Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri

G. Şengül, F. K. Atsan, ve A. Bostan

***Özet*—Adli olayların sayısal sistemler üzerinde incelenmesi ve delillendirilmesi süreçlerini kapsayan adli bilişim, bilişim hukuku alt alanına yardımcı bir disiplindir. Adli bilişim kapsamında sayısal sistemler üzerinde inceleme yapmak ve delil araştırmak oldukça karmaşık teknik bilgiye hâkim olmayı gerektirmekte ve aynı zamanda bu sistemlerdeki veri ve kayıtların çok büyük boyutlarda olması nedeni ile bu süreçler çok zahmetli ve zaman alıcı olabilmektedir. Hiç şüphesiz adli bilişim incelemesi kendine özel cihaz, sistem ve yazılımlara ihtiyaç duymaktadır. Bu alanda teknik inceleme yapan şahıslar da adli bilişim uzmanı/bilirkişisi olarak adlandırılmaktadır. Bu çalışmada ulusal ve uluslararası düzeyde adli bilişim ile ilgili durum tespiti yapılmış, alandaki problemler ve çözüm önerileri sunulmuş ve adli bilişimle ilgili gelecek öngörüleri vurgulanmıştır.**

***Anahtar Kelimeler*—Adli bilişim, sertifikasyon, araçlar, adli bilişim uzmanı**

I. Giriş

Sayısal ortamlar ve bilgi sistemleri kullanımı toplumsal hayat ve iş dünyasının vazgeçilmezi haline gelmiştir. İnsan yaşantısının ve etkileşimlerinin sayısallaşması ile sayısal ortamlardaki bir kısım olay ve etkileşimler de hukuki anlamda suç kabul edilmeye başlamıştır. Bu alanda ilk adli uygulamalara dünya genelinde 1970 sonlarında rastlanırken [1] ülkemizde bu kapsama girebilecek ilk uygulamalara 1990'lı yıllardan sonra rastlanmaktadır [2]. Sayısal ortamlarda gerçekleştirilen bazı eylemlerin suç kabul edilmesi ise, sayısal delil kavramını da beraberinde getirmiştir. Zira bu ortamlarda gerçekleştirilen eylemlerin iz ve kayıtları yine bu ortamlarda bulunmaktadır. Buna ek olarak, gelişen sayısal cihaz kullanımı ile daha önceden sayısal olmayan birçok bilgi ve kayıt sayısal hale gelmiş ve dolayısı ile bu bilgiler adli olay incelemelerinde kullanılmaya başlamıştır. Örneğin bir kişi veya aracın belirli zamanlarda nerede bulunduğunun göstergesi olarak cep telefonu veya GPS cihazının sistem üzerindeki kayıtları kullanılabilmektedir.

Gelişen teknoloji sayesinde, daha ekonomik ve daha yüksek performanslı sayısal sistemlerin izleme ve güvenlik amaçları ile kullanılması da sürekli artış göstermektedir. Bu tür cihaz ve sistemlerde de delil araştırması ve olay incelemesi için sayısal teknik bilgiye ihtiyaç duyulmaktadır. Gönümüzde kayıt yapan sayısal güvenlik kamera sistemlerine hemen hemen her yerde rastlamak mümkündür.

Toplum yaşamını inkâr edilemez şekilde değiştiren sayısal sistemler, aynı zamanda suç işlenmesini ve delil yok edilmesi/karartılmasını da daha kolay hale getirmiştir. Artık başkalarına ait cihaz, sistem ve bilginin kullanılması, alınıp-satılması veya bozulması-kullanılmaz hale getirilmesi için çoğu kez aynı fiziki ortamda bulunmaya veya fiziki temasa gerek duyulmamaktadır. Coğrafi ve fiziki engeller suçun engellenmesinde etkisiz kalmaktadır. Ayrıca sayısal teknoloji ile sayısal sistemler üzerinde adli delil olarak kullanılabilecek iz ve bilgileri de değiştirmek veya yok etmek daha kolay hale gelmiştir.

Sayısal sistemler üzerinde delil ve adli olay incelemesi yapabilmek özel bilgi ve tecrübe gerektirmektedir. Bu alanda adli süreçlere yardımcı olacak ve bilirkişilik yapacak personelin bilgisayar ve sayısal sistemler konusunda yeterli teknik bilgiye sahip olmasının yanında, temel hukuk ve adli olay araştırma prensiplerine de hâkim olması beklenmektedir.

Bu araştırmada, adli bilişim araştırmalarının Türkiye ve dünyadaki genel durumu hakkında özet bilgi verilmekte, sorun ve problemler ortaya konarak çözüm önerileri sunulmaktadır.

II. Adli Bilişimin Tanımı ve Mevcut Durum

A. Adli Bilişimin Tanımı ve Adli Bilşim Uzmanlığı

Adli olayların sayısal sistemler üzerinde incelenmesi ve delillendirilmesi süreçlerini kapsayan adli bilişim, bilişim hukuku alt alanına yardımcı bir disiplindir [3]. Zira hızla gelişen, teknolojisi değişen ve her geçen gün yaygınlaşan sayısal sistem ve cihazlar aracılığı ile gerçekleştirilen suçların ve olayların incelenmesi özel teknik bilgi ve altyapıya ihtiyaç duymaktadır. Dilimizde adli bilişim olarak yaygın olarak kullanılan, bu disiplinin farklı tanımları vardır. Bu tanımlardan örnek olabilecek üç tanesi şu şekildedir.

Gökhan Şengül, Atılım Üniversitesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak çalışmaktadır; e-posta: gokhan.sengul@atilim.edu.tr).

F.K.Atsan., TÜRKSAT A.Ş. 40 km. Gölbaşı, Ankara da kıdemli güvenlik uzmanı olarak çalışmaktadır. (e-posta: fkatsan@turksat.com.tr).

Atila Bostan, Atılım Üniversitesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak çalışmaktadır; e-posta: atila.bostan@atilim.edu.tr).

1) Adli olayların aydınlatılması amacıyla, olay yerinden, dijital veri saklama ve iletme özelliğine sahip cihazların toplanması, cihazların içerisindeki dijital delillerin tespit edilmesi ve adli otoritelere dijital delillerin raporlanması süreci içerisinde yapılan çalışmaların bütünü [4]

2) Elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak hukuki delillere dönüştürülme süreci [3]

3) *Bir olayın aydınlatılmasına yönelik olarak, olayla ilgili bilgi içerebilecek bilişim cihazlarının incelenmesi* [5].

Örnek tanımlarda da görülebileceği gibi, adli bilişim kavramının hukuki yönünden daha ziyade teknik yönü daha ön plandadır. Sayısal sistemler üzerinde inceleme yapmak ve delil araştırmak oldukça karmaşık teknik bilgiye hâkim olmayı gerektirmekte ve aynı zamanda bu sistemlerdeki veri ve kayıtların çok büyük boyutlarda olması nedeni ile bu süreçler çok zahmetli ve zaman alıcı olabilmektedir. Hiç şüphesiz adli bilişim incelemesi kendine özel cihaz, sistem ve yazılımlara ihtiyaç duymaktadır. Bu alanda teknik inceleme yapan şahıslar da adli bilişim uzmanı/bilirkişisi olarak adlandırılmaktadır. Ancak İngilizce "computer forensics", "digital forensics" ve "network forensics" gibi tabirlerden tercüme ile dilimizde kullanılan adli bilişim terimi İngilizcede "forensics" kelimesinin tam karşılığını ifade etmemektedir. Zira "forensics" İngilizcede genellikle adli amaçlı olmakla birlikte, adli olsun veya olmasın, bir olayın nasıl gerçekleştiğine ilişkin tüm teknik incelemeleri kapsamaktadır [5]. Ancak Türkçede adli kelimesi doğrudan ve sadece adli işlemlerle ilgili kavramını çağrıştırır. Bu açıdan değerlendirildiğinde adli bilişim olarak ifade edilen kavramın "sayısal sistem ve cihaz incelemesi" şeklinde ifadesi daha uygun olabilir.

Adli bilişim disiplininin çalışma alanları gelişen teknoloji ve kullanım yaygınlığına bağlı olarak sürekli olarak artmakta ve kapsamı gelişmektedir. Ancak çalışma konuları ana başlıklar halinde şunlardır;

- Sistem (işletim sistemi veya uygulama) kayıtlarının incelenmesi
- Farklı sistemler arasında kayıt ilişkilendirilmesi ve olay/işlem takibi
- Veri saklama
- Veri kurtarma
- Veri dönüştürme
- Veri imha etme
- Şifreleme
- Şifre çözme
- Gizlenmiş dosya bulma

Bu işlemleri yaparken incelenen veya delil olabilecek sayısal bulgu ana balıkları ise şu şekilde listelenebilir.

- Sistem olay kayıtları
- Video görüntüleri
- Fotoğraflar
- Uygulama dosyaları (Word, Excell, Open Office vb.)
- Bilgisayar programları
- Sistem veya uygulama ayarları
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb.)
- Gizli ve şifreli dosyalar / klasörler
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son gerçekleştirilen işlem kayıtları
- İnternet ortamından indirilen dosyalar
- Silinmiş dosya/klasörler

Ana başlıkları verilen bu alanlar ve kayıtların incelenmesi becerileri sadece adli olayların incelenmesinde değil son zamanlarda bazı şirket ve şahıslar tarafından kendi iç iş süreçlerinde de yoğunlukla kullanılmaya başlamıştır. Günümüzde veri kurtarma, veri imha etme gibi hizmetler adli inceleme alanı dışındaki dünyadan da yüksek oranda talep almaktadır.

Adli bilişim inceleme süreci ise en geniş anlamda aşağıda belirtilen beş aşamada gerçekleştirilmektedir. Bu aşamalar sırası ile;

- Hazırlık
- Toplama
- İnceleme
- Çözümleme
- Raporlama

şeklinde listelenir. Ancak bazı yazarlar burada belirtilen ilk aşama olan hazırlık aşamasını bu süreç dışında tutarak bu listeyi dört aşama olarak kaleme almışlardır [6].

B. Mevzuat ve Mevcut Durum

Türkiye Cumhuriyeti hukuk mevzuatında adli bilişim ile ilgili hükümler Ceza Muhakemesi Kanun (CMK) madde. 134 ile Adli ve Önleme Aramaları Yönetmeliği'nin 17nci Maddesinde yer almaktadır. Bu iki düzenlemenin dışında adli bilişim konusunda başka bir hüküm bulunmamaktadır[3]. Ancak konu ile ilgili olarak Adalet Bakanlığı'nca hazırlanan "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları" başlıklı bir kanun tasarısı halen kanunlaşma aşamasındadır [7].

Ceza Muhakemeleri Kanunundaki düzenlemeler doğrultusunda, bilgisayar, bilgisayar programları ve bilgisayar kütüklerine inceleme yapılması amacı ile savcının talebi üzerine hâkim tarafından karar verilebilmektedir [8]. Kanun gerekli ve uygun durumlarda bu bilgilerin bir kopyasının alınarak bu kopya üzerinde inceleme yapılmasına da imkân tanımaktadır. Ancak kopya alınması durumunda alınan kopyanın bir suretinin şüpheliye veya vekiline teslimini de öngörmektedir.

Adli ve Önleme Aramaları Yönetmeliği'nin 17nci Maddesinde ise kanun tarafından düzenlenen el koyma ve kopya alma işlemlerinin kapsam ve usulleri belirlenmiştir [9]. Ayrıca yönetmelikte kanunda geçen bilgisayar, bilgisayar programları ve bilgisayar kütükleri ifadelerine ek olarak uzak bilgisayar kütükleri, bilgisayar ağları ve çıkartılabilir donanımlardan da bahsedilmektedir.

Adalet Bakanlığı tarafından düzenleme çalışmaları takip edilen "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı" özellikle adli bilişim uzmanını tanımlaması açısından önemlidir. Bu hususta kanun taslağı;

- adli bilişim uzmanı yetki belgesi olanların bilirkişilik yapabileceğini
- adli bilişim uzmanlığı ve yetki belgesine ilişkin esas ve

usullerin yönetmelikle belirleneceğini
- adli bilişim uzmanları hakkında CMK'nın bilirkişilikle ilgili hususlarının uygulanacağını

düzenlemektedir [7]. Ayrıca taslağın yürürlük maddesinde adli bilişim uzmanlığı konusundaki düzenlemelerin kanunun kabulünden iki yıl sonra yürürlüğe girmesi öngörülmektedir.

C. *Uluslararası Mevcut Durum*

Dünya genelinde ulusal sınırları aşan bir boyutta genişleyen İnternet ağı sayesinde, sayısal sistemler üzerinden işlenen bilişim suçları çok kolay uluslararası bir boyut kazanabilmektedir. Hatta uluslararası hukuki ve teknik işbirliği noksanlığından/zorluğundan faydalanan suçlular, bu tür suç oluşturan eylemlerini özellikle uluslararası bir tasarım üzerinden gerçekleştirmektedir. Suçlular kolay erişilebilir ve genellikle denetimden uzak iletişim ağından faydalanarak uluslararası katılımlı suç çeteleri, terörist gruplar ve menfaat birliktelikleri oluşturabilmektedir. Son yıllarda sayısal sistemler ve özellikle İnternet üzerinden siyasi amaçlı güvenlik saldırıları gerçekleştiren gönüllü saldırgan gruplarının miktarında da artışlar gözlenmektedir [10]. Ayrıca bu tür uluslararası sayısal saldırıların siyasal ve ekonomik kaygılarla diğer devletler tarafından organize edildiği ve düzenlendiği konusunda da çok güçlü iddia ve örnekler mevcuttur.

Adli olay incelemelerinde sistem ve olayların uluslararası boyut kazanması, inceleme süreçlerini ve metotlarını genellikle olumsuz yönde etkilemektedir. Bu alanda diğer suç türlerinde olduğu gibi adli inceleme yapma, kontrol ve yaptırım uygulama konularında uluslararası düzeyde beraberlik ve eşgüdümü sağlayacak antlaşma ve prensiplere ihtiyaç duyulmaktadır. Bu amaçla uzun yıllardır çeşitli resmi kuruluş ve gönüllü birlikteliklerle çabalar sarf edilmiştir. Bu çabalardan önemli olanlar şunlardır;

Birleşmiş Milletler (BM)

Birleşmiş milletler örgütü sayısal suçlar alanının Uluslararası Telekomünikasyon Birliği (ITU) tarafından yayımlanan düzenlemeler ile kontrol etmeye çalışmaktadır. Birleşmiş Milletler bünyesindeki Uyuşturucu ve Suçlarla Mücadele Bürosu (UNODC) da sayısal suçlarla ilgilenmektedir. Sayısal suçlar konusunda ilk ITR düzenlemesi 1988 yılında kabul edilmiştir [11]. Bilgisayar suçlarının kanunlaştırılması konusundaki karar ise 1990 yılında Havana-Küba'da yapılan Sekizinci BM Suçun Önlenmesi ve Suçlu Muamelesi kongresinde imzalanmıştır [12]. BM Genel Meclisi ise 2000 yılında 55/63 numaralı kararı ile;

- Üye ülkelerin bilgisayar teknolojilerinin suç işleyecek şekilde kullanılmasına imkân tanıyan ortamların azaltılması konusunda kanun ve uygulamalar geliştireceğini garanti etmesi
- Adli sistemlerin, bilgisayar sistemlerinin ve verinin gizliliği, bütünlüğü ve erişebilirliğini yetkisiz erişimlerden koruyup, suça yönelik kullanımların cezalandırılması

hususları imza altına alınmıştır. 2010 yılında ise yine BM Genel Meclisi tarafından sayısal suçlarla mücadele konusunda en iyi uygulamalar, ulusal kanunlar hakkında bilgi değişimi, teknik yardım ve uluslararası koordinasyon amaçları ile çok katılımlı çalışma grupları oluşturulmasını 65/230 numarası ile karara bağlamıştır [13]. ITR düzenlemesinin son güncellemesi ise Dünya Telekomünikasyon Konferansı (WCIT-12) esnasında 2012 yılında Dubai'de 89 ülke tarafından imzalanmıştır [14-15].

Avrupa Konseyi (Budapeşte Sözleşmesi)

Avrupa konseyi 1997 yılında Siber Uzayda Suç Uzmanları komitesini kurdu ve 2001 yılında Budapeşte Sözleşmesi olarak anılan Siber Suçlar Sözleşmesini kabul etti. Bazı raporlara göre 100'den fazla ülke kendi iç hukuk düzenlemelerinde bu sözleşmenin belirlediği esaslardan faydalanmıştır [16]. Bu güne kadar 35 ülke sözleşmeyi imzalamıştır.

İktisadi İşbirliği ve Kalkınma Örgüt (Organisation for Economic Co-operation and Development: OECD)

OECD bilgisayar suçları konusunda öngörülerde bulunan ilk uluslararası örgüttür [17]. Bu örgüt doğası gereği anlaşmalar imzalamamaktadır. Bunun yerine dünya çapında koordine edilmiş bir politika oluşturmaya çalışmaktadır. OECD bünyesinde kurduğu çeşitli çalışma grupları aracılığı ile 2002 yılında "Bilgi Sistemleri ve Ağ Güvenliği: Güvenlik Kültürüne Doğru"[18], 2008 yılında "Çevrimiçi Kimlik Hırsızlığı Raporu"[19] (bu dokümanda aynı zamanda kimlik hırsızlığının suçlar hukukunda bir suç olarak kabul edilmesini öngörmektedir), 2009 yılında da "Çevrimiçi Kimlik Hırsızlığı Konusunda OECD Politika Rehberi"[20] dokümanlarını yayımlamıştır.

Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization: NATO)

NATO örgütü kuruluş amacı doğrultusunda, daha çok üye ülkeleri hedef alan siber saldırılara odaklanmaktadır. NATO Kıdemli Sivil Acil Durum Planlama Komitesi (SCEPC) sivil halk ve kritik altyapının terörist saldırılara karşı korunması konusunda üye ülkelere yardımda bulunmaktadır. Ayrıca NATO Sivil İletişim Planlama Komitesi (CCPC) ise genel ve özel iletişim altyapılarından sorumludur. NATO Sivil Koruma Komitesi 2003 yılında Kritik Altyapı Koruma Konsept Dokümanını yayımlamıştır [21]. NATO Terörizmle Mücadele Mükemmeliyet Merkezi 2008 yılında Ankara'da kurulmuştur [22].

Asya Pasifik Ekonomik İşbirliği Kuruluşu (Asia-Pacific Economic Cooperation: APEC)

APEC süper güçler olarak bilinen ABD, Rusya ve Çin'i aynı çatı altında toplaması açısından önemli bir kuruluştur [23]. APEC 1990 yılında Bilgi ve İletişim Çalışma Grubunu kurmuştur. Bu çalışma grubu ise Liberalleşme Yönlendirme Grubu, Bilgi ve İletişim Teknolojileri Geliştirme Yönlendirme Grubu ve Güvenlik ve Gelişme Çalışma Grubu olmak üzere üç alt çalışma grubu oluşturmuştur. Güvenlik ve Geliştirme Çalışma Grubu ağlar/altyapılar/servisler/ teknolojiler/uygulamalar/e-ticaret konularında güvenlik ve karşılıklı güven oluşturma konusunda çalışmaktadır. Bu gurup

spam e-postalar, casus yazılımlar ve siber suçların önlenmesinde Bilgisayar Acil Durum Müdahale Ekibi (Computer Emergency Response Team: CERT) ve Bilgisayar Güvenliği Olay Müdahale Ekibi (Computer Security Incident Response Team: CSIRT) yapılanmalarını desteklemektedir. Bu kuruluş bünyesinde yürütülen önemli çalışmalardan birisi de e-güvenlik Görev Grubu tarafından 2003 yılında başlatılan Siber Suçlar Mevzuatı ve Uygulama Kapasitesi Oluşturma Projesidir.

Şanghay İşbirliği Örgütü (Shangai Cooperation Organization: SCO)

SCO örgütü üyelerini Rusya, Çin ve bazı eski Sovyet cumhuriyetleri oluşturmaktadır. Bu örgüt de 2009 yılında yayımladığı Yaketerinburg Açıklaması ile bilgi güvenliğini uluslararası müşterek sistemlerde öncelikli alanlardan biri olarak belirlemiştir. SCO ülke başkanlarının 2012 yılındaki Pekin toplantısında SCO'nun terörizm, aşırılık ve aynı zamanda siber suçlarla mücadelede sıkı işbirliği yapacağı duyurulmuştur [4,14].

Sanal Küresel Görev Gücü (Virtual Global Taskforce:VGT)

VGT Avustralya, İngiltere, Kanada, ABD, İtalya, Birleşik Arap Emirlikleri, Yeni Zelanda, İnterpol ve Europol'ün üyesi olduğu bir kanun uygulama birimleri birlikteliğidir [24]. Bu örgüt özellikle çocuk cinsel istismarı konusunda sivil sektörle de beraber çalışmalar yapmaktadır.

Siber Suçlar Çalışma Grubu Stratejik İttifakı

Bu ittifak 2006 yılında Avustralya, ABD, Yeni Zelanda, Kanada ve İngiltere'den beş kanun uygulama biriminin katılımıyla siber suçlarla mücadele amacıyla kurulmuştur.

İlgilenen okuyucular uluslararası bilgi güvenliği, siber suçlar ve kanun uygulama birimleri ile bu konuda birliktelikler, organizasyonlar ve inisiyatifler hususunda detaylı bir çalışmayı "Institutions for Cyber Security" başlıklı araştırmada [25] bulabilirler.

Son yıllarda ülkeler sürekli olarak, ikili ve bölgesel işbirliklerinin siber suçlarla mücadele ve siber ortam güvenliği için yeterli olmadığına dikkat çekerek, uluslararası müşterek bir siber-uzay antlaşmasının gerekli olduğunu belirtmektedirler [10].

Bütün bu uluslararası çalışmaların ilk hedefi sayısal suçların önlenmesi olarak özetlenebilir. Ancak bu hedefe ulaşmak için suç araştırma, inceleme ve delillendirme süreçlerinde de eşgüdüm ve karşılıklı uygulanabilirliğin sağlanması kaçınılmaz bir ihtiyaçtır. Bu anlamda adli bilişim incelemesi konusunda uluslararası bir uygulama ve birliktelik bulunmamaktadır.

III. ADLİ BİLİŞİM TRENDLERİ VE GELECEK ÖNGÖRÜLERİ

Adli bilişim sürekli değişen ve gelişen bir alandır. Bu ise adli bilişim ile ilgilenen kişi ve kurumların yeniliklere sürekli adapte olma zorunluluğunu gerektirmekte, aynı zamanda da bu kişi ve kurumlar için bazı problemlere neden olmaktadır. Bu problemler arasında; sürekli boyutları artan sabit disk gibi depolama ortamları, sabit disk kullanımını gerektirmeyen bazı yöntemler geliştiren saldırganlar ve kötücül yazılımlar ve siber olaylara müdahale esnasında daha hızlı karar vermeye olan ihtiyaç sayılabilir.

Bilgisayarların ve mobil telefonların hızlı gelişimi hayatı kolaylaştırmasının yanı sıra bu cihazların suç teşkil eden faaliyetlerde de kullanılmasına yol açmıştır [26]. Bu cihazların karmaşıklığı ise hem güvenlik kontrollerinin uygulanmasını hem de bu cihazların kullanıldığı suç faaliyetlerinin araştırılmasını zorlaştırmaktadır.

Bilgisayarlarla işlenen suçların üssel olarak artması ile adli bilişim, dolandırıcılık, siber taciz, öldürme ve çocuk istismarı gibi geniş bir yelpazedeki suç faaliyetlerinin araştırılmasında kullanılmaktadır. Burada adli bilişimin amacı, sayısal kanıtları, mahkemelerde kullanılmak üzere muhafaza etmek, araştırmak ve analiz etmektir. Analiz faaliyeti, basit olarak bilgilerin elde edilmesinden bir dizi olayın aydınlatılmaya çalışmasına kadar değişebilir.

Adli bilişim uzmanları, depolama ortamları, elektronik dosya türleri gibi teknolojilerin ve cihazların gelişimini sürekli takip edebiliyor olmalıdır. Bunların kullanımı ise sürekli gelişmekte ve değişmekte ve adaptasyonu zorlaştırmaktadır. Buna örnek olarak on yıl önce sürekli kullanılan CD/DVD ROM'ların, flash belleklerin çıkması ile birlikte kullanımlarının oldukça azalması, yine SSD disklerin yaygınlaşması ile birlikte mekanik disklerin kullanımlarının azalmaya başlaması gösterilebilir.

Adli bilişim alanında günümüzde yaşanan ve yakın gelecekte yaşanmaya devam edecek en belirgin değişikliklerden biri, depolama ortamları, bellek ve işlemcilerin türleri, boyutları ve hızlarında yaşanacak değişikliktir. Önümüzdeki 2-3 sene içinde standart bilgisayarlar 5TB depolama alanı veya daha düşük kapasitede fakat elektronik olan SSD diskler ile gelecek, flash bellekler ise 250 GB veriyi taşıyabilecektir. Bu nedenle, bugün olduğundan çok daha büyük boyutta verilerin analiz edilmesi ve ayrıştırılması söz konusu olacaktır. Bununla beraber bilgisayarlar da 7 veya 8 kat daha hızlı çalışacaktır. Geleneksel adli bilişimin zorluklarından biri, sabit disklerin boyut ve sayılarına göre veri toplamanın saatler hatta bazen günler almasıdır. Doğrulama yaptıktan sonra adli bilişim uzmanları, uzun zaman alan yüksek boyutlu veriler üzerinde çalışmaktadırlar.

Bu problemi aşmak ise "Canlı adli bilişim" 'in yaygınlaşması ile mümkün olabilecektir. Canlı adli bilişimden kasıt, çok yüksek miktarda veri ile karşılaşıldığında; geçici verinin toplanması, sabit diskin bazı alanlarının bazı soruların cevaplanması için analiz edilmesi ve tüm sabit diskten veri toplanmasının veya diğer sistemlerin analiz edilmesinin gerekip gerekmediğinin belirlenmesidir.

Diğer yaşanacak gelişmeleri ise; Uzmanlık olarak adli bilişim alanının genişlemesi ve adli bilişim araçlarının daha özel hale gelerek veri toplama ve işlemenin otomatikleşmesi olarak sıralamak mümkündür. Her ne kadar bu gelişme, daha az eğitimli insanların bu araçları kullanabileceği anlamına gelse de, donanım ve yazılımların daha karmaşık hale gelmesi ile geleceğin adli bilişim uzmanlarının, bunları yönetebilmek için daha detaylı teknik bilgilere sahip olmasını gerektirebilecektir.

Öte yandan, adli bilişim, suç araştırmalarının dışında güvenlik ve mahremiyet risk değerlendirmesinde veri eşleştirmesi, fikri mülkiyet haklarının otomatik olarak aranması gibi diğer alanlarda da kullanılmaya başlanmıştır. Bu kullanımların yakın gelecekte daha da yaygınlaşması söz konusu olabilecektir. Bu şekilde adli bilişimin sadece bir inceleme mekanizmasından çıkarak bir önleme ve uyumluluk sağlama mekanizmasına dönüşmesi de söz konusu olabilecektir.

Siber Suçlarla Mücadele

Adli bilişim alanındaki teknoloji ve araçların sürekli ve hızlı değişiminin diğer bir boyutu da siber suçlar ve suçlularla ilgilidir. Emniyet güçlerinin ve ulusal güvenlik kuruluşlarının, yeni teknolojileri farklı kanunsuz yollarla kullanma eğiliminde olan suçlular, organize suç örgütleri, devlet destekli veya desteksiz gruplara karşı mücadelede adli bilişim kapasitelerini teknik ve prosedürel olarak sürekli güncel tutmaları ve geliştirmeleri gerekmektedir. Emniyet güçleri tarafından bu kapasitenin sağlanabilmesi için ise, bu alanda ar-ge faaliyetlerine kaynak tahsis edilmesi gerekmektedir.

Fiziksel Bellek Adli Bilişimi

Siber suçlar ile ilgili olarak adli bilişimin en temel güçlükleri, fiziksel bellek (elektronik sabit diskler de dâhil olmak üzere) ve bulut bilişimdir.

Statik depolama ortamlarına kıyasla, fiziksel bellekler, aynı somut sayısal delilleri sağlamamakta, delillerin muhafazası, toplanması ve analiz edilmesi de daha zor olmaktadır [27]. Fiziksel bellek ortamlarında depolanan verilerin geçici nitelikte olması, genellikle belirli bir işleme yönelik olarak doğrudan bir kanıt oluşturmamasına yol açmaktadır.

Bunula birlikte, fiziksel belleklerde artık verilerin bulunması, geleneksel yöntemler ile toplanamayacak olan bilgilerin toplanması için fiziksel bellek adli bilişim tekniklerinin geliştirilmesi için fırsat oluşturmaktadır. İşletim sistemi veya uygulamalar tarafından kullanılan veriler fiziksel bellekte uzun süre kalabilmekte ve kullanıcının buna müdahale imkânı kısıtlı olmaktadır. Öte yandan, fiziksel bellek boyutları ve depoladıkları veri miktarları gitgide artmakta, elektronik sabit disklerin kullanımı da yaygınlaşmaktadır.

Bulut bilişim gibi günümüz teknolojik gelişmelerinin ışığında, fiziksel bellekten veri toplanması ve analizinin getirisi, risklerine göre daha ağır basar hale gelmiştir.

Bulut Bilişim Ortamında Adli Bilişim

Bulut bilişim ise artan bir şekilde yaygınlaşan ve adli bilişim uzmanları için zorluklar olduğu kadar fırsatlar da sunan bir alandır[2]. Bulut bilişim ortamları, siber suçlular tarafından sıklıkla saldırıya maruz kalan ortamlardır. Bu da siber suçların tespitinde daha yüksek hacimde analiz edilecek olan sayısal delil anlamına gelmektedir.

Bulut bilişimin suçlular tarafından kullanımı, kullandıkları cihazların sanallaşması, coğrafik olarak dağıtık olması ve kısa süreli olması anlamına gelmektedir. Bu ise bunların tespit edilmesi ve ele geçirilmesinde emniyet güçlerine teknik ve yasal olarak zorluklar getirmektedir.

Sanallaştırma ve buna istinaden mevcut adli bilişim analiz araçlarının kullanılamaması, sayısal kanıtların bulunduğu ortamların net bir şekilde bilinememesi, mahremiyet hususları ve yasal sınırlar adli bilişim alanında en çok zorluk yaşanacak konular olacaktır.

Bu noktada, sadece kısmi verinin, bir den fazla lokasyondan ve çeşitli formatlarda ve farklı kanuni düzenlemeler altında yasal olarak nasıl temin edilebileceği konusunda araştırmaların yapılması ve birlikte çalışmaya ihtiyaç vardır.

Yukarıda belirtilen adli bilişimin önündeki zorluklara istinaden, bu alanda yeni bazı yaklaşımların getirilmesinin kaçınılmaz olduğu değerlendirilmektedir [28]. Temel olarak adli bilişim alanındaki yönelimler özetlenecek olursa; Cihaz inceleme yaklaşımından, olayın incelenmesi yaklaşımına geçilmesi, veri merkezli analizden, inceleme merkezli analize geçilmesi ve araç tabanlı adli bilişimden, hizmet tabanlı adli bilişime geçiş yapılması şeklinde tanımlanabilir.

IV. BİLİRKİŞİLİK VE BİLİRKİŞİ ÇALIŞMA USULLERİ

Mahkemelerde yapılacak bilirkişilik ile düzenleme 01.10.2011 tarihli 6100 sayılı Hukuk Muhakemeleri Kanununda (HMK) düzenlenmiştir. Kanunun dördüncü kısmının beşinci bölümü mahkemelerde bilirkişinin nasıl görevlendirileceği ve bilirkişinin çalışma usullerini kapsamaktadır. Ancak kanunda tanımlanan ve çalışma usulleri belirlenen bilirkişi hizmetleri genel kapsamda olup, bilişim suçlarının incelenmesinde ihtiyaç duyulan detayları doğal olarak içermemektedir. Bilirkişi teriminin farklı tanımları bulunsa da en geniş yaklaşım ile "hâkim tarafından görüşüne başvurulan kişidir" şeklinde ifade edilebilir. HMK'da bilirkişi görüşüne başvurulacak durumlar "çözümü hukuk dışında, özel veya teknik bilgiyi gerektiren hâller" olarak belirlenmiştir. Mahkemelerde bilirkişi görevlendirmesi ise mahkeme tarafından kendiliğinden veya tarafların birinin talebi üzerine yapılır. Mahkemelerde görevlendirilecek bilirkişiler ise bölge adliye mahkemesi adli yargı adalet komisyonları tarafından, her yıl düzenlenecek olan listelerle belirlenmektedir. Görüşüne başvurulacak bilirkişi miktarı için ise HMK 267/1 maddesinde mahkemelerin bilirkişi olarak yalnızca bir kişi görevlendirebileceği, ancak gerekçesi açıkça belirtilmek suretiyle tek sayıda birden fazla kişiden oluşturulacak bir kurulun görevlendirilmesine de imkân tanınmaktadır. Bilirkişilere görüşlerine başvurulan konularda raporlarını hazırlamak üzere en çok üç ay süre verilebilir. Gerekli görülen durumlarda ise bu süre üç ay daha uzatılabilir. Bilirkişi raporlarının nasıl olması gerektiği konusunda ise kanunda sadece bilirkişilerin hukuki değerlendirmede bulunamayacağı belirtilmektedir. Bilirkişi raporun hazırlanma şekli ve örnek raporlar ile ilgili literatürde birçok yayın mevcuttur [26]. Ancak bu yayınların hiç birisi sayısal sistemler ve bilişim suçlarının incelemelerinde hazırlanacak raporlar için özelleşmiş bir yapıyı içermemektedir.

Bilirkişilik ve bilirkişi çalışma usulleri ile ilgili mevcut düzenleme ve uygulamalar incelendiğinde bu hizmetlerin adli bilişimin gerek ve ihtiyaçları doğrultusunda özelleşmediği görülmektedir. Mevcut genel bilirkişilik düzenlemelerinin de adli bilişim hizmetlerinin ihtiyaçlarını karşılamada yetersiz kaldığı görülmektedir [29].

V. ADLİ BİLİŞİM HİZMETLERİ ALANINDA PROBLEMLER VE ÇÖZÜM ÖNERİLERİ

Adli bilişim kavramı göreli olarak yeni bir kavramdır ve gelişen teknolojilere paralel olarak suç türlerinin değişmesi ve dolayısı ile kanıt toplama ve analiz etme yöntemlerinin değişmesi sonucu ortaya çıkmıştır. Bu açıdan bakıldığında adli bilişim ile ilgili en temel problem alanla ilgili yeterli sayıda ve yetkinlikte personel bulunmamasıdır. Bu husus hem adli bilişim alanında görev alan teknik personel anlamında hem de işin hukuki boyutunda görev alan hukukçular anlamında geçerlidir. Bu anlamda son yıllarda adli bilişim alanında yüksek öğrenim seviyesinde önemli gelişmeler yaşanmaktadır. Bazı üniversitelerde adli bilişim yüksek lisans programları açılmaktadır. Bunun yanında lisans seviyesinde de hem bilgisayar bilimleri alanındaki bölümlerde adli bilişim teknik altyapısı ile ilgili, hem de hukuk fakülteleri bünyesinde konunun hukuki yönleri ile ilgili dersler açılmaktadır. Teknolojik gelişmeler ışığında sayısal ortamlardaki suç miktarındaki artışa paralel olarak adli bilişim uzmanlarına duyulan ihtiyacın da artacağı göz önünde bulundurulursa, adli bilişim alanındaki eğitim-öğretim faaliyetlerinin artırılması gerektiği sonucuna varılabilir.

Adli bilişim alanındaki bir diğer problem ise adli bilişim alanında görev alacak bilirkişilerin belirlenmesi ve yetkinliklerinin ölçülmesi konusudur. Yukarıda da belirtildiği üzere adli bilişim konusunda görev alabilecek teknik personelin eğitimi konusunda ülkemizde çeşitli çabalar olmasına rağmen henüz adli bilişim uzmanının resmi bir tanımlaması yapılmış değildir. Bunun yanında hangi eğitimleri almış kişilerin adli bilişim uzmanı olabileceği, bir adli bilişim uzmanının taşıması gereken yetkinlik şartları, bu şartların karşılanıp karşılanmadığının nasıl belirleneceği konusunda ortaya konmuş gerek ulusal bazda gerekse de uluslararası düzeyde bir standart/kriter ya da benzeri bir uygulama bulunmamaktadır. Adli bilişim uzmanlarının yetkinliklerini belirleyen ve belgeleyen bir sertifikasyon programının bulunmaması, mahkemelerce görevlendirilecek bilirkişilerin hakimlerce belirlenmesi aşamasında ciddi sıkıntılar yaratmaktadır. Bu problemin çözümü için öncelikle Türk Standardları Enstitüsü bünyesinde ulusal düzeyde bir sertifikasyon programının başlatılması ve adli bilişim uzmanı olma yetkinliğine sahip kişilerin belgelendirilmesi, sonrasında da bu sertifikasyon programının ulusalararası bir standarda dönüştürülmesi için çalışmaların başlatılması önerilmektedir.

Yukarıda bahsedilen yetkinlik problemine ilave olarak uzmanlık alt alanlarının da belirlenmesinin yapılacak çalışmalar için faydalı olacağı değerlendirilmektedir. Zira adli bilişim kapsamında inceleme yapılması gereken birçok sayısal ortam söz konusu olabilir ve bu ortamların her biri özel bir uzmanlık gerektirebilir. Bu kapsamda değerlendirildiğinde adli bilişim; veri kurtarma, işletim sistemi, veri tabanı incelemesi, bilgisayar ağları alanı, cep telefonu ve mobil cihazlar gibi alt alanlara ayrılabilir. Bu alt alanlardan birinde uzman olan bir kişinin diğer alanda bilgisi bulunmayabilir. Bu problemin çözümü için belki de yapılması gereken yukarıda önerilen sertifikasyon programının alt alanlara göre ayrıştırılması ve her bir alan için ayrı ayrı sertifikasyon işleminin gerçekleştirilmesidir.

Buradaki hususlara ek olarak dikkat edilmesi gereken bir diğer husus da teknolojinin hızlı değişimine paralel olarak adli bilişim yetkinlik şartlarının da değişebilme gereksinimidir. Bu nedenle uygulanacak sertifikasyon programının belirli sürelerle yenilenmesi ve gelişen teknolojilere paralel olarak kişi yetkinliklerinin periyodik aralıklarla (örneğin 2 yıl gibi) yeniden gözden geçirilmesi, kontrol edilmesi ve gerekli şartları taşıyan kişilere sertifikasyonun yeniden verilmesinin uygun olacağı değerlendirilmektedir.

Adli bilişim alanındaki bir diğer problem ise kullanılan araçlarla ilgilidir. Adli bilişimde yapılan tüm incelemelerde bazı hazır yazılım ve/veya donanım araçları kullanılmaktadır. Bu araçlara örnek olarak SANS-SIFT, EnCase, FTK, Sleuth Kit, Wireshark, vb verilebilir. Bu araçların her biri adli bilişim alanında önemli bilgiler sağlamaktadır. Ancak bu araçların performanslarının ve işlevselliklerinin ölçülmesi anlamında bir değerlendirme bulunmamaktadır. Bu araçlardan elde edilen bilgilerin ne derece sağlıklı olduğu ve ne derecede güvenilir olduğu konularında bir değerlendirme yapılması ve belki de bu araçların performans ve güvenilirliği üzerine sertifikasyonlarının yapılması, adli bilişim alanında kullanılabilirliklerini artıracaktır. Ayrıca bu araçların kullanımı durumunda bilgi güvenliği riskleri oluşup oluşmadığı hususunun da ayrıca değerlendirilmesi gerekmektedir. Bu araçların hazırlanacak bir koruma profiline göre güvenlik sağladıklarının belgelendirilmesi için Ortak Kriterler Belgelendirme Programı kapsamında değerlendirilmeleri faydalı olacaktır.

Adli bilişim alanında bilirkişi olarak görevlendirilen kişilerin yetkinliklerinin tam olarak belli olmaması, bu kişilerin kullandıkları adli bilişim araçlarının güvenilirlikleri konusunda bir fikir birliği sağlanmamış olmasının yanında bilirkişilerce hazırlanan raporların içerik ve kapsamı konusunda da belirsizlikler söz konusudur. Her bilir kişi yaptığı çalışmalar ve elde ettiği bulgular ışığında bir rapor hazırlamaktadır. Oysaki hem bu raporların okunabilirliğinin ve anlaşılabilirliğinin sağlanması hem de bu raporlara güvenilirliğin sağlanması için, rapor kapsamında hangi hususların yer alması gerektiği, hangi araçların kullanıldığı, hangi analizlerin yapıldığı ve hangi bulguların elde edildiğinin belirli bir format kapsamında sunulması faydalı olabilir. Bunun için bir rapor formatının geliştirilmesi ve bu formata uyumun sağlanması faydalı olacaktır.

VI. SONUÇ VE ÖNERİLER

Bu çalışmada ulusal ve uluslararası düzeyde adli bilişim konusu ele alınmış, mevcut durum özetlenmiş, gelecek öngörüleri yapılmış ve alandaki problemler ve çözüm önerileri sunulmuştur.

Adli bilişim göreceli olarak diğer bilgi teknolojileri alanları ile karşılaştırıldığında yeni bir alan olup teknolojinin gelişimine paralel olarak hızlı değişim gösteren bir alandır. Bu alandaki en temel problem konuya hakim uzman personel eksikliğidir. Bunun yanında adli bilişim alanında çalışacak ve özellikle de mahkemelerde bilirkişi olarak görevlendirilecek personelin taşıması gereken niteliklerin belirlenmemiş olması

da bu konuda etkendir. Bu nedenle adli bilişim uzmanlarının yetkinlik şartlarının belirlenmesi ve bu yetkinlik şartlarının ölçülmesi kritik önem arz etmektedir. Bu probleminin çözümü için hem ulusal düzeyde hem de uluslararası düzeyde standartların hazırlanması ve belgelendirme programlarının başlatılması elzemdir.

Diğer bir problem ise, adli bilişim alanında yerli ürün ve teknoloji olmaması ve bu alandaki gelişmelerin yeterince takip ve adapte edilememesidir. Adli bilişim alanında önümüzdeki dönemde önemli gelişmelerin yaşanacağı ve hukuki süreçlerin sağlıklı yürütülmesi açısından bunların takip edilmesi gerektiği aşikârdır. Bu alanda özellikle yerli ürünlerin geliştirilerek, kullanımlarının yaygınlaştırılması yakın gelecekte adli bilişim çalışmalarının yaygınlaşacağı düşünüldüğünde isabetli olacaktır.

KAYNAKLAR

[1] WaveFront Consulting Group, A Brief history of Cybercrime, http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html, internet adresinden 11.07.2014 tarihinde erişilmiştir.
[2] Mustafa Yücel, Bilişim Suçları, Ankara Barosu Dergisi, Y.49, Sy.4, 1992, Ankara, s.505
[3] Edirne Barosu, Adli Bilişim (Computer Forensic), http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic internet adresinden 15.07.2014 tarihinde erişilmiştir.
[4] Adli Bilişim Derneği, Adli Bilişimin tanımı, http://www.adlibilisim.org.tr/index.php/hakkimizda/2013-04-25-04-43-07/adli-bilisimin-tan-m internet adresinden 15.07.2014 tarihinde erişilmiştir.
[5] Yunus Ballı, Adli Bilişim Nedir?, http://www.dijitaldeliller.com/adli_bilisim_nedir.html internet adresinden 15.07.2014 tarihinde erişilmiştir.
[6] Ş.Sağıroğlu, M. Karaman, Adli Bilişim, http://www.telepati.com.tr/agustos12/konu8.htm internet adresinden 10.07.2014 tarihinde erişilmiştir.
[7] Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçlari Hakkinda Kanun Tasarisi, http://www.tbd.org.tr/index.php?dummy=1&sayfa=raporlar&mi=3&vkid=194&t=1290232819&jfr=true&keepThis=true&TB_iframe=true&height=500&width=800 internet adresinden 10.07.2014 tarihinde erişilmiştir.
[8] Caza Muhakemesi Kanunu, 04.12.2014 kanun numarası: 5271, http://www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm internet adresinden 15.07.2014 tarihinde erişilmiştir.
[9] Adli ve Önleme Aramaları Yönetmeliği, 01.06.2005 Resmi Gazete Sayısı: 25832 , http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.8203&MevzuatIliski=0&sourceXmlSearch= internet adresinden 12.07.2014 tarihinde erişilmiştir.
[10] A.Levin, D. Ilkina, (2013), International Comparison of Cyber Crime, Privacy and Cyber Crime Institute, Ted Rogers School of Management, Ryerson University, March 2013. http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf internet adresinden 10.07.2014 tarihinde erişilmiştir.
[11] International Telecommunication Regulations (ITR), International Telecommunications Union (ITU), http://www.itu.int/oth/T3F01000001 internet adresinden 15.07.2014 tarihinde erişilmiştir.
[12] Guidelines on the Role of Prosecutors, Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August to 7 September 1990, U.N. Doc. A/CONF.144/28/Rev.1 at 189 (1990). http://www1.umn.edu/humanrts/instree/i4grp.htm internet adresinden 12.07.204 tarhinde erişilmiştir.
[13] UN General Assembly resolution 65/230, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, https://www.unodc.org/documents/justice-and-prison-reform/AGMs/General_Assembly_resolution_65-230_E.pdf internet adresinden 13.07.2014 tarihinde erişilmiştir.
[14] Signatories of the Final Acts: 89, World Conference on International Telecommunications, 3-14 December 2012, Dubai UAE, http://www.itu.int/osg/wcit-12/highlights/ signatories.html internet adresinden 13.07.2014 tarihinde erişilmiştir.
[15] Oliver Moore, Debate over Internet regulation's future rages at Dubai meeting , http://www.theglobeandmail.com/technology/debate-over-internet-regulations-future-rages-at-dubai-meeting/article6016228 internet adresinden 14.07.2014 tarihinde erişilmiştir.
[16] The Hon Nicola Roxon MP, (2012), New Laws in the Fight Against Cyber Crime, http://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/1867175/upload_binary/1867175.pdf;fileType=application%2Fpdf#search=%22cyber%20crime%22 internet adresinden 15.07.2014 tarihinde erişilmiştir.
[17] Schjolberg, S., Cybercrime Law. Global organizations: OECD, (2013), http://www.cybercrimelaw.net/OECD.html internet adresinden 14.07.2014 tarihinde erişilmiştir.
[18] OECD Guidelines for The Security of Information Systems and Networks: Towards A Culture of Security, OECD, http://www.oecd.org/sti/ieconomy/2002-security-guidelines-review.htm internet adresinden 13.07.2014 tarihinde erişilmiştir.
[19] Scoping paper on online Identity theft, OECD, http://www.oecd.org/internet/consumer/40644196.pdf internet adresinden 15.07.2014 tarihinde erişilmiştir.
[20] OECD Policy Guidance on Online Identity Theft, OECD, http://www.oecd.org/sti/consumer/40879136.pdf internet adresinden 15.07.2014 tarihinde erişilmiştir.
[21] The Protection of Critical Infrastructures, NATO Parliamentary Assembly, http://www.nato-pa.int/default.asp?SHORTCUT=1165 internet adresinden 15.07.2014 tarihinde erişilmiştir.
[22] Centre of Excellence Defense Against Terrorism, NATO, http://www.coedat.nato.int/index.htm internet adresinden 15.07.2014 tarihinde erişilmiştir.
[23] History of Asia-Pacific Economic Cooperation (APEC), http://www.apec.org/About-Us/About-APEC/History.aspx internet adresinden 10.07.2014 tarihinde erişilmiştir
[24] Virtual Global Task Force ,Who we are, http://www.virtualglobaltaskforce.com/who-we-are internet adresinden 14.07.2014 tarihinde eişilmiştir.
[25] Nazli Choucri, Stuart Madnick & Jeremy Ferwerda (2014) Institutions for Cyber Security: International Responses and Global Imperatives, Information Technology for Development, 20:2, 96-121, http://dx.doi.org/10.1080/02681102.2013.836699 internet adresinden 15.07.2014 tarihinde erişilmiştir.
[26] Digital Forensic Trends and Future, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 48-76 http://wp.vcu.edu/hsep/wp-content/uploads/sites/3338/2013/06/Digital-Forensic-Trends-and-Future-.pdf adresinden 14.07.2014 tarihinde erişilmiştir
[27] Contemporary Trends in Asian Criminal Justice: Paving the Way for the Future , Korean Institute of Criminology http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2421339 adresinden 16.07.2014 tarihinde erişilmiştir.
[28] The future of digital forensics , SungKyong Un ETRI, RSA Conference Asiapacific 2013, https://www.rsaconference.com/writable/presentations/file_upload/cle-w04_final.pdf adresinden 13.07.2014 tarihinde erişilmiştir
[29] Erhan Bulut, Bilirkişi Seçimi ve Bilirkişi Raporlarinin Bağlayiciliği, Mevzuat Dergisi, yıl:4 sayı:47, Kasım 2001, http://www.mevzuatdergisi.com/2001/11a/02.htm internet adresinden 13.07.2014 tarihinde erişilmiştir.