Kritik Altyapılara Yönelik Bilişim Suçları; Türkiye ve AB Uygulamaları

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Muhammet Karaca

tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Ensar Gül .....
(Tez Danışmanı)

Dr. Öğretim Üyesi Hüseyin Yüce .....

Dr. Öğretim Üyesi Ahmet Bülter .....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 30. 10. 2019

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Muhammet KARACA, başlığı, 'Kritik Altyapılara Yönelik Bilişim Suçları; Türkiye ve AB Uygulamaları ' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: 30.10.2019

Tarih:

Kritik Altyapılara Yönelik Bilişim Suçları; Türkiye ve AB Uygulamaları

Muhammet Karaca

Öz

Kritik altyapı, işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar olarak ifade edilmektedir. Teknolojik gelişmeler birçok bakımdan büyük kolaylıklar sağlasa da, çe- şitli güvenlik sorunlarını da beraberinde getirmektedir. Bualanda işlenen suçların gün geçtikçe artması, devletler bünyesinde yankı uyandırmakta ve güvenlik önlemlerinin ar- tırılması gerektiğini ortaya koymaktadır. Türk Ceza Kanunu'nda, Avrupa Siber Suçlar Sözleşmesi'nde ve farklı devletlerde bu alanda farklı uygulamalar da dikkat çekmekte- dir. Makalede, öncelikle bilişim alanında işlenen suçlar belirtilmiş ve açıklanmıştır. Daha sonra, kritik altyapılar belirtilerek, bu alanda yapılan siber saldırılardan bahsedilmiş- tir. Bu saldırılara karşı yapılan çalışmalardan ve alınan tedbirlerden bahsedilerek gerekli önerilerde bulunulmuş ve sonuçlar değerlendirilmiştir.

Anahtar Sözcükler: Kritik Altyapılar, Bilişim, Siber Saldırı, Güvenlik, Hukuk.

Critical Information Infrastructure For Crimes; Turkey and Eu Practices

Muhammet Karaca

Abstract

Critical infrastructures are defined which cause loss of lives, large scaled-economical damage, national security flaw or public order break down when their info / data confidentiality, integrity or accessibility is broken. Technological developments provide us many huge conveniences but also bring along various security problems. The rise of counts of the cyber-crimes is creating reactions amongst countries and revealing the need of precaution increases. In Turkish Criminal Law, European Cyber-Crimes Contract and some different countries have different executions and practices in that field. In this article, cyber-crimes are defined and explained. After that, critical infrastructures and cyber attacks in this area were mentioned. The studies and the measures taken against these attacks were mentioned and the necessary suggestions were made and the results were evaluated.

Keywords: Critical Infrastructures, IT, Cyber Attack, Safety, Law.

Teşekkür

Yüksek Lisans eğitimim boyunca ve tezimin hazırlanmasında çok değerli yardımlarını gördüğüm tez danışmanım Sayın Prof. Dr. Ensar Gül'e değerli katkılarından dolayı sonsuz şükranlarımı sunuyorum.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

AFAD	**Afet ve Acil Durum Yönetim Başkanlığı**
AİHM	**Avrupa İnsan Hakları Mahkemesi**
BDDK	**Bankacılık Düzenleme Ve Denetleme Kurumu**
BİLGEM	**Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi**
BTK	**Bilgi Teknolojileri Veİletişim Kurumu**
BM	**Birleşmiş Milletler**
CSİ	**Computer Security İnstitute**
DNS	**Domain Name System**
DPT	**Devlet PlanlamaTeşkilatı**
EGM	**Emniyet Genel Müdürlüğü**
EİK	**Elektronik İmza Kanunu**
ENISA	**European Union Agencyfor Cybersecurity**
FSEK	**Fikir ve Sanat Kanunu**
FTP	**File Transfer Protokol HTTP**
	Hypertext Transfer Protokol
İP	**İnternet Protokol**
İTU	**Uluslararası Telekomünikasyon Birliği**
MİT	**Milli İstihbarat Teşkilatı**
ODTÜ	**Orta Doğu Teknik Üniversitesi**
OECD	**Ekonomik Kalkınma ve İşbirliği Örgütü**
PİN	**Personel İdentification Number**
RİPE NCC	**Reseux İp Europens Network Coordination Center**
SGE	**Siber Güvenlik Enstitüsü**
SMTP	**Simple Mail Transfer Protokol**
SOME	**Siber Olaylara Müdahale Merkezi**

SPAM	**Spiced Park And Ham**
TBMM	**Türkiye Büyük Millet Meclisi**
TİB	**Telekomünikasyon İletişim Başkanlığı**
TBB	**Türkiye Barolar Birliği**
TCK	**Türk Ceza Kanunu**
TRİPS	**Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme**
TR-BOME	**Türkiye Bilgisayar Olayları Müdahale Ekibi**
TSK	**Türk Silahlı Kuvvetleri**
TÜBİTAK	**Türkiye Bilimsel ve Teknolojik Araştırma Kurumu**
UDHB	**Ulaştırma, Denizcilik Ve Haberleşme Bakanlığı**
USOM	**Ulusal Siber Olaylara Müdahale Merkezi**
WWW	**World Wide Web**

Bölüm 1

Giriş

Bilişim sistemlerinin gün geçtikçe gelişmesi ve değişmesi, farklı şekillerde işlenen bilişim suç fiillerinin de artmasına neden olmaktadır. Her ne kadar teknoloji büyük bir kolaylık sunsa da, hukuka aykırı olarak bu teknolojinin kullanıldığına ve siber saldırıların artarak devam ettiğine her geçen gün şahit olunmaktadır. Bu konu ile ilgili olarak hem Türk Ceza Kanunu'nda hem de Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi'nde önemli bir yer ayrılmıştır.

765 sayılı Türk Ceza Kanunu'nda(mülga), bilişim suçlarına yönelik hükümlerin oldukça kısıtlı olması, 5237 sayılı yeni yasanın yürürlüğe girmesi ile genişletilmiş ve kapsamı da artırılmıştır. Bu bağlamda hem bilişim sistemleri ile işlenen suçlar hem de bilişim sistemlerinekarşıişlenensuçlar, TCK'ninilgili maddelerindeyerini almıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesi'de küreselleşmenin kaçınılmaz bir sonucu olan bilişim suçlarının da küreselleşmesi sorununa bir çözüm üretilebilmesi için ortaya konmuş, birçok ülke tarafından kabul gören ve imzalanan bir sözleşme olmuştur. Bugün bu sözleşme kapsamında birçok bilişim suçu ile ilgili hükme yer verilmektedir. Avrupa Birliği'ne üye ülkeler ve ülkemizde bilişim suçlarının ceza hukukundaki karşılıklarının bilinmesi oldukça önemlidir. Bu nedenle hem Türk Ceza Hukuku hem de Avrupa Konseyi Siber Suçlar Sözleşmesi ile ilgili bilişim suçlarının yaptırımları irdelenmeli ve detaylı olarak ele alınarak karşılaştırılmalıdır.

Çalışmamızda, bilişimteknolojilerinin kullanılarakişlenebilecek suçları, ülkemizvedünyamız açısından kritik sayılan altyapıların siber saldırılara karşı korunmasına yönelik çalışmaları ve yine bualtyapılara yapılan saldırılar işlenerekalınacaktedbirler hakkında 1

bahsedilmiştir. Türk Ceza Kanunu, bunun yanı sıra Avrupa Konseyi Siber Suçlar Sözleşmesi'nin ve farklı ülkelerde bilişim suçlarına yönelik ceza hükümleri yahut yaptırımlar ile ilgili detaylı bir ilerleme söz konusudur. Yeri geldikçe tüm kanunların konumuz ile ilgili maddeleri açıklanmış ve yorumlanmıştır. Kritik Altyapı Sistemlerine ilgilendiren bilişim suçlarına karşı yeni öneriler yapılmıştır.

Bölüm 2

Bilişim Suçları Kavramsal Çerçeve

Bilişim suçlarının Ceza Hukukunda yer alış şekillerinin inceleneceği bu çalışmada öncelikle bilişim terminolojisinde yer alan kavramların kısa da olsa açıklanmasının gerekli olduğu değerlendirilmektedir. Bu sebeple çalışmanın başlangıcında bilişim alanında öne çıkan kavramlara dair açıklayıcı bilgilere yer verilmiştir.

2.1 Donanım

Donanım terimi, bilgisayarların tüm parça ve aksesuarlarını ifade eder [1]. Bilgisayarın monitör, klavye, ROM, RAM, mikro işlemciler gibi ekipmanları donanım olarak kabul edilmektedir.

- **Çevre Giriş - Çıkış Birimleri:** Verilerin bilgisayarda bir işleme tabi tutulmadan önce bilgisayara aktarılması gerekmektedir. Bunu sağlayan bilgisayar birimlerine, giriş birimleri adı verilmektedir. Bilgisayara aktarılan verilerin kullanıcıların anlayabileceği ve kullanabileceği hale dönüştürülmesini sağlayan birimlere ise çıkış birimleri adı verilmektedir. Yazıcı, klavye, ekran vb. donanımları bilgisayarın giriş-çıkış birimlerine örnek olarak göstermek mümkündür.
- **RAM(Random Access Memory):** Geçici bellek olarak da ifade edilmektedir. Bilgisayara gelen güç kapatıldığında buraya yapılan kayıtlar silinmekte ve depolama yapılmamaktadır.

- **ROM(Read-Only Memory):** Kullanıcı tarafından müdahale edilemeyen salt okunur bellektir. Bilgisayarın bu bölümüne herhangi bir kayıt yapılması söz konusu değildir. ROM, bilgisayara gelen güç devamlılığından bağımsız olarak çalışmaktadır. Güç kesintisinde etkilenmemektedir.
- **Sistem Yazılımı:** Bilgisayarların işlevlerini yerine getirebilmeleri için gerekli olan yazılımlarıdır. Bilgisayarlarda hazır olarak yer alan ve belirli kodlardan oluşan yazılım bütünüdür.
- **Mikro İşlemci:** Bir nevi bilgisayarın beynidir. Daha önce açıklanan bilgisayar donanımlarından olan "giriş birimleri" aracılığıyla ulaşan verilerin gereğini yapmaktadır.
- **Uygulama Yazılımları:** Bilgisayarlarda kurulu işletim sistemlerine entegre olarak yüklenen programlardır. Temel amaçları bilgisayarla belirli işlevleri yerine getirebilmeye yarayan paket programları kullanabilmektir.

2.2 Veri

Bilgilerin, bilgisayar tarafından kullanılabilecek belirli bir formata dönüştürülmüş haline verilen addır [2]. Bilgisayar terminolojisine göre işlenmeye hazır haldeki tüm bilgileri kapsayan bir terimdir.

2.3 Program

İstenilen sonuçları elde edebilmek için bilgisayar tarafından kullanılan bir çeşit talimat şeklidir [3]. Programlar sayesinde elde bulunan veriler anlamlı bir hale getirilebilmekte ve ihtiyaca göre dizayn edilebilmektedir.

2.4 İnternet

Çok sayıda haberleşme ağından müteşekkil bir bilgi ağıdır. Tüm dünyada geçerli olan TCP/IP protokolüvasıtasıyla dünya genelinde bir bütün olarak işlev gören bilişim ağıdır

[4]. TCP/IP protokolü, dünyanın herhangi iki yerindeki bilgisayarın ya da yerel ağın birbirleriyle iletişimlerini sağlayan ortak bir dildir [5].

İnternet ağı üzerindeki iletişim ve bilgilerin paylaşımı belirli kurallar çerçevesinde gerçekleşmektedir. Bahse konu kurallara genel olarak "internet protokolleri" adı verilmektedir. Bunlardan TCP terimi; bilginin iletimi protokolü iken; IP terimi, temel olarak internet protokolünün adıdır. İnternet vasıtasıyla yapılan hemen her işlem belirli süreçlere ve kurallara bağlıdır. Bu kuralların genel çerçevesi ise, protokoller ile çizilmektedir. Bahse konu protokollerden öne çıkan bazılarını örnek vermek gerekirse;

FTP (File Transfer Protokol), internet kullanılarak dosya gönderimi ve dosya alımı işlemlerini düzenlemektedir. SMTP (Simple Mail Transfer Protokol), e-posta iletimlerine ilişkin düzenlemeleri içeren protokoldür. TELNET protokol, Bir bilgisayarın internet aracılığıyla ağdaki diğer bilgisayarlarla etkileşimli olarak ortak çalışmalar yapabilmesi işlemlerini düzenleyen protokoldür. HTTP (HyperText TransferProtokol) ise, www (World wide web) ortamında birbirleriyle bağlantılı olan farklı cinslerdeki verilerin iletimi husus-larını düzenlemektedir [6].

İnternet ağına bağlanan her cihaz bir IP adresine ihtiyaç duyar. IP adresi internete bağlı olan cihazların birbirlerine veri (bilgi) göndermek için kullandığı adres olarak tanımlanabilir. Bu adreslerin her biri 4'erli 8 grup şeklindedir. İlk olarak 1980'lerde IPv4 olarak kullanıma başlayıp bugün IPv6 sürümü kullanılmaya başlanmıştır. Çünkü IPv4 32 bitlik bir adres yapısına sahiptir. Bu yapı artık yetersiz kaldığı için 128 bitlik geniş bir adres yapısına sahip IPv6 sürümü kullanılmaya başlanmıştır. IPv6 teknolojisini dünyada ilk kez 1999 yılında Çin'de kullanılmaya başlandı. Türkiye de IPv6 kullanımının yaygınlaştırılması ULAKBİM tarafından 2003 yılı başlarında Avrupa bölgesel IP adresi dağıtım sorumlusu kurumundan 2001:a98::/32 IPv6 adres aralığının temini ile başlamıştır. 8 Aralık 2010 tarih ve 27779 sayılı genelge "Kamu Kurum ve Kuruluşları için IPv6'ya Geçiş Planı" başlığı ile resmi gazetede yayınlanarak kamu kurum ve kuruluşlarının IPv6'ya ge- çiş süreci planlanmıştır [7]. IPv6 kullanımı; Türkiye de, Ocak 2011 de %1.56 - Haziran 2019 itibariyle %15.66, OECD ülkelerinde ise %26.60 ve AB ülkelerinde ise %33.77 olarak tespit edilmiştir [8]. Oranlar bazında bakıldığı zaman 2011 yılından bu zamana Türkiye de IPv6 kullanımı artarak yükselmiş lakin OECD ve AB ülkelerinin gerisinde kalmıştır.

İnternette arama yaparken adres çubuğuna yazılan site ismini, gidilmek istenen sitenin gerçekte bulunduğu IP adresine çeviren sisteme, "Domain Name System (DNS)" olarak

adlandırılmaktadır. İnternet adresinin ilk kısmı bulunduğu domainin ağ adresini son bölümü ise "host" numarasını vermek üzere ikiye ayrılmaktadır. İnternete bağlı olan bir bilgisayarın ağa bağlı olduğu anda aldığı bir adresi bulunmaktadır. Söz konusu adres, aynı bilgisayarın her internet bağlantısında değişim göstermektedir. Sizin bilgisayarınıza tanımlanmış olan bir IP adresinin sürekli olarak kullanımı durumuna ise statik IP adı verilmektedir [9].

Tüm dünyada ortak bir uygulama olarak kullanılan alan adlarındaki uzantılar şu şekildedir;

- ac: Akademik kuruluşlar,
- com: Ticari kuruluşlar,
- org: Sivil toplum kuruluşları,
- edu: Eğitim kuruluşları,
- int: Uluslararası kuruluşlar,
- gov: Devlet kuruluşları,
- mil: Askeri kuruluşlar,
- net: Kendi özel ağları olan kuruluşlardır.

Ülkemizde internet bağlantısının yapıldığı ilk tarih 1993'tür. İlk internet bağlantısı; ODTÜ tarafından ortak bir projeyle gerçekleştirilmiştir. Türkiye'de alan adı ve IP no dağıtımları TTnet, ODTÜ ve ULAKNET aracılığıyla gerçekleştirilmiştir.ODTÜ'nün ".tr alan adları yönetimi yetkileri" BTK'ya devredildi. Bu devir, 05.11.2008 tarihli 5809 sayılı Elektronik Haberleşme Kanunu ile verilen göreve dayanılarak, Ulaştırma ve Altyapı Bakanlığı'nın, internet adreslerinin tahsisine ilişkin işlerin ve işlemlerin yürütülmesi görevini BTK'ya vermesi ve 2010 tarihli İnternet Alan Adları Yönetmeliği doğrultusunda başlatılmıştır.

ODTÜ ve BTK tarafından üzerinde uzlaşılmış ilkeler kapsamında, kurulacak ".tr" ağ bilgi sisteminin (TRABİS) faaliyete geçmesi için gerekli çalışmalar 2016 yılında başlatılmıştır. Nihayetinde 3 Mayıs 2019 tarihinde resmen BTK'ya devredildi. Bu dağıtımlar Avrupa'da ise, yerel internet kayıt merkezleri (Local Internet Registries) vasıtasıyla yapılmaktadır. Amerika'da IP numarası dağıtımı konusundaki yetki ise, RIPE NCC (Ripe Network Coordination Center) kuruluşunda bulunmaktadır [10].

2.5 Bilişim Kavramı

Bilişim kavramı, TDK sözlüğünde, bilimin kaynağı olan bilginin özellikle elektronik araçlar yardımıyla sürekli bir şekilde işlenmesi bilimi olarak ifade edilmektedir [10]. Bilişim kavramı köken itibariyle Fransızca "informatique" kelimesinden doğmuştur. Dilimize ilk olarak enformasyon olarak dâhil olan bu kavram, sonradan bilişim olarak ifade edilmeye başlanmıştır.

Bilişim, esasen paylaşmak manası da gelmektedir. İnternet aracılığıyla herhangi bir yerden yüklenen veriye başkalarının da çok rahat bir şekilde erişebildiği uçsuz bucaksız bir alanı temsil eden, kişilerin ihtiyaçlarına göre yazılımlar ve bilgisayarların tasarımlandığı bir ortamdır [12].

Sonuç olarak bilişimi; verilerin toplanıp, işlenip, değerlendirilerek tekrar dağıtımını sağlayan bir bilim dalı olarak ifade etmek mümkündür.

2.6 Bilişim Suçu Kavramı

Bilişim Suçu, TCK 5237 sayılı kanunun 10. bölümünde, "Bilişim Alanında Suçlar" başlığı altında düzenlenmiştir. Bilişim suçu temel olarak, bilgi işlem kayıtlarına yasadışı şekilde ulaşarak amacı dışında kullanılmalarını sağlamaktır. Bahse konu kayıtların yasadışı yollardan değiştirilmesi, silinmesi vb. eylemler olup literatürde "bilgi tecavüzü" olarak ifade edilen her türlü eylemin yapılmasıdır [13].

Bilişim suçlarının genel çerçevesi yukarıdaki şekilde çizilse de konuyla ilgili literatürde bir görüş birliğinden söz edilmesi güçtür. Başka bir deyişle bilişim suçları kavramının tanımı konusunda tüm araştırmalarca kabul edilmiş bir tanımlama bulunmamaktadır. Literatürde öne çıkan çalışmalardan Dülger tarafından yapılan çalışmada bilişim suçları; bilişim sistemlerinin kullanılarak verilerle bağlantılı olan sistemlere izinsiz erişim durumu olarak tanımlanmaktadır [14].

Bilişimsuçu kavramınınsınırlarınıçizenaraştırmalararasındaöne çıkanbir diğerçalışma da Avrupa EkonomikTopluğuUzmanlar Komisyonu'nca 1983 yılındayapılan Paris top- lantısı sırasında belirlenen ilkeler olmuştur.(Avrupa Ekonomik Topluğu'nun ismi 1992

yılında Avrupa Birliği olarak değiştirilmiştir).Bu toplantıda belirlenen ilkelere göre bilişim suçu, çeşitli verilere ulaşım imkânı olan sistemlere yasadışı şekilde, gayri ahlaki eylemlerle ve yetkisiz olarak erişim imkânı sağlayan her türlü girişime verilen addır [14]. Avrupa Ekonomik Topluluğu tarafından yapılan toplantı sonrası alınan kararlara göre bilişim suçları beş ayrı gruba bölünmüştür. Bunlar [16].

- Bir bilgisayarda yer alan veriye ulaşabilmek amacıyla, yetkisiz şekilde gayri meşru yollar kullanılması işlemidir. Bu verilere erişilmesi, transferinin sağlanması, verilerin karıştırılması, silinmesi veya üzerinde herhangi bir oynama yapılması gibi tüm işlemler bir çeşit bilişim suçu türüdür.
- Sahtekârlık amacıyla bilgisayar veri ve programlarına erişerek ekleme ve silme de dâhilhertürlüişleminizinsiz olarak yapılmasıdır.
- Bilgisayar sistemlerinin çalışmasını engelleyebilmek amacıyla çeşitli müdahaleler yapılmasıdır.
- Ticari bir menfaat sağlamak amacıyla bilgisayar programlarına erişerek üçüncü kişilerin zarara uğramasına neden olmaktır.
- Bilgisayar sisteminden sorumlu kişi ya da kişilerden izin almadan güvenlik tedbirlerini aşarak erişim hakkı bulunmayan bölümlere ve sistemlere kasten müdahalede bulunmaktır.

Bilişim suçları her geçen gün yeni bir faaliyet alanında yer bulabilmektedir. Gittikçe yaygınlaşan bu suç türü, teknolojinin ve özellikle internetin yaygınlaşması ile alan kazanmaktadır. Özellikle bu suçların çoğunluğu toplum mühendisliği şeklinde kullanılan metodlardan yararlanılarak yapılmaktadır. Bilişim suçlarının bilinen ilk örneği 1960'lı yıllarda yaşanmıştır. Bu alanda kaydedilmiş ilk suç ise, 1966 yılında Minneapolis Tribune'de de yayımlanan ve bir bilgisayar uzmanının banka hesaplarına yetkisiz erişim sağlaması olayı olarak tarihe geçmiştir [17].

2.6.1 5237 Sayılı TCK'da Bilişim Suçları

TCK 5237 sayılı kanununda, bilişim suçları toplu bir şekilde belirtilerek 243-245. Maddeler arasında açıklanmıştır. Buna göre bilişim suçları;

- **Bilişim Sistemine Girme (m.243)**

  Bilişim suçları içinde en rahat işlenen ve en çok karşılaşılan bu durumdur. Saldırgan ya doğrudan fiziki yakınlıkla sisteme erişim sağlamaya çalışır ya da uzaktan erişim metoduyla sisteme girmeye çalışır. Örneğin, kişilerin sanal hesaplarına (instagram, twitter, e-mail vb.) kişiden izinsiz bir şekilde şifre kırarak ya da güvenlik önlemlerini devre dışı bırakarak girmeye çalışmak. Kişiler sanal hesaplarda hangi bilgilerinin görülebilir ve erişime açık olduğunu kendileri belirlemektedir. Kişinin erişime kapalı bilgilerini usulsüz elde etmeye çalışmak bir bilişim suçudur. Belirtmek gerekir ki böyle durumlarda önemli olan mağdurun rızasıdır. Mağdurun rızası varsa eğer durum suç olmaktan çıkacaktır. Bilişim sistemlerine girme suçu, suçun özelliğine göre 6 ay ile 3 yıl arasında hapis cezalarına ya da adli para cezalarına sebebiyet vermektedir.

- **Sistemi Engelleme, Bozma, Erişilmez Kılma, Verileri Yok Etme veya Değiştirme Suçu (m.244):**

  Bir önceki bilişim suçundan farklı olarak burada seçimlik suç durumu vardır. Saldırgan, bu maddelerde belirtilen suçlardan herhangi birini işlemesiyle bilişim suçu ortaya çıkmış bulunur.

  Seçime dayalı bu suçları örneklerle inceleyecekolursak eğer;

  Verileri Değiştirme ve Yok Etme;

  Örneğin, bir kişinin sanal hesaplarına girerek o kişiye ait verileri, kişinin kendini tanıtmak için kullandığı profil bilgilerini vs. değiştirerek ya da silerek işlenen bir suçtur. Bu tarz suçlarda mağdurların özellikle karşılaştığı durum rencide olma durumudur.

  Sistemi Erişilmez Kılarak Engelleme;

  Sistemde yetkisi bulunan kişinin o sisteme girişinin engellenmesi şeklinde ortaya çıkar. Örneğin, yetkisi bulunan kişinin şifresini elde ederek değiştirilmesi sonucu o kişinin sisteme girmesi engellenmiş olacaktır. Bu durumla ilgili olarak Yargıtay'ın verdiği karar aşağıda ki gibidir;

  "Sanığın babasına ait internet hesabından katılana ait e-posta hesabına birçok kez girildiğine ilişkin TİB ve Microsoft'tan gelen yazı yanıtlarına ve tüm dosya kapsamına göre; elektronik posta hesabının şifresini ele geçirerek bu adrese giren ve şifreyi değiştirmeksuretiyle katılanın e-postalarına erişimini engelleyen zanlının,

eylemine uyan 244/2. madde uyarınca "Bilişim Sistemini Engelleme, Bozma, Erişilmez Kılma, Verileri Yok Etme veya Değiştirme Suçu" nedeniyle cezalandırılmasına karar verilmesi gerekirken yazılı gerekçeyle beraat hükmü kurulması kanuna aykırıdır" [18].

Kararın, Yargıtay'a kadar çıkmasından anlaşılıyor ki bir önceki mahkeme (Bölge Adliye Mahkemesi) Yargıtay'ın aksine karar vererek şifrenin elde edilmesinin ve şifrenin değiştirilerek e-posta hesabına erişimin engellenmesini suç olarak kabul etmemiştir. Mağdurun mahkeme kararına razı gelmeyerek Yargıtay'a gitmesi sonucu doğru olan karar verilebilmiştir aksi durumda mağdurun mağduriyeti giderilmiş olmayacaktı. Buradan da anlaşılacağı üzere, gerek savcıların gerek hâkimlerin bilişim suçları alanında karar verirken zaman zaman yetersiz kalabildiği gözükmektedir. Devletin giderek yaygınlaşan bilişim suçları alanında yargı erkine eğitimler vermesi gerektiği ortaya çıkmıştır.

Sistemi Bozmak;

Sistemin teknik yapısına uygun bir şekilde çalışmasını engellemek ve o sistemi kullanan kişilerin sistemi kullanamamasına sebebiyet verecek şekilde işlenen suçlardır. Bilişim sistemlerine yapılan bu seçimli suçlarda, suçun özelliğine göre 6 ay ile 6 yıl arasında hapis cezalarına ya da adli para cezalarına sebebiyet vermektedir. Bu tarzda işlenen suçlar kimi zaman küçük çapta kimi zaman çok büyük çapta olumsuz etkiler yaratabilmektedirler. Örnek vermek gerekirse, reklam ve tanıtım faaliyetle- rini ağırlıklı olarak sosyal medya üzerinden yapan bir işyerinin hesabına girerek erişimi engellemek ya da o hesabı kapatmak o işyerine ciddi mana da maddi ve ma- nevi kayıplar verdirebilmektedir. Ya da yine bir işyerine ait hesapları ele geçirip, uygunsuz içerikler paylaşarak o işyerinin itibarını zedeleyerek ciddi kayıplar yaşatılabilmektedir. Bu tarz itibar zedeleyici ve ciddi maddi kayıplar yaşatan suçlarda yargı erkenin, suç işleyenlere özellikle adli para cezaları yerine doğrudan mahkumiyet cezası vermesi, caydırıcılık açısından faydalı olacaktır. Ülkemizde bu tarz işlenen suçlarda mahkemelerde genelde 2 yıl ya da aşağı ceza verilmekte ve bu cezada paraya çevrilmektedir. Cezanın paraya çevrilmesi durumu caydırıcılık açısından çok etkin olmamaktadır. Bu caydırıcılığın yeterli olmamasından dolayı da bu alanda işlenen suçlar yıllar itibari ile artarak sürmektedir.

- **Banka veya Kredi Kartının Kötüye Kullanılması Suçu (m.245):**

Bilişim suçları arasında yer alan, hile ve dolandırıcılık suçlarında en fazla kullanılan yöntem olan banka ve kredi kartlarının kötüye kullanılması ile ilgili de 5237 sayılı kanunda çeşitli hükümler yer verilmektedir. Buna göre;

245. Madde, bir kişinin, bir başkasına ait olan banka ya da kredi kartını haksız yollarla ele geçirmesi, kart sahibinin bu durumda herhangi bir şekilde rızasının olmaması ve kartın kart sahibine verilmemesi gibi durumlarda, kartı ele geçiren kişinin kart sahibinin rızası ve izni olmaksızın bu kartı kullanması durumunda ya da kullandırması halinde, " üç yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası ile" cezalandırılması hükmüne yer verilmektedir.

Bu madde, yeni kanunda yer alan en önemli gelişmelerden bir tanesidir. Ancak dikkat edilirse burada banka ve kredi kartı kullanımı bilişim suçlarına dâhil ise cezai yaptırım söz konusudur. Burada bir kanun açığı söz konusu olmaktadır. Söz gelimi bir kişi bir başkasının kartını haksız şekilde ele geçirip bunu bilişim sistemleri dışında, misalen bir pos cihazında kullandığında, suç artık bir bilişim suçu olmaktan çıkmakta ve artık bu bir hırsızlık ya da dolandırıcılık suçu haline gelmektedir. Sahte kimlik bilgilerinin kullanımı ile kredi ve banka kartlarının kullanımı, birçok bakımdan nitelikli dolandırıcılık ile ilgili kanunlara dâhil edilmektedir. Bu nedenle yasa koyucunun bu konuda çok daha açıklayıcı bir ibare eklemesi önemlidir.

Aynı maddenin ikinci ve üçüncü fırkasında ise, şu hükümlere yer verilmektedir:

(2) "Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretimi yaparak satan, devreden, bu kartları satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası ile cezalandırılır."

(3) "Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanarak kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beş bin güne ka- dar adli para cezası ile cezalandırılır" şeklindeki ibare de suçiçin caydırıcılık özelliğine sahiptir (TCK 5237).

Belirtmek gerekir ki; gerçek bir kişi kullanılmadan yalnızca bilişim sistemi kullanılarak bankalardan haksız yolla çıkar sağlamaya yönelik işlenen bilişim suçları bu maddeye göre cezalandırılacaktır. Bankaya ait çek, hesap cüzdanı, dekont, vs. gibi araçlarla kişilerle muhatap olarak onları kandırmakla birlikte bilişim sistemi de kullanılarak bankalardan

haksız menfaat elde edilmişse eğer bu kez bilişim suçları değil, TCK md. 158/1-f'deki nitelikli dolandırıcılık suçu işlenmiş olur.

Yasak cihaz veya program kullanma suçu (m.245/a);

Bir bilgisayar programının, şifrenin veya cihazın; Bilişim sistemlerinin araç olarak kullanılarak işlenebilen diğer suçların işlenmesi için, oluşturulması veya yapılması halinde, bunları üreten(imal) eden, ithal-ihraç eden, depolayıp kabul eden, satışa arz eden, satan, satınalan, bulunduran kişi suç işlemiş sayılır.

Yasak cihaz veya program kullanma suçu, 3 yıla kadar hapis ya da adli para cezalarına sebebiyet vermektedir. Kanun maddesinde bu suçtan dolayı kimlerin cezalandırılacağı geniş bir şekilde belirtilmiş ve suç işleme kastı ile bu cihazların yapılması durumunda ceza öngörülmüştür. Kanunda doğrudan kasıt ile ilgili durumdan bahsedildiği için taksir durumunda cezalandırmanın olup olmayacağı konusunda belirsizlikler bulunmaktadır. Çünkü bu tür suçlar kasıtla olabileceği gibi taksirlede işlenebilmektedir.

Dikkat edilmesi gereken bir diğer husus ise kullanımı yasak gözetleme ve dinleme cihazları ya da programları bilişim hayatının olmazsaolmazlarındandır. Çünkü bu tür cihaz ve yazılımlar yasal faaliyetlerde de kullanılabilmektedirler. Örneğin bir keylogger prog-ramı yasak olmasına rağmen Etik Kurulu onaylı yasal izinle "Türkiye de ki klavyelerde en çok tıklanan harf anketinde" kullanılabilecektir [19]. Böyle bir durumda ya da benzer olaylarda hukuki olarak yoruma açık alanlar ortaya çıkacaktır. Çünkü keylogger prog- ramının amacı zaten izinsiz veri elde etmektir. Bunu bulundurmak suç sayılabilecekken, anketin suç amacıyla yapılmaması ve bir kasıt bulunmayışından dolayı herhangi bir suç oluşmayacaktır.

2.6.2 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Bilişim kavramının geçtiği bir alanda muhakkak akla ilk gelen kelime internettir. İnternetin varlığı ve yaygınlaşması ile birlikte bu alanda yasal düzenlemelere ihtiyaç duyulmaya başlanmıştır. Ülkemizde internet ile ilgili ilk ve kapsamlı düzenleme 23 Mayıs 2007 yılında, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile yapılmıştır.

Kanun ile internet erişimlerini kontrol altına alınması amaçlanmıştır. Böylece internet üzerinden işlenecekolan bilişim suçları büyük ölçüde önlenmekle beraber suç öğesi barındıran olası bir olay sonrasında sorumlu/sorumlular ya da suçlu/suçluların tespit edilerek suçsuzdan ayırılmasını sağlanacaktır.Ayrıca kullanıcıların internet aracılığı ile aldatılmalarının ve kötü amaçlı içeriklerden korunması amaçlanmaktadır.

Kullanıcılar internet ile birlikte web sayfalarından iletişim kurmak, bilgi paylaşımı yapmak, eğlence, hizmet vermek ve kendilerini tanıtmak gibi birçok ihtiyacını karşılayabilmektedirler. Bu durum haksız kazanç elde etmek isteyen kötü niyetli kullanıcılar için fırsatlar doğurabilmektedir. Kullanıcılara ait kişisel bilgileri çalarak kişiler üzerinden haksız kazançlar elde edebilmekte ve kullanıcıları mağdur edebilmektedirler.

5651 sayılı kanun tüm bu olumsuzlukları en düşük seviyeye indirmeyi amaçlayarak hizmet veren kurumların, hizmet sundukları ve internette savunmasız bulunan kullanıcıları korumasını istemektedir.

Kanun; yasal içerik taşımayan, kullanıcıların bilgilerinin çalınmasına neden olabilecek sahte web sayfaları, suç unsuru barındıran tüm web sayfalarının engellenmesini ve kullanıcıların ister bilinçli ister bilinçsiz bir şekilde bu sayfalara erişimlerinin engellenmesini zorunlu kılmıştır.

Büyük bir hızla yayılan web sayfalarını kontrol altına almak neredeyse imkânsız olmaya başladı. Bu sebeple henüz kara listeye alınmamış web sayfasında işlenebilecek suçların sonradan takip edilebilmek ve kim/kimler tarafından nasıl gerçekleştirildiğinin öğrenilmesi amacıyla web sayfalarına erişen tüm kullanıcıların kayıtlarının (loglarının) zaman tarih mührü ile tutulması ve saklanması istenmektedir. Bahsedilen kayıtların kapsamı şu şekildedir. Internet sağlayıcı konumunda bulunan kurumlar ve kuruluşlar kendi ağları içerisinde dağıtılan IP adreslerinin bilgilerini, kullanıma başlanıp bitirilme saatlerini ve kullanılan IP adresleriyle bağlantı kuran bilgisayarların MAC adreslerini elektronik ortamda kayıtaltına almak zorundadır. Ayrıca, bu kayıtların doğruluk ve bütünlüğünü için elde edilen verileri dosyanın oluşturulduğu zaman bilgisi ile (HASH) günlük olarak kayıt altına almalıdır. Erişim kayıtlarının 1 yıl ila 2 yıl arasında saklanması istenmektedir.

Ücretli ya da ücretsiz birden çok kişiye internet erişim hizmeti sunan tüm kurum ve kuruluşlar bu kanuna uymak zorundadırlar. Aksi takdirde ceza yaptırımı uygulanmaktadır.

Kanun, birçok kesimden destek almış olsa da eleştiri konusu da olmuştur. Eleştiri konularının başını "özgürlük" ifadesi çekmiştir. İnternette yapılan yayınların kısıtlanmasının, ifade özgürlüğü açısından sıkıntılar yaratabileceği tezi en yaygın itiraz ve eleştiri başlığı olmuştur.

Kanunun, internet üzerinden halkı kışkırtan, terör propagandası yapan, aile yapısını bozucu, gayri ahlaki vs. yayınların yapılmasının önüne çekilmiş bir engel olması itibariyle faydalı olduğu gözükmektedir. Lakin nelerin gayri ahlaki ya da terör propagandası kabul edileceği o günün hükümetine göre değişecekse, böyle bir durumda da kanunun amacından sapma ve keyfiliğe açık bir hale gelebilme durumu açısından olumsuzluk teşkil edebilmektedir. Bu vesile ile yapılan kanunların hükümet politikası mantığıyla değilde devlet politikası mantığıyla hazırlanması gerektiği önem kazanmaktadır.

2.6.3 5070 sayılı Elektronik İmza Kanununda Düzenlenen Bilişim Suçları

TBMM tarafından 15 Ocak 2004 tarihinde kabul edilen ve bundan altı ay sonrayürür- lüğe giren 5070 sayılı Elektronik İmza Kanunu, Avrupa Birliği direktifleri nihayetinde hazırlanmıştır. Kanunda amaçlanan, elektronik imzanın hukuki ve teknik yönleri ile ilgili çeşitli yaptırımların sağlanabilmesidir.

Elektronik İmza Kanunu Madde 16'da, "Elektronik imza oluşturma amacı ile ilgili kişi-nin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adli para cezasıyla cezalandırılırlar. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır" şeklinde yer alan ibare, elektronik imzanın korunması ve buna güven duyulması bakımından Kanun'a eklenmiştir. Suç fiilinin işlenmesi için elektronik imza oluşturmayayönelikkasıtlı bir hareket vehaksızlıkaranır [20].

Aynı Kanun'da madde 7'de şu ibare bulunmaktadır: "Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerekkullananlar, iki yıldan beş yıla

kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılır. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır" [21].

Bu madde ile elektronik araçlar kullanılarak oluşturulan rızasız, hukuka aykırı ve aynı zamanda da izinsiz şekilde düzenlenen elektronik imzaların yaptırımları net olarak ifade edilmektedir.

Elektronik imza kullanan kişilerin mağduriyet yaşamaması için bir takım tedbirler almasında fayda bulunmaktadır. Elektronik imza, gerekli aparatla(Tokken) bilgisayara takıldığı zaman aktifleşmek için e-imza sahibinin daha önce belirlemiş olduğu şifreye ihtiyaç duyar. Güvenlik açısından gerekli olan bu şifre, unutulmamak adına saklandığı yerde gizliliğinden emin bir şekilde muhafaza edilmelidir ya da şifre girilirken bir başkasının göreceği şekilde girilmemelidir. Aksi takdirde elektronik imza şifreyi bilen kötü niyetli kişilerin eline geçtiği zaman, kişi aleyhinde kullanılabilir ve kişiyi çözülmesi zor ya da imkânsız durumlara sokabilir.

2.6.4 5846 Sayılı Fikir ve Sanat Eserleri Kanunu

5846 Sayılı Fikir ve Sanat Kanunu (FSEK) madde 2'de, 7 Haziran 1995 tarihinde 4110 sayılı kanunu neklenmesi ile değişikliğe gidilmiş ve "eser" kavramının tanımlaması yapı-lırken bilişim programları da koruma altına alınmıştır. Madde 2'de bahsi geçen eserler, dil ve yazı ile ifade edilen eserler, bilgisayar programları ve bunların hazırlıkları olarak ifade edilebilir.

FSEK madde 6'da ise yeni eklenen kanun maddesi yer almaktadır. 10 numaralı bende şu ibareler eklenmiştir: "Bir bilgisayar programının uyarlanması, düzenlenmesi ya da program üzerinde değişim yapılması da fikir ve sanat eseri sayılmaktadır." yapılan bu değişiklik ile Avrupa Konseyi direktifine uygun olarak bir uyumya kalanmıştır [22].

Yine FSEK üzerinde yapılan madde değişiklikleri ile fikri mülkiyet kapsamında yer alan eserler ile ilgili düzenlemeler 71, 72 ve 73. Maddelerde yer almıştır. Buna göre "eser olarak kabul edilen bilişim sistem yazılımları üzerindeki maddi ve manevi hakların kasten ihlal edilmesi durumunda cezalandırılması" öngörülmüştür. Madde 71'de manevi hakların ihlali, madde 72'de maddi hakların ihlali ve madde 73'te diğer suçlar adı altında farklı suç tipleri ile ilgili düzenlemeler yapılmıştır [23].

FSEK 71. maddede, yaptırıma bağlanan bazı fiiller yer almaktadır.

Bunlar şöyle sıralanabilir:

- Bir eserin, hak sahibi kişinin yazılı halde izni olmadan işlenmesi, çoğaltılması, değiştirilmesi, dağıtılması, her çeşit ses, işaret, görüntü nakleden bilişim araçları ile kamuya açılması, yayınlanması; aynı şekilde hukuka aykırı bir biçimde çoğaltılan bir eserin satışa açık hale getirilmesi, kiralanması, ticari amaçlarla kullanılması, kişisel kullanım dışında bir eserin muhafazası, bir yıldan beş yıla kadar hapis cezası ile cezalandırılmaktadır.
- Eser bir başkasına ait iken bir kişi tarafından esere yeni bir isim konması, bu eseri kendi eseri gibi lanse etmesi altı ay ila ilki yıl hapis cezası ile hükmolunmuştur. Eser dağıtılır ya da yayınlanır ise, hapis cezası alt sınırı beş yıl olur, adli para cezasına hükmolunmaz.
- Bir eserden, kaynak göstermemek suretiyle alıntı yapan ya da iktibasta bulunan bir kişi, altı ay ila iki yıl arasında hapis cezası ya da adli para cezası ile cezalandırılır.
- Hak sahibi olan kişiden izinsiz olmak koşuluyla, aleni bir hale gelmemiş bir eserin içeriğini kamuya açan kişi, altı aya kadar hapis cezası ile cezalandırılır.
- Bir eserle ilgili olarak yanlış ya da kandırıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezasıalır.
- Bir eserin ya da bir sanat eserinin tanınmış bir başka kişi adına çoğaltılması, yayınlanması ve dağıtılması, üç ay ile bir yıllık bir hapis yahut adli para cezası ile cezalandırılmaktadır [24].

Madde 72'de ise;

"Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır" ibaresi ile yazılım güvenliğinin korunması amaçlanmaktadır. Bir eserin, sahibinin izni ve rızası olmadan yayınlanması, çoğaltılması ve dağıtılması ya da bir şekilde ticari amaçlar için kullanılır hale getirilmesi, yaptırıma bağlanan durumlardır [25].

2.7 Bilişim Suçlarının İşlenme Şekilleri

Bilişim alanı gelişen teknolojiyle birlikte her geçen gün daha fazla faaliyet alanı kazanmaktadır. Bu sebeple bilişim faaliyetleri ile orantılı olarak bilişim suçlarında da sürekli olarak çeşitlilik ve yeni yöntemlerde artış görülmektedir.

Aşağıda literatüre girmiş olan çeşitli bilişim suçlarına dair bilgilendirmeler yer almaktadır.

2.7.1 Salam Yöntemi

Özellikle bankaların teknik altyapılarına yönelik olarak sıklıkla kullanılan bir bilişim suçu tekniğidir. Bu teknikte banka hesaplarına yatırılan paraların fark edilemeyecek derecede küçük küsuratları başka hesaplara aktarılarak menfaat sağlanmaktadır[26].

Çok sayıda işlem için bu durum tekrarlandığında küçük küsüratlardan büyük meblağlar elde edilmesi söz konusu olmaktadır. Bu yöntem aslında günlük hayatımızda da çokça karşılaştığımız bir duruma da benzemektedir. Bu duruma örnek verecek olursak; herhangi bir markete alışverişe gittiğiniz zaman fiyatların göze batmayacak şekilde küsuratlı olduğunu ve kasaya gelindiği zaman ise bu küsüratların yukarıya yuvarlatılarak paha biçildiği görülür. Bu işlemin her ürün için yapıldığı varsayıldığında ortaya katlanarak artan maliyetsiz bir kazanç çıkmaktadır. Bu durumda aslında bilişimsiz bir Salam Yöntemi sayılabilir. Salam Yöntemi olarak bilinen bu bilişim suçu tekniği yoğun olarak Truva Atı programı ile birlikte kullanılmaktadır.

2.7.2 Truva Atı (Trojan Horse)

Bu suç tekniği, bilgisayar kullanıcısından bağımsız olarak çeşitli işlemler yapabilme imkânı sağlamaktadır [27]. Aslında basit bir bilgisayar programı olarak görünen bu program, sahip olduğu zararlı yazılım ve komutlarla bilgisayar işleyişini bozmaktadır ve iyi sayılabilecek bilgisayar bilgisi olmayan biri tarafından fark edilmesi çok zor bir durumdur. Bu programın kullanılmasıyla bilgisayarın kontrolü, kullanıcısı farkında olmadan başka bir kullanıcının kontrolüne girmektedir. Böylece bilgisayarasıl kullanıcısının değil, Truva Atı yazılımını bilgisayara bulaştıran kişinin kontrolüne geçmiş olmaktadır.

2.7.3 Gizli Kapılar (Trap Door)

Literatürde hile kapıları, arka kapı vb. çeşitli isimlerle de anılan bu bilişim suçu tekni- ğinin en büyük özelliği sistemin güvenlik kontrollerine takılmamasıdır. Bir tür bilgisayar programı olan bu tekniğin uygulanabilmesi için bir şifre gereklidir. Bu teknikle hedef bilgisayarın sistem ayarları ele geçirilmiş olmaktadır. Bu yöntemi kullanan kişiler genelde o sistemin yazılımını yapan kişilerdir. Yazılımı yapan kişi, yazılımın içine gizli bir şekilde virüs programı yerleştirir ve böylece kendine gizli bir açmış olur. Böylelikle amacına çok daha rahat şekilde ulaşabilmektedir.

2.7.4 Ağ Solucanları (Network Worm)

Destek bir programa ihtiyaç duymadan sistem içerisinde çoğalabilme özelliğine sahip zararlı bir yazılımdır. Bu da ağ solucanlarını var oluşundan daha tehlikeli hale büründürür. Bu yöntem herhangi bir kişinin kontrolüne ihtiyaç duyulmadan hedeflenen verilerin, dosyaların vb. tüm kopyalarını ağa bağlı olan ve istenilen bilgisayarlara aktarabilmektedir. Böylece kullanıcısının bilgisi olmadan istenilen tüm verilerin kopyalanıp aktarılabilmesi sağlanmaktadır [28].

2.7.5 Çöpe Dalma (Scavenging)

Bir diğer adı atık toplama olan bu yöntemde, seçilen bir bilgisayar sisteminin işlevlerini yerine getirmesinden arta kalan verilerinin toplanması işlemi yapılmaktadır [29]. Kısaca artık işinize yaramayacağını düşünüp sildiğiniz bilgilerin gelişmiş yazılım programlarıyla geri getirilerek istenilen bilgiye ulaşma çabasıdır.

2.7.6 Bilişim Korsanlığı (Hacking)

En yaygın ve bilinen bilişim suçlarından olan bilişim korsanlığı, hedef sistemle ilgili kritik değerdeki bilgilere ulaşılabilmesini sağlamaktadır. Bu faaliyette bulunan kişilere "hacker" adı verilmektedir. Bilişim korsanı olarak da ifade edilebilen bu kişiler, hedef sistemlerin

güvenlik zafiyetlerinden istifade ederek söz konusu sisteme müdahalede bulunabilmektedir. Günümüz koşullarında bu korsanlık saldırısı sebebiyle saldırılar kişileri aşarakuluslararası bir şekle bürünmüştür. Böylece saldırılan ülkelere ciddi boyutta maddi ve manevi zararlar verdirilebilmektedir.

2.7.7 Veri Aldatmacası (Data Didding)

Bilişim suçu işleyen kişilerce en çok kullanılan yöntemlerdendir. Çünkü basit ve kullanımı nispeten daha kolaydır. Buna ek olarak en önemli özelliği ise ortaya çıkarılması oldukça zor bir bilişim suçudur. Bu yöntemde veriler sisteme girilirken değiştirilebilmekte, kasıtlı olarak hatalı bilgiler girilebilmektedir. Özellikle de veri girişlerinin kontrolünü yapan ikinci bir gözün olmaması bu saldırının tespitini daha da zor hale sokmaktadır. Böylece verilerin sisteme aktarılması sırasında tahrifat yapılması mümkün olabilmektedir.

2.7.8 Mantık Bombaları

Bilgisayar sistemini çalıştırmamak üzerine kurulu bir yazılımdır. Truvaatı yazılımının bir başka çeşididir. Hedef sistemi karıştırabilmek, işleyişini bozabilmek ve bir nevi felce uğratmak amacıyla programlanmaktadır. Bunu sağlayabilmek için sisteme sürekli olarak mantık dışı komutlar ve yapılan işlemle tezat oluşturacak bilgiler gönderilmektedir. Bu özelliklere sahip olmasısebebiyle oldukçayıkıcı vezararlı bir yazılımdır [30].

2.7.9 Gizli Dinleme (Eavesdropping)

Çeşitli yöntemlerle verilerin elde edilmesini içermektedir. Veriler elde edildikten sonra gerekli yerlere servis edilebilir. Bu yöntemlerden biri de sistem tarafından yayılan elektromanyetik dalgaların yakalanarak yeniden veri haline dönüştürülmesi işlemidir [31].

2.7.10 Tarama (Scanning)

Özellikle sistemgirişlerine konulmuş olan şifrelerin bulunabilmesi amacıyla kullanılan bir yöntemdir. Telefon numaraları, internete erişimi olan cihazların IP adreslerini vb. numaraları bulmaya yönelik bir uygulamadır [32].

2.7.11 İstem Dışı Alınan Elektronik Postalar (Spam)

Gönderilmesi konusunda açık bir izin olmayan çeşitli konularda ki reklami çerikli e-postalardır. Literatürde spam (spiced park and ham) olarak ifade edilen bu durum, herhangi bir yolla elde edilmiş olan e-postalara kişilerin herhangi bir hakkını ihlal etmese de rahatsız edici nitelikteki e-postaların yollanmasıdır. Suç teşkil etmeyen içerikler yollanmış olsa bile, eğer bu e-postalar belirli bir sayıyı geçerek rahatsız edici ve kişinin e-postasını kullanamayacağı hale gelirse TCK 244 gereği "bilişim sistemini kullanımın engellenmesi" kapsamına girebilecektir [33].

Yukarıda örnekleri verilen bilişim suçu teknikleri en sık karşılaşılan ve literatürde öne çıkan teknikler olup, burada ifade edilenlerin dışında çok sayıda başka bilişim suçu tekniği de bulunmaktadır. Örneğin burada yer verilmeyen ancak önemli bilişim suçu teknikleri arasında değerlendirilebilecek olan; Tavşanlar (Rabbits), Bukalemun (Chameleon), Süper Darbe (Super Zapping) ve Eş Zamansız Saldırılar isimleriyle bilinen teknikler de bilişim suçu tekniklerinden bazılarıdır. Bilişim teknolojisi alanındaki gelişmelerle birlikte bilişim suçlarında görülen tekniklere de her geçen gün yenileri eklenmektedir. Bu sebeple bu alan oldukça dinamik ve güncel olarak takip edilmesi gereken konulardandır.

2.8 Bilişim Suçlarının Sınıflandırılması

Bilişim suçları çeşitli uluslararası sözleşmelerde ele alınmıştır. Bunlardan Avrupa Ekonomik Topluluğu tarafından yapılan toplantı sonucu yayınlanan tavsiye kararlarında bilişim suçları beşe ayrılmıştır. Bu sınıflandırmaya daha önce değinilmişti. Buna benzer şekilde bilişim suçlarının ele alındığı diğer önemli belgeler şunlardır:

Avrupa Konseyi tarafından 2001 yılında yayımlanan Bilişim Suçları Sözleşmesine göre bilişim suçları dört gruba ayrılmıştır. Bunlar:

- Bilgisayar veri sistemlerinin erişilebilirliği ve gizliliğinin ihlalini içeren suçlar. (Bilgisayar sistemlerine yasadışı erişim (m. 2), Verilere yasadışı müdahale (md. 3), Bilgisayar sistemlerinin çalışmasının engellenmesi (md. 5), bilişim cihazlarının kötüye kullanılması (md. 6).

- Bilgisayar Bağlantılı Suçlar (Bilgisayar bağlantılı sahtekârlık ve dolandırıcılık (m. 7 ve m. 8).
- İçerik kaynaklısuçlar (m. 9).
- Telif hakları veilişkili diğer hakların ihlalini kapsayan suçlardır.

Bilişim suçlarının sınıflandırıldığı başka bir uluslararası toplantı ise, Birleşmiş Milletler 10. Kongresi kararlarıdır. Bu kongrede bilişim suçları dar ve geniş anlamda bilişim suçları olarak ikiye ayrılmıştır. Bunlardan dar anlamda bilişim suçlarından, bilişim sistemlerinin güvenliğini ya da data işlemlerini hedef alan faaliyetler kastedilmektedir. Geniş anlamda bilişim suçlarından kasıt ise, bilişim ağı vasıtasıyla söz konusu ağ üzerinden gerçekleştirilen tüm yasadışı faaliyetlerdir [34].

Sonuç olarak bilişim suçları ve kapsamı konusunda literatürde tümçalışmaların üzerinde mutabakata vardığı bir tanım ve kapsam bulunmamaktadır. Ancak bilişim suçlarına yönelik tasniflerde nispeten benzerlikler bulunduğunu söylemek mümkün - dür.

Bilişim suçları, farklı birçok teknolojik ürün ya da bağlantının kötü amaçlarla kullanılmasını kapsamaktadır. Bilişim suçlarında sınıflandırma, genel itibariyle bilişim teknolojilerinin "amaç" ya da "araç" olarak kullanımından kaynaklanmaktadır. Bu sınıflandırma dört ana başlık altında incelenebilir.

2.8.1 Veri Suçları

Verilerin yetkisi olmayan kişilerin eline geçmesi ve dolayısıyla veri içeriğinde gizli kalması gereken bilgilerin de yetkisiz kişiler tarafından öğrenilmesi, veri suçlarının genelini kapsamaktadır. Veri tasarrufu, yetki sahibi kişilerde olması gerekmektedir. Yetki sahibi herhangi bir kişi ya da kurumun tasarrufunda olmamalıdır. Bu nedenle verilerin korunması, veri güvenilirliğinin de temel gereksinimidir.Nitekim Kişisel Verileri Koruma Kanunu'nun17. maddesindekişisel verilerin hukuka aykırı birşekilde işlenmesi durumunda TCK'nın 135 - 140. maddelerine göre cezalandırılacağı belirtilmiştir.Verilerin korunması, hukuki bakımdan iki ana şekilde gerçekleştirilmektedir. İlkinde, verinin hukuki bir mal veya eşya olarak kabul edilmesi ve veri üzerindeki mülkiyetin korunmasını içermektedir. İkinciside verininbir sırolarak korunmasıdır.

Veri suçları da üç temel başlık üzerinden değerlendirilebilir:

- Verilere Müdahale
- Verilerin Değiştirilmesi
- Verilerin Çalınması (Veri Hırsızlığı)

Bu üç suç türünde de dolandırıcılık ve sahtekârlık suçlarında kullanım ortak özelliktir ve bu suçlar aynı zamanda "özel hayatın gizliliği" ilkesinin de ihlali anlamına gelmektedir [35].

Verilere müdahale ya da verilerin durdurulması, hukuka aykırı bir biçimde verilerin birtakım değişikliklere maruz kalması ve verilere ulaşımın bir şekilde engellenmesi şeklinde ifade edilebilir.

Verilerin değiştirilmesi, bir bilişim sistemi içerisinde yer alan verilerin tahribi ve bozulması anlamına gelmektedir. Genellikle dolandırıcılık suçlarında büyük ölçüde kullanılmaktadır. Verilerin çalınması ya da veri korsanlığı ile ifade edilen suç, veri sahibinin izni ve haberi olmaksızın verilerin aktarılması ya da kopyalanması anlamını taşır. Bu, genellikle veri sahibinin zarar görmesi ve hırsızlık amacıyla kullanılmaktadır [36].

2.8.2 Bilişim Ağlarına Yönelik Suçlar

Bilişim sistemlerini işlev dışı bırakmak amacıyla farklı yöntemler kullanılarak bilişim sistemlerinin bilgisayar programlarına eklenmesi, bazı program ve sistem dosyalarının silinmesi gibi suçları kapsar [37].

2.8.2.1 Ağ Engellenmesi

Kullanılmakta olan bilgisayar ağlarının kısmen ya da tamamen erişime kapatılmasıdır. Bu işlem için yönlendirilmiş bir bilgisayardan sürekli olarak veri gönderimi gerçekleştiri- lir ya da korsan metotlarla elde edilmiş birden fazla bilgisayar ya da wifi bağlantısı olan cihazlarla hedef noktaya aşırı istek gönderilerek hedefi kısmen ya da tamamen engellenebilir hale getirilir. Bu durum, 5237 sayılı TCK'nın 244. Maddesinde düzenlenmiş olup suç sayılmaktadır.

2.8.2.2 Ağ Sabotajı

Bilişim ağlarının fiziksel olarak zarara uğratılmasını ifade eder [38]. Verilen bu zarar ile hedef noktada tahribatlar yapılabilmekte, sistemin verimli çalışması engellenebilmektedir

2.8.3 Yetkisiz Giriş Suçları

Yetkisiz erişim, bilişim sistemlerine izinsiz olarak erişim sağlanarak sistemdeki fonksiyonların kullanılması ve bu sistem dâhilindeki verilere, yetkisiz kişilerin ulaşmasıdır. Kurum ya da kişiye ait olan bilişim sistemleri ile ilgili ceza hukukunda yaptırımlar bulunmaktadır.5237 sayılı TCK'nın 243. maddesinde kanun koyucu, yetkisiz giriş yapmayı bir suç olarak tanımlamıştır. Bu suçtipi en yaygın görülen siber suçlardan bir tanesidir [39].

Yetkisiz olan üçüncü kişilerin bilişim sistemleri dâhilinde işlem yapabilmesi, yetkisiz olarak bu sistemlere girmesi veri işleme ve verilere erişim yetkisiz giriş suçları dâhilinde değerlendirilmektedir. Bilişim sistemine yetkisiz olarak giren bir kişi, bilişim verilerinin içeriğine yönelik bilgi sahibi olabilir, verilerde değişiklikler yapabilir ve verileri kopyalayabilir.

Aynı zamanda verilerin kullanılarak programların çalıştırılması, değiştirilmesi yahut silinmesi de yetkisiz girişle yapılabilecek eylemlerdir. Bu eylem çeşitliliği o veriyle yapılabilecek birçok işlem kadar çeşitlendirilebilir.

Yetkisiz giriş, bilgisayar sistemi ve veri güvenliğine yönelik saldırı ve tehditleri kapsar. Bu durum, düzeltilmesi için yüksek maliyet gereken bazı düzenlemelere yol açabilir, aynı zamanda veriler üzerinde tahribat da söz konusu hale gelebilir. Söz konusu maliyetlendirmenin boyutu, sosyal medyanın çok yaygın olduğu günümüz dünyasında çok büyük oranlarda olabilmektedir.Gizli kalması gereken bir bilginin gündeme getirilerek yayınlanmasına sebebiyet vererek tamiri imkânsız zararlara sebebiyet verebilecektir. İzinsiz şekilde giriş neticesinde sistemin izinsiz kullanılması, bilişim sisteminde sahtecilik yahut dolandırıcılık gibi tehlikeli birçok durumun ortaya çıkması gibi olumsuz durumlar ortaya çıkabilir [40].

2.8.3.1 Bilişim Sistemlerine İzinsiz Giriş

Yetkilisiz kişi veya kişilerin, bilişim sistemine yetkisiz olarak girmeleri, sistemdeki ka-yıtlı önemli bilgilere ulaşmasıdır. Yetkisiz dinleme ve hesap ihlali, buna örnek olarak gösterilebilir.

Yetkisiz dinleme, iki bilgisayar sisteminin arasında gerçekleşen iletişimin dinlenmesi yani network ağının dinlenmesidir ve yasa ihlalidir. Suçun kapsamı, aynı kişiye ait iki ayrı bilgisayarın dinlenmesi, iki farklı kişi bilgisayarının dinlenmesi ya da bilgisayar ve bir kişi arasındaki iletişimin dinlenmesi biçiminde gerçekleşebilir. Suç, yalnızca bilgisayarla sınırlı değildir, genel olarak tüm telekomünikasyon iletişimlerini kapsamaktadır.

2.8.3.2 Virüs Yayılması

Sisteme ve verilere zarar verilmesi amaçlanarak zararlı programların harekete geçirilmesi eylemidir. Virüslerin yayılması, sonuçları nedeniyle bir suç kapsamında değerlendirilmek-tedir[41].

2.8.4 Bilgisayarla İlgili Diğer Suçlar

2.8.4.1 Dolandırıcılık

Bilgisayar yoluyla dolandırıcılık, bir kişinin aleyhinde ve bir başka kişinin lehinde olay-ların gelişmesidir. Dolandırıcılık bir tür menfaat edinme şeklinde de tanımlanabilir. Ya da kısaca kanunsuz menfaat sağlama da denilebilir. Burada amaç, bir kişiye ait verilerin alınması, değiştirilmesi ya da silinmesi ile bu kişiye ekonomik açıdan zarar verilmesidir. Suçu işleyen kişi, bilgisayar dolandırıcılığı ile kendisine ya da suç ortağına maddi bir kazançsağlamayıamaçlar. Hedef noktanınmahiyetinegöre debukazancınboyutu az ya da çok olabilmektedir.

Bilgisayarla dolandırıcılık farklı birçok şekilde yapılmaktadır. Özellikle sahte bir hizmetin gerçekmiş gibi gösterilmesi sık karşılaşılan durumlardan bir tanesidir. Sosyal ağlar üzerin-den zayıflama, arkadaşlık, fal bakma, ünlü kişilerle alakalı ilgi çekici haber linki ve daha birçok farklı ilgi çekici uygulama bu amaç için oluşturulmakta ve bununla maddi kazanç sağlama amaçlanmaktadır. Bununla birlikte, kullanılan banka ya da telefon operatörü

adının kullanılarak da para talep edilmesi bilgisayar dolandırıcılığı örneklerindendir [42]. Ne yazık ki teknoloji konusunda yeterli bilgisi olmayan ya da iyi niyet besleyerek yaklaşan birçok kişi bu sebeplerden dolayı dolandırılmaktadır.

2.8.4.2 Girdi / Çıktı Program Hileleri

Dolandırıcılık türlerinden bir tanesi olan girdi/ çıktı program hileleri, bir bilişim sistemi içine kasıtlı biçimde hatalı veri girişi yapılması yahut sistemden çıktı alınmasını kapsamaktadır. Hatalı veri girişi yaygın olarak kullanılan bir dolandırıcılık yöntemidir. Hatalı çıktı da bu yöntem dâhilinde kullanılan tekniklerden bir tanesidir ve sahte doküman üretiminde kullanılmaktadır. Program hileleri ise teknik bakımdan çok daha zor tanımlanmaktadır.

Program hileleri genel olarak üç ana temelde incelenir. İlki ticari piyasada kullanılan yazılımlardır ve bunlar satışa açık durumdadır. İkincisi, yasal olarak satın alınan yazılımların daha sonra çeşitli değişikliklerle satılmaya çalışılması ve üçüncüsü ise özel bir amaç için yazılmış olan, satışı olmayan ve dağıtılması için izni bulunmayan yazılımlardır [43].

2.8.4.3 İletişim Servislerinin Yetkisiz Olarak Kullanımı

Kişisel ya da toplu bir menfaat sağlanması maksadıyla iletişim sistemlerinin içinde yer alan prosedür ve protokollerin açıklarının kullanılması, bilişim sisteminin iletişim servis-lerinin haksız ve izinsiz şekilde kullanılması ve yine iletişim sistemlerinin değişik şekillerde yahut kötü amaçla kullanılması şeklinde ifade edilebilir [44].

2.8.4.4 Kredi / Banka Kartı Dolandırıcılığı

Kredi kartı ya da banka kartının kullanılması ile yapılan hırsızlık ve dolandırıcılık suçları, bu kapsamda değerlendirilmektedir. Kart ödeme sistemleri (ATM) genel olarak banka gibi finansal kuruluşlarca kullanılmaktadır. Bu ödeme sistemlerine erişim ise genel ola-rak bir tanımlama numarası kullanılır ve bu PIN (Personel Identification Number) ile sağlanır. Dolandırıcılık ile bu ödeme sistemlerinde mevcut olan kartların çalınması ve

çoğaltılması sonucunda yapılan hırsızlık söz konusudur [45]. 5411 sayılı Bankacılık Kanunu'nun 135 maddesinde, " . . . . bankacılık işlemleri ile ilgili sahte evrak düzenlemek ve ibraz etmek, ...zimmet, dolandırıcılık, bilişim sistemini engelleme, bozma, verileri değiştirme veya yok etme . . . ." suç olarak tanımlanmıştır [46]. Gelişen teknoloji ile birlikte artık kartların çalınmasına da gerek kalmamıştır. Özellikle internet bankacılığı karta fiziksel olarak ihtiyaç duymayı ortadan kaldırmıştır.

2.8.4.5 Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

Bazı yazılımların kanunlarla korunduğu bilinmektedir. Zira 5846 sayılı FSEK'in 2. maddesine 4110 sayılı kanunun eklenmesi ile bilgisayar programları eser olarak kabul edilmiştir. Yine FSEK üzerinde yapılan değişiklikler ile fikri mülkiyet kapsamında yer alan eserlerle ilgili düzenlemeler 71, 72 ve 73. maddelerde yer alarak "eser olarak kabul edilen bilişim sistem yazılımları üzerindeki maddi ve manevi hakların kasten ihlal edilmesi durumunda cezalandırılması" öngörülmüştür. Bu koruma altındaki yazılımların, birden fazla bilgisayarda kullanımı, bu yazılımın izinsiz kullanımı anlamına gelmektedir. Yazılım lisansları tekil bir bilgisayar için hazırlanmaktaolduğu için, aynı zamanda ek lisans alınmadan başka bilgisayarlarda kullanılmaması gerektiği için, bu durum yasal bir suç kapsamına girmektedir. Lisans, bilgisayar özelinde alınması gereken bir sistemdir ve aksi halde lisans sözleşmesine aykırı hareket edilmiş olur.

Buna ek olarak, lisans haklarına aykırı bir biçimde çoğaltma işlemi de kanunlarla korunmuş bir yazılımın izinsiz kullanımı anlamına gelir. Her yazılımın bir lisans sözleşmesi olmalıdır. Bu yazılımın kopyalanması ve başka bir ortamda kullanılması suç teşkil etmektedir. Bu suçun işlenmesinde ödemeden kaçma amacı bulunur ve bu kapsamda daha önce satın alınan ya da daha önceden sözleşmeye aykırı bir biçimde kopyalanmış olan yazılım, bir başka medya ortamında kullanıma açık hale getirilir. Hem kopyalamayı sağlayan hem de buna göz yuman iki taraf da suçun ihlalinde pay sahibidir. Lisans kullanım hakkının alınmasının maliyetli olması bu suçun yaygınlaşma sebeplerinin içinde belki de en önemlisi olarak yerini almaktadır. Son olarak, bir başka ihlal türü olması nedeniyle bahsedilmesi gereken yasanın ihlal edilerek lisansın kiralanması durumu da söz konusu olabilmektedir. Farklı medyalar üzerinde kayıtlı olan film, oyun ya da yazılıp programlarının kiralanması, lisans haklarının ihlal edilmesi anlamına gelmektedir [47].

2.8.4.6 Yasadışı Propaganda

Yasadışı propaganda, yayınlanması suç olan çeşitli materyallerin bilişim sistemleri kullanılarak yayınlanması ya da dağıtılması olarak tanımlanmaktadır. Kanun tarafından yasaklanmış olan bu materyaller e-postalar, internet siteleri ya da iletişim için kullanılan her tür araç ve kayıt yapan tüm cihazları kapsamaktadır.

Yasadışı olarak tanımlanan bu propaganda araçları arasında, vatanın bütünlüğüne yönelik terör saldırıları, belli bir kişiye ya da topluluğa karşı gerçekleştirilen tehdit ve hakaret içerikli propagandalar, bu niteliklere sahip elektronik doküman ya da web siteleri olabilmektedir. Bunlar motive olmuş ya da edilmiş, belli bir amaca hizmet eden kişisel ya da siyasi oluşumlardır [48]. Kanun Koyucu bu duruma karşı caydırıcı cezalar koymuştur.

2.8.4.7 Verilerin Suiistimali

Kişisel ya da ticari bilgilerin yahut sırların, sahibinin rızası olmaksızın, bir başka bireye ekonomik menfaat sağlanması için kullanılması, verilerin suiistimali olarak tanımlanır. Buna müşteri bilgileri, hasta bilgileri, alışveriş merkezleri ya da devlet kurumlarında tutulmakta olan her türlü bilginin kişisel ya da toplu bir menfaat için ya da bilgilerin sahibine bir tür zarar verilmesi için rıza dışında kullanılmasıdır [49].

Kişisel verilerin ticari bir mal haline getirilmesi, geçen her gün yeni bir boyutta bu bilgilerin ihlal edilmesi ve tehditlerin artması, teknolojinin gelişimi ile birlikte kişisel verilerin güvenliğini de zorunlu kılmaktadır. Günümüzde kişisel veriler çok açık bir biçimde gerek internet sitelerinde gerekse sosyal mecralarda kullanılmakta, bu da korumanın yetersiz kalmasına neden olmaktadır. Bu konuda gerek bireylerin tedbirsizliği gerekse de yazılım ve teknoloji şirketlerinin bir takım istekleri durumu daha da önlenmesi zor hale getirmektedir. Buna verilebilecek en güzel örnek aslında günlük hayatta sıkça yaşadığımız ve birçoğumuzun farkına varmadığı, telefonlarımıza indirdiğimiz uygulamalar. Bu uygulamaları indirmek başlı başına kullanım için yetmemektedir. Uygulama kullanılmak istendiği zaman sizden çeşitli erişim izinleri (rehbere erişim, resim galerisine erişim vs.) talep etmektedir. Bu taleplere olumlu cevapverildiği an artık bize özel olan mahrem birçok durumumuz gizlilik açısından tehlikeli bir duruma girecektir.

Kişisel verilerin korunması ve suiistimale açık durumda olmaması ya da bu duruma getirilmemesi, hukuk ve devlet açısından büyük önemtaşımaktadır [50].

Bölüm 3

Adli Bilişim

Kritik altyapıların artık bilgisayar tabanlı sistemler tarafından yönetildiği ve bu sistemlerin güvenliği de yine bilgisayarlarla ya da teknolojik bir takım araçlarla sağlandığı günümüzün gerçeklerindendir. Olası bir siber saldırı durumunda olayların incelenmesi, fail ya da faillerin bulunması için devreye hukuk sistemi girmektedir. Saldırı bilişim yoluyla işlendiği için saldırı tespiti için de bilişim sistemlerinin kullanılması gerekmektedir. Tam da bu nokta da hukuk ve bilişim bir araya gelmekte ve ortaya adli bilişim kavramı çıkmaktadır.

"Computer Forensics" kelimesinden türeyen bir İngilizce kavramdır. Forensic, "mahkeme ile ilgili, adli" anlamına gelmektedir [51].Çok çeşitli tanımlamaları mevcut olmakla birlikte bu tanımların bazıları şuşekildedir.

Adli bilişim, sabit ve çıkartılabilir belleklerden delil elde etmek için veri(bilgi) kurtarma işlemi olan ve elektronik delillerin içerdiği bilgileri, delil inceleme süreçlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak, delilin bütünlüğünü bozmadan ve maddi gerçekleri açığa çıkarmak amacıyla; kopyalayarak belirlemek ve belirlenen bu gerçekleri çözümleyerek yorumlayıp belgeleme süreçlerinin bütünüdür [52].

Adli bilişim, genellikle bilişim sistemlerindeki verilerin delil olarak toplanması, muhafazası, derlenip analiz edilmesi konusunda belirli standart ve ilkelerle oluşturan disiplinli bir yapıdaki yapıda ki bilim dalıdır.

Adli bilişim, elektromanyetik ve elektro optik ortamlarda tutulan veya bu ortamlarca iletilen ses, görüntü, veri veya bunların birleşiminden oluşan her türlü bilişim nesnesinin,

mahkeme ortamında sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür [53].

Bu tanımlar incelendiği zaman adli bilişimin, elektronik ve sayısal bulgulara dayalı bir olgu olduğunu görmekteyiz. Bu sebepten dolayı adli bilişim sürecine girmeden önce elekt- ronik ve sayısal bulgu kavramları bünyesinde barındıran dijital delil kavramının ne oldu- ğunu anlatmak gerekmektedir.

3.1 Dijital Deliller

Delil, kelime anlamı olarak, istenilen amaca ulaşmayı sağlayan bir iz demektir. Hukuk literatüründe ise herhangi bir uyuşmazlığa sebebiyet veren bir olgu ya da nesnenin kanuna aykırı(suç) olup olmadığı hakkında güvenlik güçlerinin, savcıların ya da yargıcın bir sonuca varıp uyuşmazlık durumunu çözmesini sağlayan ve elde edilmesi kanun tarafından yasaklanmamış her şeye delil denilebilir. TCK 5271 Sayılı CMK'nın 217. maddesinin ikinci fırkasında, bu konuya değinilmektedir. Buna göre,

217. madde ikinci fırkada, "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir." hükmüne yer verilmiş ve yine TCK 5271 Sayılı CMK'nın 206. Maddesinin ikinci fırkasının a bendinde de "kanuna aykırı olarak elde edilmiş olan delillerin ortaya konulmasının reddolunacağı" öngörülmüştür.

Dijital delil, İşlenen bir suç için, niteliği itibariyle delil sayılabilecek, yargıç önünde delil niteliğiyle kullanılabilecek elektronik ve manyetik ortamlarda verileri saklayıp tutabilen bilgisayar, hard disk, CD/DVD, flash bellek, tarayıcı, akıllı telefon, kredi kartı okuyucu, e-mail kayıtları vb. farklı birçok dijital alet ve araçlar dijital delil olarak sayılmaktadır.

Dijital deliller hassas bir yapıda olduklarından dolayı bozulmaya, değişmeye ya da yok olmaya meyillidirler. Bu hassas yapı dijital delilleri diğer delillerden ayıran özellikler arasındadır.

3.2 Dijital Delillerin Bulunma Ortamları

Dijital deliller, günümüzün yaygın teknoloji ortamından dolayı birçok yerde ve birçok farklı şekilde karşımıza çıkmaktadır. Öyle ki, bu veri dosyalarını internet geçmişinden,

sunucuların kayıt dosyalarından, abone kayıtlarına kadar birçok ortamda karşımıza çıkmaktadır. Bu şekilde doğrudan bilgisayar ve bilişim sistemleriyle alakalı olabileceği gibi gömülü sistemlere sahip ve program hafızası olan teknolojik aletlerde de karşımıza çıkabilmektedir. Örneğin, akıllı bir evde eve yapılan bir kundakçılık ya da hırsızlık olayında kullanılan akıllı ev sisteminde ki verinin kullanımı da bir dijital delil olarak kullanılabilmektedir.

Hangi donanımlarda dijital delillerin olduğuna bakılacak olursa;

- Bilgisayar ve monitörler
- Ram (Hafıza)
- USB bellek kartları
- Cep telefonları (özellikle de akıllı cep telefonları)
- CD / DVD, disket
- Modem, Firewall
- Yazıcılar ve tarayıcılar
- Fotokopi makineleri
- Hafıza kartları
- Fax cihazları
- Kameralar
- Taşınabilir ya da sabit diskler
- Fotoğraf makineleri

şeklinde sıralanabilir.

Bu dijital aletler daha da çeşitlendirilebilir. Teknoloji geliştikçe, yeni yeni aletler ve yeni yeni delil/delil yöntemleri ortaya çıkacaktır.

3.3 AdliBilişim Süreci

Dijital delillerin uygun bir şekilde araştırılması için belirli yöntem ve prosedürlere ihtiyaç vardır. 12 basamaklı dijital delil araştırma süreç modeli bunlardan biridir [54].

Sırasıyla;

- **1. Suçlama ve Vaka Alarmı**

  Süreç başlangıç noktasıdır. Bu başlangıç çeşitli şekillerde olabilmektedir. Bir sistemin alarm vermesi ya da bir kişinin şikâyeti/ihbarı bir başlangıç olarak kabul edilir.

- **2. Değer Değerlendirmesi**

  İhbarın önemi ve riski belirlenip değerlendirilir. Bu değerlendirmeye göre de araştırmanın detaylı ya da yüzeysel olacağına karar verilir. Bu karar sonucuna bağlı olarak hazırlıklar yapılır.

- **3. Suç/Olay Yeri Protokolleri**

  Olay yerine gitmeden önce uygulanabilecek tüm prosedürler ve protokoller belirlenmelidir. Belirlenen protokollere uygun hazırlık çalışmaları yapılmalıdır. Aksi takdirde suç mahallinde yetersiz kalınılma riski ile karşılaşılabilir.

- **4. Tanımlama ve Toplama**

  Belirlenen kurallar ve verilen kararlar neticesinde ki bulgular toplanılır. Toplanan deliller hukuk kurallarına uygun bir şekilde toplanılır. Toplama işleminin her aşamasında kesinlikle belgelendirme işlemi yapılmalı ve doğrulanabilir raporlar hazırlanmalıdır. Burada ki delil toplama işi normal delil toplama işinden biraz daha farklıdır. Çünkü dijital deliller biraz daha fazla özen ister. Herhangi bir özensizlik sonucunda veri kaybı vs. gibi durumlar sözkonusu olabilmektedir.

- **5. Koruma**

  Toplanan delillerin muhafazası iyi yapılmalı. Öyle ki mahkeme anına kadar dijital ve fiziksel olarak korunması gereklidir. Aksi durumda olay çözümü neticesiz kalabilir. Bu gibi olumsuzluklarla karşılaşılmaması için deliller paketlenip etiketlenmeli ve bulunduğu ortam koşullarına benzer yerlerde saklanıp taşınılmalıdır.

- **6. Kurtarma** Toplanan deliller için hemen analiz yapma işlemi eksik ya da yanlış sonuç ve karar doğurabilecektir. O yüzden analize başlamadan önce dijital delil üzerinde gizlenmiş ya da silinmiş verilerin olup olmadığı araştırılır ve varsa o veriler gerekli programlarla geri getirilir. Bu geri getirme işlemi ise orijinal delil yerine kopyası üzerinden yapılır.

- **7. Ayrıştırma**

  Bu safhada asıl detaylı inceleme yapılır. Belirli özellikte ki veriler bir araya toplanır. Böylece incelemenin ilerleyen safhalarında kolaylık sağlanılarak işlem sonuca daha hızlı gidilmesi sağlanmaktadır. Örneğin, pornografi ile ilgili bir veri aranıyorsa ki bu genellikle görsel verilere dayandığı için dosya uzantısı jpeg, png, gif vb. olanlar bir araya getirilir.

- **8. İndirgeme**

  Bu safhada ise konu ile ilgili veriler üzerinde durulur ve ilgisiz olan kısımlar çıkarılır. Biraz daha genelden özele yönelme aşaması da denilebilir bu safhaya. Lakin özele yönelme durumunda ki ilgisiz diye ayrıştırılan noktalarda hangi kritere göre eleme yapıldığına dikkat etmek gerekmektedir. Mahkeme esnasında sorgulanabilir bir durum olduğu için büyük bir titizlik isteyen bir aşamadır.

- **9. Organizasyon ve Araştırma**

  Analiz aşamasındaki araştırmacıların verilere kolay ulaşıp tanımlama yapabilmesi ve tanıklık esnasında anlamlı bir referans verilmesi için bu safhada indirgenmiş verilerin içerikleri kontrol edilerek gruplandırılır. Daha sonra etiketleme işlemi yapılarak anlamsal birimlere yerleştirilir.

- **10. Analiz**

  Teknik bilgiye en çok ihtiyaç duyulan nokta olduğu için toparlanan veriler adli bilişim uzmanları tarafından analiz edilir. Teknik donanım sahibi uzmanlar 4 aşamalı bir safhada analiz işlemi yapmaktadır. Bu safhalar,

  Değerlendirme safhası

  Deney safhası

  Birleştirip korelasyon yapma safhası

  Onaylama safhası, şeklindedir.

- **11. Raporlama**

  Bu noktada araştırma sürecinin nihai sonu için bir rapor hazırlanır. Buraya kadar ki süreçte izlenen prosedürlerde ve izlenen metotlarda önem arz edecek detaylar mutlak şekilde anlatılmalıdır. Raporda, sonuca götürücü analizler ve bu analizleri destekler nitelikte delillerin tanımları yapılmalıdır. Bu raporun büyük bir kısmı da bu tanımlarla ilgilidir. Doğru yapılan tanımlamalar sonuca ulaşmada ve verilecek kararlarındahasağlıklıolmasındabüyükönemarz etmektedir.

- **12. İkna Etme ve Tanıklık**

  Son basamak olan bu noktada artık karar noktasındakilerin karar süreci başlar. Bu süreçte karar vericiler olayı sonuca bağlamadan evvel rapordaki delillerin sunulmasını isteyebilirler. Genelde rapor hazırlanırken üst düzey mühendislik bilgisi gerekir. Bu da akabinde raporda terimsel ve anlaşılması zor kelimeleri getirebilir. Karar vericilerin bu zorluklarla karşılaşmaması için raporun açık ve yalın bir dille hazırlanması büyük önem arz eder. Gereksiz teferruatlardan ve cümle karmaşalarından kaçınılmalıdır.

3.4 Adli Bilişim Sürecinin Hukuksal Altyapısı

Bu süreç CMK. 134. Maddesinde düzenlenmiş olup aşağıdaki şekildedir.

(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 haline getirilmesine hâkim tarafından karar verilir."

(2) "Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi ya da gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyalarınalınabilmesiiçin, buaraç vegereçlere elkonulabilir." Burada ki kanun maddesinde her ne kadar ". . . . şifre çözülememesi durumunda el konulur." ibaresi bulunsa da uygulamada bu şekilde olmamaktadır. Çünkü detaylı bir inceleme yapılması gerekiyorsa bunun için ortam ve şartların müsait olması gerekmektedir. İnceleme ekibi bilgisayarların imajını alırlar. Suç mahali ya da ev-işyeri vs. buna uygun olmayabilir ve

bir bilgisayara dışardan bakıldığı ya dayüzeysel bir inceleme ile bazı gizli noktaların şifreli olup olmadığı bilinemeyebilir. Bu sebeplerden ötürü önce suç unsurunun HASH'i alınarak bir örneği zanlıya verilir bir örneği de soruşturma ekibinde tutulur. Böylece olası bir veri değiştirme durumunun önüne geçilmiş olur.İstenilen bilgisayara el konularak adli bilişim laboratuvarına incelemeye götürülebilmektedir.

"Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir...." kanunun bu kısmı uygulanırken sadece şifre çözümünden sonra hemen iade edilmez. Şifre çözümünden sonra bilirkişi incelemesi de yaptırılmaktadır. Geri verme süresi ülkede ki adli bilişim uzmanı ve laboratuvarlarının yeterliliğine göre uzar ya da kısalır. Yeterli sayıda bulunmaması durumunda bu süre beklenenden fazla uzayabilmektedir. Bazı durumlarda ise el konulan cihazlar işlenen suçun mahiyetine göre geri verilmemesi gerekmektedir. Çünkü hard diski bir kenara bırakıp sadece bilgisayardasalt bir şekilde dahi bulunması suç olan unsurların hard diskte ol- ması durumunda bu hard disk geri verilemez. Örneğin, çocuk pornografisi. Kanun burada yoruma açık bırakılmış durumda.

(3) "Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bü- tün verilerin yedeklemesi yapılır." Bu yedekleme işlemlerinde ki asıl amaç orijinal aletin bozulma, kaybolma ve sahibine geri verilmesi gibi durumlarda elde bulundurulup incelenmesi için yapılmaktadır. Lakin bu yedekleme işlemi tek başına normal bir boyutta gibi gözükse de ülke çapında bu tür işlemlerde ki yedekleme ve saklama işlemi ciddi manada büyük bir yükbarındırmaktadır.

(4) "İstemesihalinde, bu yedekten bir kopyaçıkarılarakşüpheliyeveyavekiline verilirve bu husus tutanağageçirilerekimza altınaalınır."

(5) "Bilgisayar ya da bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının ya da bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır." Böylece yapılan işlemler soyut olmaktan çıkar somut bir kimliğe bürünür. Burada bir takım zorluklarla karşılanabilmektedir. Alınan veriler cüz-i miktarda ise bunu yazıya dökmek kolay olacaktır, lakin alınan veriler büyük boyutlara ulaşmışsa eğer bunu kâğıda dökmek çok zor hatta imkânsızlaşabilmektedir.

Bölüm 4

Kritik Altyapılar

4.1 Kritik AltyapıTanımı

Kritik altyapıların tanımı yapılırken, gerek ülkelere gerekse de uluslararası kuruluşlara göre farklı tanımlamalarla karşılaşılmaktadır.

Türkiye'nin "2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planı'n da kritik altya- pılar; "İşlediği bilgi/verinin gizliliği, bütünlüğü ya da erişilebilirliği bozulduğunda, can kaybına, ulusal güvenlik açıklarına, büyük ölçekli ekonomik zararlara veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" şeklinde tanımlanmıştır [55].

OECD'ye göre kritik altyapıları;

"İşlevselliğini kaybetmesi durumunda toplumsal emniyet ve güvenliğe, sağlık hizmetlerine, vatandaşların ekonomik refahına ya da hükümetin/ekonominin verimli çalışmasına ciddi yönde etki eden bilgi ağ ve sistemleri" olarak tanımlamaktadır [56]. Amerika Birleşik Devletleri'ne göre kritik altyapılar;

"Eksikliği ya da tahribi, güvenliğe, milli ekonominin güvenliğine ve kamu sağlığına ya da kamu emniyetine zayıflatıcı bir etkisi olan sanal veya fiziksel sistem ve varlıklar" şeklinde tanımlanmıştır [57].

Bu tanımlar her ne kadar çeşitlenip farklılaşsa da hepsi özü itibariyle "yokluğunda ya da eksikliğinde devleti ve milleti zora sokacak kurumları " kritik altyapılar olarak tanımlamaktadırlar.

4.2 Kritik Altyapı Sistemleri

4.2.1 ABD Kritik Altyapı Sistemleri

ABD'de 2013 yılında yayınlanan "Kritik Altyapı Güvenliği ve Dayanıklılığı Konusundaki Cumhurbaşkanlığı Politika Direktifi (PPD)" de aşağıda belirtilen 16 sektör kritik altyapı sektörü olarak belirlenmiştir. Bunlar[58];

- Ticari Tesisler
- Kimya Sektörü
- Kritik İmalat Sektörü
- İletişim Sektörü
- Savunma Sanayi Baz Sektörü
- Acil Servis Sektörü
- Barajlar
- Enerji Sektörü
- Devlet Tesisleri
- Sağlık ve Halk Sağlığı
- Su ve Atık Su Sistemleri
- Ulaştırma Sektörü
- Nükleer Reaktörler, Malzemeler ve Atık Sektörü
- Bilgi Teknolojileri

4.2.2 AB ye Göre Kritik Altyapılar

2006 yılında Avrupa Konseyi tarafından yapılan bir taleple, AB tarafından hazırlanan, "Kritik Altyapıların Korunmasına yönelik Avrupa Programında (EPCIP)" raporda kritik altyapılar aşağıda ki gibi belirlenmiştir. Bunlar;

- Su ve Gıda
- Nakliye ve Ulaşım
- Sağlık ve Finans
- Kamu Düzeni ve Emniyet
- Nükleer ve Kimyasal Endüstri
- Uzay ve Araştırmalar
- Bilgi ve İletişim Sektörü

4.2.3 Türkiye'deki Kritik Altyapılar

Türkiye'de Bakanlar Kurulunun 20.06.2013 tarihli ve 2 sayılı Siber Güvenlik Kurulu kararınca, gerek 2013-2014 Eylem Planı'nda gerekse de 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde teyit edilen kritik altyapıları şu şekilde belirtilmiştir. Bunlar;

- Enerji
- Su Yönetimi
- Kritik Kamu Hizmetleri
- Ulaştırma
- Bankacılık
- Finans
- Elektronik Haberleşme

Ulaştırma ve Altyapı Bakanlığı'na resmi bir hüviyet taşımasa da görüş beyan ederek çalışan "Bilgi Güvenliği Derneği" tarafından yayınlanan 2012 tarihli "Ulusal Siber Güvenlik" çalışmasında kritik altyapılar şu şekilde tanımlanarak yerli ve milli teknoloji vurgusu yapılmıştır. [59]. Bu altyapılar;

- Bilişim

- Enerji
- Mali İşler
- Sağlık
- Gıda, Su
- Ulaşım
- Savunma, Kamu Güvenliği
- Nükleer-Biyolojik-Kimyasal Silahlar

Kritik altyapı sektörlerinin belirlenmesi sonuçlarına bakıldığında ABD'nin devletendeksli ve ekonomik güvenliğe yönelik bir belirleme içinde olduğu görülmektedir. Kritik altyapı niteliğinde ki işletmelerin birçoğunun özel şirketler tarafından yürütüldüğü ABD'de, devletin amaçlarından biride bu şirketler arasında en yüksek seviyede işbirliği yapmaktır. Olası bir saldırı da ya da saldırı öncesinde bu şirketler arasında koordinasyon sağlanması ve bilgi paylaşımı yapılması hedeflenmektedir.

AB'de kritik altyapılar ise ABD'nin aksine güvenliğe ya da savunmaya yönelik değil, bireylerin özgürlüklerinin ve haklarının korunmasına yönelik olduğu söylenebilir. Daha sivil bir anlayışın olduğu söylenebilmektedir. Bu kapsamda da siber alanda teşvikler sunmakta ve tedbirlerin alınmasının kolaylaştırıcı önlemler almaktadır.

Türkiye'deki kritik altyapı sistemleri ise ekonomik ve kamu güvenliği endeksli belirlenmiştir. Ülkemizin bu alana girişi ABD ve AB'ye göre daha yeni olduğu için belirlenen sektörlerin çeşitliliği de değişmektedir. Örneğin, bilişim alanının kritikliği bizde sonra ki yıllarda ortaya çıkan bir durum olmuştur. Ülkemizde, son dönemlerde gerek siber alan gerekse siber alan ve kritik altyapı ilişkili çalışmalara hız vermiş ve yeni bir takım düzenlemelerin yapılmasına başlanmıştır.

Türkiye'nin, kritik altyapı sistemi olarak tanımladığı alanları genişletmesi gerektiği tablodan anlaşılmaktadır. Teknolojinin hızlı gelişimi ve yaygınlaşmasından dolayı Bilgi Teknolojilerini, Türkiye Uzay Ajansı'nın kurulması ile birlikte Uzay Araştırmalarını ve Sinop ile Mersin'de yapılmakta olan nükleer santrallerden dolayı Nükleer Reaktörleri kritik altyapı sistemlerine dahil etmesi gerekmektedir.

4.3 Kritik Altyapılara Yapılan Siber Saldırılar

Siber saldırı; yer ve zaman kısıtı olmaksızın, bilgisayar alanında uzmanlaşmış kimseler(hacker) tarafından, başkasının kontrolünde bulunan ve internete bağlı sistemlere izinsiz bir şekilde erişerekkontrol etme ya da zarar verme durumudur.

Teknolojinin gelişimi ve dünyanın global hale bürünmesi yeni yeni kavramlar ve suçların ortaya çıkmasını da zemin hazırlamıştır. Eski sistemcephe ve cephe arkasısavaşlarher ne kadar devam etse de artık bu savaş ve saldırı sistemine yeni, daha az maliyetli ve duruma göre daha fazla zarar verici bir saldırı olan siber savaşlar ve saldırılar ortaya çıkmıştır. Bu saldırılar özellikle de saldırı şiddetinin sonuç etkisini artırmak için ülkelerin kritik altyapı olarak nitelendirdikleri sektörlere yapılmaktadır.

Siber ortamı diğer ortamlardan farklı kılan en büyük sebeplerden biri de hissedilmemesi, görünmemesi ve çoğu zaman anlaşılmaz olmasıdır. Bu yönüyle diğer saldırılara göre daha sinsi bir saldırı türüdür. Böylelikle, saldırılan hedefteki yazılım ve kodları etkileyerek devre dışı bırakabilir, bozulmasına ya da el değiştirmesine(hırsızlık) sebepolmaktadır [60].

Dünya genelinde yapılan bazı siber saldırı örnekleri aşağıda verilmiştir. Bunlar;

- 2000 yılında Avustralya'da, atık kontrol sistemine sızan eski bir çalışan, birçok atık istasyonunun komutasını ele geçirerek bir milyon litrelik bir atığın nehir ve deniz sularına karışmasına sebebiyet vermiştir [61].
- 2008 yılında,"Conficker" adı ile piyasaya çıkan ve Microsoft işletim sistemlerini alan solucan, dünya genelinde milyonlarca bilgisayara virüs bulaştırarak, kişilerin ve kurumların olumsuz etkilenmesine sebebiyet vermiştir. Öyle ki bu saldırı sonucu Fransızsavaş uçakları, uçuş planlarının yüklenememesi sonucu kalkış yapamamıştır [62].
- 2010 yılında İran nükleer enerji altyapısını hedef alan bir siber saldırı gerçekleştirilmiştir. Daha sonra ismi açıklanan bu zararlı yazılımın adı Stuxnet olarak açıklanmıştır. Bu zararlı yazılımı farklı kılan ise daha önce hiçbir saldırıda kullanılmayan yalnızca İran da ki nükleer reaktör türbinleri ile uranyum işleme tesisleri santrifüjler için özel geliştirilmiş olmasıdır. Öyle ki bu yazılım ile yapılan saldırıda büyük

çoğunluğu İran da bulunan bilgisayarlar kullanılmıştır. Çok karmaşık yapıda hazırlananbu yazılım ile yapılansaldırıda, yalnızcanükleertesislerdekullanılancihazlar ve SCADAsistemlerietkilenmiştir.

Dış dünyadan soyutlanmış bir internet ağına sahip olan bu mekâna saldırı yapmak içerden destek almaksızın yapılması imkânsız bir durumken, araştırmalar neticesinde şirkete hizmet veren üçüncü şahıs şirketlerin(taşeron) yardımıyla içeriye sokulan virüslü bir USB ya da Hard Disk kullanılarak sisteme erişim sağlanmıştır. Böylece sistemin kumanda kontrolü arka planda başkalarının eline geçmiştir. Bu sayede sistem yavaşlatılmış ve bu saldırı fark edilene kadar ciddi boyutlarda maddi kayıplara sebep olmuştur.

- 2016 yılında Türkiye, tarihinde ki en kapsamlı siber saldırıya maruz kalmıştır. Gerek internet trafiğimizi, gerekse de ".tr" alan adlarını hedef alan bir DDOS (distributed denial of service attack) saldırısı gerçekleşmiştir. Bu saldırılar ilk başta ".tr" adlarının ROOT DNS sunucularına yapılarak başlanmıştır. Bu saldırıyla Türkiye daha önce 2005 yılında karşılaşmıştı. Oradan çıkardığı dersle 2016 yılında ROOT DNS sunucularınayapılansaldırıdaherhangi bir zarar görmemiştir.

  Lakin saldırı yön değiştirip bankalara yapılmaya devam edince bankaların web sitelerine erişim durdu ve POS cihazlarıyla işlemler gerçekleştirilememiştir.

- SSCB'nin dağılmasından sonra yaşanmıştır. Estonya da bulunan "Kahraman Kızıl Ordu Askeri" sebebiyle ortaya çıkan gerilimler ve bu gerilimlerin çatışmaya dönmesi sonucu 2007 yılında Estonya Hükümeti bu bronz heykeli kaldırmıştır. Bunun üzerine Rus Hacker'lar tarafından Estonya'nınneredeyse tüm kamu ve özel kurumlarına siber saldırılar yapılmıştır. Sitelere erişim durdurularak ciddi mana da zarar verdirilmiştir.

- WannaCry Fidye Yazılım; 2017 yılında tüm dünyayı etkileyen bu fidye yazılım en büyük fidye yazılımı olarak dikkat çekmektedir. 150 ülke ve 300 binden fazla bilgisayarı etkisi altına almıştır.

  Genel saldırı şekli şöyledir. Hedefteki kişi ya da kuruluşun bilgisayarındaki dosyaları erişip şifreli hale getirir. Daha sonra ise dosyayı eski haline getirmek için kurbanından fidye talep eder. İlk başlarda kişilere karşı yapılan bir saldırı olsa da daha sonra büyük kurumlara saldırmaya başlamıştır. Çok sayıda fabrika ya da

kurum işleyişini durdurmak zorundakaldı. Şifreleme karşılığında fidye verilmediği zamanda bu engel devam ettirildi.

Son olarak 2018 yılında Amerikan menşeli uçak üreticisi Boeing firmasının uçak üretim tesislerine saldırı yapılmış ve başarılı sonuçlar elde etmiştir.

- ABD ve SSCB'nin dünyayı adeta ikiye böldükleri soğuk savaş dönemlerinde bu iki ülke karşılıklı siber saldırılarda gerçekleştirmeye başlamıştır. Gerek doğrudan birbirlerine gerekse de karşı tarafın müttefiki sayılan ülkelere bu saldırılar yapılmıştır.1982 yılında SSCB, ABD müttefiki Kanada'nın doğalgaz hatlarının kontrolü amacıyla kullanılmakta olan bir yazılımı elde etmeyi başarmış ve kontrolü ele geçirmiştir. Durumun farkına varan ABD, saldırıyı durdurmak yerine akıllıca davranarak yazılımın içine SSCB'ye fark ettirmeden virüs yerleştirmiştir. Bu virüs sayesinde doğalgaz boru hattından geçen gazın seviyesi aşırı derecede yükseltti-rilmiştir. Sonuç olarak uzaydan görülebilecek bir büyüklükte(nükleer sayılmayan) patlama meydanagelmiştir[63].

4.4 Kritik Altyapı Güvenliği için Sızma Testleri

Kritik altyapıların güvenliği için her ne kadar önlemler alınsa da bu tek başına yeterli olmamaktadır. Çünkü teknoloji hızlı bir gelişim içerisinde ve bununla beraber saldırı çeşitleri çoğalmaktadır. Bu sebepten dolayı şirketler bu önlemleri güncel tutmak zorundadırlar.

Güncel durumun gerek teyidi için ve gerek önlemlerin ne ölçüde olduğunu görebilmek için kurum ya da şirketler sızma testleri yaptırmaktadırlar. Aslında bu durum özünde " benim göremediğimi başkası görebilir" varsayımına dayanmaktadır. Böylelikle başka bir gözün test yapması ve bunu raporlaması mevcut durumumuzun ne düzeyde olduğunu, ne gibi tedbirler almamız gerektiğini ortaya koyacaktır.

2011 yılında, 4022 sayılı BDDK kararı " Bilgi Sistemlerine İlişkin Risk Yönetimi" başlıklı ikinci kısım birinci bölümünün "Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi" başlıklı 7. maddenin 3. fıkrası (ç) bendinde ifade edilen;

" Bilgi sistemlerinin. . . . güvenlik ile ilgili hükümlerin gereklerinin yerine getirilmesi hususunda herhangi bir icrai görevi bulunmayan bağımsız ekiplere düzenli aralıklarla sızma

testleri yaptırılır. . . . .” hükmü ile sızma testleri bankacılık sektörü için zorunlu hale getirilmiştir. 2012 yılında sızma testlerinin yapılması zorunlu hale getirilmiş ve senede en az bir kere yapılmaşartıkonulmuştur[64].

Kritik altyapılar, yüksek düzeyde önem arz ettiği ve teknolojiyle paralel ilerlediği için senede bir kez sızma testine tabi tutulması yeterli gelmeyecektir. Teknolojinin günlük bazda farklılaşıp geliştiği bir ortamda sızma testinin senede bir olması olası riskler karşısında geç kalınma ihtimali doğurabilmektedir.

Kritik altyapılarda, gerekli önlemler alınmadığı zaman bünyesinde çok önemli riskler taşıyan bir durum ise, nesnelerin internetidir(iot). Bu durumu örneklendirmek gerekirse, akıllı sensörlerin kullanıldığı bir altyapı sisteminde olası bir tedbirsizlikte bu sensörle- rin saldırganlar tarafından ele geçirilip kendi çıkarları uğruna kullanılabilme ihtimalleri mevcuttur. Dolayısıyla, akıllı nesneleler ile iç içe geçmiş kritik altyapılara yönelik sızma testlerinin yıl içinde en az iki kez ve detaylandırılmış bir şekilde yapılması gerekmektedir.

Sızma testleri yapılırken, yöneticilerin reel davranmaları uzun vadede menfaatlerine olacaktır. Örneğin bu testleri alanında yetkin olmayan kişilere sırf kanuni zorunluluğu yerine getirmek amacıyla yaptırılırsa reel sonuçlar elde edilemeyecektir. Bu ise var olan eksikliklerin ya da ilerde yaşanabilecek sorunların görülmemesine sebep olacaktır. Konu özü itibariyle büyük önem arz etmektedir. Bu yüzden bu testler yaptırılırken maddi kaygı- larla yaklaşılmamalı ve işinde uzman kişiler tarafından yaptırılmalıdır. Sızma testleri de kendi içinde uygulanış şeklinegöreüç gruba ayrılmaktadırlar [65].

4.4.1 Açık Kutu Sızma Testleri

Burada amaçlanan şey; firmada daha önce çalışan şimdi çalışmayan birinin firmaya zarar verebilme ihtimalinin tespitidir. Eski çalışanın firmanın birçok bilgisine vakıf olduğundan hareketle, testi yapan şirkete firmayla ilgili maksimum bilgi verilir ve bu bilgiler eşliğinde sızmatestleriyapılır.

4.4.2 Kapalı Kutu Sızma Testleri

Bu test yönteminde ise Açık Kutu Sızma Testi'nin tam aksiyle olaya yaklaşılır. Öyle ki testi yapan şirkete firmanın hiçbir bilgisi verilmez. Tamamen dış dünyadan şirketle

herhangi bir bağı oluşmayan kimselerin yapacakları saldırılara hazırlık için bu test yapılır. Test şirketi, firmanın domainler üzerinden test yaparak elde edilebilecek en çok veriye ulaşmaya çalışır.

4.4.3 Zaafiyet Değerlendirme Testleri

Bu test yöntemiyle hedeflenen ise açıklık tespit etmektir. Firma içinde çalışan ve sınırlı yetkilere sahip kimselerin zarar verebilme ihtimalleri ölçülür. Bu ölçüm yapılırken bir takım özel programlar kullanılır. Bu testler sonucunda, test şirketleri genel olarak 2 türlü rapor hazırlar. Bunlar; Yönetimsel Sonuç Raporları ve Teknik Sonuç Raporları olmak üzere ikiye ayrılırlar. İsimlerinden de anlaşılacağı üzere Teknik Rapor da testle ilgili sonuçlar teknik bir şekilde ele alınır. Yönetimsel Raporda ise teknik detaylara girmeden sade bir dil kullanılarak yöneticilerin anlamasının sağlanması hedeflenmektedir. Ülkemizde, bu tür sızma testleri genel olarak BİLGEM tarafından yapılmaktadır.

4.4.4 Sızma Testleri ile İlgili Dikkat Edilmesi Gereken Hususlar

Sızma testleri yapılırken ve yapıldıktan sonraki süreçte testi yapan şirket/kurum bir takım kurallara uymakla mükelleftir. Bunlar; [66]

- Yapılan bu sızma testinden dolayı gerek elde edilen doküman, form, anket vb. evraklar gerekse de sızma testi sonuç raporları gizli belge niteliğine haizdir. Bu belgelerin çalınma, yetkisiz kişiler tarafından erişilme ya da ortadan kaybolma gibi durumlara karşı korunması gerekmektedir.
- Elde edilen raporların saklanması konusunda ilgili şirket/kurumun görüşlerine göre hareket edilmesi gerekmektedir. Saklanılması gereken raporlar personele ait taşınabilir sistemlerde(Laptop, Flash Bellek vs.) bulundurulmamalıdır. Elektronik ve yazılı kopyalar güvenli bir şekilde aklanmalıdır.
- Elde edilen bu raporlar örnek mahiyetinde dahi olsa başka kuruluşlara gösterilmemeli ve sunum vs. gibi dokümanlarda kullanılmamalıdır. Raporların saklanıyor olması test firmasının bir sonraki test işleminde önceki tespit edilen eksikliklerin giderilip giderilmediğini görmesi açısından yarar sağlayacaktır.

- Testi yapan firma, test sonucunda elde edilen raporları saklayabilmek için test yaptıran kurumdan kesinlikle resmi yazı niteliğinde yazılı izin almak zorundadır. Aksi takdirde raporları saklayamaz.
- Firma, personellerinin görev aldıkları testleri en az 2 yıl süreli kayıt altına alıp muhafaza etmeli. Raporu hazırlayan personellerin isimleri raporda yer almalıdır.
- Test sonucu elde edilen raporlar saklanılırken bu raporlara erişim yalnızca o testi yapan ya da doğrudan yöneten kişilerle kısıtlı olmalıdır. Bunun tek istisnası önceki testin devamı niteliğinde bir test yapıldığı zaman yeni test işlemini gerçekleştirecek kişiye erişim yetkisi verilebilir.
- Firma eğer, farklı iş kollarında faaliyette bulunuyorsa ISO/IEC 27001:2013 ek maddelerine uygunluk yalnızcailgili birimiçinaranmaktadır.

4.5 Türkiye'de Kritik Altyapıların Siber Güvenliğine Yönelik Gerçekleştirilen Yasal ve Kurumsal Düzenlemeler

4.5.1 Bilgisayarla İşlenen Suçlar üzerine Mevzuat

Sibersaldırılar, henüz ileri boyuta geçmediği 1980'lerin sonlarında normal hukuki konular içinde asayişle ilgili bir düzenleme niteliğindeydi. Dolayısıyla da ülkeler bu alanla ilgili düzenlemelerinide yalnızcahukuki değerlere aykırı bir suçolarakdeğerlendirmekteydiler. Bu algılama şekli yalnızca hukuki açıdan değil askeri açıdan ya da uluslararası güvenlik açısından da böyle değerlendirilmekteydi.

Bu alanla ilgili ilk düzenleme 1991 yılında 3756 sayılı Türk Ceza Kanunu'nun 20. maddesinde ki değişiklik ile yapılmıştır. 20. maddeye eklenen "Bilişim Alanında Suçlar" başlığı ile herhangi bir bilgisayardan verilerin ele geçirilmesi, bu verilerin başkalarının zararına olacak şekilde kullanılması, başka bir yere aktarılması ya da kopyalanması ceza sebebi olarak nitelendirilmiştir [66].

2004 yılında yürürlüğe giren 5237 sayılı TCK ile "Bilişim Alanında Suçlar" tanımı teknolojinin gelişimine paralel genişletilmiştir. Bu kanun ile 243. madde ile Bilişim sistemine girme, 244. madde ile girilen sisteme müdahale, 245. madde ile kredi kartlarının ve banka

kartlarının kötüye kullanımı ve 246. madde de ise 243-245.maddede belirtilen suçları işleyerek haksız kazanç sağlayan tüzel kişinin durumuyla ilgili suçları tanımlanmıştır. Yine bilişim sistemleri kullanılarak işlenen hırsızlık, sahtecilik, kişisel hayata karşı işlenen vs. bu kanun ile düzenlenmiştir.

2006 yılında yapılan bir değişiklik ile 3713 sayılı Terörle Mücadele Kanununda siber suçların terör kapsamında değerlendirileceği durumlarda belirtilmiştir. Kanunun 1. maddesinde "suç işlemek üzere kurulmuş bir terör örgütünün 5237 sayılı kanunda belirtilen 243-244. maddeler kapsamında suç işlemesi" düzenlenmiş. Kanunun 2. maddesinde ise, " bu suçları, terör örgütüne üye olmadan, terör örgütü adına işleyenlerinde terör suçu işlemiş sayılacağından bahsedilmiştir.

Kanunsal bazda bu gibi eklemeler ya da var olan tanımlar güncellenirken, eski adıyla Devlet Planlama Teşkilatı, sonra Kalkınma Bakanlığı olan ve 2018 yılı Cumhurbaşkanlığı Hükümet Sistemi ile sonlandırılan kurum tarafından, kamu hizmetlerinin daha işlevsel görülmesi ve internet kullanımıyla ilgili 2002 ve 2005 yılları arasında "e- Dönüşüm . . . ." projeleri yayınlamış ve bununla ilgili politika üretmeye çalışmıştır. Yine Devlet Planlama Teşkilatı tarafından 2005 yılında "Bilişim Toplumu Stratejisi" çalışması yapılmış, 2006-2010 yıllarını kapsayan strateji belirlenerek yayınlanmıştır. Bu strateji özünde kişisel bilgi mahremiyeti ve güvenlik başlıklarını taşımıştır [68].

2008 yılında, 5809 numaralı kanunile BTK'ya (Ek: 6/2/2014-6518/102 md.) ile "ulusal siber güvenliğin sağlanması amacıyla politikastrateji ve hedefbelirlemek,(. . . .), kritik altyapılar ve ait oldukları kurum ve konumları belirlemek,(. . . .), siber güvenlik alanında milli çözümler üretilmesi,(. . . .)" yetkisi verilmiştir.BTK, bu kanundan aldığı yetki ile si- ber güvenlikalanındaçokönemli bir yeri bulunan sibergüvenlik tatbikatlarıdüzenlemek- tedir. Bu tatbikatlar ile katılımcıların; siber saldırılar karşısında yeteneklerinin gelişmesi, siber saldırı durumunda kurumlar arası koordinasyonların geliştirilmesi ve bu saldırılar karşısında ulusal düzeyde farkındalığın artırılması amaç edinilmiştir.

2016 yılında, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile kişisel verilerin korunması kanun nezdinde koruma altına almıştır. Kişisel verileri dijital ortamda saklayan kişiler/kuruluşlar kanunla korunmuş bu verilerin, sızdırılması ya da çalınması gibi si- ber saldırılara karşı önlem almak mecburiyetinde sayılmaktadırlar. Aksi takdirde ceza-i işlemlerle karşılaşacaktırlar.

Bu gelişmelerle beraber, siber politikaların yürütülmesi sorumluluğu adına kurumlar kurulmaya başlanmıştır. Hem hukuksal hem de güvenlik boyutuyla ilgilenip Türk Silahlı Kuvvetleriyle yakın bir ilişki içinde bulunarak faaliyet göstermeleri hedeflenmiştir. Bu kurumlardan konumuzu ilgilendiren çerçeveleriyle ilgili bahsedecek olursak;

4.5.1.1 Bilgi Teknolojileri ve İletişim Kurumu (BTK)

Telekomünikasyon sektörünün düzenlenmesi ve denetlenmesi, bağımsız bir otorite eliyle yürütülmesi için 2000 yılında kurulan Telekomünikasyon Kurumu'nun 2008 yılında 5809 sayılı Elektronik Haberleşme Kanunu ile düzenlenerekismi Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir.

Kurumun amacı; Uluslararası sözleşmeler ile garanti altına alınan haberleşme ve mahremiyetin korunmasını sağlamaktır. Bu koruma faaliyetini 5070 sayılı Elektronik İmza ve 5809 sayılı Elektronik Haberleşme kanununa dayanarak yapmaktadır. Kurumun bir diğer amacı da; 2007 tarihli 5651 sayılı kanun gereği " . . . . İnternet ortamında işlenen belirli suçlar ile içerik, yer ve erişim sağlayıcılar üzerinden mücadeleye ilişkin usul ve esaslar belirlemektir"

BTK, 29059 sayılı ve 13.07.2014 tarihli çıkardığı yönetmelik ile bilgi ve şebeke güvenliğinin sağlanmasına yönelik işletmecilerin uyacakları usul ve esasları da düzenlemiştir. Bu yönetmelikte kritik sistemler ile ilgili olarak işletmecilerin uyacağı aşağıdaki esaslar belirlenmiştir;

- Madde 6, " . . . . kritik sistemleri kapsayıcı bilgi güvenliği yönetim sistemi kurar. "
- Madde 9, 3. Bent, " . . . . varlıkları kritiklik derecesi ve veri hassasiyetine göre etiketler. "
- Madde 11, " . . . . doğal afet ve siber saldırı durumlarında kesintiyi engellemek ve minimum kayıpiçiniş sürekliliğiplanı yapar ve uygular. "
- Madde 17, " . . . . kritik sistemlerin bulunduğu alanlara giriş ve erişim yetkisi sadece yetkili kişilerle sınırlandırılır. "
- Madde 20, 2. Bent, " Kullanımdan kaldırılması veya başka amaçlarla yeniden kullanılması planlanan ekipmanda veya elektronik ortamda yer alan kritik bilgilerin

yedekleri ile birlikte geri döndürülemez şekilde silinmesi sağlanır. Silme işleminin mümkün olmaması durumunda söz konusu bilgi depolayan parçalar kullanılamaz hale getirilir. ”

- Madde 27, “ . . . . yedekleme yapılırken, sistemin kritiklik seviyesine uygun yedekleme periyodu belirlenir ve uygulanır. ”
- Madde 29, “ . . . . bilgi güvenliği ihlal olaylarının tanımlanması amacıyla kritik sistemleri izler ve kayıt dosyalarını en az 2 yıl süreyle tutar. ” İşletmecilerin bu yükümlülükleri yerine getirip getirmediği re'sen ya da şikayet üzerine BTK tarafından denetlenir.

4.5.1.2 Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)

1963 yılında kurulan TÜBİTAK 'ın asıl amacı, kamu adına AR-GE yapmak, AR-GE yapan kurum-kuruluş ve kişileri desteklemek ve nihayetinde de bilim insanı yetiştirmek için teşvikler ve imkânlar sunmaktır. Yine asıl amaçlardan biride ülkemizde, bilim ve teknoloji alanında ki politikalarını belirlemektir.

1997 yılında UEKAE altında kurulan Ağ güvenlik Grubu ile açık kaynak kodlu işletim sistemleri, Microsoft, veri tabanları ve e-postasunucularıyla ilgili güvenlik zafiyetleri üzerinde çalışılmıştır. Ayrıcasızmatespit sistemleriyle ilgili olarakta çalışmaya başlamıştır.

2006 senesinde ise Türkiye için önemi çok büyük olan ve aynı zamanda çok kritik bir yapı olanGÖKTÜRK uydu projesiyle ilgili güvenlik görevi UEKAE'ye verilmiştir.

UEKAE, kısaca SOME diye tabir edilen Siber Olaylara Müdahale Ekipleri arasında gerçekleştirilmekte olan SOME tatbikatlarının düzenlenmesini sağlar.

2010 yılında 'a bağlı yeni bir Merkez Başkanlığı kurulmuştur. Bilişim ve Bilgi Güvenliği Araştırma Merkezi (BİLGEM) adını alan bu merkez başkanlık bünyesine alınan UEKAE, 2012 yılında BİLGEM'e bağlı bir enstitü olan Siber Güvenlik Enstitüsü(SGE)'nin kurulmasıyla beraber siber güvenlikle ilgili yetkilerini SGE ye devretmiştir. Böylelikle, sızma testleri ve SOME tatbikatları SGE koordinasyonunda düzenlenmeye başlamış ve devam etmektedir.

4.5.1.3 Siber Güvenlik Kurulu

Kurul, 20 Ekim 2012 tarihinde 3842 sayılı " Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin" Bakanlar Kurulu Kararı ile kurulmuştur. 9 Temmuz 2018 yılında yayınlanan 703 sayılı KHK ile Siber Güvenlik Kurulu, Cumhurbaşkanlığına bağlanmıştır.

5809 sayılı Elektronik Haberleşme Kanunu'na eklenen Ek Madde 1 ile Siber Güvenlik Kurulu'nun görevleri tanımlanmıştır. Bu görevler şu şekildedir;

- Siber güvenlik alanında belirlenen politikaları, eylem planlarını ve stratejilerin onayını yaparak ülke çapında bu doğrultuda etkin kararlar almak.
- Kritik altyapıların belirlenmesi sürecinde ki teklifleri karara bağlamak.

Siber Güvenlik Kurulu, Türkiye tarihinde bir ilk olan ve 2013/4890 sayılı 25.03.2013 tarihli Bakanlar Kurulu kararı ile yürürlüğe girecek olan " Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" hazırlanmıştır. 2016 senesinde ise "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" yayınlanmıştır. Bu plan bir öncekine göre kapsamları genişletilmiş ve ulusal siber uzayın ülkemiz genelinde ki bütün bileşenleri kapsayacak şekilde hazırlanmıştır.

4.5.1.4 Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Merkezi(SOME)

USOM, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" nın 4. Eylem maddesinde alınan karar ile Bilgi Teknolojileri ve İletişim Başkanlığı bünyesinde kurulmuştur.

USOM'un amacı; ülkemize karşı siber ortamda ortaya çıkacak tehditlerin belirlenmesi, bu tehditlerin bertaraf edilmesi ya da zararlarının en az seviyeye indirgeyecek şekilde tedbirler alması ve bu tedbirleri ilgili kuruluşlara paylaşmaktır [69].

USOM, gerek ulusal gerek uluslararası ortamda siber alanda kendisine gelen ihbarları değerlendirir. Bu tehditlerle ilgili kamu kuruluşları ve özel kişilerle koordinasyon sağlayarak tehdidin tespiti ve bertaraf edilmesiyle ilgili çalışmalar yapmaktadır.

Farkındalık yaratmak, eksikleri tamamlamak, bilinçlendirmek ve gerekli yönlendirmeler yapmak amacıyla kamu kurum ve kuruluşlarına yönelik ulusal ve uluslararası düzeyde siber güvenlik tatbikatları düzenlemektedir [70]. USOM, SOME'lere eğitim vermek gibi bir sorumluluk altındadır ve gerekli görüldüğü zamanlarda SOME'lerle doğrudan çalışabilmektedir.

SOME, tıpkı USOM gibi "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" nın 4. Eylem maddesi kapsamında ve 28818 sayılı karar ile kurulmuştur. SOME'ler USOM'un koordinasyon ve denetiminde kurulurlar.

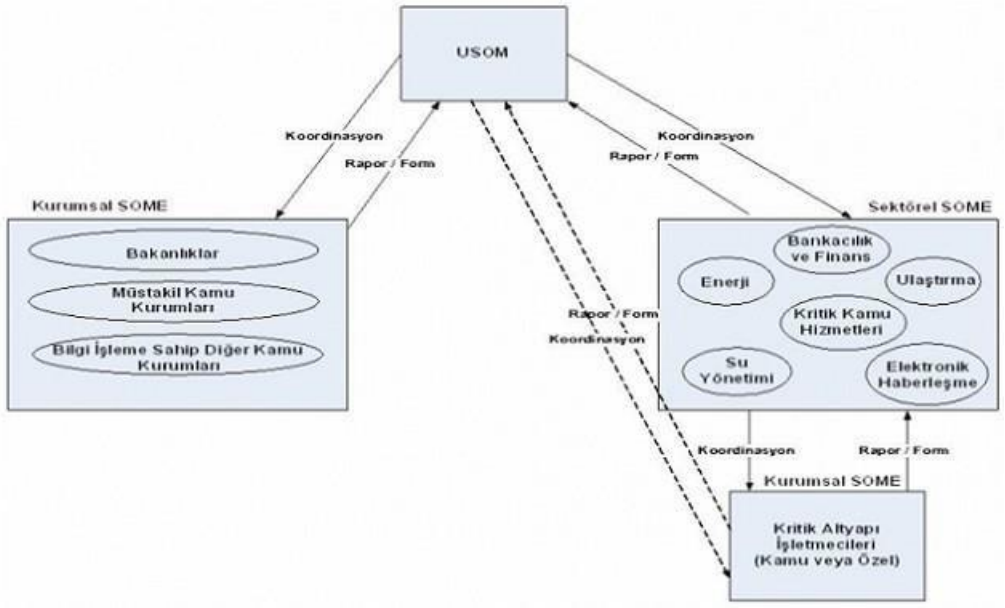
SOME, kendi içinde iki alt başlığa ayrılmaktadır [71]. Bunlar;

- **Kurumsal SOME;** Kamu kurum, kuruluşları ile kritik altyapı sektöründe faaliyet gösteren özel kurumların bünyesinde oluşturulur. Kurumsal SOME'nin amacı; siber güvenlikle ilgili daha önce belirlenmiş olan politikalara uygun bir faaliyet içinde bulunmak, gerekli durumlarda ilgili makamlarla iletişime geçerek gerekli doküman ya da kayıtları aktararak gerekli müdahale yapılırken yardımcı olmak. Kurumsal SOME'ler siber olaylar öncesinden de faaliyetler gerçekleştirir. Rutin olarak bilgi işlem kaynaklarına yönelik güvenlik testleri yapar. Kayıt yönetim sistemi ara yüzünde iz kayıtlarının takibini rutin bir şekilde takip eder.
- **Sektörel SOME;** Kritik sektörü düzenleyici ve denetleyici kuruluşlar ile bu kuruluşlar kurulana kadar ilgili bakanlığın bünyesinde kurulurlar. Kritik altyapı sektörü ile ilgili alanlarda hizmet yaparlar.

  28818 sayılı kanunun 6.maddesinin 3. Fıkrasında " Kritik sektörlerde, sektörel SOME kurulması zorunludur. Kritik sektörlerin listesi Kurul(Siber Güvenlik Kurulu) tarafından belirlenir, ilgililere duyurulur ve güncellenir." ibaresi bulunmaktadır.

  Sektörel SOME'ler, USOM ile koordineli bir şekilde çalışarak siber olayları önlemeye çalışır ve verilmiş bir zarar varsa bu zararı azaltacak faaliyetler yürütür. Siber olayları gecikmesizin USOM'a bildirirler ve diğer çalıştıkları SOME'lerle iletişim halinde bulunurlar.

Ülkemizde gerek kamu kurumlarını gerek kritik altyapıları içine alan Ulusal Siber Olaylara Müdahale Merkezi ile Kurumsal ve Sektörel SOME'lerin ilişki şekli aşağıdaki gibidir [72].



Şekil 4.1: USOM, Kurumsal ve Sektörel SOME İlişkisi

Şekilde de görüldüğü üzere; Kurumsal SOME'ler Kamu kurum, kuruluşları ile kritik altyapı sektöründe faaliyet gösteren özel kurumların bünyesinde oluşturulur. Sektörel SOME'ler ise; Kritik sektörü düzenleyici ve denetleyici kuruluşlar ile bu kuruluşlar kurulana kadar ilgili bakanlığın bünyesinde kurulurlar ve sürekli olarak USOM ile iletişim halindedirler.

Şekilden anlayacağımız bir diğer durum ise, arada ki iletişim ve koordinasyonun ne kadar önemli olduğudur. Gerek siber olay öncesi gerek siber olay esnasında kurulacak kuvvetli bir iletişim sayesinde yapılan saldırının bertaraf edilmesi ya da zararın engellenme ihtimali artacaktır. Herhangi bir kurumda ki saldırı USOM'a bildirildiği takdirde, USOM diğer SOME'lere uyarı yapar ve böylece diğer kurumlar saldırı olmadan tedbirlerini artırma imkânı bulabilirler. Yine bu noktada USOM'un merkezi otoritesinin güçlü olması çok önemlidir. Güçlü bir merkeze sahip olduğu ve bürokrasiden yalıtılmış bir halde bulunması SOME'ler ile olan koordinasyonun ve işbirliğinin kalitesini artırmaya ve yapılan çalışmaların dahaverimli bir hale gelmesine katkısunacaktır.

4.5.1.5 Afet ve Acil Durum Yönetim Başkanlığı (AFAD)

Ülkemizde afetlerle ilgili politika sürecinin başlangıcını şu şekildedir [73]. Süreç 1939 yılı

Erzincan depremi ile başlamaktadır. Yine 1959 yılında bu alanda ki yasal boşluğun doldurulması amacıyla 7269 sayılı "Umumi Hayata Müessir Afetler Dolayısıyla Alınacak Tedbirlerle Yapılacak Yardımlara Dair Kanun" yayınlanmıştır. 1988 yılında yapılan kanunsal düzenlemelerle ise herhangi bir afet durumundadevletinelindeki tümimkânlarıyla enhızlı bir şekilde ulaşma veyardımetmesine yönelikçalışmalaryapılmıştır.

Ülkemizde ki afet yönetimi için bir miat sayılacak asıl olay ise 17 Ağustos 1999 da gerçekleşen Marmara Depremidir. Bu depremle birlikte bu alanda koordinasyon yetersizliği, sorumlulukların tam tanımlanmamış olmadığı ve birçokeksikliğin olduğu fark edilmiştir. Bu karmaşanın giderilmesi ve daha işlevsel bir mekanizma geliştirilmesi amacıyla; 2009 yılında, Sivil Savunma Genel Müdürlüğü, Türkiye Acil Durum Yönetimi Genel Müdürlüğü ve Afet İşleri Genel Müdürlüğü kapatılarak 5902 sayılı kanun ile Başbakanlığa bağlı olarak Afet ve Acil Durum Yönetimi Başkanlığı kurulmuştur. Böylece, tümyetkiler tekbir merci altında toplanarak daha etkin bir hale gelmesi amaçlanmıştır. 15 Temmuz 2018 yılı tarihli Cumhurbaşkanlığı 4 nolu kararnamesiyle de Kurum artık kaldırılan Başbakan- lık yerine İçişleri Bakanlığınabağlanmıştır.

5902 sayılı kanun ile AFAD artık Türkiye'de ki Siber Kriz Yönetimi ve Kritik Altyapı Koruması görevini üstlenmiştir. Bu kanun eşliğinde AFAD, gerek afet anında gerek afetten sonra yetkili kurumlar arasında iletişimi ve koordinasyonu sağlar ve durumla ilgili düzenleyici politikalar geliştirme görevini yüklenmiştir.

AFAD'a göre afetler iki gruba ayrılmaktadırlar. Bunlar;

- Doğal Afetler (İnsan unsurunun dışında doğadan kaynaklanan)
- Teknolojik Afetler(İnsan unsurunun etkisiyle oluşan; kritik altyapı ve siber güvenlik kaynaklı afetler)

Tüm bu bağlamlar eşliğinde 2014 yılında, "2014-2023 Kritik Altyapıları Korunması Yol Haritası Belgesi" AFADtarafından hazırlanarak yayınlanmıştır. Bu belge ile olası bir afet durumunda etkin görev alacak kurumlar belirlenmiş, gereksinimler ve gereksinim kapsamında kieylemler belirlenerek tanımlamalar yapılmıştır. Belgede aşağıdaki gereksinimler tanımlanmıştır;

- Sorumluluğu bulunan merciler

- Koordinasyon yetkilisi
- Nelerin kritik altyapı olarak belirlenebileceği kıstaslar
- AB direktifleri ile uyumlu taslak veyönetmenlik hazırlanması
- Kritik altyapıların tespitedilmesi, koruyucutedbirler alınması, etkinkorunması, AB ve ulusal düzeyde ortaklarla iletişim veişbirliği
- Kritik Altyapı Koruma Planıhazırlanmasının
- AB Kritik Altyapı Uyarı Bilgi Ağı (KAUBA) çalışmalarıyla ilgili bütünleşme

şeklindedir.

AFAD tarafından, kritik altyapılara yönelik gerçekleşecek olası siber saldırılara karşı ile işbirliği yapılarak, "Bilgi Güvenliği Farkındalık Eğitimleri" düzenlenmektedir. Siber saldırılara kapı aralayan ve bir çok siber saldırının etkisini artıran önemli sebeplerden birinin farkında olmama olduğu düşünüldüğünde bu eğitimlerin çok önemli yer edindiği gözlemlenmektedir.

4.5.1.6 Türk Silahlı Kuvvetleri (TSK)

Son yıllarda artan siber tehditlerin artışı ve NATO'nun da bu alanda stratejiler belirlemesine binaen, Türk Silahlı Kuvvetleri (TSK) bünyesinde SOME niteliğine haiz 2012 yılında Siber Savunma Merkez Başkanlığı kurulmuştur.

2013 yılında TSK çok daha büyük bir adım atarak Siber Savunma Merkez Başkanlığını, Siber Savunma Komutanlığına dönüştürmüştür. Bu komutanlık, kapsamları daha geniş tutmuş, Milli Savunma Bakanlığı - - ODTÜ ile işbirliği yapacak şekilde faaliyetlerini gerçekleştirir. Kısa süre sonra ismi, Muhabere ve Elektronik Bilgi Sistemleri(MEBS) ve Siber Savunma Komutanlığı olarak değiştirilmiştir.

Komutanlık ülkemizi siber saldırılara karşı korumak amaçlı çalışmalar yapar ve bu kapsamda NATO ile tatbikatlar icra etmektedir.

4.5.1.7 Emniyet Genel Müdürlüğü (EGM)

Emniyet, TSK'ya göre bu alanda daha erken faaliyetlere başlamıştır. Bu alanda ilk çalışmasını 1998 yılında "Bilgisayar Suçları ve Bilgi Güvenliği Kurulu" nu kurarak başlamıştır. 2000'li yıllarda artan siber saldırı olayları emniyet birimlerini harekete geçirmiş "Siber Suçlarla Mücadele Daire Başkanlığı" (ilk adı, Bilişim Suçlarıyla Mücadele Daire Başkanlığı) kurulmuştur.

4.5.1.8 Milli İstihbarat Teşkilatı (MİT)

Siber dünya yapısı gereği karanlık bir ortamdır. Saldırganın kim olduğunu, nerede olduğunu ya da nereden saldırıldığını tespit etmek hem çok zordur hem de bu alanda ciddi manada uzmanlaştırmaya gerektiren bir durumdur. Dolayısıyla da bu gibi saldırılarda işin arkasında kimin ya da kimlerin olduğunu tespit etmek ve bu saldırıları gerçekleşme- den önlemek için devletler istihbarat servislerini kullanmaktadırlar. Ülkemizde bu görev, Milli İstihbarat Teşkilatı (MİT) ayağıyla yürümektedir. Bu yetki, 2937 sayılı, " Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu"nun 4. Maddesinin i bendinde geçen kanuna göre; MİT, " Dış istihbarat, milli savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı hak- kında bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak." şeklinde belirtilerek MİT'in görev tanımını güncellemiş-tir. Yine 2937 sayılı kanunun 6. Maddesinde, " Telekomünikasyon kanallarından. . . . siber güvenlikle ilgili veriler toplayabilir." yetkisi tanımlanmıştır.

4.6 Türkiye'de Kritik Altyapılar İçin Denetleyici ve Düzenleyici Kuruluşlar

- **Enerji alanında;** Enerji Piyasası Düzenleme Kurumu (EPDK), "EPDK Teşkilat ve Görevleri Hakkındaki Kanun" ile bu göreviyapmaktadır.
- **Finans alanında;** Bankacılık Düzenleme ve Denetleme Kurumu(BDDK), "BDDK -Teşkilat Yönetmenliği" esasına dayanarak bu görevi yapmaktadır.
- **Bilgi ve İletişim alanında;** Bilgi Teknolojileri ve İletişim Kurumu(BTK), "BTK Kuruluş Kanunu" ile bu göreviyapmaktadır.

- **Sermaye alanında;** Sermaye Piyasası Kurumu (SPK), "6362 Sayılı Sermaye Piyasası Kanunu" esasına dayanarak bu göreviyürütmektedir.

4.7 Türkiye'de Kritik Altyapılar İçin Gerekli Standartlar

Siber alanda yaşanan saldırıların sürekli arttığı ve etkilerinin daha yıkıcı boyutlara ulaştığı günümüzde, bilgi güvenliğinin kurumsal anlamda en üst seviyelerde sağlanabilmesi için, süreklilik gerektiren bir süreç olduğu ve bu sürecin kurumsal bilgi güvenliği standartları çerçevesinde yönetilerek ve denetlenmesi gerektiği unutulmamalıdır. Ülkemizde kritik altyapı sayılan sistemlerin bir takım standartlara uyma zorunluluğu bulunmaktadır. Bu standartlar kritik altyapının hangi alanda olduğuna göre değişiklik gösterebilmektedir.

ISO 27000-Bilgi Güvenliği Standartları içinden kritik altyapılarla ilgili olan standartlar aşağıdaki gibidir; [74]

- **TS ISO/IEC 27001:** Telekomünikasyon kuruluşları için ISO / IEC 27002'ye dayalı bilgi güvenliği denetimleri için uygulama prensipleri içerir.
- **TS ISO/IEC 27015:** Finansal hizmetler için bilgi güvenliği kılavuzudur.
- **TSE ISO/IEC TR 27019:** Enerji hizmet endüstrisine özgü süreç kontrol sistemleri için ISO / IEC 27002'ye dayalı bilgi güvenliği yönetim kurallarını içerir.

TSE standartlarına uyulduğunun göstergelerinin ilk şartı, bu standartları belgelemektir. Bu standartlar, kurum ve kuruluşlara uymaları gereken şartları belirtir. Her ne kadar şart olarak konulsa da bunlar kurum ve kuruluşları korumaya yönelik alınan tedbirlerdir. Bu standartlara uyulmadığı takdirde ise TSE tarafından bir takım yaptırımlara tabi tutulmaktadırlar. 05.05.2014 tarihinde yürürlüğe giren, TSE Belgelendirme Yönergesi 'nin 34. Maddesi ile uyarı bildirimi, 35. Maddesinde faaliyeti askıyaalma ve 36. Madde de iptal ve fesih uygulanacağı belirtilmiştir. Bu maddelerin uygulanmasında ise madde sırasına göre işlem yapılır. Uymayan kurum ya da kuruluş önce uyarılır, eğer uyarıya rağmen gerekli düzenlemeleri yapmazise faaliyeti askıya alınır ve buna rağmen hala düzenlemeler yapmazsa sözleşme iptal edilerek fesih işlemleri gerçekleştirilir.

4.8 Kritik Altyapılara Yönelik Siber Güvenlik Konusunda Türkiye'de Yapılan Çalışmalar

Ülkemizde, siber güvenlik ile ilgili çalışmalar yapılırken yalnızca kritik altyapılara haiz çalışmalar yapılmamıştır. Lakin kritik altyapılarıda kapsayan ve diğer sistemlerinde si- ber saldırılara karşı korunmasına yönelik 2000'li yılların başlangıcından itibaren siber güvenlik alanında çalışmalar ve düzenlemeler yapılmıştır. Bunlar; [75]

- **2003/10 Sayılı Başbakanlık Genelgesi (2003);** Öncelikle kamu kurum ve kuruluşlarının olmak üzere, bilgi sistemleri ve internet ağlarının korunmasına yönelik yapılan çalışmalarda, "Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri'nin referans alınarak hareket edilmesi istenilmektedir.
- **2003/12 Sayılı Başbakanlık Genelgesi (e-Dönüşüm Türkiye Projesi);** e-Dönüşüm Türkiye Projesi'nin amaç ve esasları belirlenerek koordinasyon, izleme ve değerlendirme faaliyetleri için Devlet Planlama Teşkilatı(DPT) Müsteşarlığı görevlendirilmiştir. (DPT artık faaliyette bulunmadığı için bu görevleri Cumhurbaşkanlığınabağlı Bilgi ve İletişim Teknolojileri Dairesi tarafındanyürütülmektedir.)
- **e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı;** Bilgi toplumuna geçiş sürecinde toplumun bütün bir kısmını içine alarak katma değeri ve ulusal değerleri artıracak şekilde bilgi ve iletişim teknolojileri, e-devlet, sanayi ve teknoloji politikaları, sosyal dönüşüm, içeren bir Bilgi Toplumu Stratejisi hazırlanması amaçlanmıştır. Bu eylem planında geçen 50 eylemin 20'sinin e-devlet ile ilgilidir.
- **Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010);** 2006-2010 yıllarını kapsayan bu eylem planı ile küreselleşen dünyanın avantajlarının etkin bir şekilde kullanılması amacıyla stratejiler belirleyen ve bütüncül bir dönüşümü sağlamak amacıyla hazırlanmıştır.
- **Ulusal Bilgi Güvenliği Programı (2007);** Devletin bilgi güvenliği faaliyetleri belirleyerek bu faaliyetlerin üretimi ve geliştirilmesi, planlar hazırlaması ve standartlar belirlemesi amacıyla "Ulusal Bilgi Güvenliği Teşkilatı" kurulmuştur [76].
- **BOME 2008 Tatbikatı (İlk Siber Tatbikatımız) (2008);** 20-21 Kasım 2008 tarihinde BİLGEM bünyesinde ki Türkiye Bilgisayar Olayları Müdahale Ekibi(TR-BOME) tarafından 8 kamu kurumunun katılımı ile gerçekleştirilmiştir. Hayali bir

senaryo hazırlanarak Sanal Siber Teröristlerin Türkiye'ye saldırması ve buna karşı alınacak tedbirlerin değerlendirilmesi amaçlanmıştır [77]

- **Ulusal Sanal Ortam Güvenlik Politikası (2009);** TÜBİTAK koordinatörlüğü ile çok sayıda kurumun(19) beraber hazırladığı bir politika dokümanıdır. Bu dokümanda ülkemize karşı yapılacak herhangi bir sanal saldırı karşısında hazır halde olmak ve bu saldırı anında hızlı geri dönüş imkânı sunacak sanal güvenlik adımları belirlemek.

- **Ulusal Siber Güvenlik Tatbikatı (2011);** TÜBİTAK BİLGEM ve Bilgi Teknolojileri ve İletişim Kurumu(BTK) koordinasyonu ile yapılmıştır. Bu tatbikata, kritik bilgi sistemleri altyapısına sahip olan 41 kamu ve özel sektör kuruluşu katılmıştır. Bu tatbikatı farklı kılan en önemli sebep ise; saldırılar yalnızca yazılı ortamlarda değil gerçek saldırı şeklinde de icra edilmiştir.

- **Siber Güvenlik Çalıştayı (2011);** Bilgi Güvenliği Derneği tarafından, çok sayıda kamu ve özel sektörden kurum ve kişilerin katılımı ile gerçekleştirilmiş ve tavsiye niteliğinde kararlar alınmıştır.

- **Siber Güvenlik Hukuku Çalıştayı (2012);** T.C. UDHB, Bilgi Güvenliği Der-neği ve Türkiye Barolar Birliği(TBB) eşliğinde düzenlenmiştir.

- **Siber Kalkan Tatbikatı (2012);** BTK ve Türkiye de internet servis sağlayıcısı olan 12 kuruluş ile gerçekleştirilmiştir[78]

- **Ulusal Siber Güvenlik Strateji Çalıştayı(2012);** Ulusal kapsamda Türkiye'nin, siber güvenlik alanında ilke ve hedeflerinin belirlenmesi ve bu hedeflerdoğrultusunda yapması gerekenleri belirtmek amacıyla Bilgi Güvenliği Derneği tarafından yapılan bir çalıştaydır.

- **TBMM Meclis Araştırma Komisyonu Raporu (2012);** 24. Yasama Dönemi ve 2. yasama yılında TBMM de alınan karar ile bilişim sektöründe ki gelişmelerin sosyal etkilerini araştırmak üzere kurulan Meclis Araştırma Komisyonu tarafından hazırlanan bir rapordur [79]

- **TSK Siber Savunma Komutanlığı'nın Kurulması (2012);** TSK'nın kritik altyapı sistemlerinin, olası siber saldırılara karşı korunması, bu saldırılara karşı atak yapılması ve saldırı neticesinde minimum olumsuz etki anlayışıyla kurulmuştur.

- **Siber Güvenlik Enstitüsü'nün Kurulması (2012);** Kamu, askeri ve özel kuruluşlara bilgi sistemleri ve bilgi güvenliği alanında danışmanlık yapmak, bu alanda politikalar belirlemek, AR-GE çalışmaları yapmak ve siber alanda çalışmalar yapmak üzere BİLGEMbünyesinde faaliyetegeçmiştir.

- **Siber Güvenlik Kurulu'nun Kurulması (2012);** Siber güvenlik alanında ki önlemleri belirlemek, hazırlanan plan ve programların yine bu doğrultuda ki raporların usul, esas ve standartların onaylanıp uygulanması ile koordinasyonunun sağlanması amacıyla UDHB bünyesinde kurulmuştur. 2013-2014 ve 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nı hazırlamıştır.9 Temmuz 2018'de Cumhurbaşkanlığına bağlanmıştır.

- **Ulusal Siber Güvenlik Tatbikatı-2 (2013);** UDHB koordinasyonu ile BTK tarafından gerçekleştirilmiştir. Gerek kamu gerek özel sektörden 61 kurum ve kuruluşun katıldığı bir tatbikattır. Gerçek saldırı senaryoları burada da kullanılmıştır. Diğer tatbikatlarda olduğugibi bu tatbikatın amacı da; siber saldırılar karşısında ki müdahale kabiliyetini geliştirmekvebilgi birikim paylaşımısağlamaktır.

- **Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) (2013);** Ülkemize karşı siber alanda ortaya çıkacak tehditleri belirleyip, bu tehditlerin bertarafedilmesiyada zararlarınınen azseviyeyeindirgeyecekşekildetedbirleralması ve bu tedbirleri ilgili kuruluşlara paylaşmakamacıyla BTK bünyesinde kurulmuş-tur.

- **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı;** UDHB adına, BİLGEM bünyesinde bulunan Siber Güvenlik Enstitüsü tarafından hazırlanan Türkiye'nin siber alanda ki ilk strateji belgesi olma özelliği taşır. Bu belgede siber alanla ilgili gerekli mevzuat çalışmalara vesiber güvenliktatbikatlarına yer verilmiştir.

- **Kurumsal SOME'lerin Kurulması (2013);** USOM ile irtibatlı bir şekilde daha önceden belirlenen siber güvenlik politikalarına uygun davranarak ve saldırı durumunda gerekli tedbirleri alarak ilgili kuruluşlarla irtibat sağlanması amacıyla; Kamu kurum, kuruluşları ile kritik altyapı alanında faaliyet gösteren özel kuruluşların bünyesinde oluşturulur.

- **2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi(AFAD);** AFAD tarafından 2014 yılında AB mevzuatları dikkate alınarak hazırlanmış bir

çalışmadır. Bu çalışma ile Türkiye'nin uzun vadede ulaşmak istediği hedefler belirtilmiştir.

- **Siber Güvenlik Faaliyetlerinin Yasalaşması (2014);** 6518 sayılı kanunun 95. maddesinin 6. fıkrasında Telekomünikasyon İletişim Başkanlığı(TİB) "ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda. . . ., gerekli tedbirlerin alınması ve faaliyetler yürütmesi. . . . " yetkisi tanınmıştır. TİB, 15 Ağustos 2016 yılında kapatılınca görev ve yetkileri Bilgi Teknoloji- leri İletişim Başkanlığı'na(BTK)devredilmiştir.

- **Sanal Ortamda İşlenen Suçlar Sözleşmesi(Budapeşte Sözleşmesi) (2014);** Avrupa Konseyi tarafından hazırlanan ve 2004 yılında yürürlüğe giren "Sanal Ortamda İşlenen Suçlar Sözleşmesi" ülkemizde 6533 sayılı kanunun onaylanması ile 2014 yılında yürürlüğe girmiştir. Bu antlaşma uluslararası alanda ki ilk siber anlaşmamız sayılmaktadır. Bu sözleşme ile birlikte üye ülkeler kendi iç hukuklarında sanal suçlarla ilgili düzenlemeler yapacak ve üye ülkeler arasında işbirliği ve koordinasyonsağlanması hedeflenmektedir. Busözleşmekapsamolarakyalnızca sibersuç olarak tanımlanan suçları değil, elektronik araçlarla işlenebilen tüm suçları kapsamaktadır.

- **Uluslararası Siber Kalkan Tatbikatı (2014);** BTK, Uluslararası Telekomünikasyon Birliği(ITU) ve ITU-IMPACT işbirliği ve 20 ülkeninSOME'lerinin katılı- mıyla gerçekleştirilmiştir. Siber güvenlik konusunda farkındalık ve işbirliği amacı hedeflenerek yapılmıştır.

- **Bilgi Toplumu Stratejisi ve Eylem Planı 2015-2018;** Bu eylem planı 10.Kalkınma Planında tanımlanmış olan bilgi toplumu politikalarının ve hedeflerinin detaylı bir şekilde ele alındığı ve bu hedefler için strateji ve eylemlerin belirlenmesi için hazırlanmıştır[80].

- **Elektronik Ticaretin Düzenlenmesi;** "6563 sayılı Elektronik Ticaretin Düzenlenmesi" kanunu ile elektronik ortamda yapılan ticaret ve sözleşmelerde uyulması gereken kuralları ve aksi durumda uygulanacak yaptırımları düzenlemiştir.

- **Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı;** Siber alan- daki güvenliğinyalnızca kamukurumları vekritik altyapısektöründeğilulusal

siber uzayda bulunan tüm kesimlere yerleştirilmesi ve bu alanda yeterli önlemlerin alınması hedeflenerek hazırlanmıştır [81]

- **TSK Siber Savunma Merkezi Projesi (SİSAMER)(2016);** Savunma Sanayi Başkanlığı tarafından, TSK Siber Savunma Komutanlığı bünyesinde kurulan bu merkez ile TSK'nın siber saldırılara karşı tek bir yerden koordine edilmesi amaçlanmıştır. Bu amaç doğrultusunda da milli yazılımların geliştirilmesi hedeflenmektedir [82].
- **Kamu Kurum ve Kuruluşlarının KamuNet'e Dâhil Edilmesi (2016);** UDHB ve Türk Telekom işbirliği ile hayata geçirilen KamuNet ile kamu kurumları arasındaki veri iletişiminin internete kapalı ve güvenli bir sanal ağ üzerinden yapılarak siber güvenlik risklerinin en düşük seviyeye indirilmesi hedeflenmiştir.
- **Ulusal Siber Savunma 2017 Tatbikatı;** T.C. Ulaştırma ve Altyapı Bakanlığı tarafından gerçekleştirilmiştir. 32 kamu kurum ve kuruluşu katılımı ile gerçekleşmiştir. Bu tatbikatta da gerçek saldırı yöntemleri ile saldırılar düzenlenmiştir.
- **Bilgi ve İletişim Güvenliği" Başlıklı Cumhurbaşkanlığı Genelgesi [83]** 6 Temmuz 2019 tarihli resmi gazetede yayınlanan bu genelge ile kamu kurum ve kuruluşlarının bilgi ve iletişime yönelik uyması gereken bir takım kurallar yayınlanmıştır. Bu kurallardan özellikle bazıları çok önemli niteliktedir. Bu önemli maddeler incelenecek olursa;

(Madde 1): "Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurt içinde güvenli bir şekilde depolanacaktır." Söz konusu madde hayata geçirildiği takdirde; kritik bilgi ve verilerin yurt dışına çıkmasının ve yabancı devletlerin eline geçmesinin önünde büyük bir engel oluşturacaktır. Ülke içinde birçok kritik alanlara girişte güvenliğin genetik ve biyometrik verilerle sağlandığı göz önüne alınacak olursa şayet maddenin hayata tez zamanda geçirilmesinin elzem olduğu da görülmektedir.

(Madde 3): " Kamu kurum vekuruluşlarına ait veriler, kurumlarınkendi özelsistemleri ya da kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır." Ülkemizde henüz yerli bulut depolama hizmeti verilmediği için bu madde ile birlikte kurum verilerinin yabancı menşeili bulut sağlayıcılarında tutulması engellenmiş olacaktır.

(Madde 17): " Milli güvenliği doğrudan etkileyen stratejik öneme haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak.... personellerin güvenlik ve arşiv araştırması yapılacaktır." Ülkemizin son dönemde yaşadığı özelliklede 15 Temmuz 2016 da yaşanan darbe girişiminden sonra kritik yerlerde çalışan insanların güvenilirliği daha da önemli bir hale gelmiştir. Öyle ki kritik yerlerde ki bir kişi ülke- nin kaderini etkileyebilecek bir takım hamleler yapabilmektedir. Dolayısıyla söz konusu maddenin hayata geçirilmesi çok önemlidir.

Yine bu genelge ile birlikte, Cumhurbaşkanlığı dönüşüm Ofisi'nin koordinasyonu ve kamu kurum ve kuruluşlarının katkısı ile " Bilgi ve İletişim Güvenliği Rehberi" oluşturulması hedeflenmiştir. Bu rehber ile kamu kurum ve kuruluşları ile kritik öneme haiz işletmelerin uyması zorunlu kurallar getirilmesi hedeflenmekte ve kurulacak denetim mekanizması ile her sene en az bir kere denetlenmesi amaçlanmaktadır. Söz konusu bu rehber söylemden ibaret kalmayıp hayata geçirildiği takdirde olumlu sonuçlar verecektir.

Yapılan bu çalışmalar ve düzenlemeler ile birlikte kritik altyapı tanımlamaları ve bu alanın siber güvenliğine yönelik bir takım düzenlemeler hayata geçirilmiştir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile birlikte artık ülkemiz için hangi sektörlerin kritik altyapı niteliğinde olduğu belirlenmiştir. Yine bu eylem planlarıyla birlikte siber alanda ki mevzuat çalışmaları derinleşmiş ve siber güvenlik tatbikatlarından bahsedilmiştir.

Ülkemizde yapılan siber güvenlik tatbikatları ilk başlarda doğrudan kritik altyapılarla ilişkilendirilerek yapılmasa da, 2011 yılında yapılan Ulusal Siber Güvenlik Tatbikatı ile birlikte doğrudan kritik altyapı sayılacak sektörleri içinde bulunduran tatbikatlar yapılmaya başlanmıştır. Yine, TSK Siber Savunma Komutanlığı'nın kurulması ve Siber Güvenlik Enstitüsü'nün kurulması ile birlikte kritik alanlarda ki siber savunma mekanizması güçlendirilmiştir.

SOME'lerin kurulmasıyla birlikte, kritik altyapılara yönelik yapılan siber saldırılara karşı USOM çatısı altında daha güçlü bir merkezi otorite oluşturulmaya çalışılmıştır. Kritik altyapı sektöründe de kurulan SOME'lerin birbirleri ile iletişimi artırılarak olası siber saldırılara karşı ortaklaşa önlem alınması amaçlanmıştır.

AFAD tarafından yayınlanan; 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi ile ülkemizin uzun vadede ulaşması gereken hedefler belirlenmiştir.

2014 yılında Türkiye, Sanal Ortamda İşlenen Suçlar Sözleşmesi(Budapeşte Sözleşmesi)'ni imzalayarak uluslararası alandaki ilk siber anlaşmasını imzalamış oldu. Sözleşme ile ilgili ayrıntılı bilgi aşağıda(4.Bölüm) detaylı bir şekilde anlatılmıştır.

Bölüm 5

Avrupa Birliği Ülkelerinde Kritik Altyapılara Yönelik Bilişim Suçları

5.1 Avrupa Konseyi Siber Suç Sözleşmesi ve Temel Hükümlerin İncelenmesi

Avrupa Birliği, bilişim ile ilgili suçların önlenebilmesi için birçok girişimde bulunmuş, bunlara ek olarak çocuk pornografisi ve çocuk istismarı ile mücadelede de bilişim araçlarının kullanılması ile mücadele etmeye başlamıştır [84].

Avrupa Birliği bilişim suçları ile mücadelede, bu alanda imzalanan ilk anlaşma olan Avrupa Birliği Siber Suçlar Sözleşmesi'ni 23 Kasım 2001'da, Budapeşte'de imzaya açmış ve bu sözleşme 1 Temmuz 2004'te yürürlüğe girmiştir. Avrupa Komisyonu'na dâhil olmayan ülkelere de söz hakkı tanınan bu sözleşmede, bugüne kadar 32 tanesi Avrupa Komisyonu üyesi olan toplamda 33 ülke sözleşmede taraf olmuştur [85].

Bugüne kadar toplamda 53 ülke tarafından imzalanmış olan bu sözleşme, 45 ülke tarafından yürürlüğe konmuştur. Sözleşme ülkemizde 10 Kasım 2010'da imzalanmış, sözleşme 2 Mayıs 2014'te yürürlüğe konmuştur. Sözleşme Türkçe'ye "Sanal Ortamda İşlenen Suçlar Sözleşmesi" biçiminde çevrilmiş olup, doktrinde "Avrupa Siber Suçlar Sözleşmesi" olarak yer almaktadır [86].

Sözleşmede yer alan temel amaçlara, sözleşme açıklayıcı raporunda yer verilmektedir. Buna göre, bilişim suçları (siber suçlar) ile ilgili ulusal düzeyde bulunan yasal düzenlemeler ile bağlantılı hükümlerin uyumlu bir hale getirilmesi, bilişim suçları ve elektronik delillerin bulunduğu diğer klasik suçların soruşturması ve takibi ile ilgili olarak ulusal yetkilerin ve düzenlemelerin sağlanması, ayrıca uluslararası anlamda oluşturulacak iş birliğinin hızlı ve etkili olmasına çalışılması sözleşmenin temel amaçları olarak ifade edilmektedir. Sözleşme bazı yönlerden eleştiriler de almıştır, ancak yine de bilişim suçları ile mücadelede ciddi bir ilerleme sağladığı da inkâr edilemez bir durumdur [87].

Yasal olarak büyük ölçüde bilişim suçları ile mücadelede destek sağlayan ve yol açan bu sözleşme, Avrupa Birliği tarafından bu alanda kapsamlı strateji geliştirme çalışmaları da devam ettirilmektedir. Buna ek olarak, Avrupaçapında bilişim suçlarının faillerinin takibi ve bilişim suçlarının soruşturması konusunda birtakım engeller bulunmaktadır. Yargı yetkisi, istihbaratın paylaşılması konusundaki yetersizlikler, bilişim suçlularının izlerinin sürülmesi önündeki teknik engeller, uzman personel sayısının az olması, hukuki imkânların uyumsuz olması gibi engellerdir.

Bahsi geçen bu zorlukların çözülebilmesi ve Komisyon'da iç güvenliğin sağlanabilmesi açısından Avrupa Siber Suç Merkezi kurulması şeklinde bir amaç mevcuttur. Bu amaç için bir fizibilite raporu yayımlanmış, bu raporda bu merkezin neden ve nasıl kurulması gerektiğine ilişkin çeşitli bilgilere yer verilmiştir [87]. Bu merkez ile ilgili gelişmeler bu çalışmanın temel konusu olmadığından, Avrupa Konseyi Siber Suç Sözleşmesi ile maddelerin irdelenmesi yerinde olacaktır.

Bilişim suçları, toplum için oldukça maliyetli ve hasar verici olabilmektedir. Son yıllarda hazırlananraporlar, bilişimsuçlarınedeniylemağdur olankişilerindünyagenelindeher yıl 388 milyar dolarlık bir kayıpyaşadığını, buişinuyuşturucu ticaretindençokdahakarşı bir iş olduğunu gözler önüne sermektedir. İnternet ve sanal platformların gün geçtikçe artması ile durum çok daha zararlı ve ciddi bir hal almıştır. Ekonomik bakımdan çok ciddi zararları bulunan bilişim suçlarına karşı, günümüzde güvenliğin sağlanması ve bu suçların engellenmesine yönelik birtakım çalışmalar yürütülmektedir.

5.1.1 Avrupa Konseyi Siber Suç Sözleşmesi Temel ilkeleri

Siber Suç Sözleşmesi'nin, diğer adıyla Budapeşte Sözleşmesi, temel olarak üç amaç üzerinde yoğunlaşmaktadır. Bunlardan ilki, bazı suçların tanımlamasının ortak şekilde yapılması ve bu sayede ulusal düzeyde de mevzuatın uyumlu hale getirilmesini sağlamaktır. İkincisi, bilişim suçlarının soruşturulmasında bilişim ortamında uygun olan ortak yetkilerin tanımlanması ve devletlerarasında kim uhakeme kurallarının tek bir kaleme indirilmesidir. Sonuncusu ise, hem geleneksel hem de yenilikçi işbirliği yöntemlerinin belirlenmesi, devletler tarafından bu hükümlerin en kısa zamanda uygulanmasının mümkün hale getirilmesidir. Sonuncu bahse konu olan amaç, Konsey üyeleri arasında ortak bir bakış açısı sağlanması açısından mümkün olamamıştır. Bunun temel nedeni ise bazı yetkile- rin çok fazla klasik yardımlaşma anlayışının ötesinde olduğunun, milli egemenliğe uygun olmadığının düşünülmesidir [89]. Sözleşmede dört kısım bulunmaktadır:

Birinci kısım, sözleşmede kullanılan terimlerin tanımlamasına yer verilen kısımdır.

İkinci kısım, ulusal düzeyde bilişim suçlarına karşı alınacak önlemlere yer verilmiştir. Bu bağlamda, bazı suç tipleri mad di ceza kanunu hükümlerine göre tanımlanmış, daha sonra da ceza muhakemesi hukukuna uygun olan bazı usuli yetkilere yer verilmiştir. Aynı zamanda bu kısımda, yargı yetkisi ile ilgili olarak bazı ilkelere de yer verilmektedir. Bu kısımda ele alınan suç tipleri ve bunların ceza hükümlerinin, gelecekte farklı bir biçimde ortaya çıkabilecek olan yeni bilişim teknolojilerini de kapsayıcı özelliklere sahip olduğu ifade edilmektedir.

Sözleşmenin üçüncü kısmı, ikinci kısımda bahsi geçen yetkilerin kullanımı, uluslararası alanda gerekli olan veya olacak adli yardımlaşmanın çerçevesinin çizildiği kısımdır. Bu bağlamda sözleşmeyi imzalayan ve yürürlüğe koyan ülkeler, ikinci kısımda yer alan usulle ilgili yetki ve sorumluluklara mevzuatlarında yer vermekle mükellef olup, üçüncü kısım ile de uluslararası düzeyde meydana gelen bilişim suçlarının yabancı ülkeler tarafından takip edilebilmesi için gerekli kılınmıştır. Yabancı devletlerarasında bilişim suçlarının soruşturulması ve takibinin sağlanmasında benzer yöntemlerin kullanılması, işlemlerin de kolaylaşmasını sağlayacaktır.

Dördüncü ve son kısımda ise, sözleşmenin uygulanması ile ilgili bazı teknik ve usuli hükümlere yer verilmektedir.

Sözleşme yalnızca siber suç adıyla anılan fiillerin değil, aynı zamanda "elektronik" her türlü suçu, bilişim sistemleri kullanılarak yapılan her türlü fiili ve klasik suç türlerini de kapsayıcı bir yapıya sahiptir [90]. Budapeşte Sözleşmesi'nin amaçları üç ana maddeye ayrılabilmektedir [91]. Bunlar;

- Mevzuatıulusal düzeydeuyumlu bir şekle büründürerek, suçtanımlamalarını yapmak,
- Siber alan ile ilgili suçların soruşturmasının yapılabilmesi amacıyla, uluslararası muhakeme kuralları tekil hale getirmek,
- Gerek geleneksel gerek yeni türdendevletlerarasıişbirliğiyöntemler belirleyip, bunları uygulanabilir kılmak.

5.1.2 Avrupa Konseyi Siber Suç Sözleşmesi İncelemesi

Avrupa Konseyi Siber Suç Sözleşmesi maddeleri ve bu maddelerde yer alan hükümler, sözleşmenin anlaşılabilmesi ve uygulama gerekleri ile yaptırım derecelerinin anlaşılabilmesi bakımından gerekli görülmektedir.

İlk bölümde, sözleşmede yer alan terimlere yer verilmektedir. Bilgisayar sistemi, hizmet sağlayıcı, bilgisayar verisi ve trafik bilgisi gibi tanımlamalar bu bölümde ele alınmıştır. Bu tanımlamaların amacı, ilerleyen bölümlerde bahsi geçen hükümlerin daha net olarak anlaşılabilmesi ve etkinolarakuygulanabilmesidir. Sözleşmekapsamında, ulusaldüzeyde alınması gereken önlemler ile ilgili bilgiler iki ana kısımda değerlendirilmektedir. İlk kısım "maddi ceza hukuku" ve ikinci kısım ise "usul hukuku" başlığına sahiptir. Maddi Ceza Hukuku başlığı altında, suç olarak kabul edilen ya da edilmesi gereken fiiller için ulusal düzeyde birtakım eklemeler yapılmış, bu bölümde daha çok BM ve OECD çalışmaları temel alınmıştır. Maddi ceza hukuku ile ilgili sözleşme maddeleri 2 ve 23. maddelerdir. Maddi ceza hukukunda ulusal düzeyde alınacak önlemler beş ana başlık altında verilmektedir. İlk başlık, bilgisayar sistemleri ve verilerde gizlilik, bütünlük, kullanım açıklığı gibi konularda işlenen suçları içermektedir.

İkinci, üçüncü ve dördüncü başlıklarda, bilişim ve telekomünikasyon sistemleri ile ilgili fiiller öne çıkmaktadır. İkinci başlığın temel konusu bilişim sistemleri ile gerçekleştiri-len sahtecilik, üçüncü başlığın temelkonusuise çocuk pornografisinin hukuka aykırı bir

biçimde üretimi ve dağıtımına yönelik fiillerdir. Dördüncü başlıkta telif hakları ile ilgili bilişim sistemleri kullanılarak yapılan ihlaller ön plana çıkmaktadır [92].

Gerçekleştirilen fiillerin suç olması için, haksız müdahale gerekmektedir. Bu, tüm maddelerde ortak yöndür. Eğer bilişim suçlarında meşru müdafaa ya da rıza mevcut ise artık bu fiil suç teşkil etmez. Bir fiilin suç olabilmesi için kasıtlı şekilde işlenmesi zorunludur.

Sözleşmenin "Ulusal Düzeyde Alınacak önlemler" bölümünün 2. kısmı, muhakeme üzerine hazırlanmıştır. İlk bölüme göre çok daha geniş kapsamlı olan bu kısımda usul ile ilgili bazı yetkilere yer verilmektedir. Söz gelimi saklanan bilişim verilerinin hızlı şekilde korunması, üretim talimatı, içeriklerle ilgili verilere müdahale edilmesi bunlar arasında sayılabilir. Usul ile ilgili düzenlemeler, 14 ve 21 maddeler arasında ortaya konmuş ve yargı yetkisi ile ilgili hükümler ise 22. maddede yer bulmuştur. Sözleşmede, bilgisayar veri ve sistemlerinde gizlilik, bilgisayar kullanımıyla işlenen suçlar, içerikle ilgili olan suç- lar ve telif haklarına yönelik ihlal suçları gibi konularda ki hükümlere, 2. ve 10. maddeler arasında yer verilmektedir (Convention on Cybercrime). Bu suçların detaylı incelemesi aşağıda yapılacaktır.

5.1.2.1 Bilgisayar Veri ve Sistemlerin Gizliliğine, Bütünlüğüne ve Ulaşılabilirliğine Yönelik Suçlar

Birinci kategoride yer alan suçlar sözleşmenin 2. maddesinde "hukuka aykırı erişim", 3. maddede "yasadışı müdahale", 4. maddede "verilere müdahale", 5. maddede "sisteme müdahale" ve 6. maddede "cihazların kötüye kullanılması" biçiminde sıralanmıştır

Madde içinde başlıklar halinde belirtilen suçlar, gerek bireysel gerek kurumsal anlamda tehditler barındırmaktadır. Teknolojinin hızlı gelişimi, ülkelerinde kritik altyapılarında teknolojik araçları kullanımını artırmakta ve bu teknolojik araçların güvenliğini de yine teknoloji ile sağlanmaya yöneltmektedir. Teknolojinin hızlı gelişimi ve kullanım alanının artması, kötü niyetli saldırganlarında(hacker) faaliyet alanını genişletmektedir. Olası bir saldırıda ülkeler için kritik sayılan sistemlerin işleyişine zarar verebilmekte, maddi ve manevi kayıplar yaşatmaktadırlar.

Aşağıda belirtilen başlıklarda ki suçlar bu kapsamda yer almak ve sık sık karşımıza çıkan suçlar kapsamında yer almaktadırlar.

- **Hukuka Aykırı Erişim;**

  Burada bahsi geçen terim, bilişim sistemleri ve verilerin gizliliği, güvenliği, ulaşılabilirliği ve bütünlüğü ile ilgili tehdit ve saldırılar ile ilgili olan suçları kapsar. Kritik altyapıların birçoğunun bilişim teknolojileriyle donatıldığı düşünüldüğütakdirde bu aykırı erişim büyük riskler oluşturabilmektedir. Başlı başına yasadışı olan fiiller, "hacking", "computer trespass" ve "cracking" olarak ifade edilmektedir. Bu durumların fiile dökülmesi halinde düzeltilmesi yüksek maliyet gerektirmektedir. İzinsiz ve hukuka aykırı bu fiiller, kişisel verilere, sırlara ya da istenmeyen sistem değişikliklerine yol açabilir. Buna ek olarak sahtecilik ya da yasadışı kopyalama gibi eylemler için de teşvik edici olabilir, sistemlerde telafisi güç ya da imkânsız zararlar verilebilmektedir. Burada "erişim" ifadesi ile kastedilen, bilgisayarın bir bölümüne ya da tamamına yönelik fiilleri ifade etmektedir.

  Ulusal mevzuatta hacking fiili ile ilgili çeşitli hükümlere birçok devletin Ceza Hukuku'ndarastlanmaktadır. Sözleşmedefarklıülkeleriçinalternatiflerdesunulmaktadır. Her devlet, hacking fiilini başlı başına bir suç olarak tanımlama yetkisine sahiptir (Convention on Cybercrime, m.2).

- **Yasadışı Müdahale;**

  Bu hükme, sözleşmenin 3. maddesinde yer verilmektedir. Bu madde ile verilerin iletilmesine müdahale yasaklanmıştır. Bu madde ile amaçlanan, iletişim gizliliğine müdahaleninengellenmesidir. Buhak, AvrupaİnsanHakları Konvansiyonu'ndayer alan 8. maddeye göre kutsal bir haktır. Sözleşmede yer alan 3. maddede yapılan tanımlama, veri transferinin e-posta, faks ya da telefon gibi teknolojik cihazlar ile gerçekleştirilmesine yöneliktir. Teknik yöntemlerin kullanımıyla iletişim içeriğinin hukuka aykırı biçimde dinlenmesi, izlenmesi yahut denetlenmesi, doğrudan ya da dolaylı olarak gerçekleştirilebilmektedir. Bu yöntemlereşifreler, kodlar veyazılımlar da dâhildir. Teknik yöntemlerin kullanılması, suçun kısıtlanması için eklenmiştir. Suç, aynı zamanda kişisel bilgisayarlardaki iletişimin korunmasını da kapsamaktadır. Yasadışı müdahalenin suç kapsamında değerlendirilmesi için, haksız ve kasıtlı olarak gerçekleştirilmesi gerekmektedir (Convention on Cybercrime, m.3).

- **Verilere Müdahale;**

Sözleşmenin bu hükmü, bilgisayarda yer alan verilerin ve bilgisayar programlarının bütünlüğü ve işleyişine kasıtlı olarak zarar verme eyleminin engellenmesine yöneliktir. Verilerin silinmesi, bir eşyanın fiziksel olarak imha edilmesine denktir. Bozmak ya da tahrip etmek, veri ve programlarda bütünlüğün ve işleyişine olumsuz yönde etkilenmesine neden olmaktadır. Sözleşmenin 4. maddesinde, verilerin saklanmasını sağlayan bilgisayar ya da bilişim sistemlerine erişim olanağı bulunan ancak hakkı bulunmayan kişilerin erişiminin engellenmesi üzerine hükümler yer almaktadır. Bu madde kapsamında aynı zamanda kötü amaçla virüslerin ya da bazı programların sisteme sokulması da kastedilmektedir. Bu fiillerin haksız ve kasıtlı olarak gerçekleştirilmesi halinde ceza hükümleri uygulanmaktadır (Convention on Cybercrime, m.4).

- **Sisteme Müdahale;**

  Bu fiil, "bilgisayar sabotajı" olarak da ifade edilmektedir. Bu maddede yer alan hükümlere göre, bir bilgisayar sisteminin yasal olan kullanım hakkının kasıtlı şekilde engellenmesi suç olarak kabul edilmiştir. Bu engelleme fiili kısmen ya da tamamen olabilir. Ancak engelleme ciddi boyutlarda olmalıdır, fiilin ciddiyet durumuna ise bazı ölçütler sonucunda taraflarca karar verilir.

  Söz gelimi, istenmeyen reklame-postalarının gönderimi, alıcıyı rahatsız edebilir. Bu fiil bu nedenle suç kapsamına girebilmelidir. Bu maddede dikkat edilmesi gereken, fiilin tamamen kasıtlı olarak yapılmasıdır (Convention on Cybercrime, m.5).

- **Cihazların Kötüye Kullanımı;**

  Bu kategorideki son madde yani madde 6'da, ikinci ve beşinci maddelerdeki fiillerin işlenmesinde gereken hazırlık evresini kapsar. Bu maddede istenen, her devletin bilişim sistemlerinin çeşitli bilişim suçları için kullanılabilir durumda olup olmadığının incelenmesidir. Mevcut suçlarda cihazın kötüye kullanımı söz konusu ise cezai yaptırım uygulanmalıdır (Convention on Cybercrime, m.6).

5.1.2.2 Bilgisayarla İlgili Suçlar

Bu bölüm, sözleşmede yer alan 7. ve 10. maddeler arasındaki bölümdür. Genel olarak bilgisayar sistemi kullanılmak suretiyle işlenen suçlar bu bölümde ele alınmıştır. Birçok

ülkede bilgisayarla işlenen suçlar klasik suçlardan ibarettir ve bu sözüedilen ülkelerin bilgisayarla ilgili mevzuatları yeterince geniş kapsamlı olmayabilir. Aynı şekilde bilgisayar sistemleri bu ülkelerde suç işlenebilecek yeterlilikte de olmayabilir. Bu ülkelerin, suç fiillerine bilgisayar sistemlerinin uygun olup olmadığını denetlemeleri gerekir. Bu bölümdeki maddelerin kapsamı şöyle ifade edilebilir:

- **Bilgisayarla İlişkili Sahtecilik;**

  Sözleşmenin 7. maddesi, somut olarak belgede sahtecilik fiili işlenmesinin bir suç olarak kabul edilmesini ve böylece bu konuda hukuki boşlukların giderilmesini amaçlamaktadır. Burada bahsedilen belgeler, yasal olan kamu belgeleri ve kişisel belgeler ile verilerdir. Verilerin bir şekilde izinsiz olarak çoğaltılması, bu belgeler üzerinde kısmen ya da tamamen değişiklik yapılması, erişilmez kılma hakkının saklanmasının engellenmesi ya da sabote edilmesi türünden fiilleri kapsamaktadır. Söz gelimi bir belgenin hukuki olarak delil olarak değiştirilmesi ya da yeni veriler oluşturularak hukukun yanıltılması bu suç kapsamında değerlendirilir (Convention on Cybercrime,m.7).

  Aynı şekilde madde 8'de, bir kişinin sahtekârlık ile kendisine ya da üçüncü bir kişiye menfaat sağlaması, bunu verilerde değişiklik, yenilik ya da eksiltme yöntemlerini kullanarak sağlaması, bunun için de bilgisayara bir müdahale söz konusu olması suç kapsamında değerlendirilmektedir. Teknolojininilerlemesi ile birlikte, suç fi- illerini gerçekleştiren kişilerin suç alanlarında bir artış ortaya çıkmıştır. Kredi ve banka kartlarının sahte olarak kullanılması, kişilerin bu bakımdan çeşitli yöntem- lerle mağdur edilmesi, verilere bir şekilde müdahale edilmesi buna örnek gösterile- bilir. Bilgisayarlarla yapılan sahtekârlık sonucunda mağdur olan kişi maddi olarak bir zarar yaşamış ise ve bu suçu işleyen kişi bu fiilden maddi bir kazanç elde etmiş ise, bu maddeye göre suç işlemiştir (Convention on Cybercrime, m.8).

  Bilgisayarla ilgili suçlar kapsamında ele alınan 9. ve 10. maddeler ise çocuk pornografisi üzerine düzenlenmiştir. Bu bölümdeki suçlar sözleşmede "Content - Related Offences" adı altında belirtilmiştir, "İçerikle İlgili Suçlar" şeklinde ifade edilebilir. Burada bahsedilen suçlar, çocukpornografisi ile ilgili olanlardır.

5.1.2.3 Suç Kapsamındaki Diğer Fiiller

- **İştirak ve Teşebbüs**

  Sözleşmede yer alan 11. maddeye göre, yukarıda bahsi geçen suçlar ile birlikte, bu suçlara teşebbüste yardım, yataklık etmek fiilleri de suç kapsamına alınması gereken fiiller olarak ifade edilmiştir. Bu maddenin ilk paragrafında, sözleşmeyi kabul eden devletlerden, bir suçun işlenmesinde yardım ve yataklık fiillerinin de suç kabul edilmesi talep edilmektedir. Bilişim sistemlerinde suç fiillerinin gerçekleştirilmesi için hizmet sağlayıcılarınkullanımıbumadde içinörnekolarak gösterilebilir.

  Aynı maddenin bir sonraki paragrafında, bazı suç ve suç unsurlarına teşebbüs edilmesinin kavramsal bakımdan bazı zorluklar doğuracağı üzerinde durulmaktadır. Taraflar, teşebbüsle ilgili sözleşme hükümlerini kısmen uygulayabilir ya da hiç uygulamayabilir (Convention on Cybercrime, m.11).

- **Kurumsal Yükümlülük**

  12. maddede tüzel kişilerin yükümlülüklerine değinilmiştir. Bu tüzel kişiler kurum, dernek ya da benzeri kişilerdir ve bunlar da işlenen suç ile ilgili ceza alabilir. Tüzel kişilerin bu kapsamda ceza almasını gerektiren dört ana durum söz konusudur:

- Sözleşmede tanımlanan suçlardan bir tanesinin işlenmesi
- İşlenen fiilintüzel bir kişiye menfaatsağlaması
- Yönetici konumundabulunanbir kişininsuçfiili işlemesi
- Yönetici konumunda bulunan bir gerçek kişinin bir yetkinin arkasına sığınarak bu fiili işlemiş olması

  Buna ek olarak, gerçek bir yöneticinin değil de bu yöneticiden daha alt bir rütbede yer alan bir başka gerçek kişinin suç fiilini işlemesi halinde yine de cezai yaptırım gerekmektedir. Tüzel kişilikte yer alan bir çalışanın suç işlemesi, işlenen bu suçun tüzel kişinin menfaatine olması, suçun işlenmesi halinde yönetici ya da bir başka gerçek çalışanın görevini yapmamış olması halinde, yükümlülük doğar (Convention on Cybercrime,m.12).

- **Yaptırım ve Önlemler**

  Sözleşmede yer alan 13. madde, 2. ve 11. maddeler arasında yer alan maddeler ile doğrudan bağlantılıdır. Bu maddede yer alan hükme göre, bahsi geçen suçlar ile

ilgili caydırıcı kararlar alınması ve gerçek kişiler söz konusu ise hapis cezası da içeren hükümlerin uygulanması şarttır. Aynı şekilde 12. maddede yer alan tüzel kişiliklerin suç fiilleri için verilen cezalar da caydırıcı olmak durumundadır (Convention on Cybercrime, m.13).

Avrupa Konseyi Siber Suçlar Sözleşmesi'ni öne çıkaran en ayırt edici özellik, uluslararası platformda bilişim suçları için ortak bir yaklaşım benimsemesidir. Suçu gerçekleştiren gerçek ve tüzel kişilerin belirlenmesinde, taraf ülkeler arasında ortak bir bakış açısı ve cezai yaptırım sağlanması ve verilerin hızlı bir şekilde korunması konusu oldukça önemlidir.

Bu noktada dünya genelinde ve Avrupa Birliği üyesi devletlerin ülke yasalarında bilişim suçları ile ilgili önlem ve yaptırımlar da son derece önemlidir. Karşılaştırmalı bir bakış açısı kazanılması bakımından, birkaç ülkenin bilişim suçları ve bu suçlara karşı kullandıkları yasalara ilişkin aşağıda bilgi verilmektedir.

5.2 Avrupa Birliği Siber Güvenlik Kanunu

Avrupa Birliği Parlamentosu tarafından 11 Mart 2019 tarihinde onaylandı ve 7 Haziran 2019 tarihinde AB resmi gazetesinde yayımlanarak 27 Haziranda yürürlüğe girmiştir [93].

Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Union Agency for Network and Information Security-ENISA) bu kanunla yeni yetki ve görevlerle donatılmıştır. Kanun, gerek tüketici cihazlarının gerek çevrimiçi alınan hizmetlerin siber alanda güvenliğini artıra-rak, AB çerçevesinde siber güvenlik sertifikası oluşturmaktadır. Güçlü bir siber güvenlik mekanizması oluşturmak ve siber saldırılarla daha etkin bir şekilde mücadele etmek için önlemler içermektedir. Kanunun konumuz ile ilgili madde içeriğini aşağıdaki şekilde toparlayabiliriz[94].

- 2020 yılında sona erecek olan ENISA'ya kalıcı görev verilmesi, daha etkin bir şekilde siber saldırılara karşı konulması için üye ülkelerin yeni siber güvenlik sertifikasyonu çerçevesinde işbirliği ve koordinasyon sağlanması,
- ENISA, işletmelerin ve vatandaşların üst düzeyde bilinçlendirilmesi, AB üye ülkelerine ve AB kurumlarına politika geliştirmede ve uygulamalarında yardımcı olma ve

AB seviyesinde siber güvenlik kapasitesinin geliştirilerek imkânların artırılmasını sağlama görevi verilmiştir.

- Kanun, AB genelinde kabul gören hizmetlere, işlemlere ve ürünlere ilişkin Avrupa Siber Güvenlik Sertifikaları içinde bir çerçeve niteliğindedir. Hizmet, işlem ve ürünlerin sertifikasyonuna yönelik alınan kararlar, insanların bu alanda yapacakları işlere ya da işlemlere güvenmeleri konusunda olumlu etki yaratacaktır. Tek bir noktadan sağlanacak olan siber güvenlik sertifikası, hem sertifika almak isteyen işletmelere kolaylık sağlayacaktır hem de maliyet açısından olumlu etki yaratacaktır.

5.3 Bazı Dünya Ülkelerinde Bilişim/Siber Suçlarının ve Cezaların İncelenmesi

Bilişim sektörünün yaygınlaşması ve bu sektör ile beraber siber saldırıların artması ülkeleri bir takım yasal düzenlemeler yapmaya zorlamıştır. Kimi ülkeler kanunlarında doğrudan bilişim başlığı altında düzenlemeler yaparken kimi ülkeler de mevcut kanunlar üzerinden bilişim suçlarını yorumlamaya çalışmıştır. Örneğin, sisteme izinsiz girişi mahremiyet ihlali üzerinden, sistemden veri çalınması nı hırsızlık üzerinden ve sistemi bozmayı mala zarar verme suçundan hareketle yorumlayarak cezalar belirlenmiştir.

Bilişim sektörünün çok büyük boyutlarda olduğu ve siber saldırıların çok yaygınlaştığı günümüzde, mevcut yasalardan hareketle bu suçların tanımlanması yeterli kalmayacak ve eksiklikler doğuracaktır. Çünkü normal hayatta ki bir hırsızlık durumunda sonuçlar bellidir. Mal izinsiz alınmıştır ve sonucu bellidir. Lakin siber saldırı yöntemiyle elde edilen bir verinin sonuçlarının ne derece etkili olacağını tam manasıyla belirleyebilmek mümkün olmayacaktır ve normal hırsızlık suçu gibi işlem yapılması yeterli olmayabilecektir. Bu yüzden bilişim alanında ki suçlar için ayrı ve detaylı yasalar yapılarak hayata geçirilmesi önem arz etmektedir.

Bazı dünya ülkelerinin bu alanlarda ki mevcut durumları aşağıda açıklanmıştır. Bunlar;

5.3.1 Almanya

Almanya Ceza Hukuku dâhilinde, bilişim/siber suçlarına yönelik ayrıca bir kanun düzenlemesi bulunmamaktadır. Fiiller, mevcut suçlar üzerinden değerlendirilmektedir. Alman Ceza Kanunu 202/a Maddesi, verilerin depolandığı veya işlendiği bilişim ağlarına izin-siz şekilde girilerek, verilerin ele geçirilmesi suç kapsamında değerlendirilmekte olup, bu suçlar bilgisayar sistemlerinde yer alan verilere yönelik olduğu için "sır aleyhine işlenen suçlar" başlığı altında değerlendirilmektedir. Alman Ceza Kanunu'nda, bilişim sistemlerine izinsiz giriş yapılması bir suç olarak kabul edilmemektedir. Suç olarak değerlendirilmesi için verilere müdahale edilmesi, zarar verilmesi ya da verilerin ele geçirilmesi gerekmektedir. Yani fiil, ikinci ve üçüncü kişilerin lehine bir durum oluşturduğu zaman suç kapsamında değerlendirilmektedir.

Alman Ceza Kanunu'nun da internet-bilgisayar suçları alanında düzenlenmiş 11/3, 176, 176a, 184, 202a, 263a, 269, 271, 274/2, 303a, 303b, 303c özel maddeleri bulunmaktadır. Alman Ceza Kanunu'nda, bilgisayar sistemlerine izinsiz giriş yapılması nın bir suç oluşumu için yeterli görmemektedir. Suç oluşumu için verilerin ele geçirilmesi şartını da aramaktadır. Avrupa Konseyi Siber Suç Sözleşmesinin 2. maddesinde "yasadışı erişim" in suç olarak kabul edildiği göz önüne alındığında Alman Hukuku'nun bu yönüyle çeliştiği görülmektedir.

Almanya, 1997 yılında kabul edilen "Teleservisler Kanunu" ile internet yayınlarından kaynaklanan ceza sorumluluğunun şekil ve esasları belirlenmiştir. Kanuna göre internette bulunan içeriğin suç unsuru bulundurması durumunda içerik sağlayıcı, genel hükümlere göre sorumlu olarak kabul edilmektedir[95].

Buna ek olarak Haksız Rekabet Kanunu, Fikri Haklar Kanunu, Verilerin Korunması Hakkında Kanun, Telekomünikasyon Müşterilerin Korunmasına İlişkin Tüzük de bilişim suçlarıyla ilgili hükümler barındırmaktadır[96].

Alman Ceza Kanunu 269 ve 279'uncu maddelerde, bilişim sistemleri kullanılarak gerçekleştirilen sahtekârlık ve dolandırıcılık fiilleri ile ilgili hükümler bulunmaktadır. Bu maddelerde, bir suçun sahtekârlık kapsamında değerlendirilmesi için hukukça hükmü haiz kılınan bir verinin yahut belgenin bilişim sistemleri kullanılarak sahte şekilde düzenlenmesi veya bu belge ya da veriye zarar verilmesi yeterli olmaktadır.

5.3.2 Fransa

Fransa Ceza Hukuku'nda da internet ile ilgili işlenen suçlara ait özel bir yasa bulunmamaktadır. Ceza Hukuku kapsamında internet ile ilgili suç teşkil eden fiilleri de kapsayan geniş kapsamlı bazı hükümlere yer verilmektedir. Söz gelimi, pornografik öğelerin küçük çocuklara yönelik olmadığı sürece suç olarak görülmemesi gerektiği, Ceza Hukuku'nun 227 ve 224. maddelerinde küçüklerin erişimine bahsi geçen öğelerin erişiminin sağlanması bir suç olarak kabul edilmektedir[97].

Fransız Ceza Hukuku'nda bu alanın yetersiz kaldığı ya da net olmadığı gibi eleştiriler üzerine yeni bir kanun düzenlemesi 1 Ağustos 2000 tarihinde yürürlüğe girmiştir. Bu kanunla birlikte iletişim özgürlüğüne yönelik maddelere "Link üzerinde özel Haberleşme Dışındaki İletişim Servisleri İle İlgili Hükümler" adı altında yeni bir başlık eklenmiştir[98].

Fransa Ceza Hukuku'nda, suç içerikli yayınların yapılması halinde, genel hükümlerin geçerli olacağı belirtilmektedir. Özellikle suç içerikli yayınların hazırlanmasında ve yayınlanmasında etkisi ve desteği bulunan kişiler için de sorumlu oldukları ve ceza alacakları vurgulanmaktadır. Erişim sağlayıcılar için bir ceza bulunmaması ise dikkat çekicidir. Buradaki bakış açısıyla, erişim sağlayıcıların suçun işlenmesine bir katkısı olmadığı, bu kişi ya da kişilerin yalnızca taşıyıcı oldukları için suça dâhil olmadıkları sonucu çıkmaktadır [99].

5.3.3 İngiltere

İngiltere'de bilişim/siber suçlarına yönelik özel kanunlar düzenlenmiştir. Bu durum Amerika Birleşik Devletleri, Portekiz ve İrlanda'da da bu şekildedir. İngiltere hükümeti, 29 Temmuz 1990 tarihinde bilişim suçları ile ilgili olarak "Computer Misuse Act" adı altında bir kanunu yürürlüğe koymuştur. Bu kanunda temel amaç, bilgisayar ve bilişim sistemlerine izinsiz olarak müdahalenin ya da değişikliklerin önlenebilmesidir. Bu kanun dâhilinde, üç ana suç tipi belirlenmiştir:

- Bilişim cihazlarına, programlara ve verilere yetkisiz olarak girilmesi
- Bir başka suçun işlenmesi için yol açmak, bu suçu kolaylaştırmak gibi amaçlarla bilişim cihazlarına yetkisiz olarak girilmesi
- Yine yetkisiz bir şekilde bir bilgisayarın içeriğinde değişiklikler yapılmasıdır [100].

5.3.4 Japonya

Japonya bilişimsistemleri ileilgili suçları veuygulamaları teknolojik gelişmelerindeetkisi ile çok erken fark etmiş, bunlara yönelik önlemleri de zaman içinde almıştır. Yasa ile ilgili düzenlemelerin yapılmasından hemen önce bilişim sistemleri ile ilgili olarak kanunda yapılacak düzenlemeler üzerinde detaylı tartışmalar ve fikir alış verişleri gerçekleştirilmiştir. Sonuç olarak "Ceza Hukuku Alanında Bazı Hükümlerde Değişiklik Yapılmasına İlişkin Kanun" 22 Haziran 1987 tarihinde yürürlüğe girmiş, bu kapsamda da kanuna yeni suç türleri ile ilgili eklemeler yapılmıştır. Buna ek olarak bilgisayar ağları ile işlenen suçlar için de detaylı bir düzenleme olan "Bilgisayarlara Yetkisiz Erişim Kanunu", 3 Şubat 2000 tarihinde yürürlüğe girmiştir[101].

Japonya mevzuatında, bir bilişim sistemine izinsiz olarak giriş yapılması, bu girişte sağlanan veriler ya da bilgiler satılmadığı ya da bozulmadığı sürece suç teşkil etmemektedir[102].

5.3.5 ABD

Ülkelerin gelişmişlik düzeyleri aynı zamanda birtakım konularla ilgili hızlı düzenlemeler yapma ve bu düzenlemeleri hayata geçirme ile de doğrudan alakalıdır. Gerek birçok teknolojide, gerek internet alanında ABD ilklerin ülkesi sayılmaktadır. Nihayetinde bilişim alanında ki düzenlemeler yapma tarihi de bu bahisle doğrudan ilişkilidir.

1984 yılında, " Bilgisayar sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Kanunu" nu çıkararak bilişim alanında ki ilk kanunsal düzenlemeyi hayata sokmuştur. "1986 yı- lında Elektronik Haberleşme Gizliliği Yasası" nı ve 1998 de çocukları internet ortamında koruyacak yasalar çıkarmıştır[103].

1992 yılında çıkarılan,"Bilgi ve Teknoloji Kanunu" ve peşinden "Ulusal Bilgi Altyapısı Kanunu" ile bilişim teknolojileri alanında ki düzenlemelere yenileri eklenmiştir [104].

ABD Federal Kanunları ile de birçok düzenleme yapılmıştır. 18 numaralı ve " Suçlar ve Ceza Muhakemesi" başlığı altında aşağıda kisuçlar düzenlenmiştir. Bunlar; [105]

- Erişim cihazlarıyla yapılan dolandırıcılık
- Bilgisayar yoluyla dolandırıcılık

- İletişimhat, istasyon vesistemlerinin korunması,
- Kablolu, elektronik ve sözlü iletişimin engellenmesi,
- Kablolu ve elektronik İletişimin kaydı ve kayıterişimi,
- Arama, adresleme, yönlendirme ve sinyal kaydı.

Maddelerden de anlaşılacağı üzere ABD, suçun türüne göre göre farklı farklı kanunlar düzenlemiştir.

Bölüm 6

İstatistiki Veriler

Bilişim teknolojisinin gelişmesiyle birlikte suç dünyasında kullanımı da artmaktadır. İşlenen suçlar, hayatta var olan nesnelere göre çeşitlilik kazanır. Hızlı bir şekilde gelişen teknoloji de suç dünyasında kendine yeni bir kapı aralayarak ve suç dünyasında bilişim suçlarının işlenmesine imkân tanımaktadır.

Ülkeler ise bu gibi suçlarla mücadele etmek için ve var olan tedbirlerle ne kadar etkili olduğunu görmek için bu suç kavramlarıyla ilgili istatistiki bilgiler toplamaktadırlar. Gerek kamu eliyle gerek özel sektör eliyle bu verileri elde etmeye çalışır. Kısacası önünü görmek için bilgi toplar, aksi halde kısa vadede pek belirgin olmayan bu suçlar uzun vadede çok büyük sorunlara sebebiyet verebilmektedir.

6.1 Ülkemizin Hukuki Açısından İstatistiki Veriler

Adli suçlarla ilgili olarak ülkemizde, dava açılması ve karara bağlanması ile ilgili istatistikler tutulmaktadır. Adalet Bakanlığı altında kurulmuş olan Adli Sicil ve İstatistik Genel Müdürlüğü bu konular hakkında veri toplar ve her yıl istatistiksel raporlar yayınlamaktadır. Son birkaç yılın istatistiki verilerine bakacak olursak eğer Bunlar; [106]

Tablo 6.1: TCK 'ya Göre Şüpheli Kişiler Hakkında Verilen Kararlar, TÜRKİYE (2017)

		KARAR TÜRÜ					
YIL	İsnad Edilen Suç Türü	TCK Madde No	Kovuşturmaya Yer Olmadığı Kararı Verilen	Kamu Davası Açılan	Diğer Kararlar	Toplam	Yüzdelik Dilim (%)
2017	Bilişim Alanındaki Suçlar	243-246	36.538	20.631	42.378	99.547	1,50
	TCK Toplamı		**3.466.942**	**2.141.895**	**922.346**	**6.531.183**	**100,00**
2016	Bilişim Alanındaki Suçlar	243-246	34.772	25.170	32.766	92.708	1,60
	TCK Toplamı		**2.840.243**	**2.310.431**	**804.151**	**5.954.825**	**100,00**

Son iki yılın rakamlarına bakıldığı zaman, toplam suçlar içinde bilişim suçlarının oranı düşmüş olsa da işlenen suçun miktar bazında arttığı görülmektedir. Bir takım önlem- ler alınsa da bu artış teknolojinin yaygınlaşması ve bilinçsiz tüketicilerin artmasıyla ile birlikte devam edecektir.

Tablo 6.2: TCK 'ya Göre Açılan Davalardaki Suç Dağılımları, TÜRKİYE (2017)

				Sanık Sayısı								
				Gerçek Kişi								
				T.C. Uyruklu						Yabancı Uyruklu		
				12-15 Yaş		15-18 Yaş		18 ve Üzeri Yaş				
YIL	İsnad Edilen Suç Türü	TCK Madde No	Açılan Davalardaki Suç Sayısı	E	K	E	K	E	K	E	K	Diğer
2017	Bilişim Alanındaki Suçlar	243-246	31.790	902	34	818	64	24.594	4.833	463	42	40
	TCK Toplamı		**2.321.788**	**70.733**	**6.761**	**100.526**	**7.344**	**1.865.405**	**223.041**	**38.688**	**7.946**	**1.344**
2016	Bilişim Alanındaki Suçlar	243-246	34.011	941	23	890	66	26.791	4.871	319	53	57
	TCK Toplamı		**2.304.512**	**78.612**	**9.227**	**110.273**	**10.656**	**1.811.739**	**245.488**	**30.822**	**6.176**	**1.519**
2015	Bilişim Alanındaki Suçlar	243-246	24.314	451	44	495	40	20.722	1.091	571	19	71
	TCK Toplamı		**2.683.676**	**101.489**	**12.691**	**139.090**	**12.620**	**2.100.808**	**278.343**	**29.469**	**6.490**	**2.676**

Son üç yılın verilerinden oluşan tablo incelendiği zaman, tabloda ilk göze çarpan muhakkak ki suç işleme miktarlarında kadın erkek arasında ki anormal farktır.

Tablo 6.3: TCK 'ya Göre Verilen Karar Dağılımları, TÜRKİYE (2017)

YIL	İsnad Edilen Suç Türü	KARAR TÜRÜ					
		TCK Madde	Mahkumiyet	Beraat	Diğer Kararlar	Toplam	Yüzdelik Dilim (%)
2017	Bilişim Alanındaki Suçlar	243-246	16.006	5.136	19.182	40.324	1,5
	TCK Toplamı		**1.156.465**	**467.464**	**1.072.028**	**2.695.957**	**100,00**
2016	Bilişim Alanındaki Suçlar	243-246	14.941	4.886	9.019	28.846	1,1
	TCK Toplamı		**1.138.452**	**562.570**	**1.034.558**	**2.735.580**	**100,00**
2015	Bilişim Alanındaki Suçlar	243-246	14.319	4.765	6.758	25.842	0,8
	TCK Toplamı		**1.186.223**	**686.398**	**1.306.730**	**3.179.351**	**100,00**

Tabloya bakıldığında yine suç oranlarının arttığı görülmektedir. Dikkat çeken bir diğer nokta ise verilen kararlarda "diğer kararlar" başlığı altında ki kararların çokluğu dikkat çekmektedir.

Diğer kararlar; yetkisizlik, birleştirme, görevsizlik, hükmün açıklanmasının geriye bırakılması başlıklarını kapsamaktadır. Diğer kararların çok olmasının sebebi ise, bilişim suçları alanının yeni sayılabilecek bir suç alanı olması sebebinden dolayı hukuki olarak hangi mercilerle ilgili olduğunun halk tarafından tam olarak bilinememesidir.

6.2 Dünya Ülkeleri Açısından

Ülkemizde olduğu gibi dünya ülkelerinde de bu alanla ilgili istatistiki veri ve raporlama çalışmaları yapılmaktadır. Gelişmiş ülkelerde bu işlemler daha sağlıklı bir şekilde işlenip raporlanırken gelişmemiş ülkelerde ya bu raporlama işlemleri yapılmaz ya da sağlıksız bir şekilde işlemektedir.

Ülkelerin bu alanda veri toplarken sadece önünü görme amaçlı yapmaz aynı zamanda bu eylemlerin maliyetini çıkarıp ona göre de tedbirlerini almak ya da iyileştirmek istemektedirler.

Dünya da bilişim ile ilgili suç alanlarında bilgilerin toplanıp, derlenip sunulduğu ve bu suçlarda hangi metotların kullanıldığı ile ilgili bilgileri, Computer Security Institute-CSI (Bilgi Güvenliği Enstitüsü) yapmaktadır. Bu alanda en geniş çaplı organizasyon sahibi

olduğu kabul görmektedir ve her yıl konferans düzenleyerek bu alanda hizmet veren firmalarla bilgi paylaşımı yapmaktadır.

- Bilgi Güvenliği Enstitüsü (CSI) tarafından 2010 yılında yapılan araştırmalara[107] göre, bilişim teknolojisinin 2005-2010 yılları arasında işlenen bilişim suçlarında en çok hangi metotları kullandığı kategorize edilmiştir.

Tablo 6.4: Bilişim Teknolojilerinin Suç İşlenmesinde Kullanma Metotları

Atak Tipleri	2005	2006	2007	2008	2009	2010
Zararlı Yazılım Kullanılması	74%	65%	52%	50%	64%	67%
Yemleme			36%	31%	34%	39%
Laptop/ Taşınabilir Cihaz Hırsızlığı	48%	47%	50%	42%	42%	34%
Kurum İçi Zombi(Köle) Bilgisayarlar			21%	20%	23%	29%
Web Kaynaklarına Ya da E-Posta Hesaplarına Kurum İçinden Erişim	48%	42%	59%	44%	30%	25%
Servis Dışı Bırakma	32%	25%	25%	21%	29%	17%
Kurum İçi Saldırılar					15%	13%
Şifre Çalma			10%	9%	17%	12%
Kurum Dışından Sistem Zaafiyetlerini Tarama					14%	11%
Web Gezginlerini İstismar					11%	10%
Dolandırıcılık	7%	9%	12%	12%	20%	9%
Halka Açık Web Sitelerinin İstismarı					6%	7%
Web Sitesi Ekleme	5%	6%	10%	6%	14%	7%
Kablosuz Ağların İstismar Edilmesi	16%	14%	17%	14%	8%	7%
Sosyal Ağları İstismar (Facebook, Instagram,...)					7%	5%
Anında Mesajlaşmayı İstismar			25%	21%	8%	5%
Mobil Cihazların Çalınarak Kişisel Verilerin Çalınması ya da İllegal erişim				8%	6%	5%
Mobil Cihazların Çalınarak Fikri Mülkiyet Haklarının İhlal Edilmesi				4%	6%	5%
Çalınan Veri İle Şantaj					3%	1%
Diğer İllegal Erişim ve Hak İhlalleri				13%	18%	16%

Zararlıyazılımlarlaişlenenbilişimsuçlarıoransal bazda enyüksekolduğugözükmektedir. Buyöntem, yeterli bilgisi olmayan ya da dikkatli olmayan bir mağdura zarar vermek için kullanılabilecek en sağlam yöntemlerdendir. Fark edilmesi zor olduğundan dolayı saldırganlartarafındançokçatercihsebebi olmaktadır.

- Saldırılar çok çeşitli şekilde gerçekleştiğinden dolayı yapılan istatistiki çalışmalarda çeşitlenmiştir. Bu alanda yapılan suç nitelikli saldırılar genelde maddi düşünce hareketli olduğu için saldırganlardasaldırılannoktanınmaddi büyüklüğünü ya dabilişimsaldırıları konusunda aldıkları önlemleri dikkate alarak saldırı planları yapabilmektedirler. Örneğin;

2017 yılında yapılan, endüstri ve organizasyon büyüklüğüyle ilgili bilişim saldırılarını incelendiğinde aşağıda ki tabloda ki veriler elde edilmiştir [108].

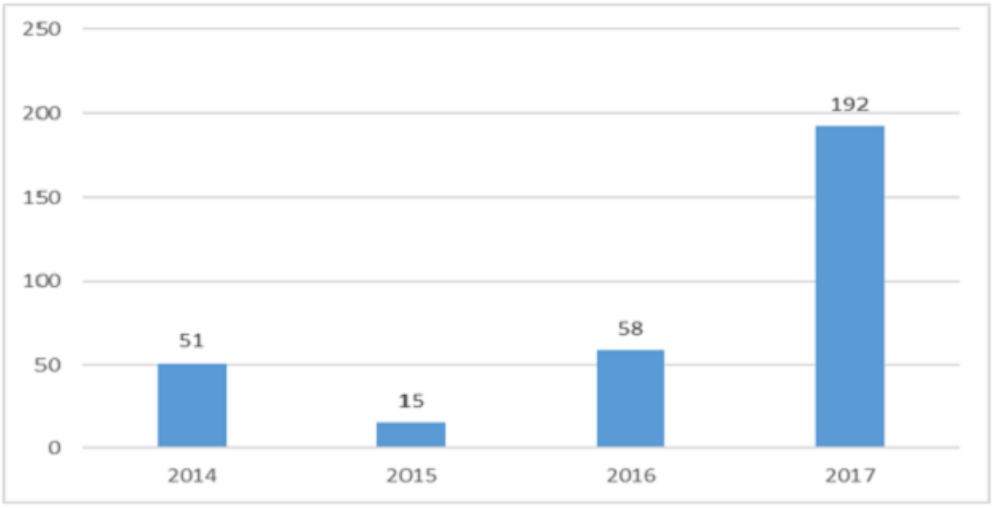
Tablo 6.5: 2017 yılı Küresel Siber Güvenlik Olay Sayısı

	Büyük	Küçük	Belirsiz	Toplam
Konaklama	40	296	32	368
İdari	7	15	11	33
Tarım	1	0	4	5
İnşaat	2	11	10	23
Eğitim	42	26	224	292
Eğlence	6	19	7.163	7.188
Maliye	74	74	450	598
Sağlık hizmeti	165	152	433	750
Bilgi	54	76	910	1.040
Yönetim	1	0	1	2
İmalat	375	21	140	536
Madencilik	3	3	20	26
Diğer servisler	5	11	46	62

Saldırılar, konaklama sektöründe ağırlıklı olarak küçük sektörlere, imalatta ise büyük sektörlere karşıgerçekleşmiştir. Eğlence sektöründe ki saldırıların ağırlığı ise büyüklük ya da küçüklük durumu belirlenemeyen sektörlere karşı yapılmıştır.

Tabloda ki sektörlerin önemli bir kısmı ülkelerin kritik altyapı olarak nitelendirdikleri sektörleri barındırmaktadır. Özellikle, sağlık, bilgi ve maliye alanında ki saldırıların çokluğu, kritik altyapılara olan saldırıların yüksek oranda olduğunu göstermektedir.

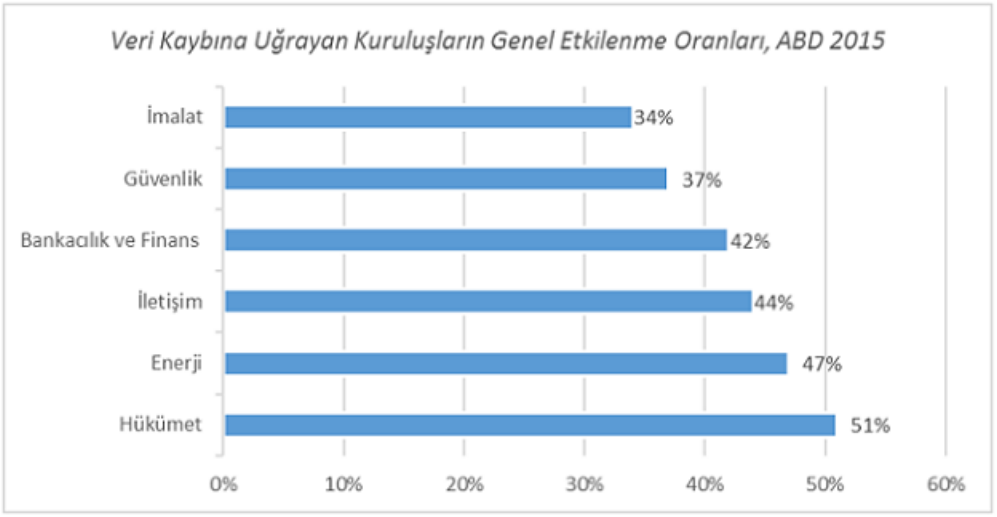
- AB ülkeleri için kritik altyapı niteliği taşıyan bankacılık(maliye) sektörünün en önemli parçalarından olan ATM'lere yönelik 2014-2017 yıllarını kapsayan siber saldırılarla ilgili yapılan bir araştırmada ise aşağıda ki veriler elde edilmiştir [109].



Şekil 6.1: AB Ülkelerinde ATM'lere Yapılan Siber Saldırılar

Bu istatistik 2014'ten 2017'e kadar Avrupa Ülkelerinde ATM'lere yapılmış olan kötü amaçlı siber saldırıları göstermektedir. İnsanların üzerlerinde nakit taşıma oranının azaldığı ve kartlı sisteme dayalı ekonominin yaygınlaştığı günümüzde, ATM'ler insan hayatı içinde önemli bir yer edinmeye başlamıştır. Bu önemlilik beraberinde riskleri de getirmektedir. ATM'lere yönelik doğrudan yapılan siber saldırı sayısının 2014'te 51 vakadan, 2017 de ise 192 vakaya çıktığı görülmektedir. Her ne kadar önlemler alınsa da saldırı- lar artarak devam etmektedir. Şekilden de anlaşılacağı üzere alınan önlemlerin yeterli olmamaktadır.

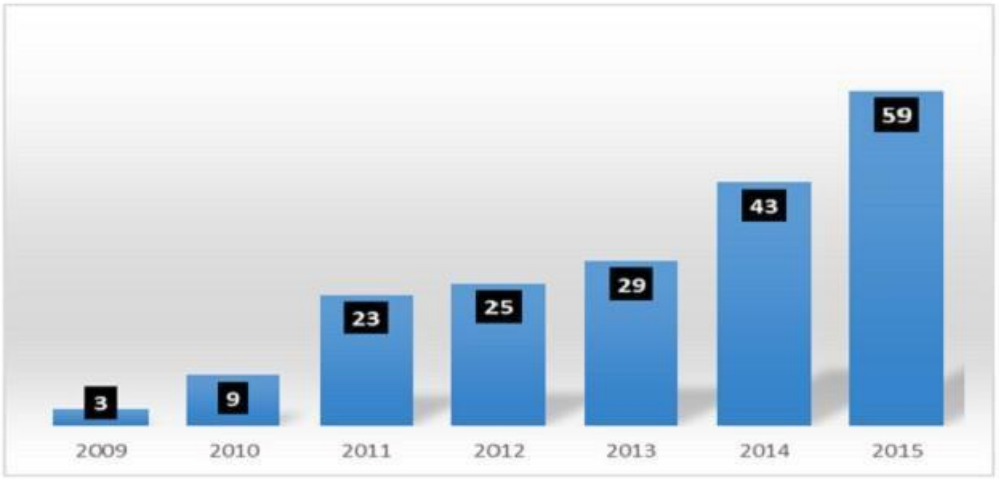
- Siber saldırılar sonucu büyük bir veri kaybı da yaşanmaktadır. Ne kadar veri kaybı olduğunu göstermek adına ABD özelinde 2015 yılına ait aşağıda ki rapor sonucu yayınlanmıştır [110].



Şekil 6.2: Yapısal Organizasyona Göre Veri Kaybı Sonucu Etkilenme Oranları

Grafikte de görüldüğü gibi Hükümet Organizasyonunun hemen ardından Enerji ve İletişim Sektörü alanında veri kaybının çok yüksek olduğu gözükmektedir. Bu da aslında yapılan saldırıların kritik altyapılara yapılmaya başlandığının kanıtı niteliğindedir.

- Teknolojinin gelişimine paralel olarak kritik altyapı niteliğinde ki bilgi teknolojileri alanına da siber saldırı sayısı artmıştır. Aşağıda ki grafikte 2009 yılından 2015 yılına kadar ki dünya genelinde ki tüm bilişim teknolojilerine yönelik yapılan siber saldırı sayısı ile ilgili istatistiki veri paylaşılmıştır [111].

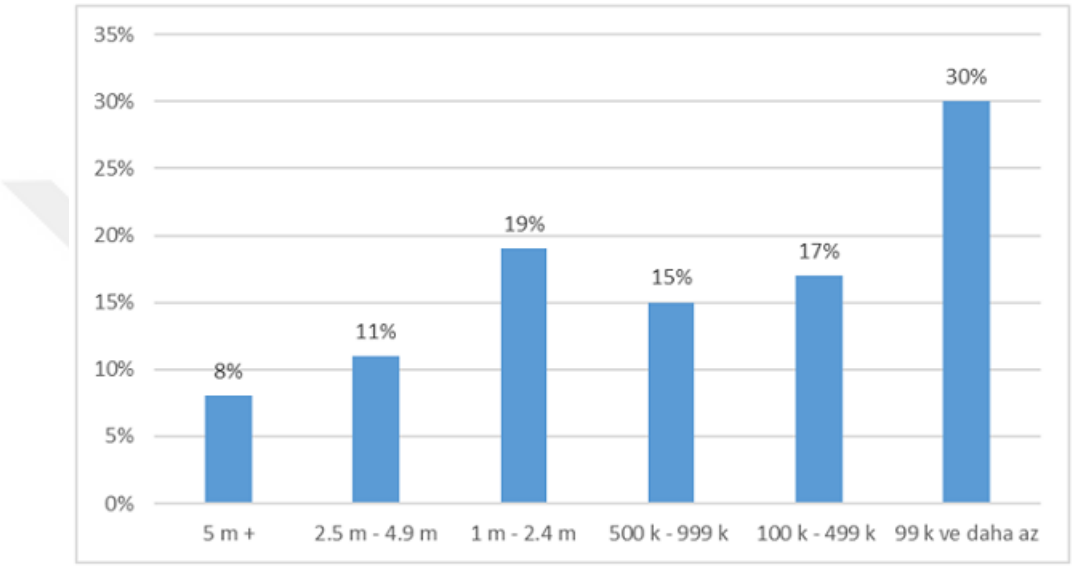


Şekil 6.3: Dünya Genelinde Bilişim Teknolojilerine Yapılan Saldırı Sayısı (Milyon)

Şekil üzerinde ki değerler, kritik altyapı niteliğinde ayrımı yapmadan dünya genelinde ki tüm bilişim teknolojilerini kapsayan verileri kapsamaktadır. Şekil incelendiği zaman Bilgi

Teknoloji alanında yapılan siber saldırı sayısında ki artışın teknoloji gelişimiyle paralellik gösterdiği gözlenmektedir. Bu artışta teknolojinin gelişimi kadar teknoloji kullanımının yaygınlaşması da etki etmektedir. Yaygınlaşmak, beraberinde tedbirsizliği de getirmektedir. Bu durum saldırganlar için bir fırsat niteliğinde sayılmaktadır. Nihayetinde grafikte artışta bu durumun sonucunu ortaya koymaktadır.

- Nisan 2018'de yapılan istatistiki bir çalışmaya göre dünya çapında ki işletmelere yapılan siber saldırılarınmaliyetleri aşağıda ki gibi belirlenmiştir[112]



Şekil 6.4: Siber Saldırıların Dünya Çapında ki İşletmelere Ortalama Finansal Zararı

Grafik incelendiği zaman, dünya çapında işlem gören işletmelere yönelik siber saldırıların %8'i 5 milyon doların üzerinde, % 19'u 1-2.4 milyon dolar arasında ve %30'unun ise 100 bin doların altında maliyete sebep olduğu gözlenmektedir.

Yukarda verilen tablo ve grafiklerden anlaşıldığı üzere, gelişen teknoloji, küresel dünya üzerinde kullanıcının niyetine göre faydalı ya da zararlı olabilmektedir. Saldırılara karşı önlemler alınsa da saldırganların profesyonelliği, kullandıkları üstün teknolojik ürünler ve yazılımlarla bu önlemler aşılabilmektedir. Hiçbir ölçüt gözetmeksizin saldırılar yapılmaktadır ve bunlarınbazılarınistatistiki değerleriyukarıda ki tablolarda gösterilmektedir.

Bölüm 7

Kritik Altyapılarda Siber Güvenlik Hususunda Yapılması Önerilen Çalışmalar

Kritik altyapılar, günümüz dünyasında insan hayatıyla iç içe geçmiş ve herhangi bir müdahalede doğrudan yaşamı etkileyen bir yapıya sahiptirler. Dolayısıyla bu altyapıların kesintisiz ve kaliteli bir hizmet vermesi milletler ve ülkeler açısından oldukça önemlidir. Teknolojik ilerleme ile birlikte bu yapılar siber tehdit altına girmiş ve dünya da pek çok kritik altyapıya saldırılar düzenlenmiştir. Olası bir saldırıda ülke genelinde hizmetlerin aksamaması ya da en az şekilde etkilenmesini sağlamak adına bu altyapılarda çeşit ve tür bakımından alternatifler geliştirilmelidir. Var olan kaynaklar ise her zaman yedek bulunduracak şekilde faaliyette bulunmalıdırlar.

Kritik altyapı alanında faaliyet gösteren kuruluşların, TCK. 5651 sayılı kanunla belirlenen durumlar için standartlar belirlenmelidir. Suçların ulusal bazda karşılığını saptayacak standartlar belirlenmeli ve bu standartlara uyum sağlanmalıdır.

Kanunla düzenlenmiş siber suçların tanımının daha şeffaf olması gerektiği, bu tanımların net ifadelerle açıklanması ve ucu açık olmaması gereklidir. Net bir şekilde belli olmayan ve yalnızca düzenlenmiş olmak amacıyla düzenlenen tanımlardan kaçınmalı, suçun ve suçlunun tanımı yapılmalı ve suçların cezai yaptırımları detaylı bir şekilde belirtilmelidir.

Olası bir Stuxnet saldırısı durumunda uluslararası arenada bu durumu şikâyet edebileceğimiz bir siber mahkemenin varlığı henüz bulunmamaktadır. Uluslararası arenada bulunan Uluslararası Ceza Mahkemesi hukuki tüm suçları kişiler bazında yargılayabilmektedir. Eksikliğinden bahsettiğimiz mahkemenin kişiler dahil devletleri de yargılama yetkisi olan ve yalnızca bilişim/siber suçları yargılayan bir mahkeme olması gerektiği-dir. Çünkü var olan mahkemeler siber suçları incelerken normal hukuk standartlarından hareketle nihai karar verebilecek yapıda dırlar. Bu nedenle Avrupa İnsan Hakları Mahkemesi şeklinde bir siber mahkeme kurulması gerekmektedir. Bu mahkemenin ulus üstü bir yapıda, büyük devletlerin baskısından etkilenmeyecek şekilde kararlar verebilecek yapıda olmalıdır. Kurulacak olan bu mahkemenin Birleşmiş Milletlerde veto yetkisi bulunan 5 daimi üye ülke olacak şekilde ki yapısal hatalara karşı korunması gerekmektedir. Aksi takdirde, Stuxnet saldırısında birçok ABD'li yetkili saldırıyı sahiplenici açıklamalar yapsa da İran'ınhukuki alanda ki girişimlerindenhiçbirsonuçalınamamıştır.

Ülkemiz açısından önemli konumda sayılan AR-GE kurumları ve gizliliği esas olan kamu kurumlarının dışardan fiziki olarak sızmalara karşı önlem tedbirleri sık sık denetlenmelidir. Örneğin dışardan herhangi bir flash bellek ile virüs sokulması gibi. Bu kurumlar, kendi iç yönetmenlikleriyle tedbirleralmıştır ve hukuki sonuçlarını da belirtmiştirler. Lakin uygulama kısmında zafiyetler gözükmektedir. Öyle ki dışardan istenildiği takdirde içeriye çok rahat bir şekilde virüslü bir flash bellek sokulabilmektedir. Olası bir siber saldırının oluşumunu engellemek için bu uygulamaların gerek kamu eliyle gerek güvenilirliği saptanmış özel kurumlar aracılığıyla denetimleri yapılmalı ve caydırıcılık açısından bu durumu ihlal edenler hukuken cezalandırılmalıdır.

Gerek kamusal alanda gerek özel alanda, siber güvenlik ile ilgili gerekli iletişim beceri- leri ve tecrübe aktarımı yapılmasına yönelik hukuki çalışmalar yapılmalı. Bu alanda ki hukuki kurallar caydırıcı nitelikte olmalı ve mecburi düzenlemeler olmalıdır. Örneğin, siber güvenlikle ilgili önlemler alması gereken bir kurumun ya da kuruluşun bu önlemleri almaması durumunda cezai işlemler uygulanmalıdır.

Kritik altyapılara sahip özel işletmeler nezdinde gerek hukuksal gerek teknik uygulamalar geliştirilmelidir. Çünkü özel işletmeler itibar kaygısından dolayı kendilerine yapılan herhangi bir siber saldırıyı gizleyebilmektedirler. Müşteri kaybetmemek ve rakiplerine karşı zayıf gözükmemek adına siber saldırıyla ilgili herhangi bir paylaşım yapmayabilirler. Bu durum ise aynı sektörde ya da aynı nitelikte ki işletmelerin benzer saldırılarda

tedbirli davranmasının önüne set çekebilmektedir. İşletmelerin itibarını koruyacak şekilde bir veri paylaşım mekanizması kurulabilir ve gizliliği hukuksal olarak sağlanabilir. Kritik altyapı tanımları yapılırken ya da hangi alanların kritik altyapı olarak değerlendirilmesi gerektiği belirlenirken geniş bir yelpazeyle bakılması gerekmektedir. Gerek "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ", gerek "Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı" nda kritik altyapıların neler olduğu tanımlanırken altyapı kelimesinden kaynaklı olarak somut çerçevede bir tanımlama yapılmıştır. Kritik altyapı denildiği zaman, maddi somut bir kavramı anlamalıyız yoksa ülke için çok kritik seviye de önemli olabilecek bir durumu mu anlamalıyız? örneğin, herhangi bir ülke için doğalgaz bor hattına yapılacak bir saldırı mı daha önemlidir yoksa o ülkenin Başkanına yapılacak bir suikast mı? Kişilere ya da devletlere göre farklı cevaplar verilebilse de her ikisi de kritik düzeyde önemlidir. Dolayısıyla, kritik altyapı tanımı yapılırken bu gibi detaylar göz ardı edilmemeli ve hukuki düzenlemeler bu ölçüde yapılmalıdır. Soyut nitelikteki kavramlarında kritik altyapı tanımlamalarının içine alınması gerekmektedir.

Kamu kurumlarının özellikle siber güvenlik alanında tek bir parça şeklinde hareket etmesinin sağlanması adına hukuki zorunluluk ülkemizde henüz bulunmamaktadır. Bu alanla ilgili tek bir denetim noktası olması ve tek bir merkezin sorumlu olması elzemdir. Kamu işleyişi yapısı itibariyle hantal bir şekilde ilerlemektedir. Tekmerkezli olmak, hem olası bir durumda bürokrasi gibi bir engelle çok az karşılaşmış olacak hem de karar alınma süreci hızlı alınacaktır. Bu alanda vazifeli birimlerin denetimlerinin sürekliliğini gerek- tirecek şekilde eylem planları ve yönetmenlik çıkarılması da bu alanı daha verimli hale getirecektir.

Kritik altyapı kavramı ülkelerin hassasiyet ölçüsünde genişletilebilir. Özellikle hayatımızın neredeyse her noktasında bulunan bilişim sistemleri çok kritik bir seviyeye ulaşmaya başlamaktadır. Öyle ki banka işlemleri, fatura ödemeleri, alışveriş vs. birçok eylemi akıllı telefonlarla yapabilmekteyiz. Bu işlemleri daha pratik bir şekilde yapabilmek için "App Store-Play Store" tarafından sunulan uygulama programları telefonlara yüklenmektedir. Bu uygulamalar telefona yüklenirken, mahrem sayılacak tüm bilgilerimizin olduğu alanlara (telefon rehberi, fotoğraf galerisi vs.) erişim izni istemekte ve erişim izni verilmediği takdirde uygulamanın faaliyete geçmediği görülmektedir. Doğrudan özel hayatın gizliliğini ihlal eden bu durum hakkında ne yazık ki hukuki bir düzenleme bulunmamaktadır. "Sırf uygulamayı kullanabilmek için erişim izni verdiğimiz alanlarda yapılabilecek mahremiyet ihlali durumunda ki hukuki süreç ve cezalandırma nasıl olacaktır?" şeklinde ki

soruların cevabı niteliğinde tüm dünya ülkelerinin hukuki bir düzenlemeye ihtiyacı bulunmaktadır.

Teknolojik gelişme pastasından büyük bir payı alan akıllı cihazlar, gerek kullanımı kolaylaştırmak gerek müşteri kazanmak amacıyla her gün yeni özelliklerle karşımıza çıkmaktadırlar. Günümüz teknolojisinde ki moda, göz(iris) bilgisi ve parmak izi bilgisi ile açılıp kapanan cihazlardır. Kişiler için son derece gizli bir veri olan göz(iris) ve parmak izi bilgisini hafızasında tutan akıllı cihazların en azından Türkiye alanında, "Kişisel Ve-rileri Koruma Kanunu" na ne kadar uygun davrandığını denetleyen herhangi bir otorite bulunmamaktadır. Bu konular hakkında ülkemiz vatandaşlarının farkındalık durumunu sorgulayan herhangi bir çalışma da bulunmamaktadır. Kritik altyapı niteliğinde ki gerek AR-GE kurumlarında gerek teknoloji ağırlıklı alanlarda son dönemlerde güvenliği artırmak adına güvenlik noktalarında göz(iris) bilgisi ve parmak izi bilgisi kullanılmaktadır. Bu sebepten dolayı akıllı cihazlarda kullanılan göz ve parmak izi bilgisi, arka planda depolanıp uygun zamanda aleyhe kullanılacak bir durum yaratabilmektedir. Bu riskli durum ile ilgili kamu namına bağımsız bir otorite kurulmasının ve vatandaşlarımızın farkındalığını artırıcı eğitimlerin düzenlenmesine çok ihtiyaç duyulmaktadır.

Hukuk sistemimiz de doğrudan kritik altyapılarla ilgili herhangi bir düzenleme yoktur. Kanunlarımız ağırlıklı olarak TCK. 5237 sayılı kanunun 243-246 maddeleri kapsamında işlenen bilişim suçlarına yoğunlaşmıştır. Bu alanda ki yoğunlaşmada da yine yeterli tanımlama yoktur. Açıklamalar genel bir düzeydedir. Suçun tarifinin, suçun kapsamının ve suç sonrası durumun detaylı bir şekilde yapılmadığı görülmektedir. Bu hukuki eksikliklerin giderilmesi ve kritik altyapılarla ilgili kanunsal tabanda net ifadelerle belirtilmiş düzenlemeler yapılması gerekmektedir.

Ülkemizin siber güvenliği açısından milli ve yerli yazılımların geliştirilmesine özen gösterilmesi gerekmektedir. 2017-2018 Türkiye'sinde daha yeni yeni çocuklar düzeyinde verilmeye başlanan yazılım eğitimlerin daha da yaygınlaştırılması ve eğitim öğretim sürecinin birçok döneminde yapılması gerekmektedir. Bu alanda ki millilik siber saldırılara karşı yapılabilecek en büyük savunma önlemi niteliğindedir. Örneğin, ülkemiz açısından kritik sayılan kurumlarının siber saldırılara karşı korunmak amacıyla kullandıkları güvenlik duvarlarının (firewall) milli olmayışı başlı başına milli yazılımın yokluğunda ki büyük tehlikenin anlaşılması açısından yeterli sayılabilecektir.

Ülkemizde kendi gayret ve çabalarıyla siber alanda yetişmiş uzmanların istihdam ve çalışma alanı bulması konusunda imkânlar sağlanmalıdır. Örneğin, ülkemizin teknoloji ve AR-GE açısından önemli sayılan kurumlarının personel istihdamında ön şart olarak konulan bir takım şartların daha uygun ve yapısal bir hale getirilmesi gerekmektedir. Örnek verecek olursak, personel mülakatları öncesinde ciddi mana da yüksek mezuniyet ortalamalarının aranmasıdır. Bu ön koşulun zorluğu, siber alanda kendi çabasıyla iyi işler başarmış kişilerin istihdam edilmesi ve uygun çalışma ortamına kavuşmasının önüne geçmektedir.

Eksikliği hissedilen durumlardan bir tanesi de; yargı alanında yetişmiş personel ile bilişim alanında yetişmiş personelin tamamen birbiri alanından kopuk olmasıdır. Bu kopukluk nedeni ile bilişim alanında düzenlenecek yargısal düzenlemelerde ve bilişim alanında işlenen suçlarla ilgili yargılamalarda yetersizlikler görülebilmektedir. Bu yetersizliklerin eksiltilmesi adına en azından lisans düzeyinde, bilişim alanında okuyanlara hukuksal dersler, hukuk alanında okuyanlara bilişimle ilgili dersler belirli seviyelerde verilebilir. Böylelikle, tamamen kopukluk yerine bir farkındalık yaratılarak meslekler icra edilirken daha verimli sonuçlar alınabilir.

Ulusal ya da uluslararası alanda yapılan siber tatbikatlar sonucu ortaya çıkan zafiyetler sadece tavsiye niteliğinde kalmamalıdır. Ülkemizde bu alanda yetkin sayılan Bilgi Teknolojileri ve İletişim Kurumu'nun sahada daha etkin davranabilmesi, tatbikat neticelerinde ortaya çıkan zafiyetlerle ilgili uygulamaya dökülen çalışmalar yapması ve bu çalışmaların bürokrasi engeline takılmaması için hukuki korumalar yapılması gerekmektedir.

Ülkemizde kritik altyapıları korur nitelikte herhangi bir strateji belirlenmemiş ve siber güvenlik alanında hazırlanan eylem planlarında ise tanımlamalar ve zorunluluklar genel çerçeveyle bırakılmıştır. Örneğin, "Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı" nın Siber Savunma ve Kritik Altyapıların Korunması başlığı altında şu madde- lere yer verilmiştir. Bunlar; sızmatestlerinin zorunlu hale gelmesi, 27001 standartının kullanım mecburiyeti ve sistem odalarında asgari düzeyde bulunması gerekenler şeklinde genel ifadelerle kullanılmış maddeler bulunmaktadır. Bu tür genel ifadelerin kullanılarak sorumlu kişilerin ne anlayabildiğinden ziyade yoruma açık olmayan net ve kesin ifadeler kullanılarak eylem planları hazırlanmalıdır.

Ülkemizin, 2016-2019 Ulusal Siber Güvenlik Stratejisinde ifade edilen ve kritik altyapı olarak belirlenen sektörlerin yetersiz olduğu gözlenmektedir. Gerek ABD, gerek AB için

tanımlanan kritik altyapı sektörlerinden bazılarının ülkemiz içinde kritik öneme sahip olduğu ve bunların kritik altyapı sayılan sektörlere dâhil edilmesi gerekmektedir. Dolayısıyla; Nükleer ve Kimyasal Endüstri, Uzay Araştırmaları ve Bilgi Teknolojileri sektörlerinin Türkiye için kritik altyapı olarak sayılması ve bunlara yönelik yasal ve teknolojik düzenlemelerin yapılması gerekmektedir.

Bölüm 8

Sonuç ve Değerlendirmeler

Hızla gelişen ve yaygınlaşan teknoloji, ülkeler için hayati önemdeki kritik altyapılarda çokça kullanılmaktadır. Kullanım alanının genişlemesi siber güvenlik açısından birtakım riskleri de beraberinde getirmektedir. Birçok bakımdan büyük kolaylıklar sağlasa da, çeşitli güvenlik sorunlarını da beraberinde getirmektedir. Yukarıda şekiller de de görüldüğü üzere, güvenlik önlemlerine rağmen siber saldırılar artarak devam etmektedir. Kritik altyapıların hayati önem taşıması ülkeleri bu alanda bir takım güvenlik tedbirlerine ve çalışmalara zorlamaktadır.

Bu alanda işlenen suçların gün geçtikçe artması, dünya genelinde devletler bünyesinde yankı uyandırmakta ve bu alanda güvenlik önlemlerinin artırılması gerektiğini ortaya koymaktadır. Güvenliğin ihlali ve bilişim suçları, devletlerin hukuk sistemlerinde bu alanda da çeşitli düzenlemeler yapılmasını gerekli kılmaktadır. Başta Ceza Hukuku olmak üzere, farklı devletlerde bu alanda farklı uygulamalar da dikkat çekmektedir. Farklı hukuk sistemleri ve teknolojik seviye ülkelerin kritik altyapı olarak belirttiği kavramları da farklılaştırmaktadır. Bu farklılığın kaynağı ise ülkelerin teknolojiye bakış açısı ve gelişmişlik seviyesiyle ilgilidir. Örneğin kritik olarak nitelendirilen altyapılar, AB ülkeleri, Türkiye ve ABD için farklılıklar gösterebilmektedir.

Ülkemizde son yıllarda siber alanla ilgili birçok çalışma, seminer tarzı uygulamalar yapılmaya başlanmıştır. Bu çalışmalar sonucunda bazı kararlar alınmış ve eksiklikler tespit edilmeye çalışılmıştır. Lakin bu eksiklikler tespit edilmeye başlandığı halde gerek bürokrasi engeli gerek başka durumlardan ötürü yeterli düzeyde kanunsal düzenlemeler yapılmamış ve yeterli önlemler alınmadığı tespit edilmiştir.

Bilişim suçları ile ilgili olarak Türkiye'de Ceza Hukuku kapsamında birçok yenilik yapılmış ve bu suçlar da çeşitli yaptırımlarla büyük oranda kontrol altına alınmıştır. Yeni Türk Ceza kanunu aynı zamanda Avrupa Konseyi Siber Suçlar Sözleşmesi ile de büyük oranda uyum içinde geçerliliğini sürdürmektedir.

Türkiye'de bilişim suçlarına yönelik yapılan ilk detaylı düzenleme, 765 sayılı kanuna eklenen 525 maddeli hükümdür. Bu kanun maddesinde bilişim suçlarının birçoğunayönelik yaptırımlar söz konusu hale getirilmiştir. 765 sayılı eski Ceza Hukukukapsamındabu tür suçlar için üç temel maddeye yer verilmiş, bu maddelerin kapsamı yetersiz kalınca Yeni Kanun'da çeşitli düzenlemeler yapılmıştır. 765 sayılı kanunda bu suçlar ile ilişkili olarak dikkat çeken maddeler 525 a/b/c/d olarak sıralanabilir.Kanunda yapılan değişiklikler sonrasında ise 5237 sayılı Yeni Ceza Kanunu'nda farklı ve kapsamlı başlıklar altında 243, 244, 245 ve 246. maddeler ön plana çıkarılmıştır. Buna ek olarak yeni Türk Ceza Kanunu dâhilinde "Kişilere Karşı Suçlar" bölümü içinde "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında "kişisel verilerin kaydedilmesi" 135. maddede, "kişisel verileri hukuka aykırı olarak verme ve ele geçirme" 136. maddede ve "verileri yok etme" 138. maddede yer bulmuştur. Aynı şekilde 142. ve 158. maddeler de bilişim suçları ile ilişkilendirilmiştir.

Bunların yanı sıra, özel kanunlarla da bilişim suçlarına karşı bir koruma altına alma durumu gözlemlenmektedir. Söz gelimi 5846 Sayılı Fikir ve Sanat Eserleri Kanunu ve 5070 Elektronik İmza Kanunu da bu alanda yapılan çalışmalardaunutulmamıştır.

Belirtmek gerekir ki, bilişim alanında önlemler almış olsak ta ne yazık ki ülkemizde henüz kritik altyapıları doğrudan ilgilendiren bir hukuki düzenleme yoktur. Kritikaltyapılar için belirlenmiş strateji planı henüz yoktur. Gerek kanunlarımız gerek hükümetler siber saldırıların bireysel düzeyiyle ceza hukuku bazında ilgilenmiştir. Kurumları doğrudan ilgilendiren bir siber güvenlikyasası yoktur veihtiyaç duyulmaktadır.

Ülkemizde eksikliği hissedilen durumlardan biri de, ulusal bazda çıkarılan siber güvenlik strateji belgelerinin içinde belirtilen hususların çerçeve bir şekilde düzenlendiği hususudur. Örneğin, 2016 - 2019 Ulusal Siber Güvenlik Strateji Belgesi içinde belirlenen amaç ve eylemler başlığı altındaki ikinci maddede belirtilen; "Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması" gerekliliği belirtilmiştir. Bu maddenin varlığına rağmen henüz böyle bir mevzuat oluşturulmamıştır. Şayet, belirlenenhedefler uygulamaya geçtiğitakdirde ülkemizaçısındançok

güvenli ve faydalı bir dijital alan yaratılmış olacaktır.

Avrupa Siber Suçlar Sözleşmesi'nde de ülkemizdekine büyük oranda benzeyen bir ceza hükmü ve yaptırımlar söz konusu hale getirilmiştir. Bu sözleşmede asıl amaç, ülkelerin uluslararası düzeyde ortak hareket etmesini sağlamak ve dünya genelinde bilişim suçlarının engellenmesine çalışmaktır. Avrupa Konseyi Siber Suçlar Sözleşmesi, birçok maddede bilişim suçlarına ve bunlara ilişkin yaptırımlara yer vermektedir. Bu bağlamda bilgisayarlarda yer alan veri sistemlerinin bütünlüğü, güvenliği ve ulaşılabilirliği gibi konularda önlemler alınmış; hukuka aykırı erişim, verilere yasadışı müdahale, sistemlere müdahale, cihazların kötüye kullanımı gibi konular ile ilgili devletlerin ulusal ve uluslararası düzeyde yapmaları gerekenler söz konusu maddeler ile belirtilmiştir.

Avrupa Siber Suçlar Sözleşmesi'nde her ne kadar siber saldırılarla ilgili düzenlemeler yer alsa da kritik altyapılarayönelikyapılansiber saldırılarıuluslararasıdüzeydeinceleyecek ve cezalar verebilecek bağımsız bir siber mahkemenin varlığına ihtiyaç duyulduğu gözlemlenmektedir. Aksi takdirde var olan düzenlemeler uluslararası alanda yetersiz kalacaktır.

Her ne kadar bugün yaptırımlar ya da cezai hükümler ile ilgili birçok eleştiri ve eksik yön bulunuyor olsa da, bu alanda yapılan çalışmaların, değişen dünya düzenine uyum sağlaması bakımından devam ettirildiği bilinmektedir. Bilişim suçlarına yönelik ceza hükümleri üzerinde gerekli olması halinde gerek ülke çapında gerekse Avrupa genelinde düzenlemeler ve kanunlarda yeniliklerin yapılacağı yahut yapılması gerektiği öngörülmektedir.

Kaynakça

[1] Yellowpages. [2019]. computer-equipment-hardware. https://www.yellowpages.com.au: https://www.yellowpages.com.au/see/ computer-equipment-hardware [Erişim Tarihi: 24 Eylül 2019]

[2] R. Y. Yazıcıoğlu, (1997)., Bilgisayar Suçları Kriminolojik, Sosyolojik Ve Hukuksal Boyutları, İstanbul, Alfa Yayınları, S. 30

[3] A.D. Helvacıoğlu, (2004)., Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerin İncelenmesi, İstanbul, İnternet Ve Hukuk İstanbul Bilgi Üniversitesi Yayınları, S.280

[4] A. Karagülmez, (2005)., Bilişim Suçları Ve Soruşturma- Kovuşturma Evreleri, Ankara, Seçkin Yayıncılık, S.36

[5] K. İçel, (1998)., Kitle Haberleşme Hukuku, İstanbul, S. 407

[6] M.V. Dülger, (2004). Bilişim Suçları, Seçkin Yayınevi, Ankara

[7] ULAKBİM, T. [2012]. https://ulakbim.tubitak.gov.tr. https://ulakbim.tubitak.gov.tr/sites/images/ Ulakbim/ Ipv6 elkitabi.pdf (Erişim Tarihi: 23 Eylül 2019)

[8] LACNİC.NET. (2019, 06 01). IPv6 Etkin Ağlar: http://v6asns.ripe.net/v/6?s=ALL (Erişim Tarihi: 19 Eylul 2019)

[9] İ. Ergün, (2008)., Siber Suçların Cezalandırılması Ve Türkiyeâde Durum, Ankara, Turhan Kitabevi, S.9

[10] İ. Ergün, (2008)., Siber Suçların Cezalandırılması Ve Türkiyeâde Durum, Ankara, Turhan Kitabevi, S.9

[11] Türk Dil Kurumu, (2018)., Bilişim Kavramı, http://sozluk.gov.tr/(Erişim Tarihi: 25.04.2018)

[12] N. Baykal, (2017)., Bilişim Nedir?, https://www.makaleler.com/bilisim-nedir ((Erişim Tarihi: 10 Ekim 2018)

[13] E. D. Aydın (1992)., Bilişim Suçları Ve Hukukuna Giriş, Ankara, Doruk Yayınları, S.27

[14] M.Volkan. Dülger, (2004)., Bilişim Suçları, Seçkin Yayınevi, Ankara, S. 67

[15] C. Özel, (2009)., Bilişim Suçları İle İletişim Faaliyetleri Yönünden TCK Tasarısı, İstanbul Barosu Dergisi C.75

[16] C. Özel, (2009)., Bilişim Suçları İle İletişim Faaliyetleri Yönünden TCK Tasarısı, İstanbul Barosu Dergisi C.75 S. 3, S.2-3

[17] E. D. Aydın (1992)., Bilişim Suçları Ve Hukukuna Giriş, Doruk Yayınları, Ankara, S.13

[18] Avukat Baran Doğan Hukuk Bürosu, (2019)., https://barandogan.av.tr/blog/ceza-hukuku/bilisim-sistemini-engelleme-bozma- erisilmez-kilma-verileri-yok-etme-veya-degistirme-sucunun-cezasi.html (Eri- şim Tarihi: 15.07.2019)

[19] Elit Hukuk, (2016)., http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/ (Erişim Tarihi: 15 Temmuz 2019)

[20] Elektronik İmza Kanunu (1) Kanun Numarası: 5070 Kabul Tarihi: 15/1/2004 Yayımlandığı R.Gazete : Tarih:23/1/2004 Sayı:25355 Yayımlandığı Düstur : Tertip: 5 Cilt : 43

[21] Elektronik İmza Kanunu (1) Kanun Numarası: 5070 Kabul Tarihi: 15/1/2004 Yayımlandığı R.Gazete : Tarih:23/1/2004 Sayı:25355 Yayımlandığı Düstur : Tertip: 5 Cilt : 43

[22] A. Karagülmez, (2005)., Bilişim Suçları Ve Soruşturma- Kovuşturma Evreleri, Ankara Seçkin Yayıncılık, S.154

[23] M. Dülger, (2004)., Bilişim Suçları, Seçkin Yayınevi, Ankara, S.112

[24] Fikir ve Sanat Eserleri Kanunu (1) Kanun Numarası: 5846 Kabul Tarihi : 5/12/1951 Yayımlandığı R.Gazete : Tarih : 13/12/1951 Sayı : 7981 Yayımlandığı Düstur : Tertip: 3 Cilt: 33 Sayfa : 49

[25] Fikir ve Sanat Eserleri Kanunu (1) Kanun Numarası: 5846 Kabul Tarihi : 5/12/1951 Yayımlandığı R.Gazete : Tarih : 13/12/1951 Sayı : 7981 Yayımlandığı Düstur : Tertip: 3 Cilt: 33 Sayfa : 49

[26] A. CELEBİ, [2019, 04 6]. Siber Saldırılar, Siber Guvenlik Olayları. âCyber-Security Manager Blog: https://abdullahcelebi.com/2019/ 04/06/siber -saldirilar-siber-guvenlik-olaylari/ [Erişim Tarihi: 20 Eylul 2019]

[27] L. Kurt, (2005)., Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, S.63

[28] L. Kurt, (2005)., Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, S.68

[29] R. Y. Yazıcıoğlu, (2001). Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı, Uluslar Arası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayını

[30] R. Y. Yazıcıoğlu, (2001). Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı, Uluslar Arası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayını, S.157

[31] L. Kurt, (2005). Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Ankara, Seçkin Yayınları, S.65

[32] O. Değirmenci, (2002). Bilişim Suçları, Marmara Üniversitesi Sosyal Bilimler Enstitüsü yayınlanmamış Yüksek Lisans Tezi, İstanbul, S77.

[33] L. Kurt, (2005)., Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, S.72

[34] R. Y. Yazıcıoğlu, (21-22 Mayıs 2001)., âBilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısıâ Uluslar Arası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, S.460

[35] İ. Ergün, (2008). Siber Suçların Cezalandırılması Ve Türkiyeâde Durum, Ankara, Adalet Yayınevi, S.30

[36] H. Pekşirin, Vd., (10-12Mayıs 2002). Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, G. Uzal (Ed), Türkiye Bilişim Şurası, Ankara, S.80

[37] L. Kurt, (2005)., Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, S.80

[38] Ö. B. Y. Uçkan, (2004). Bilişim İletişim Teknolojileri Ve Ceza Hukuku İnternet Ve Hukuk, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, S.429

[39] L. Kurt, (2005)., Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, S.81

[40] K. Burden, et al. (2003). Cyber Crime â A New Breed Of Criminal? Computer Law And Security Report, 19(3), S. 222-227)

[41] L. Kurt, (2005)., Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, S.83

[42] Ş. Gökçearslan, (2016). Bilişim Suçları Ve Etik, Sami Şahin, Çelebi Uluyol (Ed.), Eğitimde Bilişim Teknolojileri I-Iı, 127-148, Ankara, Pegem Akademi Yayıncılık, S.136

[43] Interpol Computer Crime Manual, 2. Offencer, S.9

[44] Interpol Computer Crime Manual, 2. Offencer, S.10

[45] O. Turhan, (2006). Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, Planlama Uzmanlığı Tezi, S.44

[46] BANKACILIK KANUNU. [2005].
http://www.mevzuat.gov.tr. http:// www.mevzuat.gov.tr/ MevzuatMetin/1.5.5411.pdf

[Erişim Tarihi: 25 Eylul 2019]

[47] Interpol Computer Crime Manual, 2. Offencer, S.15

[48] B. Atıcı, Ç. Gümüş, (2003). Sanal Ortamda Gerçek Tehditler: Siber Terör. Polis Dergisi, Y:9 S.37, 57-66

[49] Emniyet MüdürlüğüRaporu, (2019)., https://www.egm.gov.tr/kurumlar/egm.gov.tr/IcSite/kom/YAYINLARIMIZ/T%C3%9CRK%C3%87E/2017%20RAPORU%20T%C3%9CRK%C3%87E.pdf

(Erişim Tarihi: 15.01.2019)

[50] KRİMİNAL, H. [2019]. KRİMİNAL HAN DANISMANLIK. https://bilirkisiraporlari.com/adli -bilisim-nedir/ [Erişim Tarihi: 23 Eylul 2019]

[51] S. Barry, [2004]. âSmoking Microchips Tells °t All: Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deletedâ, http://www.dataforensics.com/articles/ smoking microchip tells it all.pdf, (15.04.2014); Keser Berber,Leyla;Adli Bilişim, Ankara,s.39.

[52] H. Oğuz, (2014). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları Ve Ülkemizdeki Durum, Çağ Üniversitesi Elektronik Ticaret Hukuku Sempozyumu

[53] A. Koltuksuz, (2010), "Adli Bilişime Giriş" s.43, Adli Bilişim Günü, Yaşar Üniversitesi, İzmir

[54] Y. Uzunay, (2002), "Dijital Delil Araştırma Süreci", http://www.caginpolisi.com.tr/50/14-15-16-17-18.htm (Erişim Tarihi: 30 Temmuz 2018)

[55] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi, http://www.udhb.gov.tr/doc/siberg/2016 -2019guvenlik.pdf (Erişim Tarihi: 5 Ocak 2019)

[56] M. Kara, S. Çelikkol, (2011), Kritik Altyapılarâ¯: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği, 4 . Ağ ve Bilgi Güvenliği Sempozyumu, 2â6. Kocaeli: TÜBİTAK-BİLGEM-UEKAE.

[57] Public Law 107-56 (2001), "USA Patriot Act." doi:107th Congress, 142.

[58] Bilgi Güvenliği Derneği, (2016). Ulusal Siber Güvenlik Stratejisi, http://www.bilgiguvenligi.org.tr/ wpcontent/ uploads/ 2016/ 03/ Ulusal Siber Guvenlik Stratejisi.pdf

(Erişim Tarihi: 27 Aralık 2018)

[59] C. Karakuş, (2013)., Kritik Altyapılara Siber Saldırı, İstanbul Kültür Üniversitesi, 11.

[60] K. Curran, et al. (2008)., Cyber Terrorism Attacks, Lech J. Janczewski and Andrew M. Colarik (Ed.), Cyber Warfare and Cyber Terrorism, IGI Global1-6, pp.2-3.

[61] H. Çifttçi, (2013). Her Yönüyle Siber Savaş, Ankara, TÜBİTAK Popüler Bilim Kitapları

[62] Y. Şenkaya, U. G. Adar, (2014)., Siber Savunmada Yapay ZekÃ¢ Sistemleri Üzerine İnceleme, Akademik Bilişim, s.4â5

[63] Bankacılık Denetleme ve Düzenleme Kurumu,(2012)., Bilgi Sistemlerine İlişkin Sızma Testleri, GENELGE, https://docplayer.biz.tr/1464820-Bankacilik-duzenleme-ve-denetleme-kurumu- bilgi-yonetimi-dairesi.html (Erişim Tarihi: 2 Aralık 2018)

[64] H. Önal, (2012)., Hedef Odaklı Sızma Testleri, Bilgi Güvenliği Akademisi, BGA Bilgi Güvenliği, Ankara, s.10.

[65] Türk Standartları Enstitüsü, (2015)., Sızma Testi Hizmeti Veren Personel Ve Firmalar İçin Yetkilendirme Programı, https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2224/07102015112307- 3.pdf (Erişim Tarihi: 30 Kasım 2018)

[66] Türkiye Büyük Millet Meclisi, (1991). 3765 sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun, Kanun No. 3756, Kabul Tarihi6.6.1991

[67] T.C Resmi Gazete, (28 Temmuz 2006)., No:2006/38, Bilgi Toplumu Stratejisi Eylem Planı (2006-2010), http://www.resmigazete. gov.tr/eskiler/2006/07/20060728-7.htm (Erişim Tarihi: 10 Ocak 2019)

[68] USOM, (2013)., https://www.usom.gov.tr/hakkimizda.html (Erişim Tarihi: 18 Aralık 2018)

[69] USOM, (2013)., https://www.usom.gov.tr/hakkimizda.html (Erişim Tarihi: 19 Aralık 2018)

[70] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2014). Kurumsal SOME Kurulum ve Yönetim Rehberi http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf

(Erişim Tarihi: 01 Ocak 2018)

[71] BTK, (2017)., https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi (Erişim Tarihi: 16 Aralık 2018)

[72] Afet ve Acil Durum Yönetimi Başkanlığı,(2018)., https://www.afad.gov.tr/tr/2211/AFAD-Hakkinda (Erişim Tarihi: 10 Aralık 2018)

[73] M. Afyonluoğlu, (2018)., Kritik Altyapılar ve Türkiye, http://afyonluoglu.org/siberguvenlik/kritik-altyapilar2/ (Erişim Tarihi: 5 Ocak 2018)

[74] H. Çiftçi, (2017)., Her Yönüyle Siber Savaş, Ankara, TÜBİTAKPopüler Bilim Kitapları

[75] Türkiye Bilişim Derneği, Ulusal Bilgi Güvenliği Teşkilatı VeGörevleri Hakkında Kanun Tasarısı, https://www.tbd.org.tr/ulusal-bilgi-guvenligi-teskilati-ve-gorevleri-hakkinda- kanun-tasarisi/ (Erişim Tarihi: 30 Aralık 2018)

[76] TÜBİTAK BİLGEM, (2011)., Siber Güvenlik Tatbikatı, http://bilgem.tubitak.gov.tr/en/node/198 (Erişim Tarihi: 20 Kasım 2018)

[77] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2012)., Sunumlar, https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/12_06%20%20Ulastirma,%20Denizcilik%20ve%20Haberlesme%20Bakanligi.pdf (Erişim Tarihi: 29 Aralık 2018)

[78] Türkiye Büyük Millet Meclisi, (2012)., Yasama Dönemi Yasama Yılı 24/2 Sıra Sayısı: 381, Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırma Komisyonu, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf (Erişim Tarihi: 10 Ocak 2019)

[79] Bilgi Toplumu Dairesi, (2015)., Bilgi Toplumu Stratejisi ve Eylem Planı 2015-2018, Ankara , S.15

[80] BTK, (2016)., 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı ile 2016-2019 Ulu- sal Siber Güvenlik Stratejisi ve Eylem Planı, https://www.btk.gov.tr/haberler/dr-omer- fatih-sayan-2016-2019-ulusal-e-devlet-stratejisi-ve-eylem-plani-ile-2016-2019-ulusal-siber- guvenlik-stratejisi-ve-eylem-plani-tanitim-toplantisina-katildi (Erişim Tarihi: 16 Aralık 2018)

[81] Savunma Sanayi Başkanlığı, (2017)., TSK Siber Savunma Merkezi Projesi, https://www.ssb.gov.tr/website/contentlist.aspx?PageID=1083&LangID=1 (Erişim Tarihi: 28Kasım 2018)

[82] T.C Resmi Gazete, (6 Temmuz 2019)., Sayı: 30823, Bilgi ve İletişim Güvenliği Tedbirleri, http://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf (Erişim Tarihi: 10 Temmuz 2019)

[83] İ. Başbüyük, (2014)., Dijital Çağda Suçla Mücadele: Bir AvrupaSiber-Suç Merke- zinin Kurulması* Avrupa Komisyonu Brüksel, 28.3.2012 Com (2012) 140 Dokuz Eylül Üniversitesi Hukuk FakültesiDergisi Cilt: 15, ÖzelS., 2013, S.1583-1594, 1583-1594

[84] Türkiye Büyük Millet Meclisi Yasama Dönemi Yasama Yılı 24 3 Sıra Sayısı: 380 Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı Ve Dışişleri Komisyonu Raporu(1/676)

[85] M. Özbek, (2015). AvrupaSiber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri, Artıcletter | Summer 2015, 73-88

[86] M.Özbek, (2015)., AvrupaSiberSuçlarSözleşmesininTürkCezaHukukunaEtkileri, Artıcletter | Summer 2015, S.77

[87] İ. Başbüyük, (2014)., Dijital Çağda Suçla Mücadele: Bir AvrupaSiber-Suç Merke- zinin Kurulması* Avrupa Komisyonu Brüksel, 28.3.2012 Com (2012) 140 Dokuz Eylül Üniversitesi Hukuk FakültesiDergisi Cilt: 15, ÖzelS.1586

[88] M. Önok, (2013)., âAvrupa Konseyi Siber Suç sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliğiâ, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C: 19, S: 2, S. 1229-1270.

[89] M. Önok, (2013)., âAvrupa Konseyi Siber Suç sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliğiâ, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C: 19, S: 2, S. 1244

[90] M. Koca, (2003)., Avrupa Siber Suç Sözleşmesiânin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalpâe Armağan, Cilt III, İstanbul,

[91] Convention On Cybercrime, (2001). https://www.coe.int/en/ web/conventions/ full - list/-/conventions/treaty/185 Budapest, 23.11.2001 (ErişimTarihi: 2018)

[92] AB Parlamentosu. [2019, Haziran 7]. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2019/881/oj [Erişim Tarihi: 22 Eylul 2019]

[93] Deloitte. [2019]. https://www2.deloitte.com/tr.
https://www2.deloitte.com/ tr/ tr/ pages/ risk/topics/cyber-risk/articles/avrupa-birligi-siber-guvenlik-kanunu.html [Erişim Tarihi: 22 Eylul 2019]

[94] R. Samlı, [2010]. Turk ve Dunya Hukukunda Bilişim Suçları, Akademik Bilişim.
http://docplayer.biz.tr/3758191 -Turk-ve-dunya-hukukunda-bilisim-suclari.html, S. 101[Eri- şim Tarihi: 23 Eylul 2019]

[95] L. Kurt, [2005]., Açıklamalı İçtihatlı Tum Yonleriyle Bilişim Suçları Ve Turk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, S.106

[96] A. Önder, (1994).,Şahıslara Ve Mallara Karşı Cürümler Ve Bilişim Alanında Suçlar, İstanbul, Filiz Kitabevi

[97] Z. T. Kangal, (2001)., Fransaâda İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu, İühfm, C. Lıx, S. 1-2, İstanbul, s. 227-240

[98] H. Sınar, (2001)., İnternet Ve Ceza Hukuku, İstanbul, Beta Yayınları, S.666

[99] H. Sınar, (2001)., İnternet Ve Ceza Hukuku, İstanbul, Beta Yayınları, S.666

[100] Y. Akdeniz, Section 3 Of The Computer Missuse Act 1990: An Antidote For Computer Viruses!, Web Journal Of Current Legal Issues, 01 Ocak 1996. 24 Aralık 2005, http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html (Erişim Tarihi: 2018)

[101] A. Karagülmez, (2005)., Bilişim Suçları Ve Soruşturma- Kovuşturma Evreleri, Ankara, Seçkin Yayıncılık, S.121

[102] Ö. Demir, (2009)., İnternet Servis Sağlayıcısının Cezai Sorumluluğu, http://bilişimşuras{\T1\i}.org.tr./dosyalar/28.txt (Erişim Tarihi: 09.09.2018)

[103] H. Akarslan, (2015)., Bilişim Suçları, Ankara, Seçkin Yayıncılık, S.145-146

[104] L. Kurt, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları Ve Türk Ceza Kanundaki Uygulaması, Seçkin Yayınları, Ankara, 2005

[105] Cornel University law School,(t. y.), Title 18 â Crimes and Criminal Procedure, https://www.law.cornell.edu/uscode18/usc_sup_01_18.html (Erişim Tarihi: 10.11.2018)

[106] Adli Sicil ve İstatistik Genel Müdürlüğü, Ankara (2017)., Yıllar itibariyle yayınlanan adli istatistik verileri,
http://www.adlisicil.adalet.gov.tr/istatistik_2017/istatistik2017.pdf (Erişim Tarihi: 5 Eylül 2018)

[107] (Computer Security Institute, (2010)., 15th Annual CSI Computer Crime And Security Survey ExecutiveSummary,

https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf (Erişim Tarihi: 5 Eylül 2018)

[108] STATİSTA, (2017)., https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/ (Erişim Tarihi: 6 Ekim 2018)

[109] STATİSTA, (2018)., https://www.statista.com/statistics/707943/attacks-atm-hacking-malware-europe/ (Erişim Tarihi: 10 Mart 2019)

[110] Report on Ceybersecurity Critical Infrastructure in The Americas, (2015). https://www.sites.oas.org/cyber/Documents/2015%20-%20OAS%20Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf (Erişim Tarihi: 11 Mart 2019)

[111] STATİSTA, (2016)., https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/ (Erişim Tarihi: 16 Şubat 2019)

[112] STATİSTA, (2018)., https://www.statista.com/statistics/881158/average-financial-damages-via-cyber-attacks/ (Erişim Tarihi: 26 Şubat 2019)