



Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Adli Bilişim Mühendisliği Eğitiminin Kurumlar Açısında Önemi

Erhan AKBAL*, Fatma GÜNEŞ

Adli Bilişim Mühendisliği Bölümü, Teknoloji Fakültesi, Fırat Üniversitesi, Elazığ, TÜRKİYE

** Sorumlu yazarın e-posta adresi: erhanakbal@firat.edu.tr*

ÖZET

Teknolojinin gelişmesiyle dünyada bilişim alanında işlenen suçlar gittikçe artmakta ve toplum hayatını olumsuz etkilemektedir. Dijital kaynaklar aracılığıyla işlenen suçlarla mücadele edebilmek için gerekli olan altyapı çalışmaları yetersiz kalmaktadır. Bilişim teknolojilerinin yaygın olarak kullanıldığı ülkeler belirtilen suçlardan etkilendiğinden bu alanın öneminin farkına varmış ve eğitim müfredatlarında adli bilişim ve siber suç kavramlarına yer vermiştir. Fakat bilişim suçlarının oluşmasından önceki ve sonraki süreçleri incelemek yeni bir bilim dalı gerekliliğini ortaya çıkarmıştır. Adli Bilişim mühendisliği bölümü bilişim suçlarıyla mücadele etmek için dünyada birçok ülkede bulunan yeni bir disiplindir. Bu çalışmada ülkemizdeki kurumların bilişim suçlarına ve güvenliğine bakış açıları ortaya konularak, adli bilişim mühendisliği eğitiminin önemi gösterilmiştir.

Anahtar Kelimeler: *Adli bilişim mühendisliği, Siber suçlar, Bilişim eğitimi*

Digital Forensic Education Importance for Institutions

ABSTRACT

In parallel to development in technology, information technology crimes are increasing and impacting life of society negatively. Infrastructure work which is necessary to struggle with crimes committed via digital resources is inadequate. Countries which effected from these mentioned crimes realized the importance of this study field and gave place digital forensics and cybercrime concepts in education curriculum. But, examining processes after and before information technology crimes revealed the necessity of a new branch of science. Digital forensic engineering department is a new discipline which exists in a lot of countries to struggle with cybercrimes. In this study, view point of corporations of our country to information crimes and security presented and importance of digital forensics engineering education showed.

Keywords: *Digital forensic engineering, Cyber crime, IT education*

I. GİRİŞ

BİLİŞİM ve internet teknolojilerinde yaşanan hızlı gelişim sürecinin hayatımızın pek çok alanında olumlu sonuçları yanında, kontrol edilmesi güç sorunları da beraberinde getirdiği görülmektedir. Bugün bilişim alanındaki hızlı gelişmeler bilişim suçları olgusuyla karşı karşıya kalmamıza neden olmuştur. Her geçen gün bu yolla işlenen suçlarda artış ve çeşitlilik görülmektedir. İnsanların sosyal yaşantı ve iş hayatlarına büyük kolaylık getiren bu teknoloji, aynı zamanda suç işleme eğiliminde olanlara, daha önce tanımı yapılmış veya yapılmamış çok geniş bir suç işleme potansiyelini de sunmaktadır [1]. Ayrıca daha önce belli bir bölge ile sınırlı olan bu suçlar bilişim teknolojilerinin sunmuş olduğu imkânlarla bu sınırları aşmakta ve küresel hale gelmektedir [2].

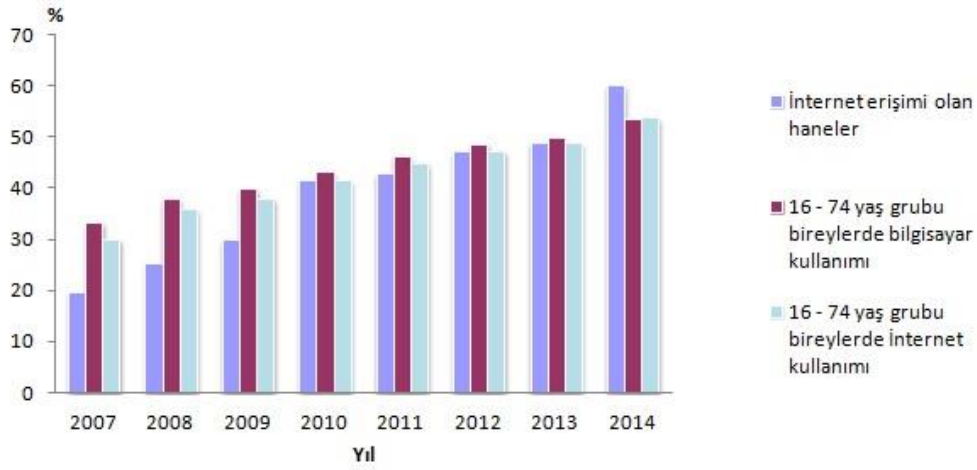
Günümüz dünyasında internetin yaygınlaşması, kişisel bilgisayarlarla akıllı cihazların kullanım oranının artması ve kişisel bilgilerin sayısal ortamlarda depolanmasına paralel olarak, bu bilgilere yetkisiz erişmek isteyenlerin sayısı da artmıştır. Yetkisiz erişim ve internet korsanlığı (hacker) siber suç kavramını ortaya çıkarmıştır. Devletleri dahi etkileyen bu tehditlerle mücadele edebilmek için Adli Bilişim Mühendisliği (Digital Forensics Engineering) disiplini ortaya çıkmıştır[1]. Adli bilişim mühendisliği eğitimin içeriği bilişim hukuku, bilgi güvenliği, siber güvenlik ve bilişim suçu ile ilgili delil toplama süreçlerinin adli takibi, analizi ve siber suçlarla mücadele edilmesi konularını kapsamaktadır.

Ülkemizde bulunan tüm kurumlar internet altyapısına sahiptir ve bu kurumların çoğu bilgilerini elektronik ortamda saklamaktadır. E-devlet uygulamasıyla birlikte tüm vatandaşların bilgileri sayısal ortamda depolanmıştır. Ayrıca özel şirketler, işletmeler, holdingler vb. kurumlarda internet ve bilişim teknolojilerini etkin olarak kullanmaktadır.

Bilişim teknolojilerinin yaygın olarak kullanılması bu bilgilerin korunması gerekliliğini de ortaya çıkarmıştır. Tüm Dünya' nın önem verdiği bilgi güvenliği hususunda ülkemizde de önlemlerin alınmaya başladığı görülmektedir. Bu noktada bilgi güvenliği sağlama, siber suç ve olaylara müdahale etme gibi gereklilikler meydana gelmiştir.

II. ADLİ BİLİŞİM KAVRAMI

Günümüzde bilgi sistemleri enerji, bankacılık, ulaşım, sağlık, eğitim, iletişim hizmetlerinin verimliliğini arttırmak amacıyla kamu ve özel sektördeki kurumların birçoğu tarafından kullanılmaktadır. Bunun ana nedenlerinin başında internet kullanımının yaygınlaşması yatmaktadır. Şekil 1'de verilen 2007-2014 yılları arasındaki TÜİK verilerine göre Türkiye'deki internet kullanım oranı bu alandaki kullanımın ne kadar hızlı yaygınlaştığını göstermektedir.



Şekil 1. Türkiye’de internet kullanım oranları[3]

Teknolojik gelişmeler kurumlara beraberinde birçok fayda sağlarken, suçlarında bu teknolojileri kullanması kaçınılmazdır. Böylece bu alanda faaliyet gösteren kurumlar için büyük riskler söz konusu olmuştur. Klasik suç kavramından farklı bir suç kavramıyla karşılaşan güvenlik birimleri bu konularla ilgilenmeye başlamıştır. Böylece bilişim suçu kavramı devlet boyutunda tanınır hale gelmiştir. Suçu aydınlatmak için mahkemeler açısından dijital deliller önem kazanmıştır[5].

Ülkemizde bu alanda belirtilen suçların açığa çıkarılması ve kurumları korumak amacıyla Adli Bilimler altında Adli bilişim kavramı ortaya çıkmıştır[6]. Ayrıca çeşitli enstitüler kurularak Adli Bilimler alanında hizmetler verilmesi sağlanmıştır. Ülkemizde faaliyet gösteren Adli Tıp Enstitüleri şöyledir.

- Ankara Üniversitesi Adli Bilimler Enstitüsü
- İstanbul Üniversitesi Adli Tıp Enstitüsü
- Karadeniz Teknik Üniversitesi Adli Bilimler Enstitüsü
- Bezmialem Vakıf Üniversitesi Adli Tıp Enstitüsü
- Polis Akademisi Adli Bilimler Enstitüsü
- Medipol Üniversitesi Adli Bilimler Enstitüsü
- Çukurova Üniversitesi Adli Tıp Enstitüsü

Adli bilişim kavramıyla çoğunlukla kolluk kuvvetleri olan Emniyet, Jandarma ve Adli Tıp kurumları ilgilenirken günümüzde bu alanda faaliyet gösteren özel sektör firmaları da bulunmaktadır. Fakat bu alanda eğitim veren eğitim kurumu sayısı yok denilecek kadar azdır. Ülkemizde Adli bilişim alanında eğitim veren kurumlar şöyledir.

- Fırat Üniversitesi
- Polis Akademisi
- Gazi Üniversitesi
- Hacettepe Üniversitesi
- Yaşar Üniversitesi

III. KURUMLARIN BİLİŞİM SUÇLARINA VERDİĞİ ÖNEM

Ülkemizde Adalet bakanlığı, Emniyet Genel müdürlüğü, İçişleri Bakanlığı, Jandarma Genel Komutanlığı, TÜBİTAK gibi kurumlar stratejik planlarında ve uygulamalarında bilişim suçlarının ne kadar önemli olduğunu sürekli vurgulamaktadır. Kurumların gelecek hedeflerini belirledikleri stratejik planlarında ve performans değerlendirmelerinde adli bilişim ve siber suçlarla ilgili hedefler belirlenmektedir. Buda bu alanda yetişmiş insan gücüne günümüzde ve gelecekte ne kadar ihtiyaç olacağını göstermektedir.

A. ADALET BAKANLIĞI

Adalet Bakanlığının görevleri, 29.03.1984 gün ve 2992 sayılı Adalet Bakanlığının Teşkilat ve Görevleri Hakkında Kanununun 2. maddesinde sayılmıştır. Buna göre Adalet Bakanlığının ülke içerisinde adaleti sağlamak kanunların uygulanmasını sağlamak gibi görevleri bulunmaktadır[4].

Adalet Bakanlığının 2010-2014 stratejik planında bulunan “**6. ADALET HİZMETLERİNDE GÜNCEL TEKNOLOJİK İMKÂNLAR İLE BİLİŞİM SİSTEMLERİNİN KULLANILMASINI VE GELİŞTİRİLMESİNİ SAĞLAMAK**” başlığı altındaki Tablo 1’de verilen hedefler incelendiğinde Adli Bilişim hizmetleriyle ilgili birçok hedefin yer aldığı görülmektedir[7].

Tablo 1. Adalet bakanlığının 2010-2014 stratejik planında bulunan hedefler

HEDEF 6.6	Stratejiler
2014 yılı sonuna kadar bilişim suçlarının tespiti konusunda güncel teknoloji takip edilerek altyapı çalışmalarının tamamlanması ve adli bilişim hizmetlerinin yürütülmesi	<ul style="list-style-type: none">• Bilişim suçlarında delillerin tespiti için laboratuvarlar kurulması ve donanım, yazılım altyapılarının tamamlanması• Bilişim suçları alanında yeterli uzman personel temini veya yetiştirilmesi• Diğer ülke uygulamalarının karşılıklı işbirliği yapılmak suretiyle incelenmesi• Bilişim suçları konusunda yargı mensuplarına eğitim verilmesi, bu konuda uzaktan eğitim modülleri geliştirilerek kullanılması• Adli bilişim hizmetlerinin geliştirilmesi konusunda diğer kurum kuruluşlarla (Jandarma Genel Komutanlığı, Emniyet Genel Müdürlüğü, üniversiteler, sivil toplum örgütleri vb.) işbirliği yapılması
HEDEF 6.7	Stratejiler
2011 yılı sonuna kadar bilgi güvenliği yönetim sisteminin geliştirilmesi ve bilişim alanında uzman teknik personel ihtiyacının karşılanması konusunda çalışmaların yapılması	<ul style="list-style-type: none">• ISO/TSE 27001 standart gerekliliklerinin sağlanması ve belgesinin alınması• ISO/TSE 27001 standardının uygulanması ve takip araçlarının temini• Teknik personelin özlük haklarının iyileştirilmesi için çalışma yürütülmesi• Teknik personel ihtiyacının giderilmesi ve bu personelin her adliyede görevlendirilmesi• Mevzuat alt yapısının hazırlanması

HEDEF 6.8	Stratejiler
2014 yılı sonuna kadar, diğer ülkelerin bilişim sistemi uygulamalarının incelenmesi ve işbirliği imkânlarının geliştirilmesi	<ul style="list-style-type: none">• Çalışma ziyaretleri gerçekleştirilmesi• Ortak bilimsel etkinlikler (toplantı, seminer, sempozyum, çalıştay vb.) düzenlenmesi• UYAP'ın diğer ülke ve kuruluşlara tanıtılması ve teknoloji transferi yapılması konusunda çalışma yürütülmesi

Adalet bakanlığının hedefleri incelendiğinde özellikle Hedef 6.6 doğrudan bilişim suçlarını ilgilendirmekte ve Adli bilişim mühendisliği eğitiminin önemini göstermektedir. Belirtilen hedeflerin sağlanabilmesi bu alanda yetiştirilecek insan gücüyle doğrudan ilgilidir..

B. EMNİYET GENEL MÜDÜRLÜĞÜ

Emniyet Genel Müdürlüğü 2009-2013 Stratejik planı ve 2012, 2015 Yılı Performans Programında Bilişim Suçları ile mücadele ile ilgili hedefler ortaya konmuştur[8-10].

Performans hedefi 2 başlığı altında; *“uyuşturucu madde kaçakçılığı, silah kaçakçılığı, her türlü yolsuzluk suçları, göçmen ve insan kaçakçılığı, örgütlü mali suçlar, terörizm, bilişim suçları ve organize suçlarla etkili mücadeleye devam etmek”* şeklinde verilmiştir.

Organize suç ve terör örgütleri ile mücadele başlığı altında; *“Bilişim Suçları ile Mücadele; Bilişim suçları ile etkin mücadele edilebilmesi için oluşturulan birimlerde görevlendirilen personelin değişen teknolojiler konusunda bilgilendirilmesi amacıyla uzmanlık eğitimleri verilmesine devam edilecektir.”* bulunmaktadır.

Suçların önlenmesi için yapılacak faaliyetler başlığı altında 2-b maddesi *“Suç soruşturma birimlerinin kapasitesinin artırılması”* şeklindedir. İçeriğinde ise *“Son yıllarda bilişim teknolojileri kullanılarak suç oranlarındaki artışı önlemek ve aydınlatılarak faillerinin yakalanması ve yapılan operasyonlar sonucunda el konulan dijital materyallerin incelenmesi amacıyla Dijital Veri İnceleme Birimleri kurulmuştur. Artan iş yükü nedeniyle bu birimlerin teknik donanım ve yazılım ihtiyaçları karşılanacaktır.”* bulunmaktadır.

Adli bilişim mühendisliği eğitiminin belirtilen hedeflerin sağlanması açısından önemi açıkça görülmektedir.

İnsan kaynakları ve eğitim stratejisi başlığı altında; bilişim suçları ile mücadelede emniyet genel müdürlüğünün öngördüğü bütçe ve bu bütçenin pay oranı Tablo 2’de görülmektedir.

Tablo 2. Emniyet Genel Müdürlüğünün öngördüğü bütçe pay oranı

Performans Hedefi	Stratejik Amaç	Açıklama	Bütçe Tutarı
2	Suç önleme ve aydınlatma oranlarını artırmak	Uyuşturucu madde kaçakçılığı, silah kaçakçılığı, her türlü yolsuzluk suçları, göçmen ve insan kaçakçılığı, örgütlü mali suçlar, bilişim suçları ve organize suçlarla etkili mücadeleye devam etmek.	1.579.610.020,00 TL

2015 yılında Emniyet Genel Müdürlüğü siber suçlarla mücadele daire başkanlığı ile Tübitak-Bilgem arasında protokol imzalanarak bu suçlarla mücadele için ortak yol haritası belirlenmesine karar verilmiştir[11]

Bu protokol ile TÜBİTAK ve EGM ortak işbirliği ile aşağıda belirtilen maddelerde odaklanmıştır. Bunlar;

- Farkındalık ve eğitim,
- Adli analiz ve veri kurtarma,
- Zararlı yazılımlarla mücadele,
- Büyük veri analizi ve paylaşımı konularında altyapı geliştirilmesi ve etkinleştirilmesi amacıyla Ar-Ge projelerine yönelik olarak mevzuat çerçevesinde destek verilmesi hedeflenmiştir.

Buradan Adli bilişim kapsamına giren konular üzerine odaklanılması gerekliliği ortaya çıkmaktadır.

C. İÇİŞLERİ BAKANLIĞI

İçişleri bakanlığını 2015 yılı performans programında bilişim suçları ve adli bilişime vurgu yapan çeşitli başlıklar bulunmaktadır [12].

2. Tehditler başlığı altında bulunan “*B. Bilgi Teknolojilerinde Gelişmeler*” alt başlığında aşağıda belirtilen içerikler bulunmaktadır.

- Bilişime yönelik altyapının oluşturulmasında yabancı kaynaklara bağımlı olunması nedeniyle, teknolojik gelişmedeki hıza bağlı olarak ulusal kaynakların dışa aktarılmasının süreklilik kazanması
- e-Devlet’e geçiş sürecinde yabancı işletim sistemleri ve yazılımlarından yararlanmanın doğurabileceği sorunlar
- Gerçek ve tüzel kişilere ilişkin geniş veri tabanının elektronik ortamda tutuluyor olmasının, bu verilerin siber suç bağlamında kötüye kullanılması ve güvenlik zafiyeti yaşanması ihtimalini artırması
- Bakanlıktaki bazı çalışanların, bilgi teknolojilerindeki gelişmelere uyum sağlamada yaşadıkları güçlüklerin, değişim sürecini yavaşlatması

“Temel Politika ve Öncelikler” başlığı altında siber suçlarla mücadele ile ilgili politikalar ve hedefler ortaya konulmuştur[7,8].

D. TÜRKİYE BİLİMSEL ve TEKNOLOJİK ARAŞTIRMA KURUMU

Ülkemizde Siber güvenlik ve adli bilişim konularıyla ilgilenen kurumlardan birisi de TÜBİTAK’tır. Bu amaçla Siber Güvenlik Enstitüsünü kurmuştur. Kuruluşun faaliyet alanı ve kuruluş amaçları şöyledir[14]. Ulusal siber güvenlik kapasitesinin artırılmasına yönelik çalışmalar gerçekleştirmek amacıyla kurulan Siber Güvenlik Enstitüsü’nün (SGE) faaliyetleri 1997 yılında Bilişim Sistemleri Güvenliği (BSG) Birimi adı ile TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) altında başlamıştır. 2012 yılından bu yana ise TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak faaliyetlerini sürdürmektedir. SGE; siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmek; askeri kurumlara, kamu kurum ve kuruluşlarına ve özel sektöre çözüme yönelik projeler gerçekleştirmektir. Siber güvenlik enstitüsünün amacının doğrudan adli bilişim alanıyla ilgili olduğu kuruluş amacıyla açıkça görülmektedir.

E. JANDARMA GENEL KOMUTANLIĞI

Jandarma genel komutanlığı ülkemizde adli bilişim incelemeleri yapan ve Avrupa Kriminal Laboratuvarları Ağı (ENFSI) tarafından akredite olan bir laboratuvara sahiptir. Adli bilişim alanındaki incelemeleri ve uzman yetiştirme süreçlerinin tümünü kendi bünyesinde gerçekleştirmektedir. Dışarıdan personel alımı yoluyla da istihdam sağlanabilmekte fakat bu alanda yeterli eğitim verilmediğinden alınan personelin tekrar eğitimden geçirilmesi gerekmektedir. Jandarma Genel Komutanlığının 2013 ve 2014 yılı faaliyet raporları incelendiğinde bilişim suçlarıyla ilgili vaka sayılarında ciddi artış olduğu görülmektedir [15,16].

E. ÖZEL SEKTÖR

Kurumların bu alanda verdikleri önem görülmekle birlikte, ülkemizde bu alanda yetişmiş insan gücünde oldukça sıkıntı yaşanmaktadır. Genellikle bu alanda alınan özel eğitimler veya bilgisayar bilimleri alanından mezun olan kişilerin kişisel merakları sonucunda insan gücü elde edilebilmektedir. Bilişim teknolojilerinin hızlı gelişimi bu alandaki insan gücü ihtiyacının da artacağını göstermektedir. Özel sektörde bilirkişilik faaliyetleri gösteren çeşitli firmalar bulursa da çalışan uzmanların birçoğu özel ilgi ile ya da çeşitli kurslarla bu alanda uzmanlaşmaya çalışmaktadır. Doğru eğitim içeriği ile bu alanda temelde yetişecek insan gücünün özel sektör açısından da önemi büyüktür.

IV. SONUÇ

Bilişim ve internet teknolojilerinde yaşanan hızlı gelişim sürecinin hayatımızın pek çok alanında olumlu sonuçları yanında, kontrol edilmesi güç sorunları da beraberinde getirdiği görülmektedir. Bugün bilişim alanındaki hızlı gelişmeler bilişim suçları olgusuyla karşı karşıya kalmamıza neden olmuştur. Her geçen gün bu yolla işlenen suçlarda artış ve çeşitlilik görülmektedir. İnsanların sosyal yaşantı ve iş hayatlarına büyük kolaylık getiren bu teknoloji, aynı zamanda suç işleme eğiliminde olanlara, daha önce tanımı yapılmış veya yapılmamış çok geniş bir suç işleme potansiyelini de sunmaktadır. Ayrıca daha önce belli bir bölge ile sınırlı olan bu suçlar bilişim teknolojilerinin sunmuş olduğu imkânlarla bu sınırları aşmakta ve küresel hale gelmektedir. Bu nedenle bu alandaki insan gücünün artırılması büyük önem taşımaktadır. Üniversitelerdeki ilgili fakültelerde açılacak Adli bilişim mühendisliği, siber güvenlik mühendisliği gibi bölümlerle ülkemizdeki bu alandaki açığın kapatılması gerekmektedir.

V. KAYNAKLAR

- [1] L. Zhijun, W. Ning, *Developing a Computer Forensics Program in Police Higher Education, 4th International Conference on Computer Science & Education*, Nanning-China , (2009) 1436.
- [2] J. Swartz, http://www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm?POE=TECISVA (*Erişim tarihi: 15th of December, 2015*).
- [3] Türkiye İstatistik Kurumu, <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=16198> (*Erişim tarihi: 11th of May, 2015*).
- [4] Adalet Bakanlığı, <http://www.abgm.adalet.gov.tr/pdf/KANUN.pdf> (*Erişim tarihi: 10th of July, 2015*).
- [5] O. Turhan, *Bilgisayar Ağları ile İlgili Suçlar*, Planlama Uzmanlığı Tezi, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Ankara, (2006).
- [6] U. Boğa, *Bilişim Suçlarıyla Mücadele Yöntemleri*, Uzmanlık Tezi, T.C. Radyo Televizyon Üst Kurulu, Ankara (2011).
- [7] T.C. Adalet Bakanlığı, 2010-2014 Stratejik Plan, Adalet Bakanlığı, Ankara, (2010).
- [8] Emniyet Genel Müdürlüğü, 2009-2013 Stratejik Plan, Emniyet Genel Müdürlüğü, Ankara, (2009).
- [9] Emniyet Genel Müdürlüğü, 2015 Yılı Performans Programı Strateji Raporu, İçişleri Bakanlığı, Ankara, (2015).
- [10] Emniyet Genel Müdürlüğü, 2012 Yılı Performans Programı, Emniyet Genel Müdürlüğü, Ankara, (2012).
- [11] TÜBİTAK, Siber Suçlarla Mücadelede TÜBİTAK ve Emniyet İşbirliği, <https://www.tubitak.gov.tr/tr/haber/siber-suclarla-mucadelede-tubitak-ve-emniyet-isbirligi>, (*Erişim tarihi: 10th of July, 2015*).
- [12] T.C. İçişleri Bakanlığı, 2015 Yılı Performans Programı Strateji Raporu, İçişleri Bakanlığı, Ankara, (2015).
- [13] T.C. İçişleri Bakanlığı, 2010-2014 Stratejik Plan, İçişleri Bakanlığı, Ankara, (2010).
- [14] TÜBİTAK Bilgem Siber Güvenlik Enstitüsü, <http://sge.bilgem.tubitak.gov.tr/> (*Erişim tarihi: 13th of July, 2015*).
- [15] Jandarma Genel Komutanlığı, 2013 Yılı Faaliyet Raporu, Jandarma Genel Komutanlığı, Ankara, (2013).
- [16] Jandarma Genel Komutanlığı, 2014 Yılı Faaliyet Raporu, Jandarma Genel Komutanlığı, Ankara, (2014).