ÜLKEMİZDE ADLİ BİLİŞİM LABORATUARI KURULUMU ve BİLİŞİM SUÇLARIYLA MÜCADELEYE KATKILARI

İlker ÇİÇEK, Ali OKATAN
Haliç Üniversitesi
ilker_cicek@hotmail.com, aokatan@halic.edu.tr

ABSTRACT

This paper is a call for building a standardized and certificated computer forensics laboratory that has become vital with the rapid development of information technology which affects the whole part of our lives and provide crime opportunities even the ones that have only basic knowledge about computers. In this scope our country's legislations and the technical problems on the application side against the computer crime is examined. In comparison with developed countries' application method in the fight against computer crime committed towards individual and government, computer forensics is still in its early stages in Turkey. Certified computer forensics mechanism and certified specialists are needed. The struggle against computer crime can't be enough if it is only used in legal side. Hence, this study can be the basis to cultivate computer forensic capabilities, building a certificated laboratory, and establishing an internationally valid computer crime mechanism in our country. In this way, law enforcement will get more help from our laboratory. Also the laboratory enhances the ability of Turkey's computer forensic professionals and provides more convincing digital evidence in court. Furthermore, it can fortify national information security systems and the e-government environment.

Key words: computer forensic, cyber laboratory, computer crime

1. GİRİŞ

Modern hayatın kritik sektörleri olan enerji, ulaşım, iletişim, bankacılık, sağlık hizmetleri ve benzeri kamu hizmetlerinde, verimlilik ve etkinliğin arttırılması amacıyla bilgi sistemleri teknolojilerine olan bağımlılık gün geçtikçe artmaktadır. Ancak gelişen teknolojinin suçlular tarafından da kullanılmasıyla, söz konusu sektörler risk altına girmiştir. Dolayısıyla, dünyada güvenlik güçleri enerjilerini, klasik suçlardan çok bu konulara yönlendirmiş, kamu güvenliği ve ulusal güvenlikte öncelikli tehdit olarak bilişim suçları kavramı yer almaya başlamıştır[1]. Bu doğrultuda mahkemelerde dijital deliller büyük önem kazanmıştır[2].

Bilişim suçları kavramı, son yıllarda ülkemizde de gündeme gelmeye başlamıştır. Bu konuda yasal mevzuatın güncellenmesine rağmen, hukuki süreci destekleyecek teknik altyapı konusunda yeterli çalışma eş zamanlı olarak yapılamamıştır.

Bilişim suçları ile mücadele, sadece kolluk kuvvetiyle değil; kamu kurumları ile özel kurumlar ve üniversitelerle işbirliği içerisinde yapılması gereken kapsamlı bir çalışmadır.

Bu noktada, siber çağın yöntemleriyle gerçekleştirilen suçların tespiti ve kanıtlanması sürecinde; yasal düzenlemeler ile uyumlu, standartları belirlenmiş, akredite uzman personeli olan, uluslararası sertifikalara sahip ve üniversitelerle işbirliği içerisindeki adli bilişim laboratuarlarının kurulması önem arz etmektedir.

Bu amaçla, bu çalışmada, bilişim suçları sürecinin hukuki, uygulama ve teknik alanındaki sorunları ortaya konmuş; konuyla ilgili literatürdeki uluslararası çalışmalar incelenerek, adli bilişim laboratuarlarının kurulumu için çeşitli öneriler getirilmiştir.

2. ÜLKEMİZDE BİLİŞİM SUÇLARI KAVRAMI VE İLGİLİ MEVZUAT İLE ADLİ BİLİŞİMİN İLİŞKİSİ:

Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması, "Bilişim suçları[1]" olarak tanımlanmaktadır[3]. Ayrıca ülkemizde, uygulamada bu sistemlerin sadece araç olarak kullanıldığı, geleneksel suçlar olarak tabir edilen tipleri de "Bilişim Sistemleri aracılığı ile işlenen Suçlar[2]" olarak isimlendirilmektedir. 26 Eylül 2004

[1] Bilişim Suçları: TCK Md.158/1-f – Nitelikli Dolandırıcılık, TCK Md.243/1, 243/2, 243/3– Bilişim Sistemine Girme, TCK Md.244/1, 244/2, 244/3, 244/4 – Sistemi Engelleme, bozma, verileri yok etme veya değiştirme, TCK Md.245/1, 245/2 – Banka ve Kredi kartlarının kötüye kullanılması, TCK Md.239/1, Md.239/2, Md.239/3 – Ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması, TCK Md. 327, Md. 328, Md. 329, Md. - Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgiler, TCK Md. 135 - Verilerin kaydedilmesi, TCK Md. 138 - Verilerin yok edilmesi, TCK Md. 132 - Haberleşmenin gizliliğini ihlal, TCK Md. 124 - Haberleşmenin engellenmesi maddelerinde yer alan hususlardır.

[2] Bilişim Sistemleri aracı kılınarak işlenen suçlar: TCK Md. 125 - Hakaret, TCK Md. 142 - Bilişim sisteminin kullanılması

tarihinde kabul edilen, 5237 sayılı Türk Ceza Kanunu kapsamında, Bilişim Suçları ile ilgili yeni hükümler getirilmiştir. Buna ek olarak, bilişim suçları ile mücadeledeki zorlukları aşmak amacıyla yeni TCK sonrasında ve 2007 yılı içerisinde de düzenlemeler yapılmıştır. Örneğin 01 Haziran 2005 tarihli Resmi Gazete'de yayınlanan Suç Eşyası Yönetmeliği Madde 9'da, el konulan bilgisayar malzemelerinin nasıl saklanması gerektiği anlatılmaktadır. Ayrıca, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (23 Mayıs 2007), İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik(1 Kasım 2007), İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik(30 Kasım 2007) yürürlülüğe giren diğer düzenlemelerdir.

Bu düzenlemeler, ülkemizde yeni bir kavram olan bilişim suçları konusunda, hukuki alanda yapılan ve yapılacak olan çalışmaların göstergesidir.

Burada bahsedilen yasal düzenlemeler ve yaygınlaşan e-devlet uygulamalarının beraberinde getirdiği riskler nedeniyle; yargı organlarının, bilişim suçlarının tespit edilmesi, incelenmesi, araştırılması ve mahkemede delil olabilecek şekilde hazırlanmasını konu edinen bir bilim dalı olan Adli Bilişime ilgi ve ihtiyacı zorunlu olarak artmıştır.

Ancak mevzuattaki yasal düzenlemeler, artan ihtiyacı karşılamakta yetersiz kalmaktadır. Örneğin, CMUK Madde 134[3], bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemleri ile ilgili bazı düzenlemeler getirilmiş; Adli ve Önleme Aramaları Yönetmeliği Madde 17 ise, el koyma işlemini bilgisayar ağları, uzaktaki bilgisayarlar ve çıkarılabilir donanımlar için de geçerli kılmaktadır. Ancak bu maddelere ek olarak, inceleme yapan şahıs ya da birimin uygulayacağı teknikler veya sunacağı rapor konusunda standartları belirleyen düzenlemelere de ihtiyaç vardır.

Savcılar veya mahkemeler, CMUK Üçüncü Kısım İkinci Bölümde yer alan maddelere göre bilirkişi atamakta ve cihazlarda delil aranması işlemini; polis, jandarma adli bilişim laboratuarları, "İl Adlî Yargı Adalet Komisyonları bilirkişi Listeleri" nde yer alan kişi ya da kurumlara veya CMUK madde 64 2. Fıkrasında verilen yetkiyle, o konuda uzman bir başkasına yaptırabilmektedirler. Kısacası adli bilişim laboratuarları ve bilirkişi tayininde savcı veya mahkemeler geniş yetkilere sahiptir. Ancak bu yetkiyle birlikte bilirkişi ya da kurumlarda ulusal veya uluslararası sertifika aranması zorunluluğu getirilmelidir.

Yukarıda bahsedilen konular nedeniyle, uygulamanın delil incelemesi aşamasında birçok problemle karşılaşılmaktadır.

3. ADLİ BİLİŞİM SÜRECİNDE TEKNİK ALANDA KARŞILAŞILAN PROBLEMLER:

a) Bilindiği üzere, suç mahallinin incelemesi uzmanlık gerektirir ve bilişim suçları konusunda dikkat edilmesi gereken özel konular vardır[4]. Ülkemizde delillere el koyma sürecinde görevlendirilen nitelikli personel sayısında, yeterli seviyeye halen ulaşılamamıştır. Dolayısıyla bu durum, bilişim suçunun failinin bulunmasında etkin sonuçlar alınamamasına sebep olmaktadır[5]. İşlemler yapılırken nelere dikkat edileceği hususu ile standartlar ve sorumluluklar henüz herhangi bir mevzuatta net olarak belirtilmemiştir. Sonuç olarak uygulamada birçok delil, daha en başta geri dönülmeyecek şekilde kaybolabilmektedir.

Son zamanlarda mevcut problemlerin çözümü için kolluk kuvvetlerinde çeşitli çalışmalar yapılmaktadır. Örneğin, Emniyet Genel Müdürlüğünde, bilişim suçlarıyla ilgili delil tespitleri ve kovuşturma, İstanbul[4], Ankara ve İzmir'de Bilişim Suçları ve Sistemleri Şube Müdürlükleri tarafından, diğer illerde aslen bilgisayar ve ağ sistemlerini işletmekle görevli,

yoluyla hırsızlık, TCK Md. 158 - Bilişim sistemi yoluyla dolandırıcılık, TCK Md. 226 - Müstehcenlik, TCK Md. 228 – Kumar, TCK Md. 107 – Şantaj, TCK Md. 28 - Cebir şiddet, korkutma ve tehdit, TCK Md. 103 - Çocukların cinsel istismarı, TCK Md. 191 - Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma maddeleri ile Fikir ve Sanat eserleri kanununda belirtilen hususlardır.

[3] **Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama ve Elkoyma**

Madde 134 - (1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

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

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

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

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

[4] Bilişim Suçları ve Sistemleri Şube Müdürlüğü 03.09.2007 tarihinde Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına bağlı olarak, İstanbul Emniyet Müdürlüğü bünyesinde faaliyete geçirilmiştir. http://bilisimsuclari.iem.gov.tr/

Bilgi İşlem Bürolarınca yürütülmektedir. Jandarma Genel Komutanlığı'nda ise; şuan ülkemizdeki uluslararası standartlara en yakın laboratuar, Kriminal Daire Başkanlığı bünyesinde Bilişim Teknolojileri İnceleme Şube Müdürlüğü adı altında açılarak, 15 Eylül 2007 tarihinden itibaren aktif olarak, cep telefonu, sabit disk, SIM kart, multimedya kart ve çeşitli veri kartlarını inceleme konularında hizmet vermektedir. Ayrıca birimde görevli bilişim uzmanları tarafından, Olay Yeri İnceleme Timlerine, bilişim suçlarında olay yeri incelenmesi, delillere el konulması ve muhafazası konusunda eğitim verilmektedir.

b) Bilgisayar veya ağ sistemlerinin incelenmesinde hâkim ya da savcıların geniş yetkilere sahip olmasına rağmen, teknik anlamda yeterli bilgiye sahip olmamaları ve onları bu konuda yönlendirecek standartların bulunmaması nedeniyle, zaman zaman ehliyet sahibi olmayan kişileri bilirkişi olarak atadıkları görülmektedir[6].

c) Ülkemizde bilişim suçları konusunda BT(bilişim teknolojileri) uzmanlarına danışılmaktadır. Ancak dijital delillerin, mahkeme esnasında gerçek delil özelliği gösterebilmesi için delillerin bütünlüğünün, doğrulanmasının, inkâr edilememesinin, doğruluğunun ve daha sonradan ele alınabilirliğinin sağlanması gereklidir[7]. Bu nedenle konunun uzmanlarına ihtiyaç vardır.

d) Uygulamada kamu bilişim laboratuarları olayların çok az bir kısmında inceleme yapmaktadır[8]. Bu oranın düşük olmasının nedeni, yeterli laboratuar olmaması ve bilirkişi seçiminde savcı veya hâkimlerin bilirkişileri atarken tercihlerini o doğrultuda kullanmamasıdır.

e) Dava ile ilgilenen hâkim/savcı, raporun sonuç bölümüne bakarak karar vermektedir. Mahkemede davacı ve hükümlülerin rapora bir itirazı olduğunda yeniden inceleme için bilirkişi ya da kriminal laboratuarlarına gönderilmektedir. Bu raporu düzenleyen şahıs ya da kurumlarda, ulusal ya da uluslararası herhangi bir standart aranmaması veya tescilli kurumsal bir yapılaşmaya gidilmemesi nedeniyle yeterli inceleme yapılıp yapılmadığı ve delil bütünlüğünün bozulup bozulmadığı konusu net değildir.

f) Bilirkişiler siber suç ile ilgili delilleri tespit ederken herhangi bir standart izlememekte ve birçoğu lisanssız program kullanmaktadır. Ortaya konulan raporda da yine belirli bir format yoktur. Mevcut uygulama uluslararası mahkemelerde tazminat ödenmesine yol açabilir. Her ne kadar rapor hazırlanırken lisanssız program kullanmanın, ülkemizdeki hukukçular tarafından başka bir suç oluşturduğuna kanaat edilmiş olsa da; teknik olarak lisanssız programın incelenen sistem üzerinde delil niteliğini bozacak işlemler yapması mümkündür. Uluslararası mahkemeler rapor hazırlanırken uygulanan süreçteki standartları ve programın lisansını da göz önünde bulundurmaktadır[8].

g) Amerika'da bilişim suçları konusunda kimi özel programların kullanımı için belirli kişilere akreditasyon verilmiştir. Dolayısıyla sadece lisanslı program kullanmak değil; o programı kullanabilecek ehliyete sahip personeli yetiştirmek de gereklidir.

h) Cihazlar öncelikle yerinde incelenir ve bunun yeterli olmadığı durumlarda özel aparatlar ile yedeği alınarak bu yedekler üzerinde inceleme yapılır. Bunun ilk sebebi çalışma esnasında gerek delillerde, gerekse kişisel bilgilerde bir bozulmaya yol açmamaktır. İkincisi ise, bir itiraz gerçekleştiği zaman o dönemdeki imajdan yeniden değerlendirme yapılmasıdır. Mevzuatımızda bazı eksikliklerle birlikte konu ile ilgili hükümler bulunmasına rağmen, bunların kimi zaman uygulanmadığı görülmüştür.

i) Delil inceleme süreci için mahremiyeti ve insan haklarını koruyucu düzenlemeler yapılmıştır; ancak toplum bu konuda yeteri kadar bilgilendirilmediği ve mevzuattaki hükümler, bu noktada da tam olarak uygulanmadığı için, bilişim suçuyla karşılaşan birçok firma, özel bilgilerini korumak amacıyla şikâyetçi olmamaktadır.

4. ADLİ BİLİŞİM LABORATUAR LARININ KURULUMU VE İŞLEYİŞ PROSEDÜRLERİ

Bilişim suçları konusundaki problemler süreçteki; hukuki, uygulama ve teknik boyut arasındaki koordinasyon eksikliğinden kaynaklanmaktadır. Hukuk ve kolluk tarafındakiler yeterli teknik bilgiye sahip değildir. Suçla, günümüzde ve gelecekte daha etkin mücadele edebilmek için daha iyi teşkilatlanma ve teknik altyapı gereklidir. Delillendirmeyi, faile ulaşmayı, diğer bir ifadeyle fiil ile fail arasındaki bağlantıyı sağlayacak standartlara sahip, Adli Bilişim laboratuarları kurulmadığı sürece, sadece yasalar ile sonuca ulaşmanın mümkün olamayacağı bilinen bir gerçektir[6].

4.1. ADLİ BİLİŞİM LABRATUARI KURULUM BASAMAKLARI

1) Adli bilişim laboratuarının temel yeteneklerinin tespiti:

a. Adli bilişim laboratuarının yapısı, fonksiyonları ve her birimin kullandığı özel teknikler ile ilgili bilgiler elde edilmeli, ülkemizdeki ve yurtdışındaki birimlerin incelenmesi ve buralarda eğitim alınması ile adli bilişim esaslarının kavranması sağlanmalıdır.

b. Adli bilişim sadece teknik açıdan düşünülmemeli, yönetim, planlama ve finansal açıdan da gerekli çalışmalar yapılmalıdır. Adli bilişim laboratuarlarının ülke çapında nerelerde kurulması gerektiğine ait etüt yapılmalı, bölgedeki gelişmişlik oranı, siber suçların işlenme oranı ve ivmesi hesaplanarak laboratuarın gerekliliği ve teçhizatı belirlenmelidir. Örneğin çok pahalı olan elektron mikroskobu sadece Ankara'daki merkez laboratuar için temin edilirken, adli bilişimi ilgilendiren, yılda 3-4 olayla karşılaşıldığı birkaç ilden oluşan bir bölgeye sadece bir adet mobil adli bilişim dijital veri platformu temin edilerek gerekli destek verilebilir.

c. Öncelikle lisanslı adli bilişim programlarının temin edilip eğitimleri alınmalı, uzmanların farklı adli bilişim programlarına hâkim olması sağlanmalıdır.

d. Çalışma ortamı standartları belirlenerek birime uygun donanım temin edilmelidir.

e. Bu konudaki bir diğer önemli nokta dijital delile uygun prosedürlerin oluşturulmasıdır. Delil kabulden inceleme ve rapor formatına kadar, detaylı talimat ve formlar hazırlanarak tutarlılık sağlanmalıdır.

2) Bilişim Suçlarının Tespiti Konusundaki Mekanizmanın Güçlendirilmesi:

a. Bilgi güvenliği konularında tepki mekanizması ve acil durum yönetimi oluşturulmalıdır. Bu konuda bir problem meydana geldiğinde, problemi çözüp bilgiyi kullanılabilir halde tutacak temel ve uygulanabilir planlar yapılmalıdır.

b. Bilişim suçlarının tespitini desteklemek amacıyla, ağ yönetimi, analizi ve paket incelenmesi konularında çalışılmalı, suç aktiviteleri kayıt altına alınmalıdır.

c. Veri güvenliği amacıyla veri savunma mekanizmaları oluşturulmalıdır.

d. Endüstri, akademi, araştırma merkezleri, konuyla ilgili askeri birimler arasında koordinasyon sağlanarak ağ teknolojilerindeki gelişmeler ve etkilerinin anlaşılması, bu konudaki yeni teknoloji ve donanımların tespiti ve ulusal adli bilişim teknolojilerinin geliştirilmesi alanındaki çalışılmalar hızlandırılmalıdır.

3) Suçu önleme amaçlı yapılması gerekenler:

Bir kolluk kuvvetinin başarısı; tespit ettiği suç miktarıyla değil, meydana gelmeden önledikleri ile ölçülür. Bu bağlamda siber suçlarla mücadelede özel birimler oluşturulmalıdır. Örneğin Almanya'da kritik bilgi sistemlerine toplumun artan bağımlığına bağlı olarak, Alt Yapı Çalışma Grubu(AKSIS) ve erken uyarı amaçlı bilgisayar güvenliği olay müdahale birimleri[5] gibi özel birimler kurulmuştur[9]. Gelişmiş ülkelerde bu tip birimlerin aktif bir şekilde görev yaptığı görülürken ülkemizde bu alanda etkin bir birim kurulmamıştır. Bu konuda yapılması gerekenler şu şekilde sıralanabilir:

a. Adli Bilişim laboratuarının akredite edilmesi; kaliteli raporların hazırlanmasını ve bunların kamu tarafından onaylanmasını sağlayacaktır. Akreditasyonda faydalanılabilecek standartlar; ISO/IEC Rehber 46 (Tüketim Mallarının ve Bunlarla İlgili Hizmetlerin Karşılaştırmalı Olarak Denenmesi- Genel Presipler), TS EN ISO/IEC 17025:2005(Deney ve Kalibrasyon Laboratuarlarının Yeterliliği İçin Genel Şartlar), ISO/IEC Rehber 58(Kalibrasyon ve Test Laboratuarları Akreditasyon Sistemleri), TS ISO/IEC 15408 (Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Teknolojisi (IT) Güvenliği için Değerlendirme Kriterleri), RFC3227 2002 (Delil Toplama ve Arşivleme Kılavuzu) olarak sıralanabilir[10]. Örneğin Adli bilişim laboratuarlarının ISO17025 adaptasyonu olmadığı takdirde dijital delil inceleme gibi çok kritik bir alanda merkezi otorite oluşturulana kadar minimum rehberlik ile ve muhtemelen yavaş işleyiş riskleriyle karşı karşıya kalınacaktır[11].

b. Tatbikatlar ile saldırı meydana geldiğinde yapılacak işlemler simule edilmelidir. Örneğin Almanya'da 2001 yılının Kasım ayında AKSIS, Münih yakınlarındaki Ottobrunn'da Siber Terör Uygulaması (CYTEX) gerçekleştirmiştir. Çeşitli federal bakanlıklardan gelen temsilciler ile endüstri ve kamu yönetimi alanında çalışanların da iştirakiyle gerçekleştirilen bu uygulamayla, Berlin'deki çeşitli kamu ve özel sektör bilişim sistemlerine yönelik şantaj maksatlı yapılan çeşitli saldırı senaryoları oluşturulmuştur[12].

c. Bilgi güvenliği ve adli bilişim eğitimi verilebilecek birim oluşturulmalıdır. Bilgi güvenliği konusunda kamu, özel kurumalar ve üniversitelerin dikkati çekilmeli, bilişim suçlarında tepki mekanizmalarının yetenekleri dolayısıyla bilgi güvenliği seviyesi arttırılmalıdır.

d. Adli bilişim sempozyumları düzenlenmeli; adli bilişim alanında uzman personel eğitilmelidir. Bu uzmanlar, uluslararası koordinasyon sağlanarak uluslararası anti terörist ağ araştırmalarına katılmalıdır[1].

e. Tüm yönleriyle mevcut hacker aktiviteleri, birbirleriyle ilişkileri ve alakalı oldukları organizasyonlar tespit edilmelidir. Böylece hem

[5] CERT-Bw-Silahlı Kuvvetlere, RUSCERT-Araştırma Geliştirmeye, mCERT ufak çaplı işyerlerine yönelik, Almanya'da hizmet veren olay yeri müdahale birimlerdir.

onların karakteristikleri ve teknikleri hem de hedeflerine ait kanun uygulayıcılarının soruşturmalarda faydalanabileceği bir veritabanı oluşturulmalıdır[1].

f. Suç önleme amacıyla internet, düzensiz bir şekilde taranmalıdır.

g. Bilişim suçları ile daha etkili mücadele edebilmek için şüpheli ve zaman kaybı yaratacak bilgi kanallarının da tespiti yapılmalıdır.

h. Sistemin en iyi testi ona saldırmakla mümkündür. Çeşitli bankaların güvenlik birimlerinin yaptığı gibi Türkiye'deki kamu, askeri ve istek dâhilinde özel kurumların güvenlik sistemlerine saldırarak açıkları tespit edilmelidir. Bu sayede bilgi güvenliği seviyesi arttırılarak, suçludan önce kullanacağı teknik belirlenmeli, uygun savunma teknikleri geliştirilmelidir.

4.2. Üniversitelerin Sürece Katkıları:

a. Her geçen gün hızla gelişen bilgi sistemleri teknolojilerinde, güvenlik başlı başına uzmanlık gerektiren bir konu olmuştur. Dolayısıyla ülkemizin gelecekte bu ihtiyacını karşılamaya yönelik bir mühendislik bölümü açılmalıdır.

b. Adli Bilişim Laboratuarları için Ulusal Standartlar tespit edilmelidir.

c. Daha verimli çalışma sağlamak amacıyla farklı tipteki dijital delile uygun, farklı inceleme süreçleri modellenmeli, her basamakta görevli olan kişi ya da birimlerin yetenekleri ve sorumlulukları belirlenmelidir.

d. Dijital delil arama sürecinde yasal yöntemler tespit edilmelidir. Böylece gelecekte hem yurt içindeki hem de uluslar arası davalarda ülkemizi tazminat ödemeye zorlayacak ya da şahısları mağdur edecek uygulamalar engellenecektir.

e. Ulusal Mobil adli bilişim dijital delil platformları tasarlanmalıdır. Amerika'da da örneğini görebileceğimiz, bir çanta büyüklüğündeki bu cihaz üzerindeki yazılım ve donanım ile farklı platformlara adapte olabilmeli, veri bütünlüğünü sağlamalı ayrıca, dijital delillere kaynak teşkil edebilmesi nedeniyle mobil telefonlar, PDA cihazları, akıllı kartlar gibi gömülü bilgisayar sistemlerine de uyumlu olmalıdır[13].

f. Şifrelenmiş veriler üzerinde dijital delilleri yakalamaya yönelik algoritmalar geliştirilmeye çalışılmalıdır.

g. Ağ üzerinde tarama yapan sniffer (ağ yoklayıcısı) cihazları araştırılmalıdır. Özellikle büyük verileri yakalayabilmeli ve ağda eş zamanlı olarak çalışmalıdır.

h. Pasif ağ kayıt sistemleri ile suç incelemelerinde kullanılmak üzere, ticari ve finansal işlemler ile ilgili kayıtlar tutulmalıdır[1].

i. Dijital delillerin şifrelenmiş olabileceği göz önünde bulundurularak, dağıtık bilgisayar sistemleri ile şifre kırma teknikleri üzerine araştırmalar yapılmalıdır.

j. Süreci daha verimli hale getirmek amacıyla, veri madenciliği ve etkili mücadele için yapay zekâ uygulama çalışmaları yapılmalıdır.

k. Suçları önleme amacıyla, yeni nesil kullanıcı ve öğreticilerinin bilişim suçları konusunda daha bilinçli olması sağlanmalıdır. Özellikle geleceğin nesillerini yetiştirecek eğitim fakülteleri olmak üzere, tüm fakültelerin müfredatında yer alan bilgisayar dersi içeriğine bilgi güvenliği konusu eklenmelidir.

l. Hukuk fakültelerinde konu ile ilgili çalışmalar yapılmalıdır[6]. Bilmesi gereken prensibine göre bilişim suçları konusunda gelecekte karar verecek personelin, teknik anlamda da bilgi sahibi olması sağlanmalıdır.

4.3. KOORDİNASYON

E-devlet uygulamalarının yaygınlaşmasıyla; resmi, özel tüm kurumları tehdit eden bilgi güvenliği riski de artmaktadır. Örneğin, e-devlet uygulamalarının yaygın olduğu ABD'den sonra ikinci devlet konumunda olan Estonya, 2007 Nisan sonunda büyük çaplı bir siber taarruza maruz kalmış ve saldırı nedeniyle birçok devlet dairesi ve finans grubu kapatılmış ve ülkede hayat durmuştur.

E-devlet uygulamaların hızla tüm kamusal alanda yaygınlaştığı ülkemizde de bilgi güvenliği açısından gerekli çalışmalar yapılmalıdır. Saldırıya maruz kalabilecek birimler, önleyici birimler, suçu takip edecek birimler, teknik desteği sağlayacak birimler ile ARGE faaliyetleri yürütecek birimlerin nitelik ve sorumlulukları belirlenmelidir. Bu noktada standartları belirleyecek ve aradaki koordinasyonu sağlayacak üst düzey bir birim oluşturmalıdır.

Koordinasyon, ulusal bazda değil internetin sınırlarına bağlı olarak uluslararası boyutta da yürütülmelidir.

Adli bilişim laboratuarlarının kurulumu, yukarıdaki birimler ile koordinasyon sağlandığı takdirde ihtiyaçları en iyi şekilde karşılayacak yapıya kavuşacaktır.

[6] İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi 06.01.2004'de kurularak bu konuda faaliyet gösteren ilk ve tek enstitü olmuştur.

5. SONUÇ

Adli Bilişim laboratuarının kurulumu ile adalete, kişisel hak ve özgürlükleri koruyarak uluslararası geçerliliği olan desteğin verilmesi amaçlanmaktır. Ancak bu alandaki çalışmaların etki ve sonuçları sadece bununla sınırlı değildir.

Çalışmalar, ulusal ağ ve bilgi güvenliği konularına ilgiyi arttıracak, hızla gelişen bilişim teknolojilerinin araştırılarak adli bilişim yeteneğine katkıda bulunmasını sağlayacaktır. Bununla beraber, adli bilişim teknolojisinin geliştirilmesi amacıyla üniversite, kamu kurum ve kuruluşları, BT sektörü ile konuyla ilgili uluslararası kuruluşlar arasında işbirliği, bilgi ve tecrübe paylaşımı sağlanacaktır.

Bu iş birliği kapsamında, resmi ve özel kurumları, bilgi ve ağ güvenliği konusunda destekleyecek, eksiklikleri tespit edecek ve sürekli olarak önlemlerin alınmasını sağlayacak bir birim meydana getirilmiş olacaktır.

Bir sonraki adımda, adli bilişim sürecinde, ulusal donanım ve yazılımların geliştirilmesine yönelik çalışmalar hızlandırılarak, maddi kazanç elde edilmesinin yanında kazanılan tecrübelerin yabancı değil yerli sistemlerin geliştirilmesinde kullanılması sağlanacaktır.

Ayrıca gelişmiş ülkelerde olduğu gibi, ülkemizde de adli bilişim ihtiyacının akredite özel laboratuarlar tarafından karşılanması teşvik edilecektir.

Ülkemizde yukarıda bahsedilen özelliklere sahip uluslararası standartlarda kurulacak özel ve resmi Adli Bilişim laboratuarları ülkemizdeki ihtiyacı karşılamanın yanında, gelişmekte olan ülkelerdeki kamu ve finans alanında da birçok kuruma hizmet verebilecektir.

KAYNAKLAR

[1] So-Lin Yen, Sou-Chan Chen,The Study on Planning and Building a Cyber Forensic Laboratory in MJIB, Taiwan, IEEE 2006

[2] M. MEYERS and M. ROGERS, The Need for Standardization and Certification, International Journal of Digital Evidence, Fall 2004

[3]PERRY, R.L. 1986. Computer Crime. New York: Franklin Watts.

[4]UZUNAY Y.,2. Dijital Delil Araştırma Süreci, Polis Bilişim Sempozyumu, Nisan 2005, Ankara

[5]ÖZDEMİR M., Bilişim Suçları Ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler Ve Çözüm Önerileri,10.01.2008,http://www.caginpolisi.com.tr/24/43-44-45-46.htm

[6]ÖZEL C.,AHİ M.G.,Bilişim Suçları'nda Usul Ve Sorumluluk Sistemi Üzerine Öneriler 2005.7.4, 15.01.2008 http: //www.turkhukuksitesi .com

[7] CHET Hosmer, "Proving the Integrity of Digital Evidence with Time", International Journal of Digital Evidence, Spring 2002

[8] DEMİRBİLEK Mesut, Emekli Emniyet Md., Citigroup Güvenlik ve Araştırma Servisi Müdürü, Görüşme 10.01.2008

[9] ŞEHİTOĞLU, Onur, Bilgisayar ve ağ üzerinden işlenen siber suçlarla mücadelenin hukuksal ve güvenlik boyutu, Kara Harp Okulu Komutanlığı, Savunma Bilimleri Enstitüsü, 2005 Ankara

[10] PATRICK S.Chen,Ying-Chieh Chen,Standardizing the Construction of a Digital Forensics Laboratory,IEEE 2005

[11] WILSDON T., SLAY J., Digital Forensics: Exploring Validation, Verification & Certification, Enterprise Security Management Laboratory School of Computer & Information Science University of South Australia

[12] BRUNO, Stefano. "CIIP Country Surveys", WENGER, A.ve J. METZGER (Ed.), CIIP Handbook An Inventory of in Eight Countries Critical Information Infrastructure Protection, 2002.

[13] UZUNAY Y., KOÇAK M., "Bilişim Suçları Kapsamında Dijital Deliller", AB'05 Akademik Bilişim Konferansı, Gaziantep, Şubat 2005