# SİBER SUÇLAR VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI

## Cyber Crimes and Turkey's Cyber Security Policies

Yrd. Doç. Dr. Hakan HEKİM *
Doç. Dr. Oğuzhan BAŞIBÜYÜK **

**Öz**

Bilişim teknolojileri bazı klasik suçların daha kolay işlenmesine imkân vermesinin yanında, yeni tip suçların da ortaya çıkmasını sağlamıştır. Günümüzde internetin sağladığı imkânlar sayesinde siber suç işlemek için eskisi kadar teknik bilgi ve beceriye sahip olmaya gerek kalmamıştır. Bununla beraber, bilişim teknolojilerine olan bağımlılığın giderek artması, bireylerin suç mağduru olma riskini artırmasının yanında siber alanı da ulusal güvenliğin önemli bir parçası konumuna getirmiştir. Bu yüzden siber güvenlik son yıllarda en fazla tartışılan konulardan birisi haline gelmiştir. Ancak siber güvenlik konusu Türkiye'de gereken önemi görmemekte, sadece sansasyonel olaylar ertesinde gündeme gelmektedir. Bu alandaki bilgi birikimine katkıda bulunmak amacıyla bu çalışmanın ilk bölümünde siber suç türleri ele alınacak, ikinci bölümündeyse Türkiye'nin siber suç istatistikleri sunulacak ve siber güvenlik politikaları incelenecektir.

**Anahtar Kelimeler:** Siber Suç, Siber Güvenlik, Siber Alan, Bilişim Hukuku

**Abstract**

Beside facilitating commission of traditional crimes, information technologies have rendered emergence of new type of crimes. With the help of opportunities provided by the internet, today criminals no longer need technical capacity to conduct cyber crimes. At the same time, the rising dependency on the information technologies has increased the risk of being a victim of cyber crime and make cyber space an important part of national security. For that reason, cyber security has become one of the most debated issues. However, cyber security issues are not given adequate importance in Turkey, and discussed only after some remarkable incidents. In order to

* Yrd. Doç. Dr., Polis Akademisi, hakanhekim@yahoo.com
** Doç. Dr., Polis Akademisi, oguz97@yahoo.com

contribute to the literature on this topic, first part of this study will cover types of cyber crimes, the second part will present cyber crime statistics of Turkey and analyze her cyber security policies.
**Keywords:** Cyber Crime, Cyber Security, Cyber Space, Cyber Law

## Giriş

Ülkelerin bilişim teknolojilerine ve özellikle internete olan bağımlılıkları her geçen gün artmaktadır. Bugün küresel ağ üzerinde günlük 294 milyar e-posta mesajının gönderildiği, bir günde 168 milyon DVD'lik bilginin üretildiği tahmin edilmektedir. Youtube sunucularına günlük 864.000 saatlik video yüklenmekte, Netflix kullanıcıları bir günde 22 milyon saat TV veya sinema seyretmektedirler. Dünya nüfusunun yaklaşık üçte ikisinin internet bağlantısı ve %20'sinin sosyal ağlara üyelikleri bulunmaktadır. Yine dünya nüfusunun %85'i cep telefonu kullanmakta ve bunların %15'i cep telefonlarıyla alışveriş yapmaktadırlar (Klimburg, 2012). Bu rakamlar bilişim teknolojilerine olan bağımlılığın ne derece arttığını göstermektedir.

Bilişim teknolojileri, hayatı kolaylaştırma adına sağladıkları imkânların yanında, güvenlik boyutunda da yeni kaygıların gelişmesine sebep olmuştur. Artık bu yeni dünyada, fiziksel temasa veya mağdurla aynı yerde bulunmaya gerek duymadan hırsızlık, dolandırıcılık gibi suç fiilleri mümkün hale gelmiştir. Bunun yanında bilişim teknolojileri suç gruplarının veya terör örgütlerinin iletişim becerilerini artırmış, propaganda imkânlarını güçlendirmiş ve yeni faaliyet sahalarının ortaya çıkmasını sağlamıştır.

Bu çalışmada siber suçlar incelenecek ve siber güvenliği sağlamak için uygulanan politikalardan bahsedilmiştir. Çalışmanın son bölümünde genel olarak siber güvenlik politikaları ve ülkemizdeki uygulamalara yer verilmiştir. Bu kısımda, UTSAM (Uluslararası Terörizm ve Sınıraşan Suçlar Araştırma Merkezi) tarafından konuyla ilgili kamu ve özel kurumlardan uzmanların katılımıyla 26-27 Şubat 2013 tarihlerinde Ankara'da düzenlenen Siber Güvenlik ve Siber Terörizm Çalıştayı'nda yapılan odak grup toplantılarından edinilen veriler kullanılmıştır.

## 1. Siber Suç

Bilişim teknolojileriyle alakalı pek çok kavramda olduğu gibi siber suçlara ve siber güvenliğe ilişkin kavramların da Türkçemizde yerleşik ve yaygın olarak kullanılan karşılıkları henüz bulunmamaktadır. Bu sebeple siber suç kavramından önce *siber* (cyber) kelimesinin açıklanması gerekmektedir. Siber, bilgisayar veya bilgisayar ağlarını ilgilendiren veya içeren kavram yahut varlıkları tanımlamak için kullanılan bir kelimedir. Yine sıkça kullanılan *siber alan* (cyber space) kelimesi de birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır (Klimburg, 2012). Bilişim sistemleriyle alakalı suçlar bu makalede olduğu gibi bazı çalışmalarda "siber suçlar" olarak isimlendirilirken; başka çalışmalarda "bilgisayar suçu," "elektronik suç," "dijital suç" veya "ileri teknoloji suçları" ifadelerine rastlamak mümkündür. Kullanılan ifadeler farklı da olsa anlatılmak istenilen kavram genelde "bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suçlar" olmaktadır (Karagülmez, 2011:44). Tanımın kapsadığı geniş alan siber suçların değişik şekil ve içeriklerde olabileceğini ve klasik suçların siber alan ile farklı biçim ve yoğunlukta temas edebileceğini ima etmektedir. Esasında teknolojideki gelişiminin tahmin edilemezliği de böyle geniş bir tarifi zaruri kılmaktadır.

Siber suç kavramıyla birlikte izah edilmesi gereken başka bir kavram da *siber güvenlik* kavramıdır. Hatta hangi aktivitelerin siber suç olduğunun anlaşılabilmesi için öncelikle siber güvenlik kavramının tanımlanması daha doğru olacaktır. Siber güvenlik kavramı da üzerinde uzlaşı sağlanmış bir kavram olmayıp *bilgi güvenliği* (information security) ve *bilgisayar güvenliği* (computer security) kavramları ile benzer manalarda kullanılmaktadır. Benzer denilmesinin sebebi bilgi güvenliği kavramının çoğunlukla kişisel ve kurumsal verilerin güvenliğiyle ilgili bir kavram olarak; bilgisayar güvenliği kavramınınsa bilişim sistemlerinin güvenliği olarak anlaşılmasındandır. Her iki kavram da ortak öğeler içermektedir ancak odak aldıkları konular açısından bazen farklılık taşıyabilmektedirler.

Siber güvenlik kavramının tarifi daha çok bilişim sistemlerinin temel malzemesi olan bilgi üzerinden yapılmaktadır. Buna göre siber âlemin güvenli olabilmesi için bilginin *gizliliği* (confidentiality), *bütünlüğü* (intergrity) ve *erişilebilirliği* (availability) sağlanması gerekmektedir (Goodrich ve Tamassio, 2010). Gizlilikten kasıt bilginin sadece ilgili kişilerce erişilebilmesi anlamına gelmektedir. Burada erişim kavramı yazılı bir bilginin okunması anlamına gelebileceği gibi bilişim sistemlerinde saklanan bilginin sadece yetkili kişilerce görüntülenmesi, çıktı olarak alınabilmesi hatta bazı hassas bilgilerin varlığından sadece yetkililerin haberdar olması gibi anlamları da ifade eder. Bilginin bütünlüğü ise bilişim sistemleri vasıtasıyla depolanan bilginin değiştirilmemiş, kısmen veya tamamen de olsa silinmemiş, yok edilmemiş olmasıdır. Son olarak erişilebilirlik, saklanan bilginin gerekli durumlarda yetkili kişilerce ulaşılabilir olmasının gerekliliğini anlatmaktadır. Özellikle erişilebilirlik ile diğer ikisi arasında ters bir ilişki bulunmaktadır. Şöyle ki; bilginin gizliliğini veya bütünlüğünü geliştirmeye yönelik alınacak tedbirler erişilebilirliği ters yönde etkilemekte, erişilebilirliğin geliştirilmesiyse gizlilik ve bütünlüğü tehlikeye atabilmektedir.

Siber suçlarının tasnifine ilişkin farklı yaklaşımlar bulunmaktadır. Literatüre bakıldığında "bilgisayar sistemleri vasıtasıyla işlenen klasik suçlar" ve "bilgisayar sistemlerine yönelik suçlar" şeklindeki (Karagülmez, 2011) genel tasnifin yanında, "kimlik hırsızlığı," "çevrim içi taciz," "yetkisiz erişim," "dolandırıcılık" ve "erişim gerektirmeyen siber suçlar" şeklinde (Easttom ve Taylor, 2011) biraz daha detaylı tasniflere rastlamak mümkündür. Tasniflerdeki farklılık bir yönüyle teknolojinin sürekli gelişmesine ve sabit bir ayrım yapılmasının zorluğuna diğer yönüyleyse yapılacak tasnifin kullanım amacına bağlanılabilir. Bu çalışmada Avrupa Komisyonu'nun 2007 tarihli bir tebliğinde yer alan "elektronik ağlar vasıtasıyla işlenen klasik suçlar," "elektronik medya üzerinde yayınlanan yasa dışı içeriğe ilişkin suçlar" ve "elektronik ağlara has suçlar" şeklindeki tasnif üzerinden bilişim suçlarının türleri anlatılacaktır. Gelecek alt başlıklarda bu gruplar altında yer alabilecek suç türlerinin sık karşılaşılanlarından bahsedilecektir.

## *1.1. Elektronik Ağlar Aracılığıyla İşlenen Klasik Suçlar*

### 1.1.1. Dolandırıcılık

Elektronik ağlar vasıtasıyla işlenen klasik suçların başında dolandırıcılık suçları yer almaktadır. TCK Madde 157'de dolandırıcılık suçu; "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağla[ma]" olarak tanımlanmıştır. Nitelikli dolandırıcılık suçunu tanımlayan madde 158 (f) bendi dolandırıcılık

suçunun; "Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenmesini nitelikli dolandırıcılık olarak kabul etmiş ve ağırlaştırıcı sebep olduğuna hükmetmiştir.

İnternet üzerinde rastlanan yaygın dolandırıcılık türlerinin başında yatırım teklifleri yer almaktadır. Bu tür dolandırıcılık tekliflerinde mağdurlar genellikle küçük bir yatırımla büyük miktarda para kazanabileceklerine inandırılmaktadırlar. Mesela, mağdurdan, piyangodan kazandığı veya kendisine miras olarak kaldığı söylenen bir meblağın hesabına aktarılması için gerekli olan işlem maliyetini ödemesi istenilir. Bu teklifler genellikle e-posta aracılığıyla mağdurlara ulaşmaktadır. Dolandırıcılar insanların çoğunun bu tip e-postalara cevap vermeyeceklerini bildiklerinden yüzlerce, binlerce adrese aynı e-postayı göndermektedir. Dolayısıyla istenmeyen e-postaların (spam) hedeflerinden birisi de dolandırıcılıktır. E-posta alıcılarının çok ufak bir kısmı bile gönderilen teklifi ciddiye alsa dolandırıcılar için önemli bir başarı olacaktır.

Yatırım teklifi dolandırıcılığının belki de en meşhuru "Nijerya Dolandırıcılığı" veya "419 Dolandırıcılığı" olarak adlandırılmaktadır[1]. Dolandırıcı kişi veya kişiler çok sayıda adrese istenmeyen e-posta atarak kendisinin Nijerya'da vefat etmiş, tanınan ve belli bir sosyal statüsü olan (bazen doktor, bazen hükümet görevlisi) bir kişinin yakını olduğunu; bu kişiden intikal eden yüksek meblağda parayı, güvenlik gerekçesiyle ülke dışına çıkartmaya çalıştığını; yine güvenlik gerekçesiyle bu transferi normal yollardan yapamadığını, eğer kabul ederse e-posta alıcısının banka hesabını kullanarak parayı transfer etmek istediğini ve karşılığında belli bir ücret ödeyeceğini belirtmektedir. Kabul edilmesi halinde mağdura normal posta yoluyla bazı sahte dokümanlar gönderilerek ikna edilmekte ve sonrasında mağdurdan vergi veya havale masrafı adı altında belli bir meblağı göndermesi talep edilerek mağdur dolandırılmaktadır. 419 Dolandırıcılığı eski de olsa hâlâ can yakmaya devam etmektedir. Amerika'da faaliyet gösteren Internet Crime Complaint Service'in (IC3) 2011 raporunda ABD'de internet üzerinden dolandırıcılık hakkında yapılan şikâyetlerin yaklaşık %21'inin bu tip dolandırıcılıklar olduğu belirtilmektedir. Bu dolandırıcılıklar başka suçlara da sebep olabilmektedir. Mesela 2003 yılında Çek Cumhuriyeti'nde yaşayan 72 yaşındaki bir kişi bu şekilde kaybettiği 600.000 dolar civarındaki parasını geri alamayacağını öğrenince bir Nijerya Büyükelçiliği çalışanını öldürmüştür (Sullivan, 2003).[2]

Sık karşılaşılan diğer bir dolandırıcılık türü de internet üzerinden satış yoluyla yapılandır. Bu tip dolandırıcılıklarda mağdur, aradığı bir malı internette iyi bir fiyata bulur veya zor bulunan bir mala internet üzerinde rastlar. Malı satın almak için ödeme yaptıktan sonra ya malı hiç teslim alamaz yahut ilanda belirtilenden daha düşük değerde bir mal kendisine gönderilir. Bu dolandırıcılık türünün ikinci el araçlar üzerinden yapılanı yaygınlaşmaktadır. Satıcı genellikle bir ihtiyaç halinden dolayı aracını acele satmak zorunda olduğunu, bu yüzden de normalden daha ucuz bir fiyat istediğini, alıcılarla yüz yüze görüşmesinin mümkün olmadığını, ücretin belirtilen hesaba havalesinden sonra aracın alınabileceğini belirtmektedir.

---

1 "Nigerian fraud," "419 scam" veya "Nigerian 419 scam" gibi farklı isimlerle adlandırılmaktadır. 419 olarak adlandırılmasının sebebi dolandırıcılık suçlarının ilgili Nijerya kanununda tanımlandığı bölümün numarasıyla alakalıdır.

2 Çalışmada yer yer yabancı ülkelere ait istatistiklere yer verilmiştir. Ülkemize ait istatistiklerin verilmeyişi, bu seviyede rakamların olmayışından yahut elde edilememesinden kaynaklanmaktadır. Yabancı ülkelere ait istatistikler her ne kadar ülkemizdeki resmi ortaya koyamasa da, konu hakkında fikir vermek açısından faydalı olacağı düşünüldüğünden çalışmaya eklenmiştir.

Yine Crime Complaint Service'in rakamlarına göre 2011 yılında bu şekilde 88,2 milyon dolar dolandırıcılara kaptırılmıştır.

Dolandırıcılık başlığı altında bahsedilecek örneklerin sonuncusu internet üzerinde kurulan romantik ilişkiler vasıtasıyla yapılanlardır. Bu tip olaylarda dolandırıcılar sohbet kanallarında, arkadaşlık sitelerinde veya sosyal ağlarda arkadaşlık ilişkisi veya romantik bir ilişki kurabileceği bir eş arayan kişileri araştırmaktadırlar. Dolandırıcılar kurbanlarının sevgisini ve güvenini kazanabilmek için türlü yola başvurmakta, kurbanlarıyla gerçek hayatta temasa geçerek çiçek vb. hediyeler gönderebilmektedirler. Mağdurun güvenini kazandıktan sonra değişik sıkıntılar içinde olduklarını ve bazı ihtiyaçlarının olduğunu belirtip para sızdırmaya çalışmaktadırlar. Crime Complaint Service istatistiklerine göre 2011 yılında bu yolla 50,4 milyon dolar dolandırıcılık yapılmıştır.

### 1.1.2. Sahtecilik

Elektronik ağlar vasıtasıyla işlenen diğer bir suç türü de sahteciliktir. Sahteciliği bir şeyin kopyasını gerçekmiş gibi sunmak olarak tanımlayabiliriz (Mobbs, 2003). Bilgisayar vasıtasıyla basılı materyallerin sahteciliğini yapmak daha kolay bir hâle gelmiş ve buna ilaveten dijital belge ve bilgilerin sahteciliği konusu da gündeme girmiştir. Bu kapsamda ilk akla gelen suç olan kimlik hırsızlığı, başkasına ait kişisel verilerin ele geçirilmesi ve bu verilerin dolandırıcılık veya aldatma amacıyla kullanılmasıdır (Easttom, 2011: 7). Amerikan Adalet Bakanlığı verilerine göre 2005 yılında toplam 6.424.900 kişi kimlik hırsızlığı mağduru olurken bu rakam 2010 yılında artarak 8.571.900'e yükselmiştir. Kimlik hırsızlığı genellikle ekonomik kazanç için yapılmakla beraber, farklı hedefleri de olabilmektedir. Mesela, kimlik bilgileri bir kişinin itibarını zedelemek amacıyla (internetten pornografik materyaller sipariş etmek gibi işlemlerde) kullanılabilir.

Kimlik hırsızlığı gibi başkasına ait kişisel verileri elde etmek için kullanılan metotların başında *oltalama* (phishing[3]) olarak adlandırılan yöntem gelmektedir. Dolandırıcılık yöntemlerinde olduğu gibi oltalama yönteminin de pek çok çeşidi bulunmaktadır. Oltalama genellikle e-posta aracılığıyla yapılmaktadır. Oltalama yapan kişiler Facebook gibi popüler sitelerin, alışveriş sitelerinin veya finansal kurumlara ait internet sitelerinin tıpatıp benzerlerini yaparak internet üzerinden yayımlar ve rastgele gönderdikleri e-postalarda belirttikleri değişik mazeretlerle mağdurları bu sahte web sitelerine yönlendirirler. Bu şekilde hazırlanmış sahte sitelere giren mağdurlar burada kullanıcı adı, şifre gibi kişisel verilerini girmek suretiyle sisteme giriş yapmaya çalışırlar ve böylelikle bu bilgileri kötü niyetli kişilerin eline geçmiş olur. Oltalama suçlarının soruşturulması bir kısım zorluklar içermektedir. Öncelikle kurbanlar kimlik hırsızlığı mağduru olduklarını çok sonradan anlayabilmektedirler. Oltalama yapan kişiler ise kimliklerini gizlemek amacıyla açtıkları sahte web sitelerini belli bir süre sonra iptal etmekte veya başka bir sunucu üzerine taşımaktadırlar. Diğer yandan bu şekilde hazırlanan sahte web siteleri genellikle başka ülkelerde bulunan sunucular üzerinde bulunmakta ve

[3] Phishing kelimesi İngilizce balık tutmak anlamına gelen *fishing* kelimesinin ilk harfinin "ph" harfleriyle değiştirilmesiyle oluşturulmuş bir terimdir. Bu özgün isimlendirmenin, bilgisayar korsanlarının siber alanda yaptıklarını tanımlarken kelimenin gerçek hayattaki karşılığından (yani phishing örneğinde sıradan bir balık tutma fiilinden) ayırt etmek, zekâ ve yüksek teknoloji kullanıldığını vurgulamak maksadıyla tercih edildiği de belirtilmektedir.

hatta çoğu zaman sunucunun sahibi de böyle bir sitenin varlığından haberdar olmamaktadır. Özellikle bilişim hukuku gelişmemiş ülkelerde bu sitelerin sahiplerini takip etmek çok kolay olamamaktadır (Easttom, 2011: 7).

Kimlik hırsızlığı için kullanılan başka bir yöntem de *malware* olarak adlandırılan kötü amaçlı yazılımların kullanılmasıdır[4]. Bunlar genelde mağdurun haberi olmaksızın bilgisayara yüklenen ve çalışan; mağdura ait kullanıcı adı, şifre, kart numarası vb. kişisel verileri yahut mağdurun bilgisayarında bulunan belirli dosyaları saldırgana ait bir adrese aktaran yazılımlardır. Bazı yazılımlar kullanıcının ekranının belli aralıklarla resmini çekip bu resimleri de internet üzerinden başkalarına aktarabilir. Bu tip zararlı yazılımlar e-posta ekinde gelen eklentilerin açılması yoluyla hedef bilgisayara bulaşabildiği gibi, internet tarayıcısıyla zararlı kod barındıran bir internet adresini ziyaret etmek gibi basit bir yolla da bilgisayara bulaşabilir. Eğer yeni üretilmiş bir kötü maksatlı yazılım ise antivirüs programlarınca tespit edilemeyeceğinden antivirüs üreticileri bu yazılımı tanımlayana kadar mağdur bilgisayardan veri çalmaya devam eder.

*Hacking* olarak adlandırılan, bilişim sistemlerine yetkisiz erişim sağlama, kimlik hırsızlığı amacıyla kullanılan diğer bir yöntemdir[5]. Bilişim sistemlerine yetkisiz erişim sağlamaya yönelik birçok farklı metot bulunmaktadır. Bunların başında yazılımlarda bulunan açıkların kullanılması gelmektedir. *Hacker* olarak adlandırılan bilgisayar korsanları genellikle işletim sistemlerinde veya uygulama programlarında bulunan açıklardan istifade ederek sistemlere erişim sağlamaktadır. Sisteme girdikten sonra belli bilgileri çalabilir, sisteme istediği zaman kolayca erişebilmek için bir *arka kapı* (backdoor) oluşturabilir veya sisteme yerleştirdiği kötü maksatlı bir yazılım vasıtasıyla sistemde bulunan bilgilerin gizlice ağ üzerinden başka bir adrese transferini sağlayabilir.

Bu sayılanların yanında, bilgisayar veya depolama cihazlarının çalınması veya kaybedilmesi, hassas belgelerin çalınması, kaybedilmesi veya kazara çöpe atılması neticesinde kötü niyetli kişilerce ele geçirilmesi gibi bilişim konusunda teknik beceri gerektirmeyen yollarla da kimlik hırsızlığı gerçekleştirilmektedir. ABD'de bulunan Identity Theft Resource Center verilerine göre 2012 yılının ilk altı ayında gerçekleşen kimlik hırsızlıklarının %15'i basılı bilgilerin çalınması veya kaybedilmesi yoluyla gerçekleşmiştir. Yine aynı rapora göre kimlik hırsızlıklarının %30,5'i bilgisayar korsanlığı yoluyla , %7,5'i taşınabilir cihazların çalınması veya kaybedilmesi sonucu gerçekleşmiştir.

### 1.1.3. Siber Taciz ve Şantaj

Elektronik ağlar vasıtasıyla işlenen iki yaygın klasik suç tipi de *siber taciz* ve *siber şantajdır*. Siber taciz internet, e-posta gibi elektronik iletişim vasıtalarıyla kişinin sistematik olarak

---

4 Kişisel verilerin hırsızlığı amacıyla kullanılan yazılımlar için *casus yazılım* anlamına gelen *spyware* kelimesi de kullanılmaktadır. Yine *truva atı* (trojan horse) adı verilen ve çoğunlukla internetten indirilen ücretsiz yazılımlar beraberinde sisteme yüklenen kötü maksatlı yazılımlar da veri hırsızlığı amacıyla kullanılabilmektedir. Günümüzde yaygın olarak rastlanılan bu tip yazılımlar genel olarak kötü maksatlı yazılımlara has özellikleri taşıdıklarından bu çalışmada *malware* olarak gruplandırılmıştır.

5 *Hack* ve *hacking* kelimeleri *sistem kırma* veya *bilgisayar korsanlığı* şekillerinde Türkçeye çevrilmekle beraber, bu tabirler yaygın bir kullanım kazanmamıştır. Kavram günlük kullanımda daha çok kelimenin Türkçe okunuşuyla *hek* şeklinde ifade edilmekte ve *heklemek*, *heklenmek* gibi kullanımları da bulunmaktadır. Bu çalışmadaysa bilgisayar korsanlığı ifadesi tercih edilmiştir.

rahatsız edilmesidir. Siber taciz bazen tehdit ve şantaj bazen de yaralama, tecavüz ve öldürme gibi daha ağır suçların başlangıç aşaması olması sebebiyle önem taşımaktadır. Siber şantaj ise, genellikle bir kişiye veya kuruma ait olan ve ifşa edilmesi durumunda kişinin veya kurumun itibarını zedeleyecek veya rakipleri karşısında dezavantajlı duruma düşürecek nitelikteki bilgilerinin saldırgan tarafından ele geçirilmesiyle başlar. Daha sonra saldırgan bu bilgileri ifşa etmemesi karşılığında mağdurdan menfaat temin etmeye çalışır.

## 1.2. Elektronik Medya Üzerinde Yayınlanan Yasadışı İçerik

Yasadışı içerik denilince pek çok insanın ilk aklına gelen internet üzerinden çocukların cinsel istismarı olmaktadır. Çocuğun cinsel istismarı, çocuğun bir yetişkin veya yaşça daha büyük bir kişi tarafından cinsel doyum sağlamak amacıyla kullanılması şeklinde tanımlanabilir (Akdoğan, 2005). Çocuk istismarının bilişim teknolojileri vasıtasıyla gerçekleşen en yaygın türü çocuk pornografisidir. Kanunlarımızda çocuk pornografisinin bir tanımı bulunmamakla beraber Türkiye'nin de kabul ettiği Avrupa Konseyi Siber Suçlar Sözleşmesinin 9. maddesinde "(1) cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı, (2) cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı ve (3) cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren ve gerçek olmasa da gerçek gibi algılanan görüntüler içeren pornografik materyaller" çocuk pornografisi olarak kabul edilmiştir.

İnternet pornografik materyallerin çoğaltılmasını ve dağıtılmasını kolaylaştırmaktadır. Aynı zamanda yüz yüze ilişkiyi gerektirmediği için bu tip materyallerin tüketicilerine bir nevi gizli kalma, kimliğini saklıyor olma hissi de vermektedir. Diğer yandan internet bu tip materyallere ulaşımı kolaylaştırdığından belki böyle bir sapkınlığı olmayan kişilerin de zamanla bu tür materyallere bağımlı hale gelmesine yol açabilmektedir. İnternetin bu suçları kolaylaştırıcı etkisi sebebiyle, alınan onca tedbire rağmen çocuk pornografisi sektörünün büyümekte olduğu görülmektedir. 2006 yılında yapılan bir araştırmaya göre internet üzerinde çocuk pornografisi içerikli materyal sunan 100.000'in üzerinde site bulunmakta ve çocuk pornografisi sektöründe yıllık yaklaşık 3 milyar dolar civarında paranın döndüğü tahmin edilmektedir (Seigfried-Spellar, Lovely ve Rogers, 2011).

Ülkemizde çocuk pornografisine ilişkin suçlar TCK'nın Müstehcenlik başlığı altındaki 266. maddesinde tanımlanmıştır. Bu maddenin üçüncü fıkrası "müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan" veya "bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan" kişilerin cezalandırılmasına hükmetmektedir. Buna rağmen ulusal mevzuatta bu konuda bazı eksiklikler bulunmaktadır. Öncelikle, çocuk pornografisinin bir tanımı yapılmamıştır. Gelişen teknolojiyle beraber gerçek görüntüler üzerinde oynamalar yapılarak yetişkinlerin çocuğa benzetilmesi veya bilgisayar ortamında bu türden görüntülerin oluşturulması mümkündür. Mevzuatta bu türden görüntülerin hangi kapsama alınacağı konusu açık değildir. İkinci olarak bilgisayarların bu tür içeriği oluşturmak ve yaymak konusunda sağladığı kolaylıklardan dolayı bu suçların bilgisayarlar vasıtasıyla işlenmesini düzenleyen özel hükümler gerekmektedir, ancak mevzuatımızda bu alanda da boşluk bulunmaktadır (Inernational Centre for Missing and Exploited Children, 2008).

Ülkemizde müstehcen içeriklerin internetten yayımlanması da TCK'nın yine aynı

maddesince suçtur. Bu içerikleri bulunduran internet siteleri hakkında 5651 sayılı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi* ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*"* uyarınca erişimin engellenmesi kararı uygulanmaktadır. Kanunda bununla beraber uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, kumar oynanması için yer ve imkân sağlama, fuhuş gibi suçların tespit edilmesi halinde de ilgili sitenin erişiminin engellenmesine karar verilebileceği hükme bağlanmıştır. İnternette sağlanan içerikle ilişkili bir diğer problemli alan *nefret grupları* (hate groups) denilen grupların yayınladıkları içeriklerdir. Nefret grubu, ana hedeflerinden birisi başka bir grubu aşağılamak ve küçük düşürmek olan kişilerce oluşturulmuş topluluk olarak tarif edilebilir (Eastom, 2011: 26). Siber Suçlar Sözleşmesinin ırkçılık ve yabancı düşmanlığına ilişkin davranışların suç sayılmasına ilişkin ek protokolünde bu konu ele alınmıştır. Ancak ülkemiz henüz bu ek protokole imza atmamıştır.

### *1.3. Elektronik Ağlara Özgü Suçlar*

Elektronik ağlara has suçlar başlığı altında yer alabilecek fiilleri, Siber Suçlar Sözleşmesinde sayıldığı şekliyle şu başlıklar altında tasnif etmek mümkündür: (1) Bilişim sistemine yasadışı erişim, (2) veri iletimine yasa dışı müdahale, (3) veri bütünlüğüne müdahale, (4) bilişim sisteminin işleyişine müdahale. Bu fiillerin nasıl gerçekleştirildiğine (modus operandi) baktığımızda üç temel saldırı yöntemi karşımıza çıkmaktadır: (1) Bilgisayar korsanlığı, (2) hizmeti engelleme (Denial of Service – DoS), (3) zararlı yazılımlar ve (4) sosyal mühendislik saldırıları.

#### 1.3.1. Bilgisayar Korsanlığı

"Hack" ve "hacker" kavramlarının anlamları üzerinde geniş sosyolojik tartışmalar mevcuttur. Bu çalışmada bu konudaki tartışmalara girmeden günümüz kullanımında hack ve hacker kavramları hakkında kısa bir bilgi vermek uygun olacaktır. Hack kelimesi hacker topluluklarında kullanılan anlamıyla "teknolojinin orijinal, alışılmışın dışında ve özgün bir tarzda kullanılması" anlamına gelmektedir. Orijinal anlamında hack eyleminin ayırt edici özellikleri sadelik, ustalık ve yasa dışı oluşudur (Jordan ve Taylor, 2004:6). Dolayısıyla hacker denilen kişi ve gruplar, bu anlamdaki hack fiilini gerçekleştirenlerdir. Yani, internetten ulaşılabilen, sistem açıklarının ve bu açıklardan nasıl istifade edilebileceğinin adım adım anlatıldığı dokümanları uygulayarak veya başkalarının bu amaçla ürettiği programları kullanarak sistemlere girmek aslında "hacking" değildir. Bu tür saldırganları tarif için hack kavramı etrafında üretilmiş, *script kiddie*, *lamer, cracker* gibi pek çok başka tabir de bulunmaktadır. Ancak günümüzde, özellikle ülkemizde, bu ayrıma çok fazla dikkat edilmediğinden, bilişim sistemlerine yasa dışı yollarla giren herkes hacker veya bilgisayar korsanı olarak adlandırılmaktadır. Yaygın kullanılan şekliyle *bilgisayar korsanlığı* yetkisiz erişim sağlamak amacıyla bir sistemin güvenlik tedbirlerini etkisiz hale getirmeye çalışmaktır.

Bilgisayar korsanlığı maksadıyla kullanılan pek çok yöntem bulunmaktadır. Bu yöntemlerin başında işletim sistemlerinde, yaygın olarak kullanılan uygulama programlarında veya ağ bağlantılarında açıklar bularak bu açıklardan istifade etmek gelmektedir. Haliyle bu türden bir açığın tespit edilmesi ve istifade etme yollarının geliştirilmesi, bu sistemler hakkında etraflı bir bilgi sahibi olmayı gerektirmektedir. Neyse ki bu seviyede bilgi sahibi

olup hacking yapacak çok sayıda insan bulunmamaktadır. Ancak bilinen sistem açıklarına ilişkin bilgilerin paylaşıldığı pek çok internet sitesi mevcut olup hacking yapma heveslisi pek çok kişi tarafından bu siteler takip edilmektedir. Dolayısıyla güncellenmemiş işletim sistemi veya uygulama programlarının üzerinde çalışan sistemlerin daima risk altında oldukları unutulmamalıdır. Diğer yandan hacker gruplarının *Zero-Day-Exploit* olarak adlandırılan, üretici firmanın da varlığından haberdar olmadığı yeni bir açığı tespit edip kullanması ihtimali de her zaman söz konusudur.

Bir kere sisteme girince saldırgan için pek çok ihtimal bulunmaktadır. Sistem erişilmez hale getirilebilir, sistemde bulunan bilgiler çalınabilir, değiştirilebilir veya tahrip edilebilir. Daha da kötüsü sisteme sızan kişi şayet yeterince ustaysa varlığından kimseyi haberdar etmeden veriler üzerinde değişiklikler yapıp yine fark edilmeden sistemi terk edebilir. Böyle bir durumda sistemde barındırılan verinin bütünlüğü hakkında kimsenin aklına bir şüphe gelmeyecek ve söz konusu işletme bütünlüğü bozulmuş veriyle günlük işlemlerine devam edecektir.

### 1.3.2. Hizmeti Engelleme

Bilişim sistemlerinin erişilebilirliğine yönelik düzenlenen en meşhur saldırı türü "DoS saldırısı" olarak bilinen hizmeti engelleme saldırılarıdır. DoS saldırılarında kullanılan pek çok yöntem bulunmaktadır. Bu yöntemlerin tamamının yapmaya çalıştığı şey, sunucusu bilgisayarla çok sayıda sahte bağlantı kurmak suretiyle sunucuya aşırı iş yükü yüklemek ve gerçekten bağlantı kurmaya çalışan kullanıcılara cevap veremez hale gelmesini sağlamaktır. Günümüzde DoS saldırıları genellikle birden fazla hatta bazen binlerce bilgisayar kullanılarak yapılmaktadır. Bu tür saldırılara *Dağıtık Hizmeti Engelleme Saldırıları* anlamına gelen *Distributed DoS* veya *DDoS saldırıları* denilmektedir. Bu tür saldırıların soruşturulması da kolay olmamaktadır çünkü DDoS saldırıları çoğunlukla bu iş için yazılmış *botnet* (bot networks) adı verilen zararlı yazılımlar vasıtasıyla gerçekleştirilmektedir. Botnet isimli yazılımlar kullanıcıların farkında olmadan bilgisayarlarına yüklenmekte ve botnet yöneticisinden talimat gelene kadar bir faaliyette bulunmamaktadır. Botnetler genellikle DDoS ataklarında kullanılmakta, yöneticiden talimat geldiğinde yazılımın bulaştığı bilgisayarlar saldırının hedefinde bulunan internet adresleriyle bağlantı kurarak sunucuyu meşgul etmektedirler.

Botnetler, zararlı yazılımların sistemlere saldırmak için nasıl kullanılabileceğine güzel bir örnektir. Amerikalı bir hacker, internet reklam şirketlerinin talepleri doğrultusunda zararlı bir kodu 400.000'in üzerinde kullanıcının bilgisayarına indirip çalıştırmış, karşılığında bu firmalardan 100.000 doların üzerinde ücret almıştır. Bahse konu şahıs bu eylemi kullanıcı bilgisayarlarına yüklediği botnet yazılımları vasıtasıyla gerçekleştirmiştir. Aynı şahıs botnetlerini başka şirketlere de kiralamak yoluyla gelir elde etmiştir. Şahıs bu eylemlerinden dolayı beş yıl hapse mahkûm edilmiştir. Botnetler günümüzde zararlı program üreticileri için iyi bir kazanç kapısı haline gelmektedir. Botnet yöneticileri sahip oldukları botnet ordusunu saatlik 200-300 dolar gibi bir ücretle isteyenlere kiralayabilmektedirler (Wilson, 2008). Dolayısıyla günümüzde bu tür bir siber saldırı gerçekleştirebilmek için saldırganın artık ileri seviyede bir teknik bilgiye sahip olmasına ihtiyacı yoktur.

### 1.3.3. Zararlı Yazılımlar

Botnet örneğinde olduğu gibi zararlı yazılımlar siber saldırıların en temel silahlarındandır. Botnet benzeri yazılımlar genellikle sistemlere truva atı olarak adlandırılan, normalde bilinen

(ve kullanıcı tarafından arzu edilen) işlevinin yanında bilinmeyen ve kullanıcının istemeyeceği işlevleri de olan yazılımlar vasıtasıyla yüklenmektedirler. Bu yazılımlar bir kere sisteme yüklendikten sonra sisteme daha kolay giriş sağlamak üzere arka kapı açabilmekte veya kayıtlı bilgileri başka yerlere aktarabilmektedir. Botnet tarzı zararlı yazılımlar e-posta ekinde gönderilen dosyalar (mesela PDF uzantılı dosyalarla bu tip zararlı kod gönderilebilir) veya mesaj içeriğinde yer alan bağlantılara tıklayarak ziyaret edilen internet sayfaları vasıtasıyla da bulaşabilmektedir.

Günümüzde bu tür yazılımların şirketler veya ülkeler tarafından üretilerek istihbarat amaçlı olarak kullanıldıklarına ilişkin iddialar bulunmaktadır. Bu türden zararlı yazılımlar *APT* (Advanced Persistent Threat) olarak adlandırılmaktadır. APT'ler genellikle hedef sistemlere sızarak bu sistemlerden veri aktarımı yapmak üzere programlanmaktadırlar. APT'lerin en önemli özellikleri enerji, ulaşım gibi belli sistemleri veya belli dillerde çalışan bilgisayarları hedef alarak bu sistemlere sızmaya çalışmaları ve birkaç virüs yazarı tarafından geliştirilemeyecek kadar karmaşık yapılara sahip oluşlarıdır. İran nükleer sistemlerini kontrol eden bilgisayarlara sızan Stuxnet bu türden zararlı yazılımlara örnek olarak verilebilir.

### 1.3.4. Sosyal Mühendislik Saldırıları

Son olarak bahsedilecek siber saldırı tekniği sosyal mühendislik saldırılarıdır. Sosyal mühendislik saldırıları, insan doğasından istifade etmek üzere değişik aldatmacalar kullanarak hedef sistem hakkında bilgi edinmek, veri ele geçirmek veya sisteme girmektir (Chen ve Walsh, 2009). Oltalama ve istenmeyen e-posta göndermek bir nevi sosyal mühendislik saldırısıdır çünkü kullanıcıları kandırarak belli eylemleri yaptırmayı hedeflemektedirler. Bunun yanında saldırganın hedeflenen kurum çalışanlarına telefon açarak kendisini bilgi işlem personeli olarak tanıtıp, bir bahaneyle sisteme bağlanırken kullandığı kullanıcı adı ve şifresini öğrenmesi de bir sosyal mühendislik saldırısıdır. Sosyal mühendislik saldırıları kişisel beceriye dayanan, basit ve etkili saldırılardır. 2011 yılında altı farklı ülkede yerleşik şirketler üzerinde yapılan bir anket sonuçlarına göre katılımcıların %43'ü en az bir kere sosyal mühendislik saldırısına maruz kalmış ve bunların %48'i her bir saldırının yaklaşık 25.000 dolar değerinde kayba yol açtığını belirtmiştir (Dimensional Research, 2011)

## 2. İstatistiklerle Türkiye'de Siber Güvenlik

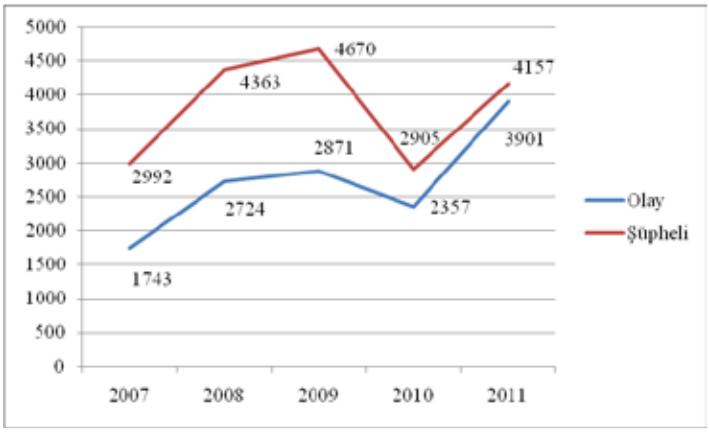
Ülkemizde, Emniyet Genel Müdürlüğüne bağlı olarak 2011/2025 sayılı Bakanlar Kurulu Kararıyla kurulan Siber Suçlar Dairesi Başkanlığından önce, Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı bilişim suçlarıyla mücadele vazifesini yürütmekteydi. Bu dairenin bilişim suçlarına ilişkin tuttuğu 2011 yılı istatistiklerine Tablo 1'de yer verilmiştir. Buna göre banka ve kredi kartı dolandırıcılığı ve bilişim sistemlerine karşı işlenen suçlar en sık rastlanan suç kategorilerini oluşturmaktadır. Grafik 1'de 2007-2011 yılları arasında kayda geçen olay ve şüpheli sayıları görülmektedir. Şekilde görüldüğü üzere bilişim suçları yükselen bir ivmeye sahiptir. 2010 yılında olay ve şüpheli sayılarında bir azalma yaşanmıştır. Şüpheli sayısındaki azalış, olay sayısındaki azalıştan daha büyük olmuş ve her iki rakam birbirine yaklaşmıştır. Değerler 2011 yılında hızlı bir artış göstermektedir.

**Tablo 1.** 2011 Yılı Olay ve Şüpheli Sayıları

| | Olay Sayısı | Şüpheli Sayısı |
|---|---|---|
| Banka ve Kredi Kartı Dolandırıcılığı | 1.819 | 1.503 |
| İnteraktif Bankacılık Dolandırıcılığı | 148 | 348 |
| Bilişim Sistemlerine Karşı İşlenen Suçlar | 1.791 | 1.898 |
| İnternet Aracılığıyla Nitelikli Dolandırıcılık | 112 | 285 |
| Diğer | 31 | 123 |
| Toplam | 3.901 | 4.157 |

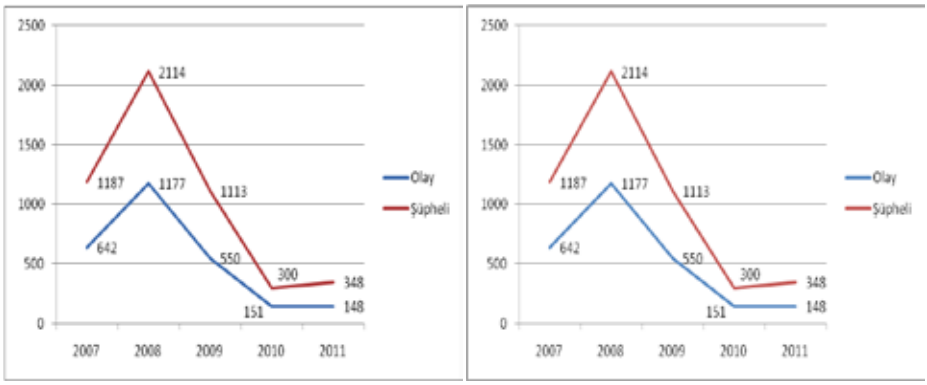
Kaynak: Kaçakçılık ve Organize Suçlarla Mücadele 2011 Raporu

**Grafik 1.** 2007-2011 Yıllarına İlişkin Olay ve Şüpheli Sayıları




Kaynak: Kaçakçılık ve Organize Suçlarla Mücadele 2011 Raporu

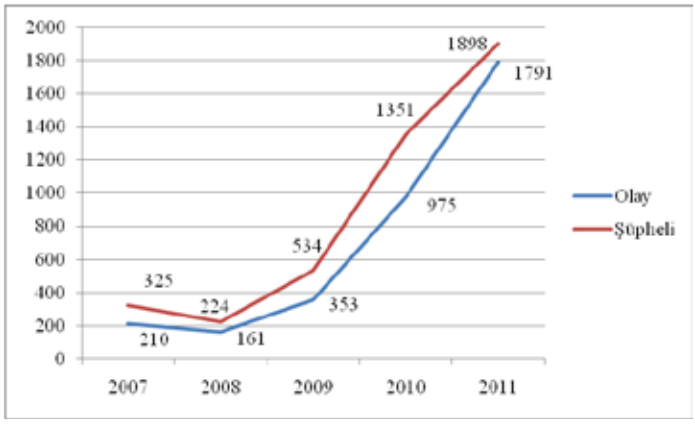
**Grafik 2.** 2007-2011 Yıllarına İlişkin Suç Türüne Göre Olay ve Şüpheli Sayıları




Kaynak: Kaçakçılık ve Organize Suçlarla Mücadele 2011 Raporu

2007-2011 yılları arasında kaydedilen olay ve şüpheli sayılarının suç türlerine göre dağılımı Grafik 2 ve Grafik 3'te gösterilmiştir. Grafik 2'de görüldüğü gibi 2010 yılında görülen düşüşün ana sebebi interaktif banka dolandırıcılığı olayları sayısındaki düşüşten kaynaklanmaktadır. Aynı şekilde banka ve kredi kartı dolandırıcılığı rakamlarında da önemli bir azalma gözlemlenmektedir. Buna karşın Grafik 3'te aynı yıl aralığında bilişim sistemlerine karşı işlenen suç ve yakalanan şüpheli sayıları yer almaktadır. Görüldüğü gibi bilişim sistemlerine karşı işlenen suçlar 2008 yılından itibaren hızlı bir yükselişe geçmiş ve 2007 rakamlarının yaklaşık sekiz katı artmıştır.

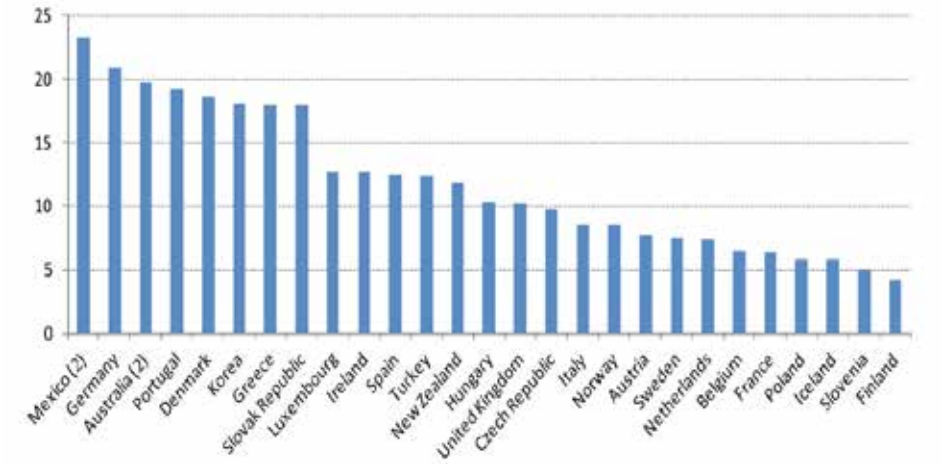
**Grafik 3.** 2007-2011 Yıllarında Bilişim Sistemlerine Karşı İşlenen Suçlara İlişkin Olay ve Şüpheli Sayıları




Kaynak: Kaçakçılık ve Organize Suçlarla Mücadele 2011 Raporu

Grafik 4'te sunulan OECD verilerine baktığımızda 2010 yılı içerisinde bilişim güvenliği problemi yaşayan işletme oranları içerisinde Türkiye 27 ülke içerisinden on ikinci sırada yer almaktadır.

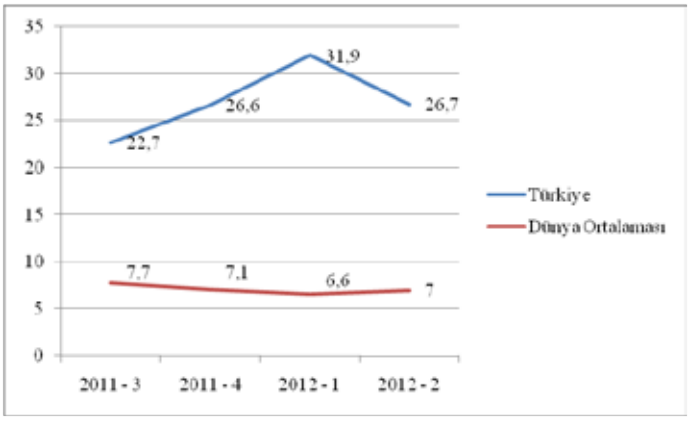
**Grafik 4.** 2010 Yılında Bilişim Güvenliğine İlişkin Sorun Yaşadığını Bildiren İşletme Oranları




Kaynak: OECD, 2012

Grafik 5, Türkiye'de ve dünyada bilgisayarlara zararlı yazılım bulaşma oranlarını göstermektedir. Bu istatistik, Microsoft firmasının zararlı yazılım temizleme araçları vasıtasıyla toplanan verilerden oluşmaktadır. Dikey eksen zararlı yazılım taraması yapılan her 1.000 bilgisayardan zararlı yazılım temizliği yapılanların sayısını göstermektedir. Şekilde, 2011 yılının üç ve dördüncü, 2012 yılının bir ve ikinci çeyreklerine ait rakamlar sunulmuştur. Görüldüğü üzere ülkemizdeki zararlı yazılım bulaşma oranları dünya ortalamasının yaklaşık 3,8 katı daha fazla olmuştur. Ülkemizde ve dünyada kullanılmakta olan işletim sistemlerinin yaklaşık % 90'ının Microsoft tabanlı olduğu düşünülünce bu grafiğin yabana atılmaması gerektiği görülmektedir.

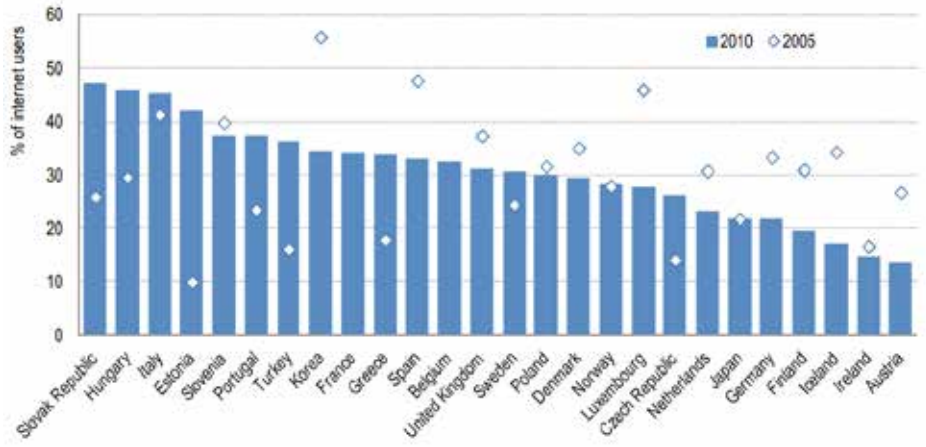
**Grafik 5.** Zararlı Yazılım Bulaşma Oranları




Kaynak: Microsoft Security Intelligence Report, 2012

Grafik 6'da ise OECD verilerine göre virüs bulaşan internet kullanıcılarının miktarı görülmektedir. 2010 rakamlarına göre Türkiye istatistiği verilen 26 ülke içinde yedinci sırada bulunmaktadır. Ülkelerin çoğunluğunda virüs bulaşma oranları 2005 yılına göre azalırken, ülkemizde ciddi oranda bir artış olduğu görülmektedir.

**Grafik 6.** OECD Verilerine Göre Bilgisayarına Virüs Bulaşan İnternet Kullanıcılarının Oranları




Kaynak: OECD, 2012

Kleiner, Nicholas ve Sullivan'ın (2013) Microsoft'un zararlı yazılım temizleme araçları vasıtasıyla toplanan veri üzerinde yaptıkları analizlerde Türkiye, virüs bulaşma oranı açısından ağırlıklı olarak Ortadoğu ülkelerinin bulunduğu kötü performanslı ülkeler grubunda yer almaktadır. Zararlı yazılımların yanında ülkemiz siber saldırılara kaynaklık etme bakımından da üst sıralarda yer almaya başlamıştır. Akamai güvenlik şirketinin istatistiklerine göre Türkiye 2012 yılının üçüncü çeyreğinde siber saldırılara en çok kaynaklık eden ülkeler listesinde %4,7 ile üçüncü sırayı almıştır. Listenin başında %41 gibi yüksek bir oranla Çin gelmekte ve ikinci sırayı %10 ile ABD almaktadır. Tablo 2'de görüldüğü üzere Türkiye'yi Rusya, Tayvan ve Brezilya takip etmektedir. Akamai şirketinin önceki yıllara ait raporlarına bakıldığında Türkiye'nin 2009-2012 yılları arasında bu alanda yükselişte olduğu görülmektedir. Bu rakamlar elbette saldırılara kaynaklık eden ülke hakkında kesin bir yargıya varılmasına imkân vermez. Bilindiği gibi Botnet adı verilen zararlı yazılımlar vasıtasıyla bir bilgisayar korsanının dünyanın başka bir köşesinde bulunan bir bilgisayara sızarak o bilgisayarı siber saldırı maksatlı olarak kullanması mümkündür. Ülkemize ait zararlı yazılım bulaşma istatistikleri de böyle bir ihtimali güçlendirmektedir. Ayrıca siber güvenlik çalışmaları gerçekleştiren Host Exploit web sitesinde yayınlanan 2013 Mart raporuna göre ülkemiz en kötü 10 ülke listesinde dokuzuncu sırada bulunmaktadır. Ülkemiz zararlı yazılım bulaşmış web sayfası, kötü maksatlı yazılım ve oltalama (phishing) siteleri barındırma kategorilerinde öne çıkmaktadır. Bu bulgular da Akamai raporunu desteklemektedir.

**Tablo 2.** Kaynak IP Adresine Göre Kendisinden En Fazla Saldırı Gerçekleşen Ülkeler

| | Ülke | 2012 – 4 (%) | 2012 – 3 ( %) |
|---|---|---|---|
| 1 | Çin | 41 | 33 |
| 2 | ABD | 10 | 13 |
| 3 | Türkiye | 4,7 | 4,3 |
| 4 | Rusya | 4,3 | 4,7 |
| 5 | Tayvan | 3,7 | 4,5 |
| 6 | Brezilya | 3,3 | 3,8 |
| 7 | Romanya | 2,8 | 2,7 |
| 8 | Hindistan | 2,3 | 2,5 |
| 9 | İtalya | 1,6 | 1,7 |
| 10 | Macaristan | 1,4 | 1,4 |
| - | Diğer | 25 | 28 |

Kaynak: Akamai, 2012

Bu kısımda sunulan Türkiye'ye ilişkin istatistikleri OECD raporunda sunulan tasnif kriterlerine göre incelediğimizde sadece meydana gelen olaylara ilişkin veri tutulduğu, aynı zamanda tutulan verilerin ağırlıklı olarak konunun teknik boyutunu ilgilendirdiği, sosyal ve ekonomik yönüyle alakalı pek bir veri bulunmadığı görülmektedir. Ülkemizin siber güvenlik performansının daha sağlıklı tespiti için bu alanlarda da veri toplanmasına ihtiyaç duyulmaktadır. Mevcut veriler ışığındaysa, ülkemizin siber güvenlik karnesinin pek iyi olmadığı görülmektedir.

## 3. Türkiye'de Siber Güvenlik Politikaları

### *3.1. Hukuki Altyapı*

Hukuki altyapı, politikaların üzerinde şekilleneceği zeminin önemli bir öğesi olduğundan bu kısımda ülkemizin siber suçlara ilişkin mevzuatı ve bu mevzuatta görülen bazı problemler anlatılarak yeri geldiğinde mukayese amacıyla ABD ve AB mevzuatındaki ilgili hususlara kısaca değinilecektir. 5237 sayılı Türk Ceza Kanununda (TCK) elektronik ağlar vasıtasıyla işlenen klasik suçlardan genellikle o suçların bahsedildiği kısımda ağırlaştırıcı faktör olarak belirtilmiştir. Mesela bilişim vasıtalarını kullanarak işlenen dolandırıcılık suçu "nitelikli dolandırıcılık" başlığı altında mütalaa edilmiş ve ağırlaştırıcı sebep olarak kabul edilmiştir. İçerikle alakalı suçlar yine aynı şekilde ilgili maddeler içerisinde yerini almış (müstehcenlik örneğinde olduğu gibi) veya aşağıda değinilecek olan 5651 sayılı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi* ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*"* belirtilmiştir. Elektronik ağlara has suçlarsa TCK'da Onuncu Bölüm olarak Bilişim Alanında Suçlar başlığı altında ele alınmıştır.

TCK Onuncu Bölüm'de bilişim sistemine girme fiilini tanımlayan 243. maddeyle başlamaktadır. Maddenin birinci fıkrasında "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren *ve* orada kalmaya devam eden kimseye" ceza verileceğine hükmetmektedir. Dolayısıyla bilişim sistemine sadece girme fiili ceza kapsamından

çıkartılmakta, cezalandırma için sistemde kalma şartını da getirmektedir[6]. Kanun koyucu muhtemelen kazara gerçekleşen yetkisiz erişimleri kapsam dışında tutmaya çalışmış olmakla beraber, kişinin bu madde kapsamında cezalandırılması için sistemde ne kadar kalması gerektiği konusu yoruma bırakılmıştır. Bunun yanında sisteme hukuka uygun olarak girip, hukuka aykırı olarak kalmaya devam edenler veya yetkisini aşanlar hakkında da belirsizlik bulunmaktadır.

Maddenin ikinci fıkrasında "yukarıdaki fıkrada tanımlanan fiillerin *bedeli karşılığı yararlanılabilen sistemler* hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir" hükmü yer almaktadır. Bu fıkrada "bedeli karşılığı yararlanılabilen sistemler" ibaresinden ne kastedildiği açık olmamakla beraber bunun, kayıtlı müşterilerine internet üzerinden belli hizmetler sunan firmalara ait sistemler olduğu anlaşılmaktadır. Kanun, saldırıya hedef olma ihtimali daha fazla olan bu sistemlere karşı gerçekleştirilecek yetkisiz girme ve kalmaya devam etme fiiline verilecek cezayı yarı oranında azaltmaktadır. Aslında daha fazla risk barındıran sistemlere ilişkin daha fazla caydırıcılık olması gerekirken bu fıkrada tam tersi bir durum söz konusudur. Kaldı ki böyle bir sisteme saldırı neticesinde müşterilerin kişisel ve finansal bilgilerinin kötü maksatlı kişilerin eline geçmesi gibi korunması gereken ciddi bir risk bulunmaktadır. Diğer yandan bir önceki fıkrada aslında "yetkisiz girme ve kalmaya devam etme" şeklinde tek bir fiilden bahsedilirken ikinci fıkranın "yukarıdaki fıkrada tanımlanan fiillerin" ibaresiyle başlaması kanun metninde yapılan değişikliğin biraz aceleye geldiği düşüncesini uyandırmaktadır. Üçüncü fıkrada ise bu fiil neticesinde istemeden verilerin yok olması halini hükme bağlamaktadır.

TCK 244. maddede bilişim sisteminin işleyişinin engellenmesi ve bozulması; bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması; sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi suçları hükme bağlanmaktadır. TCK 245. madde kredi kartı dolandırıcılıklarına ilişkin hükümler içermekte ve son madde olan TCK 246. madde ise bu suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine başvurulacağını belirtmektedir.

TCK'nın ilgili hükümlerine genel olarak bakıldığında elektronik ağlar vasıtasıyla işlenen suçların pek çoğunu kapsadığı görülmektedir. Yukarıda belirtilen problemli hususların yanı sıra kanunda anılan suçlara verilen cezaların failin motivasyonu ve hedef alınan sistemin hassasiyeti göz önünde bulundurularak yeniden düzenlenmesi uygun olacaktır. Bu haliyle casusluk veya terörist eylem amacıyla siber saldırı düzenleyen bir kişiyle, arkadaş grubu içerisinde statü edinmek için siber saldırı düzenleyen kişi arasında bir fark gözetilmemiştir. Yine aynı şekilde çalışmaması veya hatalı çalışması halinde doğabilecek hasardan çok sayıda insanın etkileneceği bir sisteme yapılan bir saldırıyla küçük bir şirketin internet sayfasına düzenlenen saldırı arasında da bir fark gözetilmemiştir.

ABD kanununda, TCK'da problemli olarak gördüğümüz bu hususların da düzenlendiği görülmektedir. ABD'de siber güvenlikle alakalı en önemli kanun Computer Fraud and Abuse Act (CFAA) isimli kanundur. ABD Kongresinde kabul edildiği 1986 yılından bu yana zaman

---

[6] Maddenin TBMM Genel Kurulu'na sunulan orijinal halinde "hukuka aykırı olarak giren *veya* orada kalmaya devam eden" ibaresi bulunmaktayken bu ibare Genel Kurul tartışmaları sonrasında "suç tanımlarında belirliliği sağlamak" gerekçesiyle şu anki haline çevrilmiştir (Karagülmez, 2011).

zaman değişikliklere uğrayan bu kanun, bilişim sistemlerine özgü suçların yanında bilişim sistemlerinin vasıta olarak kullanıldığı suçları da ele almaktadır. CFFA'da göze çarpan önemli bir özellik siber suçların hedef sistemin özelliği bakımından ayrıştırılmasıdır. Bu maksatla kanunda *koruma altındaki bilgisayar* (protected computer) kavramına yer verilmiştir. Yapılan tanıma göre koruma altındaki bilgisayar "(1) finansal bir kurum ya da devlet kurumlarına münhasıran kullanılan veya bunlarca dolaylı olarak kullanılıp suç fiilinin bunları etkilediği veya (2) ABD dışında da olsa eyaletler arası ya da uluslararası ticaret veya iletişim maksadıyla kullanılan bilgisayardır." Bazı mahkeme kararlarında ağ üzerinde çalışan her bilgisayar koruma altındaki bilgisayar kavramı kapsamına sokulsa da, kanunun özünde böyle bir ayrıma yer verilmesi önemlidir. Kanunda bulunan diğer bir özellik siber suçları ve öngörülen cezaları failin motivasyonuna göre de ayrıştırıyor oluşudur. Aynı şekilde diğer bir olumlu yön kanunda yorum farklılığına sebebiyet vermemek maksadıyla bilgisayar, finansal kurum, zarar, kayıp gibi pek çok temel kavramın tanımlarına yer verilmesidir.

Bu alanda ülkemiz için önemli bir hukuki metin de Avrupa Konseyi Siber Suçlar Sözleşmesidir. 2001 yılında kabul edilen, 2004 yılında yürürlüğe giren sözleşmeye Türkiye 2010 yılında taraf olmuştur. TCK ile karşılaştırdığımızda sözleşmenin daha detaylı hazırlandığı ve çocuk pornografisinin tanımı gibi başka ilave tanım ve hükümler içerdiği görülmektedir. Ülkemizin sözleşmeye taraf olması olumlu bir gelişme olup, sözleşmenin TBMM tarafından onaylanmasının ardından mevzuatta önemli bir boşluğun dolmuş olacağı düşünülmektedir. Sözleşmeye ilave olarak Avrupa Birliği üyesi ülkelerin hukuki ve kurumsal uyumlarının sağlanması amacıyla çerçeve kararlar alınarak yürürlüğe konulmuştur. Bu çerçeve kararlar da yerli hukuk sistemimizde yapılacak değişikliklerde göz önünde bulundurulması gereken metinlerdir.

Bilişim suçlarını ilgilendiren diğer bir kanun 5271 sayılı Ceza Muhakemesi Kanunudur (CMK). CMK'nın "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıklı 134. maddesinde dijital delillerin toplanması ve muhafaza edilmesi usulüne ilişkin hükümler bulunmaktadır. Maddenin ilk fıkrasında dijital medya üzerinde yürütülmekte olan bir soruşturma kapsamında başka surette delil elde etme imkânının bulunmaması halinde arama yapılabileceği belirtilmektedir. İkinci fıkrada sadece "şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde" dijital medyaya el konulabileceği; kopyalama işleminden sonra cihazların gecikme olmaksızın iade edilmesi gerektiği belirtilmektedir.

Buradaki birinci problemli husus, bilgisayarın şifrelenmiş olduğunun veya gizlenmiş bilgiler barındırdığının nasıl anlaşılacağıdır. Bilindiği üzere dijital bir cihazı çalıştırmadan yahut adli bilişim yöntemleriyle incelemeden içeriği hakkında dışarıdan bir fikir yürütmek, şifrelenmiş olup olmadığını, gizli bilgiler barındırıp barındırmadığını anlamak mümkün değildir. Bu yüzden bu fıkranın nasıl uygulanacağı soru işaretleri barındırmaktadır. Diğer yandan el koyma yetkisinin bu iki durumla sınırlanması, olay yeri inceleme birimlerinin çalışmasını zorlaştırıcı mahiyettedir. Mesela, kopyalanması gereken çok fazla miktarda bilgisayar bulunan bir olay yerinde sadece kopyalama çalışmaları personelin çok uzun bir süre bu işe kilitlenmesine diğer görevlere gidememesine sebep olacaktır. Bu maddeyle alakalı ikinci problemli husus, içinde suç unsuru, örneğin çocuk pornografisi, bulunan dijital medyanın da kopyalandıktan

sonra iade edilip edilmeyeceğidir. Mevcut haliyle buna mani bir durum bulunmamaktadır.

CMK 134. maddenin üçüncü ve dördüncü fıkralarında el konulan medyanın yedeğinin alınacağı ve istemesi halinde bu yedeğin bir kopyasının şüpheliye veya vekiline verileceği belirtilmektedir. Bir önceki fıkrada belirtilen yasa dışı içerik problemi burada da bulunmaktadır. Yasa dışı içerik bulunan medyanın bir kopyası şüpheliye verilecek mi, şüpheliye hangi formatta, nasıl bir medya üzerinde verilecek, bu medyayı kim sağlayacak? Bu sorular meseleye dışarıdan bakan birisine önemsiz gibi gelebilse de, uygulamada inceleme birimleri için aksaklıklara sebebiyet verebilmektedir. Diğer bir problem, bu yedeklerin kimin tarafından, nasıl ve ne kadar süre muhafaza edecekleri hususudur. Veri depolama aygıtlarının kapasitelerinin giderek arttığı göz önüne alındığında, ilgili birimlerde bu kadar medyayı saklayacak depolama üniteleri bulunmakta mıdır? Her dijital delil saklanmalı mıdır, bunu belirlemek için ne gibi kriterler kullanılmalıdır? Delil saklanacaksa ne kadar süreyle saklanmalıdır? Bu ve benzeri hususların açıklığa kavuşturulması gerekmektedir.

CMK 134. maddenin beşinci ve son fıkrasında sisteme el koymaksızın da kopyasının alınabileceği, bu durumda alınan verilerin kâğıda yazdırılacağı belirtilmektedir. Burada edinilmek istenen hukuki fayda delil bütünlüğünün korunmasıdır. Ancak verilerin kâğıda yazdırılması ibaresinden kasıt, alınan dosyaların içeriklerinin yazdırılmasıysa bu durumda sayfalarca belki ciltlerce çıktı alınması gerekecektir. Sadece dosyaların isimleri yazdırılacaksa da bunun delil bütünlüğünü sağlamak açısından bir faydasının olmayacağı ortadadır. Dolayısıyla her iki durumda da maddenin uygulanması problem teşkil edecektir. Görüldüğü üzere CMK 134. madde konuyla ilgili önemli hususlar göz önüne alınarak ve şüphelinin hakları gözetilerek düzenlenmiştir. Ancak kanunun uygulamada yukarıda sayılan sorunlara sebep olması muhtemeldir.

Siber suçlarla mücadele hedefli diğer bir kanun 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dur. Kanunun yürürlüğe girmesinden sonra uygulamayı düzenlemek için bazı yönetmelikler de çıkarılmıştır. Kanun hangi içeriğin yasa dışı olduğunu ve içerik sağlayıcıları gibi internette faaliyet gösteren aktörlerin rol ve sorumluluklarını belirlemektedir. Kanunda yasadışı içerikle mücadele yöntemi olarak erişimin engellenmesi yöntemi benimsenmiştir. Ancak erişimi engelleme yönteminin uygulamada pek bir etkinliği bulunmamaktadır çünkü ağ ayarlarında yapılacak bazı kolay değişikliklerle yasaklı sitelere ulaşmak mümkündür. Diğer yandan sitelerin yasaklanması ülkemizin uluslararası imajını da olumsuz yönde etkilemektedir.

### *3.2. Siber Güvenlik Stratejilerinde Öne Çıkan Unsurlar ve Türkiye'deki Durum*

Siber güvenlik, bilişim teknolojilerinin yaygınlaşması ve internet kullanımının artmasıyla beraber ulusal güvenlik stratejilerinde yer almaya başlamıştır. Bu kapsamda başta gelişmiş ülkeler olmak üzere pek çok ülke ve NATO, AB gibi uluslararası kuruluşlar siber güvenlik stratejileri üretmiştir. 19 ülkenin ulusal siber güvenlik stratejileri üzerinde yapılan inceleme sonucunda strateji belgelerinde şu ortak hedeflere değinildiği görülmektedir (Luiijf ve diğ.'den aktaran Klimburg, 2012: 56):

- Güvenli, saldırılara karşı dayanıklı ve güvenilir bir siber alanın sağlanması.
- [Bilişim sistemleri vasıtasıyla] ekonomik ve sosyal refahın, güvenli iş ortamı ve

ekonomik büyümenin teşvik edilmesi.
- Bilişim ve iletişim teknolojilerinin barındırdığı risklerin kontrol altında tutulması.
- Bilişim altyapılarının dirençli hale getirilmesi.

Klimburg (2012) ulusal siber güvenliği düşünülürken göz önünde bulundurulması gereken beş alan olduğunu belirtmektedir. Mevcut siber güvenlik stratejilerine bakıldığında bu alanların işlendiği görülmektedir. Siber güvenlik stratejilerinde temas edilen ilk alan askeri siber operasyonlardır. Askeri siber operasyonlar denilince öncelikle akla gelen ülkenin sahip olduğu bilişim altyapısının korunmasına yönelik olarak siber savunma olmaktadır. Siber savunma istihbarat odaklı olup CERT tarzı, acil durumlara hızlı müdahaleye imkân sağlayan bir organizasyonel yapı gerektirmektedir. Siber savunma yukarıda bahsedildiği gibi pasif ve aktif savunma biçimlerini içermektedir. Aktif savunma yöntemleri saldırganın saldırı maliyetini arttırarak caydırıcılığı arttırmayı hedeflemektedir. İkinci önemli askeri beceri, düşman unsurların bilişim altyapılarına stratejik nitelikli siber operasyonlar yapabilmektir. Üçüncü önemli askeri beceri, ikinciyle yakından alakalı olarak, savaş halinde düşmanın sahip olduğu bilişim altyapılarına yönelik siber saldırı gerçekleştirebilmektir. Dördüncü ve son beceri, geleneksel askeri yapıların, bilişim teknolojilerinin sunduğu imkânlardan yararlanılarak modernize edilmesi yoluyla kapasite ve etkinliğin arttırılmasıdır.

İkinci alan siber suçlarla mücadele edilmesi konusudur. Mücadelenin ilk aşaması ulusal ve uluslararası hukuki altyapının oluşturulmasıdır. Bu görev genellikle adalet bakanlıkları aracılığıyla yürütülür. Adalet bakanlıkları ulusal seviyede insan hak ve hürriyetlerini gereğinden fazla kısıtlamayan, caydırıcılığı olan ve polis birimlerine mümkün olduğunca rahat bir çalışma ortamı sağlayan bir hukuki altyapının tesisi için çalışmalıdır. Siber suçların küresel özelliği nedeniyle diğer ülkelerin hukuk sistemlerinin gelişmesine katkı sağlanmalı ve bu alanda işbirliği mekanizmaları geliştirmeye çaba göstermelidir. Siber suçlarla mücadelede belki en önemli rol polis birimlerine düşmektedir. Genellikle içişleri bakanlıklarınca yönetilen polis birimleri dijital soruşturma becerilerini geliştirebilmek için adli bilişim alanında uzmanlaşmış daha fazla soruşturmacıya ihtiyaç duyacaktır. Aynı şekilde sınır aşan suçların soruşturulabilmesi için yabancı ülke polis teşkilatlarıyla ikili ilişkiler kurulması bu alanda ihtiyaç duyulan hız ve esnekliği sağlayacaktır. Siber suçlarla mücadelenin diğer bir boyutu da ticari kurumlar ve sivil toplum kuruluşlarıdır. Ticari kurumlardan bilişim suçları açısından en önemlilerinden birisi servis sağlayıcılardır. Servis sağlayıcılar, sunucularına yönelen e-posta trafiğini süzerek kullanıcılara daha az istenmeyen e-posta (spam e-mail) gitmesini sağlayabilir. Aynı şekilde domain hosting (internet sayfalarının belli bir kira karşılığında barındırılması ve yayınlanması hizmeti) firmaları içerikleri üzerinde yapacakları denetimlerle siber suçlarla mücadele faaliyetlerine katılabilirler. Sivil toplum kuruluşları da kullanıcıların bilişim sistemlerini kullanırken daha bilinçli davranmasına katkı sağlayabilirler.

Üçüncü alan olan istihbarat/karşı istihbarat faaliyetleri konusu ilk iki alanla yakından ilişkili olsa da kendine has bir özelliği bulunmaktadır. Günümüzde istihbarat faaliyetleri sadece devlet kurumları arasında değil, ticari sırların çalınması amacıyla özel şirketler arasında da gerçekleşmektedir. ABD istihbarat yetkilileri, 2009 yılında ABD firmalarının yaklaşık 50 milyar dolar değerinde fikrî mülkiyet hırsızlığına maruz kaldığını iddia etmektedir (Robinson, 2012). Bunun gibi siber casusluk operasyonlarının hedefi olmamak için karşı istihbarat faaliyetleri önem arz etmektedir. Dolayısıyla, ulusal siber güvenliğin temellerinden birisi siber alanda

istihbarat operasyonları yapabilme ve bu tür operasyonlara karşı koyabilme becerisidir.

Dördüncü alan siber güvenlik kriz yönetimi ve kritik altyapıların korunmasıdır. Kriz yönetimi becerileri siber saldırılara maruz kaldıktan sonra hasar tespiti, saldırılara karşılık verme, gerekli noktalara acil müdahale ve hasar gören sistemlerin tekrar ayağa kaldırılması gibi kritik fonksiyonlar ihtiva etmektedir. Bu vazifeler genellikle ulusal CERT (Computer Emergency Response Team) birimlerince ifa edilmektedirler. CERT birimlerinin gelişen tehditlere yönelik olarak eğitimli olmaları ve güvenlik birimleriyle işbirliği yapmaları önemlidir. Kritik altyapıların korunması öncelikli olarak ulusal çapta bir risk analizinin yapılarak, risk faktörlerinin düzenli olarak güncellenmesini gerektirmektedir. İkinci olarak kritik altyapılara yönelik standartlar geliştirilerek gerekirse kanunlar aracılığıyla özel ve kamuya ait kritik altyapıların bu standartlara kavuşturulması gerekmektedir.

Beşinci ve son alan siber diplomasi ve internetin yönetimidir. Önceki bölümlerde belirtildiği gibi uluslararası hukukta siber alana özgü bağlayıcı nitelikte bir metin bulunmamaktadır. Siber alan yeni yeni şekillenmekte olduğundan, özellikle güçlü devletler bu yeni alana ilişkin kuralların kendi ulusal çıkarlarıyla paralel olması için sürekli girişimlerde bulunmaktadırlar. Bu sebeple, ulusal menfaatlere ters bir takım gelişmelerin yaşanmaması için siber diplomasiye önem verilmelidir. Diğer bir konuysa internet ve internete yön veren politika ve standartlardır. İnternet, kuruluşundan bu yana herhangi bir devletin veya özel kuruluşun doğrudan etkisi altına girmemiştir. Merkezi bir yapının olmayışı her türlü fikrin özgürce ifade edildiği bir ortamın oluşmasına katkı sağlamakla birlikte, internetin güvenliğini olumsuz yönde etkilemektedir. İnterneti daha güvenilir bir hâle getirmek içinse şirketler ve bağımsız kuruluşlarca güvenli iletişim protokollerinin ve standart işlemlerin geliştirilmesi yönünde çalışmalar yapılmaktadır. Bu çalışmalar internetin geleceğinin şekillenmesinde etkili olabileceğinden, ulusal güvenlik açısından bu çalışmalara katkı yapmak ve gelişmelerin dışında kalmamak gerekmektedir.

Ülkemizde siber güvenlik stratejisi çalışmalarının çok fazla bir geçmişi bulunmamaktadır. Siber güvenliğin tesisi açısından göze çarpan önemli faaliyetlerin başında bu alanı düzenleyen bazı kanunların kabulü gelmektedir. 2004 yılında kabul edilen 5070 sayılı Elektronik İmza Kanunu, 2008 yılında kabul edilen haberleşme sektörünü düzenlemeyi hedefleyen Elektronik Haberleşme Güvenliği Yönetmeliği bunlardan ilklerindendir (Ünver ve Canbay, 2010). Bunların yanında 2006 yılında 28242 sayılı Resmi Gazete'de yayınlanan 2006/38 sayılı Yüksek Planlama Kurulu Kararında bulunan Bilgi Toplumu Stratejisi ve Eki Eylem Planında "Güvenlik ve Kişisel Bilgilerin Mahremiyeti" başlığı altında iki eylem sayılmıştır. Bunların ilki, bilgi güvenliğine ilişkin yasal düzenlemelerin yapılmasını; ikincisi, bilgisayar olaylarına acil müdahale merkezinin kurulmasını ve kamu kurumlarının bilişim güvenliğinin sağlanmasına yönelik faaliyetleri planlamaktadır. Bu kapsamda, yukarıda CERT olarak anılan yapıya eşdeğer, Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME), TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde kurulmuş ve faaliyete geçirilmiştir.

Siber güvenliğe ilişkin olarak makro planda atılmış en somut adım 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" başlıklı Bakanlar Kurulu Kararıyla gerçekleşmiştir. Kararın kamuoyunda en çok konuşulan hükmü "siber güvenlikle ilgili alınacak kararları belirlemek, hazırlanan

plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla" bir Siber Güvenlik Kurulu'nun kurulması olmuştur. Kurul Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarlığı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır. Kurulun ilk toplantısı 24 Aralık 2012'de yapılmıştır.

Bunun yanında kararda, ulusal siber güvenliğin sağlanması için politika, strateji ve eylem planlarının hazırlanması görevinin Ulaştırma Bakanlığına verildiği belirtilmiştir. Bu madde uyarınca Ulaştırma Bakanlığı, ilgili kurum ve kuruluşların da görüşünü alarak bir siber güvenlik eylem planı hazırlamıştır. Ancak eylem planı bu makalenin kaleme alındığı tarihte henüz kamuoyuyla paylaşılmamıştır. Siber güvenliğe ilişkin önemli hususları içerdiği belirtilen eylem planının uygulamaya geçirilebilmesi durumunda bu alanda önemli bir mesafenin alınacağı yetkililerce ifade edilmektedir.

Yukarıda anılan Bakanlar Kurulu Kararında; Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilen görevler arasında "ulusal bilgi teknolojileri ve iletişim altyapısı ve sistemleri ile veritabanlarının güvenliğini sağlamaya, kritik altyapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik" çalışmalar yapmak sayılmaktadır. Bu kapsamda Telekomünikasyon İletişim Başkanlığı bünyesinde, Ulusal Siber Olay Merkezi (USOM) adı verilen bir yapının oluşturulmasına eylem planında yer verilmiş ve hazırlıklarına başlanılmıştır. USOM'un görev ve sorumluluklarına ilişkin detaylar henüz mevcut olmayıp, Merkezin siber güvenliğe ilişkin olaylarda daha çok ulusal koordinasyon ve uluslararası işbirliği birimi olarak faaliyet göstereceği, ilerleyen zamanlarda kurulacak Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleriyle (SOME) bir arada siber güvenliğin sağlanmasına yönelik faaliyetler yürüteceği belirtilmektedir (Korkmazer, 2013).

## Sonuç ve Öneriler

Ülke olarak bilişim altyapılarına ve internete olan bağımlılığımız artmakta ve buna bağlı olarak siber alanda taşıdığımız risklerimiz de giderek büyümektedir. Siber tehdidi doğru ölçebilmek ve strateji geliştirebilmek için öncelikle gözlem, takip, analiz ve tahmin kapasitesi olan birimlere ihtiyaç vardır. Siber güvenliğin sadece internet güvenliğini değil tüm iletişim altyapılarını kapsayan geniş bir kavram olması nedeniyle sonraki adım olarak çok sektörlü bir yaklaşımla ulusal siber güvenlik politikasının belirlenmesi gerekmektedir. Ülkemizin ciddi bir siber saldırıya maruz kalmamasını, terör örgütlerinin bu potansiyellerinin olmadığı şeklinde değerlendirmek yanlış olacaktır. Bu yüzden pasif savunma alanında yapılanların yanında aktif savunmaya da yönelik tedbirler alınmalıdır. Siber güvenlik alanında tedbirler geliştirirken güvenlik-demokrasi, fayda-maliyet dengelerinin gözetilmesi gerektiği gözden kaçırılmamalıdır.

Siber suçlarla mücadeleye yönelik hukuki altyapımız pek çok ülkeyle kıyaslandığında

gelişmiş gözükse de, önceki bölümlerde değinildiği gibi bir takım önemli eksiklikleri bulunmaktadır. Bu sebeple TCK ve CMK'da, siber suçlarla daha etkin mücadeleye imkân verecek düzenlemelerin yapılması gerekmektedir. Bu konuda önemli bir eksik de siber teröre ilişkin ilgili mevzuatta bir tanımın yapılmamış olmasıdır. Siber terörle hukuk devleti çerçevesinde mücadele edebilmek için kavramın tanımının yapılması ve bu tür faaliyetlere yönelik yaptırımların belirlenmesi gerekmektedir. Mevzuat açısından diğer bir önemli eksik kişisel verilerin korunmasına yönelik kapsamlı bir kanun olmayışıdır. Bilişim teknolojilerinin ve internetin yaygınlaşmasıyla eskisine göre daha fazla risk altında bulunan kişisel verilerin korunmasına ilişkin olarak hazırlanan ve TBMM'de bekleyen yasanın bir an önce gündeme getirilmesi gerekmektedir. Bütün bu konuların tartışılması ve işbirliği mekanizmalarının geliştirilmesi için Ulaştırma, Denizcilik ve Haberleşme, Adalet, Dışişleri ve İçişleri Bakanlıklarının ortak çalışmalar yürütmeleri isabetli olacaktır.

İnsan unsuru, güvenlikle alakalı pek çok alanda olduğu gibi siber güvenlikte de en önemli etken olarak karşımıza çıkmaktadır. Bir sistemde ne kadar güvenlik tedbiri alınmış olursa olsun, dikkatsiz bir kullanıcının sebep olacağı açıklara mağlup olma riski her zaman vardır. Dimensional Research firmasının 2011 yılında yaptığı sosyal mühendislik saldırılarına ilişkin çalışmaya göre ankete katılan bilişim uzmanlarının %43'ü işletmelerinin sosyal mühendislik saldırısına maruz kaldığını, %48'i her bir sosyal mühendislik saldırısının kendilerine ortalama 25 bin dolara mal olduğunu belirtmişlerdir. Sosyal mühendislik gibi insan temelli saldırıların riskini azaltmak için çalışanların siber güvenliğe ilişkin konularda eğitilmeleri ve bilinçlendirilmeleri gerekmektedir.

Kurumsal olarak alınacak ufak tedbirler, ulusal siber güvenliğe önemli katkılar yapabilecek niteliktedir. Bu tedbirlerden birisi kamu ve özel kurumlarda başlatılan bilişim projelerine güvenlik ayağının eklenmesidir. Güvenliğin geri planda bırakıldığı bir sistemin sonradan güvenli hale getirilmesi daha zor olacak ve istenilen ölçüde gerçekleştirilemeyecektir. Buna ilaveten, kurumların gerek normal kullanıcıları gerekse bilgi-işlem personeli için standart çalışma politikaları belirlemeleri ve bu standartların uygulanmasını denetlemeleri sistemlerin güvenliğine yönelik tehditlerin önemli bir kısmını ortadan kaldıracaktır. Denetimlerin düzenli olarak yapılabilmesi için kurumlarda bir iç denetim mekanizması kurulabilir ve bu yolla siber güvenlik bilinci artırılabilir. Kurumların ayrıca iç denetim birimlerince yahut bağımsız kuruluşlarca yapılacak bir risk analizi çalışmasıyla sistemlerinin ne kadar güvenli olduğu, herhangi bir saldırı durumunda hizmetlerin ne kadarının aksayacağı ve saldırıya uğramış bir sistemin ne kadar zamanda toparlanabileceği gibi hususları belirleyip bunlara ilişkin tedbirleri almaları isabetli olacaktır. Hepsinden önce özellikle kamuda ve kritik sektörlerde kullanılan donanım ve yazılımların test edilmiş ve güvenlik açıkları kapatılmış olmaları gerekmektedir. Zira sistemlerin temel öğesi olan donanım ve yazılımlarda olabilecek açıklar, alınacak tedbirleri baştan işlevsiz hâle getirecektir.

Kurumsal olarak öneme sahip diğer bir husus kurumlar arası işbirliğidir. Özellikle siber güvenlikten sorumlu kurumlar arasında hızlı bilgi paylaşımı sağlanması ve işbirliktelikleri bu kurumların etkinliğine olumlu etki edecektir. Sadece kamu kurumları arasındaki bilgi paylaşımı ve işbirliği değil, kamu ve özel sektör arasında da bilgi paylaşımı ve işbirliği mekanizmalarının kurulması oldukça önemlidir. Bu türlü bir beraberlik kamu için özellikle faydalı olacaktır çünkü kamuya ait bilişim sistemlerinin önemli bir kısmı özel sektörce işletilmektedir. Bu yüzden

özel sektöre ait bilişim altyapılarına siber güvenliğe ilişkin belli standartların kazandırılması hedeflenmelidir.

## Kaynakça


Akamai (2012). *The state of the internet.* Erişim tarihi: 20.04.2013, http://www.akamai.com/stateoftheinternet/

Akdoğan, H. (2005). Çocuğun cinsel istismarı ve Türkiye'de çocuk cinsel istismarını önlemeye yönelik çalışmalar. *Polis Bilimleri Dergisi, 7*(1), 1-15.

Ballard, J. D., Hornik, J. G., &McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal and policy issues. *American Behavioral Scientist*, *45*(6), 989-1016.

Chen, T. ve Walsh, P. J. (2009). Guarding against network intrusions. Vacca, J. R. (Ed.) *Computer and Information Security Handbook* (ss. 53-66). Morgan Kaufmann Publishers

Dimensional Research (2011). *The risk of social engineering on information security: A survey of IT professionals*. Erişim tarihi: 16.04.2013, http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf

Easttom, C. ve Taylor, J. (2011). *Computer crime investigation and the law*. Course Technology.

Goodrich, M. ve Tamassio, R. (2010). *Introduction to computer security*. Addison-Wesley.

Host Exploit (2013). *World hosts report*. Erişim tarihi: 23.04.2013, http:// www.hostexploit.com

Identity Theft Resource Center (2012). *Knowing less and less about less and less*. 23.04.2013, http://www.idtheftcenter.org/artman2/publish/m_press/Breaches_2012_First_Half.shtml

Inernational Centre for Missing and Exploited Children (2008). Çocuk pornografisi: Mevzuat modeli ve *global inceleme*. 15.02.2013, http://polis.osce.org/library/f/3648/2806/GOV-USA-RPT-3648-TR-2806

Internet Crime Complaint Service (2011). *2011 internet crime complaint report*. Erişim tarihi: 17.03.2013, https://www.ic3.gov/media/annualreport/2011_IC3Report.pdf

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars: Rebels with a Cause?*. Routledge.

Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı (2011). *Kaçakçılık ve Organize Suçlarla Mücadele 2011 Raporu.* Erişim tarihi: 13.04.2013, http://www.kom.pol.tr/Documents/Raporlar/ 2011tur.pdf

Karagülmez, A. (2011). *Bilişim suçları ve soruşturma-kovuşturma evreleri*, Seçkin.

Kleiner, A., Nicholas, P. and Sullivan, K. (2013). *Linking cybersecurity policy and performance, Microsoft Corporation, Measuring the Impact of Policy on Global Cybersecurity.* Erişim tarihi: 03.04.2013, http://www.microsoft.com/en-us/download/details.aspx?id=36523

Klimburg, A. (2012). *National cyber security framework manua*l. NATO CCD COE

Publication,Tallinn. Erişim tarihi: 03.04.2013, http://www.ccdcoe.org/369.html

Korkmazer, S. (2013). *Siber güvenlikte USOM'un rolü*. Siber Güvenlik ve Siber Terörizm Çalıştayı, 26-27 Şubat 2013, UTSAM, Polis Akademisi Başkanlığı.

Microsoft (2012). *Microsoft security intelligence repor.* Erişim tarihi: 27.04.2013, http://www.microsoft.com/sir

Mobbs, B. (2003). *Computer crime the law on the misuse of computers and networks*. http://www.internetrights.org.uk/briefings/irtb08-rev1-draft.pdf

OECD (2012). *Improving the evidence base for information security and privacy policies: Understanding the opportunities and challenges related to measuring information security, privacy and the protection of children online*. OECD Digital Economy Papers, No. 214, OECD Publishing.

Robinson, J. (2012). McAfee explains the dubious math behind its 'unscientific' $1 trillion data loss claim. *Forbes*, Erişim tarihi: 24.03.2013, http://www.forbes.com/sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim/

Seigfried-Spellar, K.C., Lovely, R. W. ve Rogers, M. K. (2011). Self-Reported internet child pornography consumers: A personality assessment using Bandura's theory of reciprocal determinism. Jaishankar, K. (Ed.) *Cyber criminology exploring* ınternet *crimes and criminal behavior* (ss. 65-78), CRC Press.

Sullivan, B. (2003). Nigerian scam continues to thrive. *NBC New*s. Erişim tarihi: 24.04.2013, http://www.nbcnews.com/id/3078489/#.UVlaQje14dU

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy* ıssues *for congress.* CRS Report for Congress.