Fırat Üniversitesi Sosyal Bilimler Dergisi
*Fırat University Journal of Social Science*
Cilt: 25, Sayı: 2, Sayfa: 229-248, ELAZIĞ-2015

# TÜRKİYE'DE POLİSİN SİBER SUÇLARLA MÜCADELE POLİTİKASI: 1997-2014

*Srugling Cyber Crime Policy of The Police in Turkey*

**Ufuk TAŞCI**[1] **Ali CAN**[2]

**ÖZET**

Siber suçlar, oldukça yeni bir suç türüdür. Özellikle internetin yaygınlaşması ve hayatın her alanına girmesiyle bu suç türü ve suçu işleyenler artış göstermiştir. Bu nedenle, siber suçlarla mücadele etmek için uzman polis birimlerinin ve yeni suç önleme politikasının oluşturulması gerekmiştir.

Bu çalışmada, Emniyet Genel Müdürlüğünün (EGM) siber suçlarla mücadelede geliştirdiği politikası, kamu politikası sürecinde Klasik Yaklaşım Modeli üzerinden analiz edilmiştir. Çalışmada kurumsal bir analiz yöntemi uygulanmıştır. EGM'nin, siber suçlarla mücadelede çıkardığı yasal düzenlemeler, oluşturduğu teknik birimler, personel politikası ve bu politikaları geliştirmeye iten etkenler incelenmiştir. EGM'nin siber suçlarla mücadelede, 2003'li yıllardan sonra biraz geçde olsa bir takım hukuki mevzuatların yürürlüğe girmesi ve devletin siber suçlarla mücadeleye önem vermesiyle politikalarına hız verdiği, 2011 yılı itibariyle kurumsal yapılanmasının büyük bölümünü tamamlayarak, diğer teknik konulara önem veren kurumsal politikaları gerçekleştirdiği görülmüştür.

**Anahtar Kelimeler:** Siber Suç, Polis, Politika, Mücadele,

**ABSTRACT**

Cybercrime is a fairly new crime typology. The spread of the internet into every area of daily life increases the number of crime and criminals of this type of crime. Therefore, establishing specialist police units and creating new crime prevention policy is a must to fight cybercrime effectively.

In this study, the fighting cybercrime policy developed by the General Directorate of Security (GDS) has been analyzed through Classic Public Policy Approach Model. Legislations by the GDS's to fight cybercrime, creating technical units, personnel policy and motivating factors to develop these policies have been discussed. After the years of 2003, GDS has started to focus on cybercrime because of a number of regulatory new legislations and the struggle of cybercrime became a state policy. As of 2011, GDS completed a large part of the institutional structure on cybercrime and perform corporate policy emphasis on other technical issues.

**Key Words:** Cybercrime, Police, Policy, Counter Cyber Crime.

## GİRİŞ

Çoğu teknolojik gelişmelerde olduğu gibi askeri amaçlar için keşfedilen internet, 1960'lı yıllarda askeri iletişim projesi olarak başlamış ve 1990'lı yıllarda toplum hayatına girmiştir (Friedman, 2011:290, Avşar ve Güngören, 2010: 30). Türkiye'ye ilk internet ODTÜ tarafından uzun yıllar süren alt yapı çalışmaları neticesi 12 Nisan 1993 yılında bağlanmıştır (internetarsivi.metu.edu.tr, 2015). Haziran 2014 verilerine göre 7 milyarı geçen dünya nüfusunun yaklaşık % 42,3'ü yani 3.035.749.340 kişi interneti kullanmaktadır. Yine Türkiye'de internet kullanımı günden güne artmakta, nüfusun % 56'7'si yani 46.282.850 kişi internet kullanmaktadır **(**internetworldstats.com, 2015).

Son yirmi yıldır en hızlı büyüyen bilişim sektörü olan internet; sınırları tanımlanamayan, kuralları konamayan, demokratik hatta anarşik bir platform olarak kabul edilmekte, vatandaşlara kendisini ve düşüncesini serbestçe, kimliğini ortaya koymadan ifade etme hürriyeti tanımaktadır (Yetim, 2014: 179). Bu gelişme, dünyayı küçük bir köy haline getirirken, bilgisayar ortamında sesli

[1] Dr. Elmadağ Polis Meslek Yüksek Okulu – ANKARA e-mail: ufuktasci@hotmail.com
[2] Dr. Polis Akademisi, e-mail: can_ali73@hotmail.com

ve görüntülü her türlü sohbet, özel hayatın paylaşılması, internet üzerinden alışveriş gibi birçok yeni gelişmelere öncülük etmiş, sonuçları olumlu veya olumsuz yeni alışkanlıklar kazandırmıştır. Hatta bu gelişme siber psikoloji olarak adlandırılan ve yeni gelişen teknolojilerin insan davranışı üzerindeki etkilerini inceleyen bir bilim dalının doğmasına neden olmuştur (EUROPOL, 2014: 62).

Verilere göre; her gün 294 milyar e-mail gönderilmekte, Google'da 6 milyar arama yapılmakta, facebook'ta 3,5 milyar mesaj gönderilmekte ve twitter'da 40 milyar tweet paylaşılmaktadır (gwava.com, 2015). Bu gelişme teknolojinin kaçınılmaz bir sonucu olarak kabul edilebilir iken; aynı zamanda ceza kanunlarında suç olarak kabul edilen dolandırıcılık, sahtecilik, özel hayatın gizliliği, casusluk, verilere izinsiz erişim gibi suçların internet ortamında işlenmesinin de önünü açmış bulunmaktadır. Ancak siber suçların sürekli yeni tipleri ortaya çıktığı için, bu suçları tümüyle kapsayan bir değerlendirme yapmak her zaman kolay olmamaktadır (Avşar ve Güngören, 2010: 123).

Kamu politikasında klasik yaklaşım modeli, basit bir çerçevede yürütülmekte olan kamu politika sürecinin, başlamasından sona ermesine kadar tüm aşamaları ayrı olarak ele almakta, her bir aşamaya etki eden faktörleri incelemekte, sonuçların kısa ve uzun zamanlardaki etkilerini değerlendirmektedir. Böylece çok karmaşık nitelenen kamu politika süreci sistematik olarak açık ve anlaşılır bir konuma gelmektedir (Kaptı, 2011: 23). Bu model, bir problemin *gündeme gelişi*, problemin çözüm yollarının bulunması, çözüm olabilecek etkili alternatif yolların belirlenmesi ve belirlenen yolların etkili şekilde *formüle edilişi,* çözüm için formüle edilen yolların politikacılar tarafından uygun olanının *kanunlaştırılması*, problemin çözümü için ortaya konan politika veya politikaların ilgili birim ve uygulayıcılar tarafından *uygulanması* ve uygulanan politikaların ne derece hedeflenen noktaya ulaştığı ve ne ölçüde çözebildiğinin *değerlendirilmesi* olarak beş aşamalı bölümden oluşmaktadır (Kaptı, 2011: 25).

Kamu politikalarının oluşturulması bazı nedenlerden kaynaklanmaktadır. Teknolojik, küresel ve yerel gelişmeler başlıca nedenler olarak sıralanabilir. Kamu politikalarının oluşturtmasından sonra politikayı icra edecek aktörlerin belirlenmesi gerekmektedir. Dolayısıyla bir kamu politikasını çalışmak disiplinler arası bir yaklaşımı zorunlu kılar. Çünkü kamu politikası bir süreç olarak kabul edilmekte, bu sürecin hangi aşamasında çalışılırsa çalışılsın süreçteki kararlar, aktörler, olaylar, hareketler ve benzeri unsurlar ele alınmak durumundadır (Çevik ve Demirci, 2012: 17). Bu çalışmada EGM'nin 1997-2014 yılları arasında uyguladığı siber suçlarla mücadele politikasının analizi, kurumsal model analizi kullanılarak yapılmıştır. EGM'nin siber suçlarla mücadele politikasının, Türkiye'de siber suçlara yönelik yasal düzenlemelerin 1991 yılında yürürlüğe girmesine rağmen, 1997 yılından başlayarak 2011 yılında ancak belirli bir noktaya ulaştığı görülmektedir. Bu nedenle EGM'nin siber suç politikasının analiz edilerek, geçirdiği aşamaların, politikanın oluşumunu etkileyen yasal ve diğer faktörlerin, politikada belirlenmesi ve uygulanmasında rol oynayan aktörlerin analiz edilmesinin, bu alanda çalışan kişi ve kurumlara, ayrıca suç önleme politikalarının analizi çalışmalarına örnek olacağı düşünülmektedir.

## 1. SİBER SUÇLAR NEDİR VE ÖZELLİKLERİ NELERDİR?

İnternetin karmaşık yapısı ve kullanımının yaygınlaşması beraberinde birtakım ciddi problemler getirmiş ve internetin kötü amaçlarla kullanılması sonucunda "siber suçlar" olarak adlandırılan yeni suç türleri ortaya çıkmıştır (Balcıoğlu, 2014: 66). Bu suçların, diğer suçlardan farklı özelliklerinin olması, kaçınılmaz olarak Kriminoloji'de yeni bir alanın yaratıcısı olmuştur. Bu alan suç literatüründe değişik adlarla anılsa da daha çok *Siber Suçlar* olarak adlandırılmaktadır. Polis kaynaklarında internete özgü suçlar olarak adlandırılan (egm.gov.tr. 2015c) bu suçlarla ilgili olarak bazı çalışmalarda siber suç kavramının; bilgisayar suçu, elektronik suç, dijital suç veya ileri teknoloji suçları gibi kavramlarla ifade edildiğini belirtilerek, bu suçun tanımın kapsadığı geniş alan nedeniyle, siber suçların değişik şekil ve içeriklerde olabileceğini, klasik suçların siber alan ile farklı biçim ve yoğunlukta temas edebileceğini ifade edilmektedir. Dolayısıyla teknolojideki

gelişimin tahmin edilemezliği böyle geniş bir tarifi zaruri kılmaktadır (Hekim ve Başıbüyük; 2013: 136).

Siber suçları, herhangi bir suçun elektronik ortam içinde işlenebilme imkânı bulunması ve bu ortam içerisinde gerçekleştirilen fiilin hukuka aykırı veya suç olarak tanımlanması halinde oluşan suç, siber suç olarak tanımlanmakta ve üç grupta tasnif edilmektedir. Bunlar; devlet ve kamu düzenine karşı işlenen siber suçlar, mal varlığına karşı işlenen siber suçlar ve kişilere karşı işlenen siber suçlardır (Balcıoğlu, 2014: 67). Siber suçlar; bilişim ortamında işlenebilen klasik suçlar arasında sayılmayan, bilgisayar ve internete özgü suçlar olarak *dar anlamda* suçlar ile bilişim sistemleri kullanılarak veya bilişim sistemlerinden yararlanılarak işlenen *geniş anlamda siber suçlar* olarak ikiye ayrılmaktadır (Avşar ve Güngören, 2010: 124-131).

Suç, "kanunlarda açıkça yasaklanan ve karşılığında bir ceza ön görülen her türlü eylem" olarak tanımlanmaktadır (Dolu, 2011: 32). Siber suçlarda, klasik suçlardan farklı olarak, bilişim teknolojileri olarak adlandırılan, bilgisayar ve dünya genelinde 2014 yılı itibariyle 1.2 milyara ulaşması beklenen akıllı telefonlar (EUROPOL, 2014: 9) gibi araçlar kullanılarak gerçekleştirilen bir suç türüdür. Nitekim bu suçların geleneksel/klasik suçlardan farkları şu şekilde sıralanabilir;

a. Siber suçun neticesi başka bir ülkede meydana gelebilmekte, uluslararası alanda suç işlendiğinde ise delil toplama faaliyetleri zorlaşmaktadır,

b. İnternet ortamında işlenen suçlarda risk azalmakta, bir kısım ülkelerdeki yasal boşluklar nedeniyle suçun işlenmesine uygun bir zemin oluşabilmektedir,

c. Siber dünyada anonimleşme ve anonim kalma, suç işlemeye uygun özgür bir ortam sağlamaktadır,

d. Siber suçlar, çok failli ve birbirini daha önceden tanımayan farklı ülkede ikamet eden insanların işbirliği yaparak işledikleri suçlar olarak ortaya çıkmakta, ancak suçlara iştirak eden kişiler çoğu zaman aynı dili dahi kullanmamaktadır,

e. Yeni çıkan siber suç işleme yöntemine karşın önlemler bulunduğu anda, daha gelişmiş ve farklı bir suç işleme yöntemi geliştirilmektedir. Teknolojide yaşanan hızlı ilerlemeler, suçun işleniş yöntemlerinin, araçlarının ve çeşitlerinin devamlı değişmesine ve gelişmesine neden olabilmektedir,

f. Siber suçların sınır tanımayan niteliğinden dolayı bu suçlarla mücadelede internetin ulaştığı bütün ülkelerin ortak bir çabasını gerektirmektedir (Yetim, 2014: 181-217),

g. Siber suçları ortadan kaldırmak veya bir çerçeve içinde sınırlandırmak mümkün gözükmemekte, çok değişik yöntemler kullanılarak bu suçlar çoğaltılmaktadır (Avşar ve Güngören, 2010: 124),

h. Siber suçları işleyenler, çok az bilgiyle ciddi siber saldırılar gerçekleştirebilmekte, 1980'li yıllara göre oldukça uzmanlık isteyen kişilerin siber suçları işleme kapasitesi günümüzde azalmakta, siber suçların işlenme oranı ise artmaktadır (Hekim ve Başıbüyük, 2013: 153),

i. Siber suçu işleyenler arasındaki ilişkiler genellikle geçici veya ticari nitelikte olup, geleneksel bir organize suç örgütünün yapısı ve hiyerarşisi bu gruplarda görülmemektedir (EUROPOL, 2014: 4),

j. Siber suçlular, saldırılarını gerçekleştirmek için güvenlik, anonimlik, esneklik ve emniyet birimlerinin müdahalesine karşı direnç sağlayan bir altyapıya ihtiyaç duymaktadır (EUROPOL, 2014: 12),

k. Siber suçları işleyenler, çok büyük zararlar verebilmelerine rağmen, suçun sanal ortamda işlenmesi ve verilen zararın gözlenememesi nedeniyle, verdikleri zarardan dolayı herhangi bir sorumluluk hissetmemektedirler (Dolu, 2011: 201). Yani normalde cinsel organın gerçek yaşamda gösterilmesi, çok ahlaki karşılanmazken ve toplumda büyük bir kesim bu davranışı yapmaya cesaret edemezken, sanal ortamda yapılan sohbetlerde kişiler cinsel organlarını yüzünü gizleyerek çok rahatlıkla yapabilmektedirler.

## 2. İÇ VE DIŞ MEVZUATTA SİBER SUÇLARA YÖNELİK DÜZENLEMLER

Kolluk hizmetleri ülke için önemli sayılan hizmetlerin başında gelmekte, suçu önlemek ve önlenemeyen suçların takibini yapmak olarak tanımlanmaktadır. İç güvenlik olarak adlandırılan alanda birçok kamu politikası alt başlığı bulunmakta, bunlardan biri de, siber suçlarla mücadele politikası olarak kabul edilmektedir (Çevik ve Demirci, 2012: 24-25). Bu suçların en büyük özelliği, teknolojik gelişmelerle çok yakın bir ilişki içerisinde olmasıdır. Bu nedenle, fiziksel kapasiteden ziyade zihinsel kapasitesi yüksek personele ve yüksek düzeyde teknolojik donanıma sahip bir polis teşkilatını oluşturacak politikanın oluşturulması gerekmektedir.

Siber suç politika veya stratejilerinin temel unsurları; önleyici tedbirlerin alınması, mevzuatın oluşturulması, siber suçlarla mücadelede özel kolluk birimleri ve özel savcılık hizmetlerinin oluşturulması, kurumlar arası işbirliğinin sağlanması, kolluk ve adli personel eğitimi, kamu/özel sektör işbirliği, etkili uluslararası işbirliği, kara para aklamanın ve dolandırıcılığın önlenmesi için mali soruşturma ve cinsel şiddete karşı çocukların korunması olarak kabul edilmektedir (coe.int, 2015). Bu unsurlar, siber suçlarla mücadele politikasının belirlenmesi ve uygulanmasında, birden fazla aktörün rol oynadığını ve birbirleriyle bağlantılı olduğunu göstermektedir.

Polisin genel olarak iki temel görevi bulunmaktadır. Bunlar, toplumsal düzenin sağlanmasıyla ilgili kanun, nizam ve emirlerin yerine getirilmesinin sağlanması ve suçun oluşmasını önleyici tedbirlerin alınması olarak polisin idari görevi ve suç işlendikten sonra suçun ve suçluların ortaya çıkarılması amacıyla suç soruşturmasının yürütülmesi işlemleri olarak adlandırılan polisin adli görevidir (egm.gov.tr, 2015a: 13). Polise adli, idari ve trafik gibi özel görevler olmak üzere; 271 kanun, 51 tüzük, 168 yönetmelik, 87 Bakanlar Kurulu Kararnamesi ve 62 yönerge görev ve sorumluluk vermektedir (egm.gov.tr, 2015a: 14). Polis teşkilatında 23.10.2014 tarihi itibariyle 257.776 adet polis memuru ve rütbeli personel bulunmaktadır (egm.gov.tr, 2015b: 19). 2015 yılı itibariyle EGM'nin merkezi teşkilatında 39 daire başkanlığı bulunmaktadır (egm.gov.tr, 2015c).

Kanunlar polise yetki ve sorumluluk vermektedir. Genel kabul gören anlayış yetki olmadan görev ve sorunluluk olmayacağıdır. Kurumlar, kanunlardan aldığı yetkiler doğrultusunda kuruluş amaçlarına göre hizmet veren organizasyonlardır. Polisin en temel görevi suçun önlenmesi ve suçun aydınlatılmasıdır. Dolayısıyla kanunlarda polise suçun önlenmesi için verilmeyen herhangi bir görev ve polisin takibini gerektirmeyen herhangi bir eylemin suç olarak yasada açıkça ifade edilmemesi durumunda polisin herhangi bir suç önleme ve aydınlatmaya yönelik politika geliştirmesi mümkün gözükmemektedir. Yani yasalarda belli olaylar suç olarak kabul edilmezse, yürütmenin eli kolu bağlanmakta ve yeterli usul hukukunun bulunmadığı durumlarda yüksek teknoloji kullanan suçluların takibatı neredeyse imkânsız hale gelebilmektedir (EUROPOL, 2014: 61). Polisin adli kolluk görevini yerine getirirken, kendisine görev ve sorumluluklar veren belli başlı kanunlar bulunmaktadır. Aşağıda özellikle siber suçlarla ilgili olarak polise öncelikli olarak yetki ve sorumluluk veren kanunlara yer verilmiştir. Ancak aşağıda belirtilen kanunların dışında sair kanunlarda, siber konusu olabilecek suçlar oluşabilmektedir (Avşar ve Güngören, 2010: 169-172).

Siber suçlar Türkiye'nin iç mevzuatında ilk defa, 1991 yılında 765 sayılı ***Türk Ceza Kanununda,*** (TCK) 3756 sayılı kanunla Md. 525/a, b, c ve d maddeleriyle eklenen Bilişim Alanında Suçlar bölümüyle girmiştir. 2004 yılında çıkarılan 5237[3] sayılı yeni TCK'da siber suçlar, siber suçların güncel gelişimi gözönüne alınarak oldukça ayrıntılı şekilde açıklanmıştır. 5237 sayılı yeni TCK'da bilişim alanında suçlar hali hazırda;

a. Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m.243),
b. Bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m.244/1-2),
c. Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m.244/4),

[3] R.G. 12.10.2004, Sayı, 25611.

d. Banka veya kredi kartlarının kötüye kullanılması suçu (m.138) olarak belirlenmiştir.

Ayrıca özel hayata ve hayatın gizli alanına karsı suçlar bölümündeki siber suçları;

a. Kişisel verilerin kaydedilmesi (m.135),
b. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme (m.136),
c. Verilerin yok edilmemesi suçları (m.138) olarak belirlenmiştir.

TCK'da bilişim sistemleriyle işlenebilecek diğer suçlar; 91. md. 6. fıkra organ ticareti, 105. md. cinsel taciz, 106. md. tehdit, 107. md. şantaj, 124. md. haberleşmenin engellenmesi, 125. md. hakaret, 132. md. 1. fıkra haberleşmenin gizliliğinin ihlal edilmesi, 134. md. 2. fıkra özel hayatın gizliliğini ihlal, 142 md. 2. fıkra (e) bendi bilişim sisteminin kullanılması yoluyla işlenen hırsızlık, 58. md. 1. fıkra 1. bendi bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık, 190. md. 3. fıkra uyuşturucu veya uyarıcı madde kullanılmasını alenen özendirme veya bu nitelikte yayın yapma, 213. md. 1. fıkrası ve 218. md. gereğince cezalandırılacak olan halk arasında korku ve panik yaratmak amacıyla tehdit, 215. md. 1. fıkra 218. md. gereğince cezalandırılacak olan suçu ve suçluyu övme 216. md. ve 218. md. gereğince cezalandırılacak olan halkı kin ve düşmanlığa tahrik veya aşağılama, 217 md. ve 218. md. gereğince cezalandırılacak olan yasalara uymamaya tahrik, 220 md. 8. fıkra örgütün veya amacının propagandasını yapma eylemi, 226. md. müstehcenlik, 258. md. göreve ilişkin sırrın açıklanması, 267. md. iftira suçu, 285. md. gizliliği ihlal suçu 299. md. Cumhurbaşkanına hakaret, 300. md. devletin egemenlik alametlerini aşağılama 301. md. Türklüğü, cumhuriyeti, devletin kurum ve organlarını aşağılama ve 318. md. halkı askerlikten soğutma olarak sıralanmaktadır (Güngör, 2007: 79-147). Görüldüğü TCK'da suç olarak kabul edilen ve aynı zamanda asayiş ve terör alanlarına giren birçok suç siber suç kapsamına girebilmektedir.

TCK'dan ayrı olarak siber suçların düzenlendiği diğer bir kanun olan 5846 sayılı ***Fikir ve Sanat Eserleri Kanununda***[4] siber suçlara konu olabilecek eylemler düzenlenmiştir. Bu kanunda, özellikle bilgisayar programlarına ilişkin telif hakkı suçları ve hukuka aykırı hareketler özel olarak düzenlenmiş, internet aracılığıyla telif haklarına aykırı fiiller de bu kapsama alınmıştır. Kanuna göre, bilgisayar programları, web sayfaları dahil olmak üzere her türlü fikir ve sanat eserlerini izinsiz olarak kullanan, çoğaltan, işleyen, bilgisayar programlarını koruyan aygıtları geçersiz kılan teknik araçları bulunduran, dağıtan ve bu tip eser ve programları izinsiz olarak yayınlayanlar siber suç olarak kabul edilmektedir (Avşar ve Güngören, 2010: 148).

Siber suçların internet ortamında artan oranda işlenmesi, internetle alakalı bazı özel kurumların oluşması ve belli bir düzenin geliştirilmesi amacıyla, 5651[5] sayılı ***İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*** kabul edilmiştir. Bu kanun; 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 usulleri düzenlemek amacıyla çıkarılmıştır (Md: 1). Kanunla internet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan; 5237 sayılı TCK'da yer alan; İntihara yönlendirme (madde 84), Çocukların cinsel istismarı (madde 103, birinci fıkra), Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190), Sağlık için tehlikeli madde temini (madde 194), Müstehcenlik (madde 226), Fuhuş (madde 227), Kumar oynanması için yer ve imkân sağlama (madde 228) suçlarıyla 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar hakkında ilgili mercilerin kararıyla erişimin engellenmesine karar verilebileceği hüküm ve esaslar hüküm altına alınmıştır (Md: 8).

[4] Bu kanunda, siber suçların düzenlenmesine yönelik olarak; 2001 tarihinde 4630, 2004 tarihinde 5101 ve 2008 tarihli 5728 sayılı kanunlarla değişiklikler yapılarak, eserlerin siber suçlardan korunması amaçlanmış, eserlerin her türlü materyallerle izinsiz çoğaltılması halinde soruşturma ve ceza hükümleri ayrıntılı şekilde açıklanmıştır.

[5] R.G. 23.05.2007, Sayı, 26530.

Klasik veya siber suçların takibi, şüphelilerin yakalanması, suç delillerin elde edilmesi, muhafazası gibi adli kolluk faaliyetlerinin Cumhuriyet Savcılarının[6] gözetiminde icrası sırasında polisin uyacağı usul ve esaslar 5271 sayılı ***Ceza Muhakemesi Kanunda***[7] açıklanmaktadır. Bu kanunda, polisin adli kolluk görevlerini yerine getirirken uyacağı usul esasları ayrıntılı şekilde yer almaktadır. Siber suçlarda toplanan deliller diğer klasik suçlardan farklı olarak bilişim sistemleri aracılığıyla işlenmeleri nedeniyle dijital deliller olarak adlandırılmaktadır (Yetim, 2014: 184). Bu nedenle 5271 sayılı kanunda ayrı bir maddede, Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve Elkoyma başlıklı bölümde, siber suçların işlendiği bilişim teknolojileri araçlarında hukuka uygun olarak kolluk tarafından yapılacak delillendirme faaliyetlerinin usul ve esasları yer almaktadır. Bu maddeye göre;

*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. İstemesi 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 (Md: 134).*

Ancak bu kanunun uygulanmasında bazı eksiklerin var olduğu ifade edilmektedir. Bunlar şu şekilde sıralanmaktadır.

a. Bilgisayarın şifrelenmiş olduğunun veya gizlenmiş bilgiler barındırdığının nasıl anlaşılacağı,

b. Elkoyma yetkisinin iki durumla sınırlanmasının olay yeri inceleme birimlerinin çalışmasını zorlaştırıcı olması,

c. İçinde suç unsuru (çocuk pornografisi vb.) bulunan dijital medyanın kopyalandıktan sonra iade edilip edilmeyeceği veya hangi formatta verileceği,

d. Yedeklerin kimin tarafından, nasıl ve ne kadar süre muhafaza edileceği,

e. Sisteme elkoymaksızın da kopyasının alınabileceği, bu durumda alınan verilerin kâğıda yazdırılması sırasında binlerce tutabilecek kâğıdın olması halinde ne yapılacağı hususlarının kolluk birimlerinde sıkıntılara neden olduğu ifade edilmektedir (Hekim ve Başıbüyük, 2013: 152).[8]

---

[6] Suçların işlenmesi halinde; suçun aydınlatılması, genel olarak delillerin elde edilmesi ve suçluların yakalanması olarak tanımlanabilecek polisin adli görevi devreye girmekte ve adli kolluk olarak tanımlanmaktadır. Bu anda polisin amiri de değişmekte ve Cumhuriyet Savcıları polisin adli amiri olarak kabul edilmektedir. Adli kolluğun görevleri ***Adli Kolluk Yönetmeliğinde***; "*Adlî kolluk görevlileri, maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, Cumhuriyet savcısının emirleri doğrultusunda şüphelinin lehine veya aleyhine olan tüm delilleri, kanunda ön görülen koşullara uyarak toplamak, muhafaza altına almak ve bunları bir fezleke ile Cumhuriyet savcısına sunmakla yükümlüdür. Hukuka aykırı delil elde edildiğinin tespiti hâlinde, fezlekede bu hususa da yer verilir. Adlî kolluk görevlileri diğer soruşturma işlemlerini de aynı titizlikle yerine getirir"* (Md: 6/6) şeklinde açıklanmaktadır.

[7] R.G. 17.12.2004, Sayı, 25673.

[8] Hâlbuki polis, yasaları egemen kılmak, yasalara uymayı sağlamak ve yargılama görevini yardımcı olmak için meydana getirilen sistemin önemli bir parçası olarak kabul edilmektedir. Sisteme ilişkin eksik ve aksaklıklar polis içinde

Türkiye'nin iç mevzuatının dışında, siber suçlarla mücadelede kabul ettiği önemli bir uluslararası sözleşme olan ve Avrupa Konseyi (AK) tarafından hazırlanan ***Siber Suçlar Sözleşmesini***[9] 10.11.2010 tarihinde imzalamış, 6533 sayılı (Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun) kanun olarak meclis tarafından uygun bulunarak 2 Mayıs 2014 tarihinden itibaren bir kısım çekincelerle birlikte yürürlüğe konmuştur (Yetim, 2014: 187). Bu sözleşme internet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası sözleşmedir. Özellikle telif haklarının ihlali, bilgisayarla bağlantılı sahtecilik, çocuk pornografisi ve güvenlik ağlarının ihlali konuları üzerine odaklanmaktadır. Sanal ortamda işlenen suçların ortak tanımlarının yapılmasını, bu alanda ülkelerin maddi ceza hukuku unsurlarını uyumlu hale getirmeyi, suçların soruşturulması ve kovuşturulması için gerekli olan yerel ceza usul hukuku yetkilerini sağlamayı ve etkin bir uluslararası işbirliği rejimi oluşturmayı amaçlayan ve küresel düzeyde etkilere sahip olabilecek bir hukuki belge olarak görülmektedir (tbmm.gov.tr, 2015). Yani Türkiye'nin iç politikasında, siber suçlarla mücadele politikasını etkileyen önemli dış faktör olarak gözükmektedir. Türkiye bu sözleşmeyi 2010 yılında imzalayıp 2014 yılında onaylasa da, 2004 tarihli 5237 ve 2007 tarihli 5651 sayılı kanunların ve 5846 sayılı kanunlarda yapılan değişikliklerin,[10] bu sözleşmenin içeriği, amacı ve tanımlarından kısmen de olsa etkilenmiş şekilde kabul edildiği söylenebilir.

## 3. POLİS İSTATİSTİKLERİNDE SİBER SUÇLAR: 2003:2012 ARASI

Polis sorumluluk alanlarında gerçekleşen siber suçların istatistikleri, EGM'nin faaliyet raporlarında ve bazı kaynaklarda yer almaktadır. Bu yayınlarda istatistikler genelde; Kredi Kartı[11] Sahteciliği ve Dolandırıcılığı, Banka Dolandırıcılığı, Bilişim Suçları ve Dolandırıcılığı, İnternet Aracılığıyla Dolandırıcılık ve Diğer şeklinde sınıflandırılmaktadır. Özellikle ilk yıllarda bankacılık sektörünü ilgilendiren siber suçlar üzerinde bir yoğunlaşma görülmektedir. 2007 itibariyle "Diğer" şeklinde sınıflandırılan suçların -ki bunlar hakaret, telif hakkı suçları, cinsel istismar, özel hayatın gizliliği gibi suçların olma ihtimali fazladır- istatistiklere dahil edildiği görülmektedir. Sınıflandırma daha çok maddi kayıpları içeren suçları içermektedir. 2003 ile 2012 yılları arasında ulaşabilen istatistiklerde olay sayıları ve şüpheli sayıları iki tablo halinde sunulmuştur (Güngör, 2007: 149, EGM, 2008: 23, kom.pol.tr, 2015[12], Tekeli, 2011: 189, EGM, 2010: 35, EGM, 2011: 95, EGM, 2012: 52).[13]

söz konusu olduğunda polisin suçla ilgili çalışmalarında yargı mercilerini de etkileyen sorunlar çıkmaktadır (Doig, 1970: 63). Bu eksikliklerin giderilmesi için yasal değişikliklerin yapılması gerekmektedir.

[9] Bu sözleşme, 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılmış ve 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. AK dışındaki ülkelerin de taraf olma imkanına sahip olduğu bu sözleşmeye, 2012 yılı itibariyle 32'si AK üyesi ve ABD olmak üzere toplam 33 ülke taraf olmuştur. 14 ülke sözleşmeyi imzalamış; ancak henüz onaylamamıştır (tbmm.gov.tr, 2015).

[10] Sözleşmenin Türkiye tarafından geç imzalanmasının nedeni, Türkiye'nin iç hukuk düzenlemelerinin tamamlanmasının ardından taraf olunmasının uygun olacağı şeklinde ilgili kurumlardan alının görüşlerdir. Nitekim, ilgili bakanlıkların Sözleşmeyle ilgili iç hukuk gereklerinin yerine getirildiğini bildirmeleri üzerine Sözleşme, 10 Kasım 2010 tarihinde Strazburg'da imzalanmıştır (tbmm.gov.tr, 2015).

[11] 2013 yılı itibariyle Türkiye'deki kredi kartı adedi, 57 milyona ulaşmıştır. Kredi kartları ile 2013'te toplam 2,6 milyar alışveriş işlemi ile 387 milyar TL alışveriş cirosu ve 90 milyon nakit çekim işlemi ile de 37 milyar TL nakit çekim gerçekleştirilmiştir (bkm.com, 2015: 33). Dolayısıyla siber suçlular için kolay yoldan para dolandırmanın bir kaynağı olarak gözükmektedir. Nitekim 2007 itibariyle de Kredi Kartı ve Sahteciliği suçlarının sayısında artış dikkati çekmektedir.

[12] Bu kaynak üzerinde KOMDB'nin yayınlamış olduğu yıllık raporlardan; 2001, 2004, 2005, 2006, 2007 ve 2008 yıllarına ait raporlarda, siber suç bölümleri incelenmiş ve tek bir kaynak olarak verilmiştir.

[13] Bu istatistiklerin çoğu EGM kaynaklarına dayanmaktadır. Polisin kendisinin yaptığı çalışmalar sonucunda oluşturulmuştur. Polis istatistiklerinde, sınırlama, kabarıklık ve eksikliklerin bulunduğu, suç tespit yetkisine haiz diğer kamu kurumlarınca müdahale edilen ve adli birimlerce doğrudan işlem yapılan suçların sadece bir kısmının polis istatistiklerinde yer aldığı ve polis istatistikleri ile Adalet Bakanlığı istatistikleri arasında çelişkilerin mevcut olduğu, ülkemizde gerçek suçluluğu ortaya çıkaracak çalışmalar yürütülmemesi eleştirileri getirildiği görülmektedir (Polat, 2008: 4). Örneğin 2004 yılı itibariyle adli kayıtlarda 429 gözüken siber suç sayısı polis kayıtlarında 184 olarak gözükmektedir Türkiye'de mahkeme kayıtlarına geçen ilk bilişim suçunun işlendiği 1990 yılından 2011 yılının Temmuz ayına kadar yıl ve il bazında mahkemelere intikal eden 40 farklı suç maddesine ait 73.185 adet ceza ve hukuk davasıyla ve toplam

**Tablo 1:** 2003-2012 Yılları Arası Siber Suç Sayıları

| *Suçun Nevi Ve Yıllara Göre Olay Sayıları* | *Kredi Kartı Sahteciliği ve Dolandırıcılığı* | *Banka Dolandırıcılığı* | *Bilişim Suçları ve Dolandırıcılığı* | *İnternet Aracılığıyla Dolandırıcılık* | *Diğer* | *Toplam* |
|---|---|---|---|---|---|---|
| *Olay Sayısı 2003* | *80* | *15* | *X* | *X* | *X* | *95* |
| *Olay Sayısı 2004* | *146* | *22* | *16* | *X* | *X* | *184* |
| *Olay Sayısı 2005* | *195* | *9* | *91* | *X* | *X* | *295* |
| *Olay Sayısı 2006* | *122* | *98* | *4* | *X* | *X* | *224* |
| *Olay Sayısı 2007* | *594* | *642* | *416* | *X* | *91* | *1.743* |
| *Olay Sayısı 2008* | *830* | *1.177* | *560* | *X* | *157* | *2.742* |
| *Olay Sayısı 2009* | *1.511* | *550* | *353* | *412* | *45* | *2.871* |
| *Olay Sayısı 2010* | *1.131* | *151* | *972* | *71* | *28* | *2.353* |
| *Olay Sayısı 2011* | *1.772* | *141* | *1.738* | *111* | *31* | *3.793* |
| *Olay Sayısı 2012* | *1.724* | *264* | *3.669* | *278* | *783* | *6.718* |

Ülkemizde kayıtlara giren ilk siber suç 1990 yılında işlenen (1) adet banka kartı dolandırıcılığıdır. 1990-2003 yılları arasında adliyeye intikal eden toplam siber suçu dava sayısı 389 adet olarak gözükmektedir. Bunların çok büyük bölümü banka ve kart dolandırıcılığıdır. Diğer suçlar telif hakkı ve bilişim sistemlerine giriş suçlarıdır. Bu tarihler arasında dava sayılarındaki düşüklüğün sebebi; 5237 sayılı TCK'nın 2004 tarihinde kabul edilmesi ve önceki yıllarda siber suçlarıyla mücadele eden özel kolluk kuvvetlerinin bulunmayışı, bu yıllar arasında bilgisayar kullanımı yaygınlığı ve bilişim okuryazarlığı oranlarının düşüklüğü ve suça maruz kalan şahısların yasal haklardan yoksun oluşu şeklinde yorumlanmaktadır (Köksal ve İlbaş, 2015). 2003-2012 yılları arasında EGM kayıtlarına göre toplam 21.018 siber suç meydana gelmiştir. 2007'den itibaren siber suçlarda artış olduğu gözlenmektedir.

**Tablo 2:** 2003-2012 Yılları Arası İşlenen Siber Suçlarda Yakalanan Şüpheliler

| *Suçun Nevi ve Yıllara Göre Şüpheli Sayıları* | *Kredi Kartı Sahteciliği ve Dolandırıcılığı* | *Banka Dolandırıcılığı* | *Bilişim Suçları ve Dolandırıcılığı* | *İnternet Aracılığıyla Dolandırıcılık* | *Diğer* | *Toplam* |
|---|---|---|---|---|---|---|
| *Şüpheli Sayısı 2003* | *268* | *49* | *X* | *X* | *X* | *317* |
| *Şüpheli Sayısı 2004* | *422* | *72* | *31* | *X* | *X* | *525* |
| *Şüpheli Sayısı 2005* | *543* | *33* | *179* | *X* | *X* | *755* |
| *Şüpheli Sayısı 2006* | *241* | *172* | *9* | *X* | *X* | *422* |
| *Şüpheli Sayısı 2007* | *907* | *1.187* | *764* | *X* | *134* | *2.992* |
| *Şüpheli Sayısı 2008* | *991* | *2.114* | *842* | *X* | *416* | *4.363* |
| *Şüpheli Sayısı 2009* | *2.176* | *1.113* | *534* | *731* | *116* | *4.670* |
| *Şüpheli Sayısı 2010* | *1.005* | *300* | *1.346* | *115* | *134* | *2.900* |
| *Şüpheli Sayısı 2011* | *1.429* | *327* | *1.842* | *283* | *123* | *4.004* |
| *Şüpheli Sayısı 2012* | *630* | *120* | *1.085* | *56* | *289* | *2.180* |

2014 yılı içerisinde başta banka ve kredi kartı dolandırıcılığı olmak üzere online kumar, yetkisiz erişim ve sistem engelleme gibi suç türlerine yönelik yapılan operasyonlarda 2.788 şüpheli şahıs yakalanarak adli mercilere sevk edilmiştir (EGM, 2015: 28). 2003-2012 yılları arasında toplam 23.098 şüpheli hakkında siber suç işlemekten yakalanmıştır. 2007'den itibaren yakalanan şüphelilerde artış olmuştur. 2012 yılında siber suçlarda artış gözükmekte iken yakalanan şüphelilerde azalma vardır.

Tablo 1 ve 2'ye göre, 2007 yılından itibaren hem işlenen siber suçlarda hem de bu suçları işleyen şüphelilerin sayısında artışlar dikkat çekicidir. Bu durumun iki nedeni olarak, sadece İstanbul'da kurulan Bilişim Suçları ve Sistemleri Şube Müdürlüğünün kurulmasıyla siber suçlarıyla

98.391 sanık bulunduğu bildirilmektedir (Köksal ve İlbaş, 2015). Tablo-1 ve 2'yle karşılaştırıldığında, adliyede devam eden ancak polis istatistiklerine yansımayan birçok olayın olduğu gözükmektedir.

mücadele eden uzman kolluk birimleri ve personel sayılarında artış ve 5651 sayılı Kanunun yürürlüğe girmesi gösterilmektedir. Yani siber suçlarla mücadelede hukuki mevzuatların yürürlüğe girmesi ve özel polis birimlerinin kurulması suçla mücadeleyi etkin hale getirirken caydırıcı olabilmektedir (TBD, 2015: 16).

## 4. SİBER SUÇLARLA MÜCADELE OLUŞTURULAN BİRİMLER: 1997-2011 ARASI

EGM içerisinde siber suçlarıyla mücadele ilk kez 1997 yılında Bilgi İşlem Daire Başkanlığı[14] (BİDB) altında Bilişim Suçları Büro Amirliğinin kurulumu ile başlamıştır (Tekeli, 2011: 185). 1991 yılında 765 sayılı TCK'da bilişim suçları tanımlanmasına rağmen altı sene sonra, siber suçlarıyla mücadele EGM'nin gündemine girmiştir denilebilir. Ancak bu birimin daha çok idari görev yapan bir birim olması nedeniyle, adli soruşturmalarda görev almayan personelin bu işi özümsemede yaşayacağı zorluk nedeniyle ilk etapta dikkatli seçilen bir politika olarak gözükmemektedir. Nitekim BİDB'nın adli bir birim olmadığı gerekçesiyle her birimin kendi yapılanmasını oluşturması kararına varılmış ve BİDB'de bulunan Bilişim Suçları ile Mücadele Şube Müdürlüğü ve Taşra Teşkilatlarında Bilgi İşlem Şube Müdürlükleri altında kurulu bulunan Bilişim Suçlarıyla Mücadele Büro Amirlikleri kapatılmıştır (Güngör, 2007: 151-152).

EGM'de siber suçlarla ilgili olarak atılan önemli bir politik adım, 18.04.1998 tarihinde Bilgisayar Suçları ve Bilgi Güvenliği Kurulu'nun oluşturulması ve yapılan görevlendirme ile 01.03.1999 tarihinde "Bilişim Suçları Çalışma Grubu" kurulmuş olması olarak gözükmektedir. Bu politikanın temel amacı; bilişim alanındaki hak ihlallerini araştırmak, bu alandaki suç tiplerini belirlemek, ilgili Daire Başkanlıklarının yönetmeliklerinde gerekli düzenlemeleri yapmak olarak belirlenmiştir. Çalışma kapsamında uluslararası kaynaklar incelenerek siber suç tasnifleri yapılmış, EGM bünyesindeki Daire Başkanlıklarının, kendi görev alanları içerisinde görev paylaşımı yapılmıştır (Bilişimsurasi.org.tr, 2015). Ayrıca Kaçakçılık Ve Organize Suçlarla Mücadele Daire Başkanlığı (KOMDB) bünyesinde uluslararası bir akademi statüsünde faaliyet gösteren TADOC bünyesinde (Turkish İnternational Academy Against Drug and Organized Crime) Bilişim Suçları Araştırma Merkezi oluşturulmuş ve daire bünyesinde 20.04.2003 tarihinde Yüksek Teknoloji Suçları ve Bilişim Sistemleri Şube Müdürlüğü kurulmuş, bu birimin ismi 2006 tarihinde Bilişim Suçları ve Sistemleri Şube Müdürlüğü olarak değiştirilmiştir (Alaca, 2008: 105, kom.pol.tr, 2015). Bu tarihlerde siber suçlar, Bilişim Suçları ve Yüksek Teknoloji Suçları olarak adlandırılmaktadır.

Özellikle 5237 sayılı yeni TCK'da siber suçların ayrı bir başlıkta ele alınmasıyla, KOMDB'nin siber suçlarla mücadelede faaliyetlerine hız verdiği, EGM bünyesinde siber suçların soruşturulması ve bu konuda çalışma yapan il birimlerine teknik destek vermenin yanında, herhangi bir suça konu dijital delillerin incelenmesi görevlerini yerine getiren teknik bir birime dönüştüğü ve ayrıca adli bilişim açısından EGM bünyesinde *Koordinatör Daire Başkanlığı* olma özelliğini kazandığı görülmektedir. Bu daire başkanlığı bünyesinde 2006 yılında Adli Bilişim Bölge Merkezleri; İstanbul, Sakarya, Bursa, İzmir, Antalya, Adana, Van, Diyarbakır, Malatya, Erzurum, Samsun, Ankara, Kayseri illerinde oluşturulmuştur (kom.pol.tr, 2015). Yani EGM bünyesinde siber suçlarla mücadele KOMDB bünyesinde uzun yıllar sürmüştür.

Siber suçlarla mücadele önemli örnek bir adım İstanbul'da yaşanmıştır. Diğer İl Emniyet Müdürlüklerinde siber suçlarla mücadelede ayrı bir polis birimi bulunmamakta iken, siber suçlarıyla yapılan mücadelede yaşanan yoğunluk ve bilişim alanında hizmet veren birçok firma ve

[14] Bu daire başkanlığı 1981 yılında kurulmuş ve daha sonra ismi Bilgi Teknolojileri Daire Başkanlığı olarak değiştirilmiştir. Görevi; Emniyet Teşkilatı tarafından yürütülen hizmetlere bilişim desteği vererek, görevin süratli, etkin ve güvenilir bir şekilde yerine getirilmesini, yurt içi ve yurt dışında da bulunan diğer kurumlarla bilgisayar ağı kurarak bilgi alışverişini gerçekleştirmek suretiyle, polisin kendisini ilgilendiren bilgilere Türkiye'nin her yerinden hızlı bir şekilde erişmesini sağlamak olarak belirlenmiştir (egm.gov.tr, 2015d). Yani adli bir birim olmaktan ziyade EGM'nin idari birimlerinden biridir. Ancak siber suçlarla mücadelenin ilk yıllarında bu daire başkanlığı üzerinden faaliyetleri yürütülmüştür.

kurumun genel merkezlerinin veya temsilciliklerinin İstanbul'da bulunması nedeniyle, İstanbul Emniyet Müdürlüğünde, Bilişim Suçları ve Sistemleri Şube Müdürlüğü, İçişleri Bakanlığının 25 Nisan 2007 tarihli onayıyla kurulmuştur (memurlar.net, 2015b). Bir il müdürlüğünün, bölgesindeki siber suçların etkisiyle kendi yapılanmasını kurması oldukça manidardır. Halbuki EGM'nin bu uygulamayı merkezden başlayarak tüm illere yayması gerekirken, 2011 yılından itibaren bu politikalar merkezi bir yapılanmayla İl Emniyet Müdürlüklerine yayılması sağlanmış, aşağıdan yukarıya uygulama modeli olarak anılan, hiyerarşik yapıda halkla temas halinde olan en uçtaki kamu politikası uygulamacılarını esas rol oynayan kişiler gören ve tabanın önemine dikkat çeken (Çevik ve Demirci, 2012: 61) uygulama modeli uygulanmıştır.

Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli daire başkanlıklarının ve taşra teşkilatındaki birimlerin dağınık yapısının tek bir çatı altında toplanması, mükerrer yatırımların önüne geçilmesi, siber suçlarla mücadelenin etkin ve verimli olarak yürütülmesini sağlamak amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı[15] ile EGM bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur (egm.gov.tr, 2015c). Bu politikadaki diğer alt amaçlar ise; zaman içerisinde bilişim suçlarının ve bilişim araçlarıyla işlenen suçların artması ve çeşitlenmesi, bu suç türü ile mücadelede daha kapsamlı uzmanlaşma ve yeni yapılanmalar ihtiyacının doğmuş olması, kaynak tasarrufunun sağlanması, birimler arası sorumluluk sahası çakışmalarının azaltılması, standart uygulamaların geliştirilmesi, farklı birimlerdeki sınırlı sayılardaki uzman personelin tek çatı altında toplanması, eğitim planlamalarının düzenlemesi, bilgi birikiminin artırılması ve bunların sonucu olarak bilişim suçlarının önlenmesi ve soruşturulması daha etkin bir şekilde sürdürülmesi olarak gözükmektedir (Tekeli, 2011: 185-186).

Bu başkanlığın ismi 28.02.2013 tarihli Bakanlık Oluruna istinaden Siber Suçlarla Mücadele Daire Başkanlığı (SSMDB) olarak değiştirilmiştir (egm.gov.tr, 2015c). Bu süreç takip edildiğinde polis teşkilatı yapılanmasının; geleneksel, yukarıdan aşağıya uzanan hiyerarşik, otoriter, merkeziyetçi ve yazılı kurallara dayanan bir ilişkiler sistemi özelliği gösterdiği görülmektedir. Teşkilatın toplumsal ve sosyal gelişmeler sonucu ortaya çıkan ihtiyaçlara göre yapısal değişiklikler gerçekleştirdiği ve yeni birimleri oluşturma anlayışına sahip olduğu kabul edilmektedir (Alaç, 2013: 131). Ancak suçla mücadelede polisin genel politikasının, başlıca şubelerin özgül suçların ardından isimlendirilmesi ve suç uygulamalarına dair biçimsel uzmanlaşmaları yansıtma eğiliminde olması da, poliste bu yapılanmayı gerekli kılan bir özellik olarak gözükmektedir (Neocleous, 2013:179).

SSMDB'nin görev alanı, interaktif dolandırıcılık, ödeme sistemleri dolandırıcılığı, istismar suçları, müstehcen yayınlarla mücadele, yasadışı bahis, kumar ve oyunlar, siber terör ile bütün adli bilişim hizmetleri olacak şekilde karar verilmiştir. Bu sayede Emniyet teşkilatı içinde kurum içi ve kurum dışı karmaşıklığa neden olan dağınık yapı ortadan kaldırılmış ve bahse konu hizmetler tek çatı altında toplanmıştır (Tekeli, 2011: 186). Yani daha teknik olarak işlenen siber suçlarla ilgilenen ve diğer birimlere teknik destek verebilen bir birime dönüştürülmüş uzman bir birim olarak kabul edilebilir.

SSMDB ile birlikte EGM bünyesinde adli kolluk görevi bulunan; uyuşturucu suçları, mali suçlar, kaçakçılık suçları ve her türlü organize suç örgütleriyle mücadele eden KOMDB, bölücü ve yıkıcı terör faaliyetleriyle mücadele eden Terörle Mücadele Dairesi Başkanlığı, hırsızlık, dolandırıcılık, gasp, cinayet ve fuhuş alanlarında gerçekleştirilen suçlarla mücadele eden Asayiş Dairesi Başkanlığı (ADB) ve görev alanı toplumsal olaylara müdahale olsa da 5846 sayılı kanunda yer alan bilgisayar programları, fikir ve sanat eserlerinin korunmasına yönelik olarak telif hakkı suçlarıyla mücadele eden Güvenlik Dairesi Başkanlığı gibi birimler mevcuttur. Bu birimler bilişim sistemleri aracı kılınarak işlenen kendi görev alanlarına giren suçlarla mücadele etmekte ve adli işlemleri yapmaktadır.

[15] R.G. 15.07.2011 tarih ve 27995 sayı.

Örneğin, ADB bünyesinde Bilişim Sistemleri Şube Müdürlüğü bulunmaktadır. Özellikle bu başkanlığın görev alanına giren fuhşa teşvik, müstehcenlik, vb. suçların internet ortamında işlenmesi durumunda, suç unsurları tespit edilerek ilgili birimlere bildirilmektedir. Hatta bu birim bünyesinde Sanal Devriye Büro Amirliği kurulmuş ve konusu cezai yaptırım öngören kanunlarda belirtilen bir suç teşkil etmese bile, içeriği itibariyle toplumun genel ahlak ve düzenini olumsuz etkileyen, özellikle çocukların psikolojik ve fizyolojik gelişimlerine menfi yönde tesir ederek kötü alışkanlıklara yönlendiren web siteleriyle mücadele edilmesi, gerek doğrudan suç unsuru içeren diğer web siteleri ya da web sitesi üzerinden yayınlanmasa bile muhtelif dosya paylaşım yazılımları vasıtasıyla internete açılan suç unsuru içerikleriyle mücadele edilmesi ve gerekse internet kullanıcılarının bilinçlendirilerek mağduriyetlerin oluşmadan önlenmesi amaçlanmıştır (egm.gov.tr, 2015c).

SSMDB'nin siber suçlarla mücadelede diğer birimlerle işbirliğini gösteren, mücadele eden birimlerin görevleri, yetkileri, eğitimleri, personel standartları vb. konularını açıklayan bir yönetmelik ve yönergenin çıkarıldığına dair herhangi bir kaynağa rastlanılmamıştır. Muhtemelen EGM'nin kurum içi genelgeler çıkararak, bu birimin görevlerini ve diğer daire başkanlıklarıyla ilişkilerini açıklayan kanunlaştırma faaliyetlerine devam ettiği söylenebilir. EGM'nin siber suçlarla mücadelede, idari yasal düzenlemeler olarak kabul edilebilecek kanunlaştırma aşamasının (Kaptı, 2011: 32-33) yeterli düzeyde gerçekleşmediği söylenebilir. Ancak basına yansıyan bir yönetmelik taslağında bu birimin muhtemel görev ve yetkileri şu şekilde sıralanmaktadır (bugun.com.tr, 2015);

a. Suçların önlenmesi için haber alma faaliyetlerinde bulunabilecek, soruşturmalarda muhbir ve gizli soruşturmacı kullanabilecek, suç örgütünün içine sızarak delil toplayabilecek,
b. Suçların önlenmesi, soruşturulması ve delillerin ortaya çıkarılması gibi özel ihtisas bilgisi gerektiren konularda gerçek ya da tüzel kişilerden hizmet satın alabilecek,
c. Her türlü iletişimi dinleme yetkisine sahip olabilecekler, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ile işyerini teknik araçlarla izleyebilecek,
d. Data, ses ve görüntü kaydı alabilecekler ve devletin güvenliği ile siyasi, sosyal ve kültürel amaçlar ile olağanüstü hizmetlerde örtülü ödenek kullanabilecek,
e. Siber polis önemli soruşturmalarda başka bir konumdaki bir bilişim sistemine uzaktan erişim sağlayabilecek.

Yukarıda sayılan yetkiler, siber suçların gelişimi ve siber suçluların muhtemel gelişimi düşünüldüğünde bu birimde olması gereken yetkiler olarak gözükmektedir. Sadece bilişim teknolojileri üzerinde çalışma yapan bir birim olarak değil, aynı zamanda operasyonel polis faaliyetlerinde bulunan bir polis birimi olarak düşünülmektedir. SSMDB'ye bağlı olarak 81 İl Emniyet Şube Müdürlüğü bünyesinde Siber Suçlarıyla Mücadele Şube Müdürlükleri kurulması planlanmaktadır. Bu şube müdürlüğünün alt birimlerinin; İdari Büro Amirliği, Adli Bilişim Büro Amirliği, Suç Araştırma Ve Soruşturma Büro Amirliği, Adli İşlemler Büro Amirliği, Sanal Devriye Büro Amirliği, Operasyon Destek Büro Amirliği, Bilgi Teknolojileri Büro Amirliği Ve Nöbetçi Amirliği olarak planlandığı görülmektedir (kayseri.pol.tr, 2015). Görüldüğü gibi daha çok adli bir birim olarak tasarlanmıştır. Burada dikkati çeken bir birim Sanal Devriye Büro Amirliğidir ve önleyici bir birim olarak tasarlanmıştır. Emniyet birimlerinin internet üzerindeki varlığını güçlendirmek, suç önleme mesajlarını yaymak ve internet topluluğu ile iletişim içerisinde olmak için sosyal medya platformlarından mümkün olduğunca faydalanmaları gerektiği ifade edilmektedir (EUROPOL, 2014: 42). Bu bağlamada Sanal Devriye Büro Amirliğinin bu açığı kapatabileceği söylenebilir.

EGM'nin siber suçlarla mücadelede, merkezi bir kurum olma konumuna doğru yükseldiği görülmektedir. Çünkü siber suçların büyük kısmının, internetin yoğun olarak kullanıldığı şehirlerde işlenmesi tahmin edilebilir bir sonuçtur. Ayrıca görev alanı şehir merkezleri olarak belirlenen polisliğin, aynı zamanda bir şehir mesleği olarak görülmesi gerektiği ifade edilmektedir (Fındıklı, 2000: 5). Polis Teşkilatının 269.898 personeli ile ülke nüfusunun %86'sına hizmet vermesi (EGM, 2015: 14), nüfusun büyük bölümünün şehirlerde yaşaması bu yargıyı doğrulamaktadır. Nüfusun

büyük çoğunluğuna hizmet veren polis teşkilatının görev sahası içerisinde, hem internet kullanımının hem de bankacılık sektörü dahil servis sağlayıcıların çoğunun faaliyet göstermesi nedeniyle polisle işbirliği içerisinde bulunmasını gerektirmektedir. Kabul edilen bir görüşe göre, kolluk birimleriyle, internet servis sağlayıcıları ve diğer özel sektör kuruluşları arasında işbirliği, internet kullanıcılarının haklarını ve onları suça karşı korumak için gerekli görülmektedir. Çünkü siber suçların etkili soruşturulması bu kuruluşlarla polisin yakın işbirliğini zorunlu kılmakta, işbirliği kültürünün geliştirilmesi tavsiye edilmektedir (coe.int, 2015). Hattizatında kamu politikaları kamu kuruluşları için önemli roller içerse de, bazen tam bazen de kısmi olarak özel sektör ve toplum temsilcileri de politikada rol oynayabilmektedir (Çevik ve Demirci, 2012: 13). Bu nedenle projelerde ve eylem planlarında EGM hem önemli bir paydaş olarak kabul edilmekte hem de uygulayacağı projelerde paydaşlarını belirlemektedir.

*Bilişim Suçlarına Karşı Kapasitenin Güçlendirilmesi Projesi* adı altında, kolluk kuvvetlerinin soruşturma ve adli makamların yargılama kapasitesine katkıda bulunmak, ulusal ve uluslararası kamu kurumları ve özel sektör arasındaki bilgi değişimi gibi konularda işbirliği seviyesini geliştirmek ve organize suçlarla mücadele eylem planına katkıda bulunmayı amaçlayan Avrupa Birliği Genel Sekreterliği tarafından 2009 yılı projeleri kapsamında değerlendirilmeye alınan projeden Adalet Bakanlığına bağlı birimler sorumlu olarak gözükmektedir. EGM'yle birlikte, Jandarma Genel Komutanlığı ve Telekomünikasyon İletişim Başkanlığı[16] (TİB) projede paydaş kurumlardır. 2013 yılında başlayan ve 2014 yılında bitirilmesi planlanan projede; yurtiçi ve yurtdışında eğitim, çalıştay ve ziyaretlerle 48 faaliyetin planlanmaktadır. Proje maliyeti 1.400.000 Euro olarak belirlenmiştir (egm.gov.tr, 2015c).

Kamu kurumlarının ve özel işletmelerin kritik öneme sahip bilişim sistemlerinin güvenliğinin sağlanması ve siber olayların etkilerinin düşük seviyede kalması, meydana gelen suçların adli ve kolluk birimlerince etkin araştırılması ve soruşturulması amacıyla çıkarılan *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: 2013-2014*'de, EGM; Siber Olayların Değerlendirilmesi, 7/24 Ulusal Siber Olaylara Müdahale Merkezinin kurulması, Siber Güvenlik Tatbikatlarının düzenlenmesi, Adli Bilişim Konusunda Hizmet Sağlayıcılara Güvenlik Belgesi verilmesi, Ulusal Siber Güvenliğin

[16] Bu başkanlık, ülkede iletişimin denetlenebilmesi, yetkilerin kötüye kullanılmasını önlemek ve uluslararası standartlara uygun olarak bu tedbirleri uygulamak ve tüm iletişimin denetlenmesi tedbirlerinin tek bir merkezden yürütülmesi amacıyla 5397 sayılı Kanunla Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesine eklenen hükümlerle kurulmuştur (Avşar ve Güngören, 2010: 88). Başkanlığın internetle ilgili olarak görevleri 5651 sayılı kanunla düzenlenmiştir. Bu kanuna göre TİB'in siber suçlarla mücadele hem polisle ortak hem de diğer ilgili kurumlarla eşgüdümü sağlayan görevleri şu şekilde sıralanmaktadır;

a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usuller dahilinde kurumca karşılanacak çalışma kurulları oluşturmak,

b) İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu kanunda öngörülen gerekli tedbirleri almak,

c) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek,

ç) Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülkî idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usulleri belirlemek,

d) İnternet ortamındaki yayınların izlenmesi suretiyle bu kanunun 8.inci maddesinin 1. fıkrasında sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak,

e) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek,

f) Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak,

g) Bu kanunun 8.inci maddesinin birinci fıkrasında sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini teminen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkânları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak (Md: 10/4). Yani siber suçlarla mücadelede görev alan; adli, idari ve güvenlik birimlerinin yolu, TİB'le bir noktada kesişmektedir.

Milli Güvenliğe Entegrasyonu gibi konularda görev verilen ilgili kuruluşlar arasında yer almaktadır.[17]

2015-2016 yıllarını kapsayacak şekilde hazırlanacak ve siber suçla mücadelede ulusal düzeyde tüm paydaş kamu kurum ve kuruluşlarının ve STK'ların koordinasyonu ve işbirliğine ihtiyaç bulunduğundan, kolluk ve adli süreçlerde takip edilmesi öngörülen kovuşturma ve yargılamanın hızlanması, personelin eğitimi, usul kanunlarında gereken iyileştirmelerin yapılması, uluslararası işbirliğini artırıcı tedbirlerin alınması, adli bilişim ve delil tespiti süreçlerinin basitleştirilmesi gibi konuların ulusal bir strateji dâhilinde ele alınması amacını taşıyan *Siber Suç Strateji ve Eylem Planı* hazırlanması görevi EGM'ye verilmiştir (KB, 2014: 140).

*İnternet Ortamında İşlenen Çocuk İstismarı Suçlarıyla Mücadele Projesi*; Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Haberleşme Genel Müdürlüğü ile yürütülmesi planlanmaktadır. Proje kapsamında, çocukların internet ortamında hızla artan istismar, suistimal, uyuşturucu kullanımını özendirme gibi suçlardan korumak için birimlerin teknik kapasitesinin artırılması ve konuyla ilgili olarak planlanan bölgelerde akıllı sınıflar kurularak çocuk ve ebeveyn farkındalığının artırılması planlandığı belirtilmektedir (egm.gov.tr, 2015a: 29). Ayrıca AK Sanal Ortamda İşlenen Suçlar Sözleşmesi gereği taraf ülkelerin kurması gereken 7/24 temas noktalarıyla ilgili olarak SSMDB 7/24 Türkiye Ulusal Temas Noktası olarak belirlenmiştir (tbmm.gov.tr, 2015). 7/24 irtibat ağı, ülkeler arası bilgi talepleri ve saklama taleplerinin ülkelere iletiminde önemli bir irtibat ağıdır. Sözleşme gereği 43 ülkenin 7/24 temas noktası bulunmaktadır (EGM, 2015: 29).

En son önemli bir protokol TÜBİTAK ile yapılmıştır. Bu protokolün amacı SSMDB'nin güncel teknik alt yapısını güçlendirerek önleyici faaliyetlerde bulunmasını sağlamak olarak gözükmektedir. Bu kapsamda, iki kurum arasında; farkındalık ve eğitimi, adli analiz ve veri kurtarma, zararlı yazılımlarla mücadele ve büyük veri analizi ve paylaşımı konularında EGM'nin altyapısının geliştirilmesi ve etkinleştirilmesi amacıyla Ar-Ge projelerine yönelik olarak mevzuat çerçevesinde destek verilmesi hedeflenmiştir (bilgem.tubitak.gov, 2015).

## 5. KURUMUN KAPASİTE ARTTIRIMI, EĞİTİM VE PERSONEL POLİTİKALARI

2013 yılı itibariyle SSMDB'de 106 ve 59 ilde 736 olmak üzere 842 polisin siber suçlar alanında çalıştığı görülmektedir (memurlar.net, 2015a). Bu birimlerde çalışan personel sivil olarak çalışmakta, hem adli hem de idari görev yapmaktadır. Polis teşkilatlarında sivil memurların kullanımı neredeyse polis teşkilatlarının kurulumu kadar eskiye dayanır. Polislerin sivil çalıştırılmasının nedenleri çok çeşitlidir. Her şeyden önce sivil memurların gerek maaş gerekse özlük haklar nedeniyle devlete olan maliyetleri düşüktür ve % 20 oranında kaynak tasarrufu sağlanabilmektedir (Şahin, 2013: 97). Yukarıda sayılan gerekçelerin yanında, operasyonel olarak görev yapması muhtemel olan bu birimin, her türlü arama, yakalama, fiziki takip gibi polise özgü faaliyetleri uygulayacağı düşünüldüğünde, sivil olarak görev yapması doğru bir tercih olarak gözükmektedir.

Siber suçlar ve elektronik deliller, ceza adalet yetkilileri tarafından uzman müdahalesini gerekli kılmaktadır. Kanun uygulayıcı birimler ve adli makamların; bilgisayar veri ve sistemlerine karşı saldırıları, bilgisayar aracılığıyla işlenen suçları ve aynı zamanda elektronik delil içeren her türlü suçu soruşturabilecek ve kovuşturabilecek kapasiteye sahip olması ve hatta halktan daha bilgili ve uzman olması gerektiğine dair oldukça yaygın bir kanat vardır (EUROPOL, 2014; coe.int, 2015, Alaca, 2008: 115-116). Ayrıca siber suçlarla mücadele eden emniyet birimlerinin, bu suçun niteliği gereği yurtdışı bağlantılarının olması vb. nedenlerle yabancı dil kabiliyetlerini yükseltmesini ve duruma göre uyarlaması gerektiği ifade edilmektedir (EUROPOL, 2014: 14; Güngör, 2007; 158) ki bu tür eğitimlerin düzenlenmesi uygun olacağı gibi ileride buna yönelik çok çeşitli eğitimlerin düzenlenmesi beklenmelidir.

[17] RG. 20.06.2013 tarih ve 28683 sayı.

Siber suçların aydınlatılması, bilişim teknolojileri üzerinde çalışılmasını gerektirmektedir. Özellikle siber suç delillerinin elde edilmesi uzmanlık isteyen bir alandır. Geleneksel/klasik suçlarda, delillerin toplanması ve incelenmesi için olay yeri inceleme birimleri bulunmaktadır. Ancak bu suçlarda deliller tamamen bilişim teknolojilerinin içerisinde yer almakta, buradan delilerin toplanması, incelenmesi, rapor haline getirilmesi başlı başına uzmanlık gerektirmektedir. Bu nedenle delilleri toplayan kolluk güçlerinin de teknik ve idari kapasiteleri geliştirilmesi gerektiği (Ünver ve Canbay, 2015) ve dijital soruşturma becerilerini geliştirebilmek için adli bilişim[18] alanında uzmanlaşmış daha fazla soruşturmacıya ihtiyaç duyulduğu ifade edilmektedir (Hekim ve Başıbüyük, 2013: 153). Aslında polis teşkilatlarının siber suçlarla mücadele kapasite, kabiliyet ve kaynak eksikliği dünya genelinde bir sorun olarak görülmekte ve yapabilecekleri sadece kurbanların kendilerine bildirdiği durumlarla ilgilenmek olarak görülmektedir (EUROPOL, 2014: 17).

Bu nedenle, siber suçların önlenmesi ve soruşturulmasıyla, geleneksel suçlara aracılık eden bilişim teknolojileri üzerinde suçu aydınlatmada kullanılacak elektronik iz ve delil elde etmeyi hedefleyen adli bilişim hizmetleri ve siber suçla mücadele kapasitesinin sürekli geliştirilmesi, suçlarının önlenmesine doğrudan veya dolaylı katkı sağlayabilecek kişi ve kuruluşlarla işbirliği yaparak ve dünya standartlarında uygulanan yeni teknolojiler kullanarak suçun ve faillerinin tespit edilmesi ve yakalanmasına önem verilmesi EGM'nin sürekli öncelikleri arasında gözükmektedir (EGM, 2008: 23, EGM, 2010: 35, EGM, 2011: 95, EGM, 2012: 52, EGM, 2015: 28, egm.gov.tr, 2015b: 21-58).

EGM'nin siber suçlarla mücadelede uzman birimlerinin sürekli olarak kapasitesinin güçlendirilmesi politikaları ve hedefleri, Avrupa Birliği tarafından desteklenen projelerde, paydaş devletlerden özellikle beklenen bir durum olarak gözükmekte, ortak kabul edilen resmi metinlerde devletlerin stratejik önceliği olması gerektiği hatırlatılmaktadır (coe.int, 2015). Ancak kamu kuruluşlarının amaç ve hedeflerin belirlenme süreci karmaşık ve zor bir süreç olarak gözükmekte, resmi anlamda ifade edilen ve belirlenen amaç ve hedeflerin ne kadar gerçekçi ve başarılabilir hedefler olduğunu bilmenin zor olduğu ifade edilmektedir (Çevik ve Demirci, 2012: 21).

Siber suçlarla mücadele eden kolluğun eğitiminde sürdürülebilir eğitim stratejilerinin uygulanması stratejik bir öncelik olması gerektiği ifade edilerek genel prensipler şu şekilde açıklanmaktadır (coe.int, 2015);

a. Yerel bir kolluk eğitim stratejisinin uygulanarak, kolluğun siber suçları soruşturmak, elektronik delillerin güvenliğini sağlamak, ceza davaları için adli bilişim analizlerini yürütmek, diğer kurumlara yardım etmek ve ağ güvenliğine katkıda bulunmak için gerekli yetkinliklere sahip olmasını sağlamak,

b. Elektronik delillere ilişkin eğitimlere sadece uzman birimler tarafından değil tüm kolluk personeli tarafından ihtiyaç duyulduğunun farkına varılmasının sağlanması, –bu ilke tüm polis birimlerine ve polis okullarına yönelik olmasını gerektirir-

c. Teknolojideki değişiklikler ve teknolojinin suçlular tarafından kötüye kullanılması nedeniyle üst düzey soruşturma yürütebilecek ve dijital delil incelemesi yapabilecek yeterli sayıda eğitilmiş uzman personel ihtiyacının karşılanması,

d. Siber suç ve adli bilişim eğitimlerinin çok pahalı olması nedeniyle, yatırımlardan en iyi geri dönüşü alınması amacıyla personelin sahip olduğu yetenek ve bilgi seviyesine göre görevlere atanması ve o görevde kalmasının sağlaması, eğitim ve insan kaynakları stratejilerinin ücretsiz olması.

[18] Adli Bilişim kavramı İngilizcede Computer Forensic olarak adlandırılmakta, yeni ve henüz yeterli standartları oluşmamış bir alan olarak kabul edilmektedir. Bilgisayar bilimi ve hukuka uygun olarak delillerin bilişim sistemlerinden, ağlardan, kablosuz iletişim sistemlerinden ve depolama aygıtlarından toplanıp ve analiz edilmesiyle kabul edilebilir deliller halinde mahkemeye sunulması olarak tanımlanmaktadır (us-cert.gov, 2015).

Siber suçlarla mücadelenin KOMDB bünyesinde sürdürüldüğü zamanlarda, siber suçlarla mücadelede; Bilgisayar ve İnternet Suçları ile Veri Kurtarma ve İnceleme Teknikleri, Suç Analizi Semineri, Dijital İzler Semineri, Dijital Delil İnceleme Prosesleri, İnternet Suçları Semineri, Encase Kursu, SECI Elektronik ve Bilgisayar Suçlarının Soruşturulması Kursu, Adli Bilişim Uygulamaları ve Veri Kurtarma Kursu, Bilişim Suçları Soruşturma Teknikleri, Windows Adli Bilişim-Vista ve İnternet Forensic gibi ulusal ve uluslararası farklı eğitimlerin, seminerlerin personele verildiği, 31 Ocak-4 Şubat 2011 tarihlerinde Bilişim Suçlarıyla Mücadelede Etkinliği Artırma Çalıştayı düzenlendiği görülmektedir. Ayrıca Arnavutluk, Bosna Hersek, Hırvatistan, Karadağ, Kosova, Makedonya, Sırbistan ve Türkiye'nin yararlanıcı olarak yer aldığı "Cybercrime@IPA Güney Doğu Avrupa'da Siber Suçlara Karşı Bölgesel İşbirliği" başlıklı projede KOMDB'nin aktif şekilde yer aldığı görülmektedir (kom.pol.tr, 2015). SSMDB'nin kurulmasıyla birlikte bu öncelikler ve politikaların belirlenmesi bu daireye geçmiştir.

EGM'nin siber suçlarla mücadeleye yukarıda sayılan ilkeler doğrultusunda performans raporunda öncelik verdiği görülmektedir. 2014 yılı raporunda; planlanan eğitim sayısının 65, toplantı sayısının 60, hazırlanan toplantı sayısının ise 860 adet olarak planlandığı görülmektedir. Ayrıca siber suçla ilgili farkındalığın artırılması, soruşturma ve elektronik delillendirme ile önleyici hizmetlerin etkin şekilde yürütülmesi için eğitim ve bilgilendirme faaliyetleriyle,[19] yeni görevlendirilecek personelin nitelikleri, seçimi, sınav şartları, eğitimi, branşa alma-çıkarma ve ilgili prosedürleri, görevlendirmeye ilişkin planlamaları ve branş[20] komisyonunun çalışma esasları hususunda gelişime açık usul ve esaslar belirlenmesi amaçlanmış ve bu faaliyetler için 6.596.000 TL'nin bütçe imkânlarıyla kullanılması planlanmıştır (egm.gov.tr, 2015a: 54).

EGM, siber suçlar ile mücadelede mevcut kurumsal kapasitenin artırılması, uzmanlaşmanın artırılması, uluslararası işbirliği ve bilgilendirme faaliyetleri kapsamında (egm.gov.tr, 2015a: 54);

a. Siber suçla ilgili farkındalığın artırılması, soruşturma ve elektronik delillendirme ile önleyici hizmetlerin etkin şekilde yürütülmesi için eğitim ve bilgilendirme faaliyetlerin yapılması,
b. Siber suçlarla mücadele birimlerinde görevlendirilecek personelin nitelikleri hususunda gelişime açık usul ve esasların belirlenmesi,
c. Ulusal Siber Güvenlik Stratejisi ve Eylem Planında kurulumu öngörülen Ulusal Siber Olaylara Müdahale Merkezi ve ilgili diğer kurumsal ve sektörel birimler ile koordinasyonun sağlanması,
d. Kurum ve şahısların suç farkındalığının oluşturulmasını sağlamak amacıyla seminerlerin düzenlenmesi planlanmaktadır.

Ayrıca adli bilişim hizmet standartlarını yükseltmek amacıyla 2014 yılı içerisinde (egm.gov.tr, 2015a: 70);

a. Elektronik delillerin en kısa süre içerisinde incelenip raporlanması için illerde tam teşekküllü adli bilişim bölge merkezleri veya bürolarının kurulması,
b. Adli bilişim alanında kullanılan yazılım ve cihazların yerli üretimi için TÜBİTAK, üniversiteler, kamu ve/veya özel kuruluşlarla çalışmalarda bulunulması,
c. Adli bilişime yönelik ilk müdahale, veri inceleme, mobil cihaz inceleme, veri kurtarma, dekriptoloji ve steganografi alanlarında eğitimler düzenlenerek uzman personel sayısının arttırılması,
d. Adli bilişim alanında ulusal ve uluslararası eğitimler düzenlenmesi planlanmaktadır.

[19] SSMDB'nin sitesinde; siber suçlara yönelik operasyonların haberlerinin verildiği, duyurular ve broşürlerle halkı uyarıcı ve bilgilendirici faaliyetlerin yapıldığı görülmektedir (egm.gov.tr, 2015c).

[20] Emniyet Hizmetleri Sınıfı Branş Yönetmeliği'nde branş; emniyet teşkilatındaki görevlerin yerine getirilebilmesi amacıyla oluşturulan özel yetenek, teknik bilgi ve beceri gerektiren özel hizmet alanlarını ifade etmektedir (Md: 4/1-ç). Eğitim Daire Başkanlığınca hazırlanan rehberde, SSMDB'de çalışan personelin branşa alındığı ve seçme sınavlarına başladığı görülmektedir (egm.gov.tr, 2015c). Siber suçlarla mücadele alanında çalışan personelin branş yani uzman birim olması yönünde bir politikanın hayata geçirilmesi önemli bir tercihtir. Çünkü siber suçlarla uzman olmayan personelle mücadele etmenin istenilen başarıyı sağlaması zor gözükmektedir.

Bu kapsamda illerde teşkilatlanmaların tamamlanması amaçlanmış, kurulumu yapılan bölge merkezi ve büro sayısı 81, program sayısı 20, toplantı sayısı 3, eğitim sayısı 23 adet olarak planlanmıştır (egm.gov.tr, 2015a: 68). Bu hedeflere yönelik olarak 2014 yılında kurulumu yapılan bölge merkezi ve büro sayısı 59 (%73), hazırlanan program sayısı 24 (%120), düzenlenen toplantı sayısı 13 (%433), düzenlenen eğitim sayısı 29 (%126) olarak hedefler gerçekleşmiştir (EGM, 2015: 70). 2014 yılı itibariyle belirlenen hedeflerin büyük kısmının gerçekleştirildiği görülmektedir.

Yine 2015 yılı itibariyle siber suçlarla mücadele kapasitesinin geliştirilmesi ve uluslararası alanda etkinliğinin artırılması amacıyla; yazılım donanım temini 15, ulusal ve uluslararası operasyonlarda işbirliği toplantı sayısı 30, il birimleriyle düzenlenecek toplantı sayısı 10, branş eğitimi verilecek personel sayısı 300, siber güvenlik tatbikat sayısı 4, uluslararası seminer, sempozyum, fuar, işbirliğine katılacak katılımcı sayısı 250, uzman eğitmen yetiştirilmesi 10, bilimsel yayın oluşturmak 1, suç farkındalık semineri ise 200 adet planlanmaktadır. Bu faaliyetler için 14.602.000 TL kaynağın bütçe imkanlarıyla kullanılması planlanmaktadır (egm.gov.tr, 2015b: 58).

Teknolojiyle birlikte değişen ve farklılaşan bilişim suçları ve suç grupları ile etkin ve başarılı bir şekilde mücadele edilebilmesine yönelik personelin temel ve ileri düzey eğitim ihtiyaçları doğrultusunda 2014 yılında, 45 dönemde 909 kursiyere eğitim verilmiştir (EGM, 2015: 29). EGM'nin yurt dışı polis teşkilatlarına siber suçlarla ilgili eğitim verdiği görülmektedir. Uluslararası ilişkiler kapsamında 2014 yılında Kosova, Kazakistan, Bosna-Hersek ve Gürcistan polisine yönelik siber suçlarla ilgili 6 dönem halinde 47 kursiyere kurs düzenlemiştir (EGM, 2015: 29).

Suç soruşturmalarında bu suçun uluslararası özelliği nedeniyle diğer ülkelerle işbirliği ve bilgi paylaşımı önemli gözükmektedir. Polis kurumları arasında işbirliğini temeli önemli olmasına rağmen siyasi ve hukuki olarak bu eksikliklerin olması durumunda polisin başarılı olması çok mümkün gözükmemektedir (EUROPOL, 2014). Bu kapsamda 2013 yılı itibariye siber suçlarla mücadelede uluslararası operasyonlar gerçekleştirmek için 39 ülkenin güvenlik teşkilatlarıyla ikili anlaşmalar yapan Türk polisinin, işbirliği yaptığı ülke sayısını arttırmayı planlandığı ve böylece siber suçlukların dünyanın neresinde olursa olsun yakalanmasının amaçlandığı ifade edilmektedir (memurlar.net, 2015a).

## SONUÇ VE DEĞERLENDİRME

EGM bünyesinde siber suçlarla mücadelede yapısal reformların 2003'li yıllardan sonra gelişme gösterdiği söylenebilir. Özellikle 2001 yılında AK Siber Suç Sözleşmesinin imzaya açılması, –bu tarihte Türkiye imzalamamıştır- 2004 tarihli 5237 ve 2007 tarihli 5651 sayılı kanunlarla, 5846 sayılı kanun üzerinde yapılan 2004 ve 2008 yıllarında yapılan değişikliklerin bu sözleşmenin içeriği, amacı ve tanımlarından etkilenmiş ve kısmen uyumlu şekilde 2010 yılında yürürlüğe girmesi, Ulusal Siber Güvenlik Eylem Planı 2013-2014'ün kabul edilmesiyle EGM'den, daha uzmanlaşmış, teknik ve ihtiyaçlara cevap verebilen siber suçlarla mücadele politikasının belirlenmesine yönelik beklentiler yükselmiş ve EGM'nin bu yönde çalışmaları artış göstermiştir. Özellikle AK Siber Suç Sözleşmesinin, Türkiye tarafından 2010 yılında imzalanması ve 2014 yılında meclisçe onaylanması ve devletin siber suçlara yönelik politikalarındaki diğer kurumlara görev veren kararları, kurum olarak EGM'nin siber suçlarla mücadele politikasına ivme kazandırmıştır.

EGM bünyesinde, 1997 yılında başlayan siber suçlarla mücadelenin hangi polis biriminde olması gerektiğine yönelik arayışların, ancak 2011 yılında SSMDB'nin kurulmasıyla sonuçlandığı görülmektedir. Aslında uzun yılların bir beklentisi olan (Güngör, 2007: 156) bu dairenin kurulması, geç kalmış bir politika olsa da gelinen noktada önemli bir adım olarak gözükmektedir. Bundan sonraki süreçte siber suçlarla mücadelenin ülke çapında çok güçlü şekilde ilerleyeceği, siber suçların oluşmadan önlenebileceği ve aydınlatılabileceği ve hatta caydırıcı etkisinin artabileceği söylenebilir. Ancak siber suçların tümüne bu dairenin bakması imkan dahilinde gözükmediğinden,

Güvenlik, Asayiş, KOM ve Terör Daire Başkanlıklarının kendi görev alanlarında meydana gelen siber suçlara yönelik çalışmalar yapması ve teknik olarak SSMDB'den destek alması, olması gereken bir politika olarak gözükmektedir. Hatti zatında diğer polis birimlerinde siber suç farkındalığının ve kapasitelerinin artmasıyla, bu daire başkanlığının çok daha teknik işlenen siber suçlar üzerinde yoğunlaşarak, iş hacminin azalabileceği bile söylenebilir.

EGM'deki siber suçlara yönelik geliştirilen politikaların ve gerçekleştirilen hem ulusal hem de uluslararası bağlantıları olan operasyonların (egm.gov.tr 2015c; kom.pol.tr, 2015; Alaca, 2006: 116-112) Türk hackerleri oldukça rahatsız ettiği görülmektedir. Nitekim hackerlerin polisin siber suçlara yönelik çalışmalarını önemle takip ettikleri, bu nedenle hackerlere, polisten nasıl korunacaklarını, delillerin nerelerde bulunabileceği, polisin çalışma ve delil elde etme usullerinin neler olduğuna dair makaleler hazırladıkları görülmektedir ki (turkhackteam.org, 2015) bu durum uygulanan politikaların suç işleyebilecek kişiler üzerinde caydırıcı etkilerinin olduğunu göstermektedir. Bu anlamda siber suçları önleyici politikaların, kişileri ve toplumu siber suçların işlenmesi konusunda duyarlı hale getireceği, suç işlemeye meyilli kişileri bir daha düşünmeye sevk edeceği söylenebilir.

Siber suç polis istatistiklerinin kamuoyuyla paylaşılmasında fayda vardır. Beş sınıfta yapılan siber suç istatistikleri yeterli gözükmemektedir. Özellikle siber suçların; hangi türlerinin işlenme oranlarının ve yakalanan şüphelilerin hangi siber suçtan yakalandıklarına dair ayrıntılı istatistiklere ver verilmesi doğru bir yaklaşım olacaktır. Ayrıca KOMDB'nin her yıl yayınladığı faaliyet raporlarının benzerlerinin SSMDB tarafından yayınlanması sağlanmalıdır. Böylece siber suçlarla mücadelenin merkezinde sayılabilecek bir kurum tarafından yayınlanan bu yayınların, polis teşkilatı dışında bu alanda çalışan farklı disiplinlerdeki uzmanlara yorum ve araştırma imkanı verilebilecektir.

Halkın internetin güvenli olduğuna inancını artırmak ve suçlulara karşı caydırıcı önlemler ortaya koymak amacıyla, siber ortamda otoritenin en düşük düzeyde olduğu görüşünü ortadan kaldırmak için, emniyet birimlerinin internet üzerinde görünürlüğünü ve varlığını artırması gereklidir (EUROPOL, 2014: 6). EGM'nin bu konuda çalışmalara yine 2003'lü yıllardan sonra ağırlık verdiği söylenebilir. Sanal Devriye Büro Amirliğinin kurulması, özellikle twitter gibi sosyal medya üzerinde yapılan yayınlar üzerine, bu yayını yapanların tespit edilmesi, polis tarafından yapılan operasyonların basında yer alması ve kamuoyunda tartışılması, siber suçların polis tarafından önemle takip edildiğinin, ceza hukukunda karşılığının bulunabildiğinin, delilerin elde edilebildiğinin, polisin yeterli donanıma ve kapasiteye ulaşabildiğini göstermesi açısından önemli gelişmelerdir ki yukarıda açıklanan amacı destekleyen politikaların varlığına işaret etmektedir.

Polis eğitiminin kendine özgü usulleri olmaktadır. Hem adli hem de idari görev yapması, her iki alana da hitap eden programları zorunlu kılmaktadır. Siber suçların yeni bir alan olması bilişim teknolojilerine hâkim olan özel yetiştirilmiş, adli bilişim konusunda uzman personele olan ihtiyacı arttırmaktadır. Bu suçların yukarıda sayıldığı gibi farklılıklarının olması, diğer klasik suçlardan farklı özelliklerinin olması kaçınılmazdır. Bunun için polis okullarından başlayarak siber suçlara yönelik olarak eğitimlerin verilmesinin uygun olacağı değerlendirilmektedir. Polis okullarının hali hazırdaki ders programlarında, 1. Sınıf Bahar döneminde Temel Bilgi Teknolojileri isimli haftada 2 saatlik bir ders bulunmaktadır ki yeterli gözükmemektedir (pa.edu.tr, 2015). Siber suçlar alanında çalışacak personelin branşlaşması, hizmet içi eğitimlerin ve seminerlerin sıkça düzenlenmesi yönündeki hedefler önemli eğitim politikaları olarak görülmelidir. Ancak bu birimlerde çalışan personelin çok dikkatli seçilmesi, çalışma güvenliğine sahip olması, tayinlerine dikkat edilmesi personel ve kurum başarısını arttırması aşısından önemli gözükmektedir.

Yıllar geçtikçe EGM'nin siber suçlarla mücadeleye verdiği önemin arttığı, polisin teknik kapasitesinin, eğitiminin, personel sayısının arttırılmasına, tüm ülke çapında özel yapılanmanın tamamlanmasına yönelik yapısal ve teknik kapasiteyi arttıracak bütçe politikalarında artış ve gelişme gösterildiği görülmektedir. SSMDB'nin kurulmasıyla bütçe imkanlarını doğrudan kendi

amaç ve hedefleri yönünde kullanabilecek bir yapının kurulması teknik ve teknolojik kapasiteyi artıracak, hatta ulusal ve uluslararası desteğin de önünü açabilecektir.

## KAYNAKÇA


Alaca, Bahaddin, (2008), "Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle)", Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi: Ankara.

Alaç, Ali Erkan, (2013), "Yönetimin Geliştirilmesi: Türk Polis Teşkilatı'nın Yapısal Açıdan Değerlendirmesine İlişkin Bir Yaklaşım", Polis Bilimleri Dergisi, C: 15, S: 1, 2013, ss.109-137.

Avşar, Zakir ve Öngören, Gürsel, (2010), "Bilişim Hukuku", Türkiye Bankalar Birliği Yayınları, No: 270, İstanbul.

Balcıoğlu, İbrahim, (2014), "İnternet Kullanımı ve Getirip Götürdükleri", Somuncubaba Dergisi, ss. 64-67.

bilgem.tubitak.gov, (2015), http://bilgem.tubitak.gov.tr/tr/haber/siber-suclarla-mucadelede-tubitak-ve-emniyet-isbirligi (07.04.2015).

Bilişimsurasi.org.tr, (2015), "Bilişim Suçları Çalışma Grubu", http://www.Bilişimsurasi.org.tr/dosyalar/9.doc, (09.03.2015).

bkm.com, (2015), "Bankalararası Kart Merkezi 2013 Yılı Faaliyet Raporu", http://www.bkm.com.tr/basin/Faaliyet-Raporu-2013.pdf, , (05.03.2015).

bugun.com.tr, (2015), Siber Suçlarla Mücadele İçin Gizlilik Yemini Edecekler, http://www.bugun.com.tr/gundem/siber-suclarla-mucadele-icin-gizlilik-yemini-haberi/717840, (09.03.2015).

coe.int, (2015), "Siber Suçlara Karşı İşbirliğinde Stratejik Öncelikler", http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Strategic_priorities_conference/2467_Strategic_Priorities_V16_TUR_final_adopted.pdf (09.02.2015).

Çevik, Hasan Hüseyin ve Demirci, Süleyman, (2012), "Kamu Politikası: Kavramlar, Aktörler, Süreç, Modeller, Analiz, Karar Verme", Seçkin Yayınları: Ankara.

Dolu, Osman, (2011), "Suç Teorileri: Teori, Araştırma ve Uygulamada Kriminoloji", Seçkin Yayınları: Ankara.

Doig, James W., (1970), "Polis Sorunları, Öneriler ve Yeniden Düzenleme Ve İçin Stratejiler", Selçuk Yalçındağ (Çev.), Amme İdaresi Dergisi ,C: 3, S: 4, ss.61-72.

Duman, Ali, (2011b), "Kamu Politikası Analizi İçin Pratik Uygulama Modeli", Ali Can Kaptı (Ed.), Kamu Politika Süreci Temel Perspektifler, Ankara: Seçkin Yayınları, ss.165-179.

EGM, (2008), "2008 Yılı Faaliyet Raporu", EGM Strateji Geliştirme Daire Başkanlığı, Ankara.

EGM, (2010), "2010 Yılı Faaliyet Raporu", EGM Strateji Geliştirme Daire Başkanlığı, Ankara.

EGM, (2011), "2011 Yılı Faaliyet Raporu", EGM Strateji Geliştirme Daire Başkanlığı, Ankara.

EGM, (2012), "2012 Yılı Faaliyet Raporu", EGM Strateji Geliştirme Daire Başkanlığı, Ankara.

EGM, (2015), "2014 Yılı Faaliyet Raporu", EGM Strateji Geliştirme Daire Başkanlığı, Ankara.

egm.gov.tr, (2015a), "2014 Yılı Performans Programı", http://www.egm.gov.tr/Documents/PERFORMANS-PROGRAMI-2014.pdf, (09.03.2015).

egm.gov.tr, (2015b), "2015 Yılı Performans Programı" ,http://www.egm.gov.tr/Documents/2015iy%C4%B1l%C4%B1performansiprogram%C4%B1.pdf,(09.03.2015).

egm.gov.tr, (2015c), http://www.egm.gov.tr/Sayfalar/DaireBaskanliklari.aspx (09.03.2015).

EUROPOL, (2014), "İnternet Organize Suç Tehdidi Değerlendirmesi (İOCTA)", Avrupa Polis Teşkilatı Yayını.

Fındıklı, Remzi, (2000). "Polis Mesleğinin Özellikleri ve Mesleki Kimlik Olgusu", Polis Bilimleri Dergisi, C: 2, S: 5-6, ss: 1-16.

Friedman, George, (2011), "Gelecek 10 Yıl Neredeydik Nereye Gidiyoruz", Tayfun TÖRÜNER (Çev.), Pegasus Yayınları: İstanbul.

Güngör, Nemci Murat, (2007), "Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları" İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

gwava.com, (2015), "How Much Data is Created on the Internet Each Day?" http://www.gwava.com/blog/internet-data-created-daily-2014/#sthash.gFJggvr5.dpuf, (06.03.2015).

Hekim, Hakan ve Başıbüyük, Oğuzhan, (2013), "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, C: 4, S: 2, ss. 135-158.

internetarsivi.metu.edu.tr, (2015), "İnternet Tarihi", http://www.internetarsivi.metu.edu.tr/tarihce.php, (11.02.2015).

internetworldstats.com, (2015), "World Internet Users And 2014 Population Stats", http://www.internetworldstats.com/stats.htm, (14.02.2015).

Kalkınma Bakanlığı (KB), (2014), "2015-2018 Bilgi Toplumu Stratejisi Ve Eylem Planı", Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Kaptı, Ali Can, (2011b), "Kamu Politika Sürecinde Klasik Yaklaşım Modeli", Ali Can Kaptı (Ed.), Kamu Politika Süreci Temel Perspektifler*,* Ankara: Seçkin Yayınları, ss.23-43.

kayseri.pol.tr, (2015), http://www.kayseri.pol.tr/Sayfalar/Birimlerimiz/Siber-Suclarla-Sube-Mudurlugu.aspx, (20.03.2015).

kom.pol.tr, (2015), http://www.kom.pol.tr/Sayfalar/Raporlar.aspx, (14.03.2015).

Köksal, Mehmet Ali ve İlbaş, Çığır, (2015), Türkiye'de Bilişim Suçları: 1990-2011, http://www.slideshare.net/melihbayramdede/trkiyenin-siber-su-haritas-19902011 (10.02.2015).

Mark, Neocleous, (2013), "Toplumsal Düzenin İnşası Polis Erkinin Eleştirel Teorisi", Ahmet BEKMEN (Çev.), h2o yayınları: İstanbul.

memurlar.net, (2015a), "Türk Polisi Siber Suçlulara Dünyayı Dar Edecek", http://www.memurlar.net/haber/356996/, (11.03.2015).

memurlar.net, (2015b), "Bilişim Suçları ve Sistemleri Şube Müdürlüğü Kuruldu", http://www.memurlar.net/haber/88791/, (25.03.2015).

Önok, Murat, (2013), "Avrupa Konseyi Siber Suç sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C: 19, S: 2, ss. 1229-1270.

Polat, Ahmet, (2008), "Suç İstatistiklerine İlişkin Sorunlar Ve Öneriler", Polis Bilimleri Dergisi, C: 10, S: 1, ss: 1-24.

pa.edu.tr, (2015), http://www.pa.edu.tr/?app=4AE70CE1-0C8A-406B-A01D-E0106BF55F69 (01.04.2015).

Şahin, Bahadır, (2013), "Kamu Tercihi Teorisi Işığında Adli Kolluk Sorunsalı ve Emniyette Sivil Personel Çalıştırılmasının Olası Hukuki-İdari Sonuçlarının Analizi", İnsan Hakları Yıllığı, C: 31, ss. 95-110.

tbmm.gov.tr, (2015), "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)", http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf (11.03.2015).

turkhackteam.org, (2015), "Polisten nasıl Korunuruz? (Polis Nasıl Takip Eder) Sosyal Mühendislik", http://www.turkhackteam.org/sosyal-muhendislik/1038307-polis-ten-nasil-korunuruz-polis-nasil-takip-eder.html (11.03.2015).

Türkiye Bilişim Dergisi (TBD), (2011), "11 Yıllık Siber Suç Haritamız Çıkarıldı", S: 137, ss. 14-19.

Tekeli, Ömer, (2011), "Bilişim Suçlarıyla Mücadelede Polisin Yeri", Sayder Dış Denetim Dergisi, S. 183, ss: 183-192.

us-cert.gov, (2015), "Computer Forensics", https://www.us-cert.gov/sites/default/files/publications/forensics.pdf, (14.03.2015).

Ünver, Mustafa ve Canbay, Cafer, (2015), " Ulusal Ve Uluslararası Boyutlarıyla Siber Güvenlik", http://www.btk.gov.tr/bilgiiteknolojileri/siberiguvenlik/dokumanlar/siberiguvenlik.pdf (21.02.2015).

Yetim, Servet, (2014), "Siber Suçlar, Yargılama Yetkisi Ve Yeni Bir Model Önerisi", Türkiye Adalet Akademisi Dergisi, S: 17, ss. 177-230.