak • Ekspertiz raporu hangi bilgileri kapsamalıdır? • Ekspertiz raporu hazırlama safhaları • Veri toplamak • Sonuçları analiz etmek • Raporu taslak haline getirmek ve organize etmek • Oluşturulan rapor hangi bölümleri içermelidir • Rapora Son halini vermek • Raporun Son halini kontrol etmek
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 8

İSMİ	Adli bilişim alanında kullanılan gereçler (Yazılımlar, Donanımlar)
SÜRESİ	60 Saat
AMACI	Bu modülün sonunda eğitime katılan personel; Adli bilişim alanında kullanılan yazılımlar ve donanımlar hakkında bilgi sahibi olur, yazılımların nasıl kullanıldığını öğrenir.
İÇERİĞİ	8.1 Adli Bilişimde Kullanılan Yazılımlar (Encase, Encase İle İmaj Alma İşlemi ve İlgili Diğer Komutlar, Anahtar kelime araştırması, dd yazılımı ve nasıl kullanıldığı) 8.2 Adli Bilişimde Kullanılan Donanımlar (Yazma-Koruma Sistemleri (Writeblocker), Sabit Diskler, Sabit Disk İmaj Alma Yöntemi)
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 9

İSMİ	Örnek Olay Çalışması ve Analizi
SÜRESİ	60 Saat
AMACI	Bu modülün sonunda eğitime katılan personel; Görsel olarak Örnek Olay Çalışması ve Analizinin nasıl gerçekleştiğini öğrenmiş olur.
İÇERİĞİ	Örnek Olay Çalışması ve Analizi
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

BİLİŞİM SUÇLARI ÖĞRETİM PROGRAMI
UZMAN PERSONEL YETİŞTİRME KURSU PROGRAMI

Toplam Kurs Süresi: 5 Ay
Toplam Modül Sayısı:10

MODÜL NO: 10

İSMİ	Encase İle Delil İnceleme
SÜRESİ	60 Saat
AMACI	Bu modülün sonunda eğitime katılan personel; Encase programı ile delil inceleme konusunu uygulamalı eğitimle öğrenmiş olur.
İÇERİĞİ	1. ENCASE KAVRAMLARI a. Delil Dosyası (Evidence File) b. Case Dosyası (Case File) c. Backup Dosyası (Backup File) d. Konfigürasyon Dosyaları (Configuration Files) 2. CASE İŞLEMLERİ a. Case Açma b. Case Kaydetme 3. ENCASE v.4 AYARLARI 4. EKRAN BÖLÜMLERİ a. Sağ Bölümdeki Sütunlar b. Rapor (Report) c. Galeri (Gallery) d. Zaman Doğrusu (Timeline) e. Alt Bölümdeki Özellikler f. Case Görünümünde Araç Çubuğu g. Menü Çubuğu 5. İMAJ ALMA a. İmaj Alma Türleri Fiziksel RAID (RAID kartı mevcut) a. Fiziksel Arıza yok ise Boot CD/Disket; Drive-to-Drive Boot CD/Disket; Drive-to-USB (Encase 4.20 >=)

	İşlem Bilgisayarı (Windows); Encase-Local Drive İşlem Bilgisayarı (Windows)-5.25" USB kutu; Encase-Local Drive, Encase, Ilook XImager, FTK Imager b. Fiziksel Arıza var ise İşlem Bilgisayarı (Windows); dd, r-studio, restorer 2000 b. PDA Cihazlarında İmaj Alma c. Cep Telefonlarında İmaj Alma d. Delil Dosyalarının Case Dosyasına Eklenmesi 6. ÖN İNCELEME 7. BOOKMARK İŞLEMLERİ 8. HARİCİ PROGRAM TANIMALAMALARI 9. KOPYALAMA SEÇENEKLERİ a. Copy/Unerase (kopyala/geri al) b. Copy Folders c. Export (Dışa Aktarma) 10. ENSCRIPT KÜTÜPHANESİ 11. WINDOWS SİSTEM İNCELEME AŞAMALARI a. Mevcut Dosya Araması b. Silinmiş Dosya ve Klasör Araması c. Unallocated Alandan Dosya Araması d. Basit Arama (Kelime Araması) e. Detaylı Arama (GREP) f. Internet işlemleri g. Link dosyaları h. Print Spool Dosyaları i. Registry İncelemesi j. Dosya İmzaları ve Analizi k. Hash Kütüphanesi ve Analizi l. Recycle Bin (Geri Dönüşüm Kutusu) Kurtarma m. Swap Dosyası n. Unused Disk Area o. Windows Açılışında Otomatik Çalışan Programlar ve Kurulu Programların İncelenmesi p. Hidden Partitions (Saklanmış Bölümler) q. Recent Links r. Sistemdeki Cihazlar Hakkında Bilgi (USB, USB ID, vb.) 12. İNCELEME RAPORU HAZIRLANMASI 13. ADLİ BİLİŞİM PROGRAMLARI a. Delil Toplama ve Muhafaza Programları (Evidence Collection and Preservation Tools)

	b. Delil Çıkartma Programları (Evidence Extraction Tools) c. Delil İnceleme Programları (Evidence Examination Tools) d. Delil Organize Etme Programları (Evidence Organization Tools) ENCASE v.4 SEMBOLLERİ
YÖNTEM	Anlatım, Soru Cevap, Gösteri Yöntemleri
DEĞERLENDİRME	Bu modülde katılımcının başarısı modül sonunda yapılacak bir test ile belirlenecektir.

Özgeçmiş

Çetin GÜMÜŞ. 01.01.1972‘de Gerede’de doğdum. 1989’da Ankara Yenimahalle Teknik Lisesi’nden, 1993’te Polis Akademisi’nden mezun oldum. Sırasıyla EGM Bilgi İşlem Daire Başkanlığı (6 yıl), Elazığ Emniyet Müdürlüğü (6 yıl) ve Kocaeli Emniyet Müdürlüğü’nde (3 yıl) farklı birimlerde (Bilgi İşlem Şube Müdürlüğü, Saraybahçe Polis Merkez Amirliği, Toplum Destekli Polislik Büro Amirliği, Rehberlik ve Danışma Büro Amirliği, Eğitim Şube Müdürlüğü) çalıştım. 1999 yılında Fırat Üniversitesi Sosyal Bilimler Enstitüsü Eğitim Bilimleri Ana Bilim Dalında yüksek lisans çalışmasına başladım. İnternet Kafeler konusunda, yurt genelinde gerçekleştirdiğim Yüksek Lisans çalışması kapsamında, çeşitli bildiriler tebliğ ettim. İnternet kafeler ve eğitim bilimleri alanında polis dergisinde ve çeşitli hakemli dergilerde yayınlanmış makalelerim bulunmaktadır. Evli ve iki çocuk babasıyım.