**T.C.**
**GEBZE TEKNİK ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**

# KRİTİK ALTYAPILARIN KORUNMASINA İLİŞKİN BELİRLENEN SİBER GÜVENLİK STRATEJİLERİ

**MEHMET ERCAN**

**YÜKSEK LİSANS TEZİ**

**STRATEJİ BİLİMİ ANA BİLİM DALI**

**GEBZE**

**2015**

**T.C.**

**GEBZE TEKNİK ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**

# KRİTİK ALTYAPILARIN KORUNMASINA İLİŞKİN BELİRLENEN SİBER GÜVENLİK STRATEJİLERİ

**MEHMET ERCAN**

**YÜKSEK LİSANS TEZİ**

**STRATEJİ BİLİMİ ANA BİLİM DALI**

DANIŞMANI

PROF. DR. ALİ EKBER AKGÜN

**GEBZE**
**2015**

| GEBZE TEKNİK ÜNİVERSİTESİ | YÜKSEK LİSANS JÜRİ ONAY FORMU |
|---|---|

GTÜ Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun 15/01/2015 tarih ve 2015/02 sayılı kararıyla oluşturulan jüri tarafından 21/01/2015 tarihinde tez savunma sınavı yapılan Mehmet ERCAN'ın tez çalışması Strateji Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

**JÜRİ**

| | |
|---|---|
| ÜYE (TEZ DANIŞMANI) | : Prof. Dr. Ali Ekber AKGÜN |
| ÜYE | : Prof. Dr. Hüseyin İNCE |
| ÜYE | : Prof. Dr. Halit KESKİN |

**ONAY**

Gebze Teknik Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun

...../...../..... tarih ve ...../..... sayılı kararı.

İMZA/MÜHÜR

# ÖZET

Bu çalışma; kritik altyapıların kontrol sistemlerinde yaygın olarak kullanılan Bilgi ve İletişim Teknolojilerinin (BİT), maruz kaldığı siber tehditlere karşı yeterli savunmanın sağlanabilmesi için yapılması gereken çalışmaları belirleyerek ilgili kurumlara tavsiyelerde bulunmayı amaç edinmiştir.

Söz konusu çalışma kapsamında Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-TÜBİTAK ile iletişime geçilmiş ve siber güvenlik enstitüsü ile yapılan koordinasyon çalışmaları ile ülkemizin siber güvenlik ve kritik altyapıların güvenliği konusunda ki çalışmaların son durumu öğrenilmiştir. Bu konuda önceden yazılan tez konularına Yüksek Öğretim Kurumu (YÖK) vasıtasıyla erişilmiş ve eksik konular belirlenmiş özellikle bu eksikliklerin çalışma kapsamında giderilmesine gayret edilmiştir. Çalıştığım kurum olan Türk Silahlı Kuvvetleri'nin bu konudaki ilgili birimleri ile iletişime geçerek dünyada öne çıkan ülkelerin siber savaş yetenekleri konusunda bilgi edinilmeye çalışılmıştır. Bunlara bağlı olarak bu konuda öne çıkan kitaplar, makaleler, gazete haberleri, konferanslar, siber tatbikatlar, raporlar, stratejik planlar, projeler ve kurumların internet siteleri dâhil olmak üzere üç yüzü aşkın kaynak incelenerek konunun en güncel haline hâkim olmaya çalışılmıştır.

Bu analiz neticesinde tüm kritik altyapıların ve kurumların siber tehditlerden korunması için ülkemizde yasal mevzuatın en ince ayrıntısına kadar belirlenmesinin, başta tüm vatandaşlar ve kritik kurumlarda çalışan personelin siber güvenlik konusunda eğitilmesinin, özellikle kurumlarımızda milli teknolojilerin kullanılması maksadıyla Ar&Ge'ye ayrılan bütçenin artırılması ve yüksek seviyede devlet desteğinin sağlanmasının, kritik altyapılarda OECD, AB, NATO, ABD'de alınan tedbirlerin ülkemizde de uygulanmasının faydalı olacağı tavsiye edilmiştir.

**Anahtar Kelimeler: Bilgi ve İletişim Teknolojileri, Kritik Altyapılar, Siber Güvenlik, Siber Savunma, Siber Savaş, Stratejik Yönetim.**

# SUMMARY

In this study; widely used in control systems of critical infrastructure, Information and Communication Technology (ICT) is exposed in order to provide defense against cyber threats by identifying the work to be done aims to make recommendations to the relevant institutions.

Comes to study Turkey's Scientific and Technological Research Council - TUBITAK were contacted and cyber security institute made with coordinating efforts with the country's cyber security and critical infrastructure security of its work on the latest situation has been learned. These pre-written theses on topics Higher Education Council (HEC ) and missing accessed through the study of subjects determined to overcome these shortcomings, especially it has been tried. The organization I worked with the Turkish Armed Forces, the relevant departments on this issue by contacting the leading countries in the world to obtain information about cyber warfare capabilities have been studied. They are depending on this issue highlights books, articles, newspaper articles, conferences, cyber exercises, reports, strategic plans, projects and institutions websites, including more than three hundred sources examining the issue the most current judges to be studied.

This analysis results in all critical infrastructure and institutions cyber threats for the protection of our country legislation the smallest detail to the determination, particularly all citizens and critical agency personnel working in cybersecurity trained in the particular institution in our national use of technologies for the purpose of R&D budget increase and the high level of state support the provision of critical infrastructure in the OECD, EU, NATO and the U.S. implementation of the measures will be useful in our country has been recommended.

**Key Words: Information and Communication Technology, Critical Infrastructures, Cyber Security, Cyber Defense, Cyber Warfare, Strategic Management.**

# TEŞEKKÜR

Hayatımda akademik anlamda ilk kez böyle bir çalışma yapmanın benim nezdimde farklı bir heyecan ve pozitif enerji meydana getirdiğini belirtmek isterim. Bu çalışmaya başladığımda ne kadar güzel ve güncel bir konu üzerinde çalıştığımı ve her geçen gün, hem devletler hem de bireyler için öneminin gittikçe arttığını görme fırsatı buldum. Bana daha tanışmamızın ilk gününden itibaren hem akademik anlamda hem de insani ilişkiler bağlamında verdiği desteklerle ışık tutarak önümü aydınlatan çok kıymetli, kadirşinas danışman hocam Gebze Teknik Üniversitesi Strateji Bilimi Başkanı olan Prof. Dr. Ali Ekber AKGÜN'e,

Yaşlarının genç olmasına rağmen bilim dünyasındaki enginlikleri çok geniş olan değerli TÜBİTAK çalışanlarından Siber Güvenlik Enstitüsü çalışanları Fikret ÖTTEKİN ve Hüseyin CAN beylere ve burada adı geçmeyen tüm TÜBİTAK çalışanlarına,

Üniversitemizin Sosyal Bilimler Enstitüsü genel sekreterliğinde çalışan bana çalışmamın daha nitelikli ve verimli hal almasında destek olan, her türlü soruma samimiyetle cevap veren değerli çalışanlara çok teşekkür ederim. Yine aynı duygu ve hislerle enstitümüzün kütüphane çalışanlarına, derslerinden çok istifade ettiğim ve keyif aldığım Prof. Dr. Salih Zeki İMAMOĞLU, Prof. Dr. Hüseyin İNCE ve Yr. Doç. Dr. Haluk ÇİFTÇİ hocalarıma,

Yaklaşık 2 yıldır hem maddi hem de manevi desteklerini yüreğimde hissettiğim, çoğu zaman isteklerine cevap vermede zorlandığım, ama bana kırılmadan her türlü desteği sağlayan değerli eşim Emine ERCAN'a, canımdan çok sevdiğim biricik kızım Cemile ERCAN'a şükranlarımı sunar çok teşekkür ederim. Benim bu günlere gelmeme vesile olan, hiçbir zaman benden hem maddi hem de manevi desteklerini esirgemeyen engin düşünceli, civanmert yürekli annem ve babam Hüsnüye - İbrahim ERCAN'a ve buraya ismini dâhil etmeyi unuttuğum, yaptığım çalışmam kapsamında emeği geçen herkese tüm samimiyetimle teşekkür ederim.

# İÇİNDEKİLER

# SİMGELER ve KISALTMALAR DİZİNİ

**Kısaltmalar**

| | | |
|---|---|---|
| AB | : | Avrupa Birliği |
| ABD | : | Amerika Birleşik Devletleri |
| ATM | : | Automatic Teller Machine |
| BDDK | : | Bankacılık Denetleme ve Düzenleme Kurulu |
| BİLGEM | : | Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi |
| BİT | : | Bilgi ve İletişim Teknolojileri |
| BT | : | Bilişim Teknolojileri |
| BKM | : | Bölgesel Kontrol Merkezi |
| BOME | : | Bilgisayar Olaylarına Müdahale Ekibi |
| BTK | : | Bilgi Teknolojileri ve İletişim Kurumu |
| DOS | : | Denial of Service |
| DDOS | : | Distributed Denial of Service |
| GPS | : | Global Posioting System |
| ISS | : | İnternet Servis Sağlayıcı |
| SCADA | : | Süpervisory Control and Data Acquisition |
| SOME | : | Siber Olaylara Müdahale Ekipleri |
| TSE | : | Türk Standartları Enstitüsü |
| TSK | : | Türk Silahlı Kuvvetleri |
| TÜBİTAK | : | Türkiye Bilimsel ve Teknolojik Araştırma Kurumu |
| UEKAE | : | Ulusal Ekonomik ve Kriptoloji Araştırma Enstitüsü |
| ULAKBİM | : | Ulusal Akademik Bilgisayar Olaylara Müdahale Merkezi |
| Ulak-CSIRT | : | ULAKNET Bilgisayar Olaylarına Müdahale Birimi |

# ŞEKİLLER DİZİNİ

# TABLOLAR DİZİNİ

# GİRİŞ

Yaşamımızın her alanına nüfuz eden teknoloji, sağladığı kolaylıkların ve faydaların yanı sıra bazı risk ve tehditleri de beraberinde getirmektedir. Bilgisayar ve ağlardaki açıklıkları fırsat bilerek sistemlerin çalışmalarına engel olmak, bilginin değiştirilmesine, çalınmasına, yok edilmesine zemin hazırlamak, maddi çıkar elde etmek maksadıyla gerçekleştirilen siber saldırılar her geçen gün artmaktadır.

Bilgi ve İletişim Teknolojileri (BİT) ile kritik altyapıların kesiştiği noktalar ve etkileşimleri gün geçtikçe genişlemektedir. Kritik altyapılar; enerji, iletişim, sağlık, finans, barajlar, boru hatları gibi işletmeleri kapsamaktadır. Bu kritik altyapılara yapılan her hangi bir saldırı durumunda hasara bağlı olarak ülkede yaşam durma noktasına gelebileceğinden konu oldukça önemlidir. Kritik altyapıların kontrol ve bakımları önceden yerinden yapılırken günümüzde teknolojinin de gelişmesi ile bilgisayar sistemleri ve ağ sistemi üzerinden gerçekleştirilebilmektedir.

Dolayısıyla kritik altyapıların BİT'ler ile etkileşimleri arttıkça bazı tehditlere de açık hale gelmektedir. Olayın toplum hayatını ve ülke savunmasını birinci derecede etkilemesinden dolayı, alınacak tedbirlerinde kapsamlı, yeterli ve güncel olması gerekmektedir.

Bu tedbirlerin belirlenmesine ve güvenlik stratejilerinin geliştirilmesine yönelik yapılan bu çalışma kapsamında, birinci bölümde; BİT'lerin tanıtılması ve kullanım alanları, ikinci bölümde; siber güvenlik ve siber saldırı çeşitleri, üçüncü bölümde; siber savunma faaliyetleri, dördüncü bölümde; siber güvenlik konusunda ülkemizde ki mevcut durum, beşinci bölümde; kritik altyapılar, altıncı bölümde; kritik altyapılara uygulanan sızma testleri, yedinci bölümde; konuya ilişkin olarak görüş ve tavsiyeler belirtilmiştir.

Bu çalışma kritik altyapıların öneminin vurgulanarak ülke çapında tüm kritik altyapıları kapsayacak şekilde bir devlet politikasının hayata geçirilmesi, gerekli denetleme ve kontrol mekanizmalarının aktif olarak işletilmesi, halkın bilinçlendirilmesi, konuya ilişkin eğitim müfredatlarının güncellenmesi ve geliştirilmesi hususlarının uygulanmasını hedeflemektedir.

# 1. BİLİŞİM TEKNOLOJİLERİ

Bilişim Teknolojisi (BT); bilginin toplanmasında, işlenmesinde, depolanmasında ağlar aracılığı ile bir yerden başka bir yere iletilmeleri ve kullanıcıların hizmetine sunulması gibi işlemlerin etkili ve verimli yapılmasına olanak sağlayan iletişim ve bilgisayar tabanlı bütün sistemleri kapsayan addır (Üzmez, 2010).

BT terimi iletişim ve bilgisayar teknolojisi ile sağlanabilen bilgi hizmetlerinin tamamı için kullanılabilmektedir. Dolayısıyla günlük yaşamın vazgeçilmez bir unsuru haline gelen BT'yi yalnızca bilgisayara ait yazılım ve donanım hizmetleri ile sınırlı tutmak yanlış olacaktır (Hamiti et al., 2014).

BT'nin bileşenleri; yazılım, donanım, hizmetler ve ekipmanlar olarak kategorilere ayrılabilmektedir.

## 1.1 Bilişim Teknolojileri Bileşenleri

Bilgi ve İletişim Teknolojileri (BİT)'lerin etkinlik alanı incelendiğinde günlük hayatta birçok alanda çok kapsamlı bir şekilde kullanıldığı görülecektir. Zira günümüzde her bir insanın cebine cep telefonu vasıtasıyla bilgisayar teknolojisinin girdiği göz önüne alındığında olayın ehemmiyeti daha net anlaşılacaktır. BİT bileşenlerine kısaca örnek vermek gerekirse; bilgisayar teknolojileri, mikro elektronik teknolojiler, uydu sistemleri ve her türlü iletişim teknolojileri, radyo, televizyon, bilgi ağları, telekomünikasyon, taşınabilir kişisel bilgisayarlar, kablosuz iletişim, mültimedya, sesli tanıma sistemleri, ATM, elektronik posta v.b. sistemler bu kategoriye girebilmektedir (Markauskaite 2006).

## 1.2 Bilişim Teknolojilerinin Önemi

Bilgi insan hayatının her aşamasında çok önemli bir yere sahiptir. Buna bağlı olarak bu bilginin işlenmesi, depolanması ve transferinin sağlanması çok özenle yapılması gereken faaliyetlerdir (Reisa et al., 2013).

İşte tamda bu nokta da teknoloji devreye girmekte ve önemi daha net kavranmaktadır. Bilgi teknolojisi ile iletişim teknolojisini birleşmesi ile meydana gelen Bilgi ve İletişim Teknolojileri (BİT)'leri bu konuda insan yaşamını kolaylaştırdığı gibi hem zaman hem de verim açısından çok ciddi kazanımlar sunmaktadır (Kağnıcıoğlu, 1998).

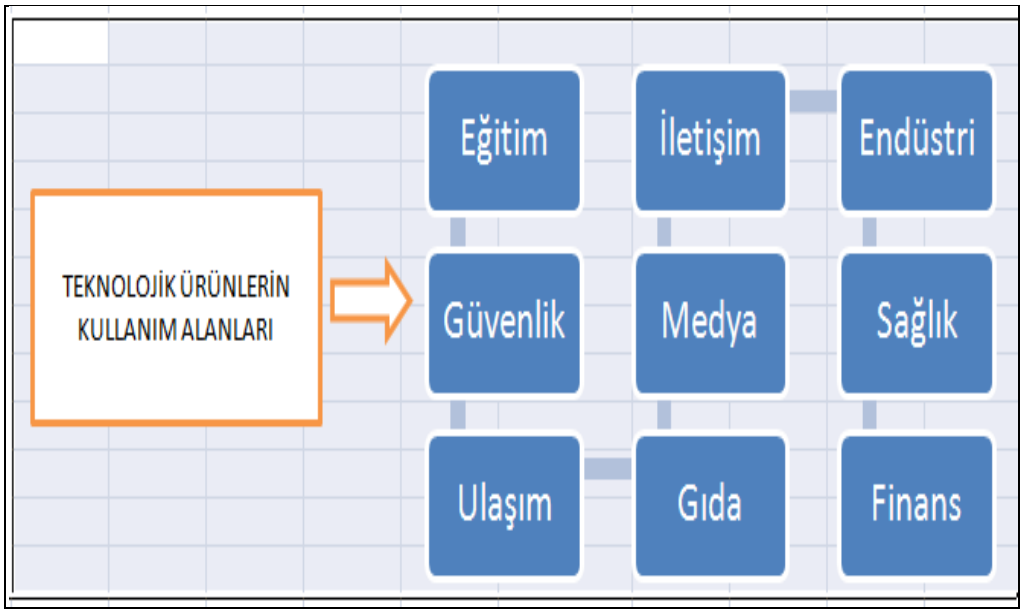
BİT'lerin insan hayatındaki etki alanı genişledikçe dünyanın da hızla küçüldüğü görülmektedir. Bilişim alanındaki bu gelişmeler diğer teknolojilerdeki gelişmeleri de doğru orantılı olarak etkilemektedir.

Özellikle bilgisayar teknolojisindeki gelişmeler toplumlar üzerinde doğrudan etki yaratmaktadır. Toplumların ekonomik refahından, sanayisine, sağlıktan eğitime kadar birçok alanda pozitif etkilerini gözlemlemek mümkündür (Rastogi and Malhotra, 2013).

## 1.3 Bilişim Teknolojilerinin Kullanıldığı Alanlar

BİT'lerin günlük hayattaki etki alanları incelendiğinde insanın tüm yaşam evreleri olarak kabul edilebilecek; sağlık, eğitim, ulaşım, üretim, güvenlik, temizlik, gıda, haberleşme, ısıtma ve soğutma, ev hayatı, eğlence, aydınlatma, iş hayatı, sosyal yaşam gibi alanlarda etkin olduğu görülebilecektir. BİT'lerin kullanım alanları Tablo-1.1'de gösterilmiştir (Alena and Libor, 2012);

Tablo 1.1: Teknolojik Ürünlerin Kullanıldığı Alanlar.



## 1.4 BİT'lerin Kullanımında Karşılaşılan Problemler

BİT'ler, toplumlarda birçok alanı etkisi altına alması ile birlikte kritik bir varlık olarak addedilmeye başlanmıştır. Dolayısıyla her kritik varlık için söz konusu olacağı üzere bilginin elde dilmesi, kullanılması, iletilmesi, depolanması v.b. aşamalarında çeşitli problemlerle karşılaşılmaktadır (Pervan, 1998).

BİT'lerin, küreselleşen dünya düzeninin de etkisiyle, bilgi toplumu olabilme yönünde verilen uğraşıların pozitif bir sonuca bağlanması kapsamında, insanlara bu teknolojileri kullanmada profesyonellik kazandırmanın önemi tartışılmaz hale gelmiştir. Profesyonelliğin kazandırılması sürecinde; eğitimin, doğru ve yanlışı öğrenme sanatına sahip olmanın, bilgi ve teknoloji toplumunda etkin olduğu görülmektedir (Aksal, 2011).

BİT'lerin bu kadar etkin olarak kullanıldığı günümüzde, çeşitli problemler ile karşılaşılması kaçınılmazdır. Bu problemlerden bazıları müteakip maddelerde sunulmuştur;

### 1.4.1 Bilgi Güvenliğinin Sağlanmasında Yaşanan Zorluklar

İnternetin yaşamımıza entegre olması ve teknolojide meydana gelen çok hızlı gelişmeler ile birlikte bilgi ve bilişim güvenliği giderek çok önemli bir öneme sahip olmaktadır. BİT'lere bağımlı hale gelen sistemler ve alt yapıların her geçen gün artması güvenlik konusunu da gündeme getirmiştir (Ünver vd., 2011).

Sadece şahıslar bazında değil, firmalar ve devlet kurumları çerçevesinde de bilgi ve bilişim güvenliği üzerinde kapsamlı çalışmalar yapılmakta ve bu konuda algıda seçiciliğin artırılması maksadıyla çok ciddi gayretler sarf edilmektedir. Hayatımızın birçok alanına etki eden bilişim teknolojileri; iletişim, banka hizmetleri, kamu faaliyetleri, savunma ve askeri sistemleri, ağ sistemleri gibi hassas argümanların baş aktörü haline gelmiştir. Teknolojinin gelişmesiyle bu bilişim teknolojilerini birer saldırı unsuru, kullandığımız sistemleri de birer hedef haline getirmiştir. Özellikle son zamanlarda bilişim sistemlerine ait saldırı ve güvenlik ihlalleri hızla artmaktadır (Oracle, 2003).

1990'ların başında ABD-Pentagon'da BİT sistemlerinin yaygın bir şekilde savunma sistemlerinde kullanılmasının meydana getirdiği zafiyetler konusunda endişeler dile getirilmeye başlamıştır.

1994 yılında ABD savunma bakanlığı ve istihbarat organizasyonları arasında "Ortak Güvenlik Komisyonu" kurulmuştur. Bu komisyonda ağ teknolojilerinin gelişmesinin riskleri derinlemesine incelenmiştir. Komisyonun sonuç raporunda üç ana konsept bulunmaktadır (Clarke and Knake, 2010).

- *"Bilişim sistemleri teknolojisi, bilişim sistemleri güvenliği teknolojisinden daha hızlı ilerliyor*."
- *"Bilişim sistemlerinin ve ağlarının güvenliği bu on yılın en önemli güvenlik sorunu ve bu alanda karşılaşılan riskler konusunda yeterli bilince sahip değiliz."*
- *"Pentagon'un yanında, özel sektöründe bilişim sistemlerine bağımlılığı ülkenin tamamının zayıflığını artırıyor."*

Bu yaşanan örnekler bilgi ve bilişim güvenliğinin ne kadar önemli olduğunu, meydana gelen tehdit ve risklerin kontrol altında tutulmasının ve yeterli tedbirlerin alınmasının ne kadar elzem olduğunu bir kez daha vurgulamaktadır. Bu kapsamda bilgi güvenliğinin temel prensiplerine hâkim olma ve bunları pratik hayatta kullanmak oldukça önem kazanmaktadır.

### 1.4.2 Bilişim Teknolojilerinin Maruz Kaldığı Tehditler

Bilgi güvenliği tehditlerini, bilişim teknolojilerinin kullanımında bir sistemin veya bilgi varlığının sakatlanmasına veya zarar görmesine sebep olan gizli neden olarak tanımlayabiliriz. Her zaman sistemlerde meydana gelen güvenlik boşluklarından sızmaya çalışan bir tehdit kaynağı mevcuttur. Bu bazen bir zararlı yazılım olabileceği gibi bazen de sahte bir internet sitesi de olabilmektedir (Xiao-yan et al., 2011).

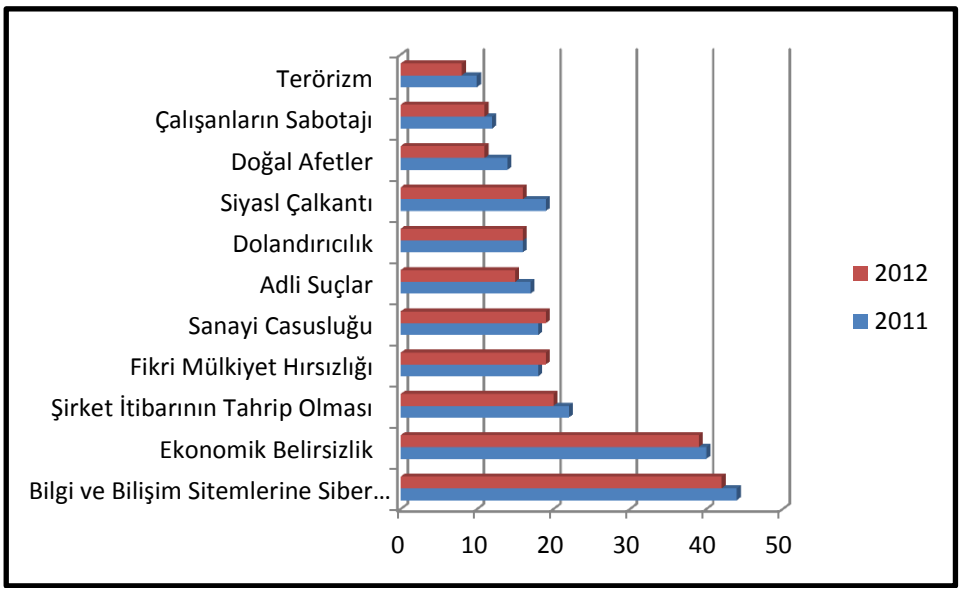
Ayrıca kaynak, yeri geldiğinde bir çalışan personel, yeri geldiğinde doğal etkenler yâda hacker (Siber Ortam Korsanı) olarak karşımıza çıkabilmektedir. ''Sistemi hangi tehditlere karşı korumalıyım?'' sorusuna verilebilecek cevaplar bilişim sistemlerine karşı olabilecek tehditleri belirleyebilmemizi sağlayacaktır.(Oracle, 2003)

BİT tehditlerinin sonuçlarını kısa ve uzun vadede ele almak mümkündür. Kısa vadedeki tehditler; hedef alınan şahıs, kurum veya organizasyonun günlük yaşamını etkileyen tehditlerdir. Bunlar dolandırıcılık, şahsi bilgilerin ele geçirilmesi, bankadan

usulsüz para çekme v.b. olarak örneklendirilebilir. Uzun vadedeki tehditler ise etkileri uzun zamana yayılan tehditler olarak nitelendirilebilir.

Bu tarz tehditlere ulusal güvenlik ihlalleri, endüstriyel casusluk v.b. şeklinde ki tehditler örnek gösterilebilir (Yılmaz ve Sağıroğlu, 2013).

Şirketlerin 2011 ve 2012 yıllarında maruz kaldıkları tehditler Şekil-1.1'de gösterilmiştir (Kaspersky, 2013). Firmaların maruz kaldıkları tehditler arasında en dikkat çekici etkenin bilişim sistemlerine yapılan siber saldırılar olduğu dikkat çekmektedir. Bu tehdidin 2011 ve 2012 olmak üzere her iki yılda da bu kadar ön plana çıkması bu konuda alınması gereken güvenlik tedbirlerinin ne kadar hayati boyutta olduğunu vurgulamaktadır.




Şekil 1.1: 2011-2012 Yıllarında Şirketlerin Maruz Kaldıkları Tehditler.

Günümüzde bilişim sistemlerinin, siyasi, eğitim, sağlık, ekonomi, endüstri gibi alanlarda ki kullanımında artış gözlemlenmektedir. Devlet hizmetleri, bankacılık ve finans uygulamaları, sağlık ve eğitim faaliyetleri, sanal market çalışmaları gibi birçok hizmet alımının internet üzerinden gerçekleştiriliyor olması pek çok güvenlik riskini de tetiklemektedir. Bu alanlara yapılabilecek siber saldırılar her geçen gün önem kazanmakta ve siber suçlar ile ilgili yasal mevzuatların ve uluslararası anlaşmaların henüz olgunlaşmamış olması bilişim sistemlerine karşı her gün büyüyen siber tehdidin önemini çok ciddi bir boyuta taşımaktadır (Şimay, 2013).

Küreselleşen dünya düzeninde hem fertlerin hem de devletlerin hayati önemde ki bilgilerini siber ortamda muhafaza etmeleri kötü kişi, kurum veya ülkelerin dikkatini çekmiştir.

Siber tehditler herhangi bir kullanıcının bilgilerini çalmaktan, ülkelerin stratejik önem arz eden sistemlerinin çalışmalarını engellemeye kadar çok geniş bir alanı risk altında bırakmaktadır. Bunun yapılması kasıtlı olabileceği gibi kasıtsız bir şekilde de olabilir. Siber tehditlerin virüs, casuslar, bilgisayar korsanları, terörist gruplar, yabancı ulusların istihbarat birimleri gibi birçok kaynaktan gelmesi muhtemeldir (Gharibi and Shaabi, 2012).

### 1.4.3 Bilişim Sistemlerine Karşı Oluşan Riskler

Bilgi sistemlerine yönelik herhangi bir tehdidin çeşitli zafiyetlerden faydalanarak bilgi güvenliği unsurlarından herhangi birisini zedelemesi risk olarak değerlendirilmektedir (Altundal, 2012). Risk değerinin hesaplanmasında "Bütünlük, Gizlilik ve Erişilebilirlik" değerlerinin ortalaması ile olasılık değeri etkin olarak kullanılmaktadır. Tehdit kaynaklarının azaltılması ve güvenlik boşluklarının en aza indirilmesi, tehdide ait olan riskleri de önemli derecede azaltacaktır (Altundal, 2012a).

Tehdit kaynağı, güvenlik boşlukları ve bu iki varlığın etkileşimi sonucu meydana gelen risk durumları aşağıda Tablo-1.2'de belirtilmiştir (Oracle, 2003).

Tablo 1.2: Tehdit Kaynaklarının Meydana Getirebileceği Bazı Riskler.

| Tehdit Kaynağı | Etkileyebileceği Güvenlik Boşluğu | Meydana Gelen Risk |
|---|---|---|
| Virüs | Anti virüs Yazılımının Eksikliği | Virüs bulaşması |
| Hacker | Sunucu bilgisayar üzerinde çalışan güçlü hizmet programları | Gizli bilgilere yetkisiz erişim hakkının elde edilmesi |
| Kullanıcılar | İşletim sisteminde yanlış ayarlanmış bir parametre | Sistemin çalışamaz duruma gelmesi |
| Yangın | Yangın söndürme cihazının eksikliği | Bina ve bilgisayar sistemlerinin zarar görmesi ve can kaybı olasılığı |
| Çalışanlar | Erişim denetim mekanizmalarının yetersizliği | Görev-kritik bilgilerin zarar görmesi |

| Tablo 1.2: Devam. | | |
|---|---|---|
| İş ortağı olan bir firmanın yetkilisi | Erişim denetim mekanizmalarının yetersizliği | Ticari sırların çalınması |
| Saldırgan | Kötü yazılmış bilgisayar programları | "Tampon Taşması" hatasının alınması |
| Kötü niyetli ziyaretçi | Güvenlik Görevlisinin olmayışı | Kıymetli cihaz veya bilgilerin fiziksel olarak çalınması |
| Çalışan | Tutulan kayıtlardaki yetersizlik | Veri işleme programına verilen giriş verileri ve çıkış olarak elde edilen veriler üzerinde değişiklikler yapılması |
| Saldırgan | Güvenlik Duvarı'nın ayarlarının iyi yapılmamış olması | Bir "Hizmet Durdurma" saldırısının gerçekleşmesi |

## 1.5 Bilgi Güvenliği Prensipleri

Bilgi güvenliğini tam anlamıyla sağlamak imkânsızdır. Çünkü tehditler her geçen gün boyut ve nitelik değiştirerek etki alanlarını genişletmektedirler. Buna bağlı olarak bilgi güvenliğini en üst seviyede sağlamak maksadıyla, tedbirlerin birçok prensip dâhilinde alınması gerekmektedir. Bilgi güvenliğine dair bazı prensipler müteakip maddelerde incelenmiştir.

### 1.5.1 Gizlilik

Gizlilik prensibi; bilginin, yetkisiz olan kişilerin eline geçmesinin engellenmesi veya başkalarına açıklanmaması anlamına gelmektedir (Hostland et al., 2010). Gizlilik prensibi, sadece soft bilgiler için değil, çeşitli depolama cihazlarında depolanan bilgiler içinde söz konusudur. Zira saldırganlar elde etmek istedikleri bilgiler için her türlü yolu denemektedirler.

### 1.5.2 Veri Bütünlüğü

Bu prensip, bilginin ilk sahibinden çıktıktan sonra hiç bozulmadan hedefine ulaşmasını amaç edinir. Öyle ki burada hedef; verinin doğruluğunun, içeriğinin, sırasının v.b. temel etkenlerinin değişmemesidir (Dardick, 2007).

### 1.5.3 Süreklilik

Bilişim sistemleri kendilerinden beklenen hizmetleri yerinen getirirken hedeflenen bir verim kalitesi mevcuttur. Bu verim sayesinde, kullanıcıların memnuniyeti artar ve elektronik sistemlere geçiş süreci hızlanır. Süreklilik prensibi, bu verimin idamesini engelleyecek içeriden ve dışarıdan gelecek tehditlere karşı koruma görevini üstlenir (Oracle, 2003). Süreklilik prensibi sayesinde kullanıcılar ve hizmet alıcılar erişim yetkilerinde olan bilgilerine zamanında ve güvenli bir şekilde erişirler. Sistem sürekliliğini engelleyen faktörler arasında saldırganlar olabileceği gibi eğitimsiz personelin, yazılım hatalarının ve ortam şartlarının da engelleyebileceği unutulmamalıdır (Oracle, 2003).

### 1.5.4 İzlenebilirlik

Bu hizmetin görevi, sistemde verilen hizmetlerin daha sonra ihtiyaç olması halinde kontrol edilebilmesi maksadıyla kayıt altına alınmasını sağlamaktır. Bu olaylar bir şahsın parolası ile sisteme giriş yapması, herhangi bir ağ sistemini veri transferi maksadıyla kullanması veya bir yazıcıdan çıktı alması gibi her türlü işlemi kapsamaktadır. Tutulan bu kayıtların incelenmesi sonucunda herhangi bir saldırı türüne rastlanırsa veya olumsuz bir girişim sezilirse alarm mesajları sayesinde sistem yöneticileri uyarılmaktadır (Çalıkuşu, 2007).

### 1.5.5 Kimlik Doğrulama

Ağ tabanlı yapılar tarafından kimlik doğrulama; alıcı ve göndericinin birbirlerinin doğru noktalar olduğundan emin olmalarıdır.

Bunların yanında bir kişinin bir bilgisayara giriş yaparken karşılaştığı parola doğrulama işlemleri bunun yanında akıllı kartların ve biyometrik cihazlarında çalışma esasları bu kapsamda değerlendirilmektedir (Oracle, 2003).

### 1.5.6 Güvenilirlik

Güvenilirlik prensibi; bilişim sistemlerinde elde edilen çıktı ile beklenen çıktı arasında tam bir uyumun gerçekleşmesi durumudur. Sistem tarafından bilginin fizyolojisi ve mana boyutunda herhangi bir değişiklik meydana gelmemesi güvenilirlik prensibini etkin kılmaktadır (Grance and Jonsen, 2011).

### 1.5.7 İnkâr Edememe

İnkâr edememe prensibi; özellikle parasal işlemlerde sıklıkla karşılaşılan gönderici ve alıcının yaşamış oldukları problemlerin bertaraf edilmesi açısından çok önem arz etmektedir. Günümüzde birçok faaliyet gerçek zamanlı yürütüldüğü için bilişim sistemlerine güveni daha da geliştirmek maksadıyla bu konuda hata yapılmamaya çalışılmaktadır (Saint, 2005).

# 2. BİT SİSTEMLERİNE KARŞI YAPILAN SİBER SALDIRILAR ve TEMEL KAVRAMLAR

Yeni buluşlarla birlikte dünyanın hızlı değişimi insanların, kurumların ve firmaların teknolojiye bağımlılığını artırmaktadır. Son yıllarda büyük bir gelişim mesafesi kat eden BT'nin günlük hayatımızda sıklıkla kullandığımız birçok işlemin altyapısını meydana getirdiği görülmektedir. Bu işlemlere internet üzerinden yapılan bankacılık işlemleri, yine internet üzerinden yaptığımız gerçek zamanlı alış veriş, fatura ödemeleri, sınav ve pasaport başvuruları, günlük gelişmelerin izlenmesi, kredi kartlarının kullanılması, kişisel bilgilerimizi elektronik ortamda muhafaza ediyor olmamız gibi birçok örnek verilebilir (Ünver ve Canbay 2010).

Buraya kadar her hangi bir problemin varlığından çok teknolojik gelişmelerin hayatımızı ne kadar kolaylaştırdığını görüyoruz. Ancak bu durum da gözden kaçırılmaması gereken bir gerçek vardır, o da teknolojik sistemlere ve bilgisayarlara bu kadar bağımlı kalmak kullanıcıların güvenliğini önemli derecede tehdit etmektedir. Yukarıda verilen örnekler tersinden düşünüldüğünde; banka hesaplarından izinsiz para çekildiği, elektronik ortamlarda muhafaza edilen kişisel bilgilerin çalındığı ve farklı amaçlar için kullanıldığı, internet üzerindeki haberleşmelerin izlendiği bir ortam şüphesiz ki insanlarda tedirginlik oluşturur.

## 2.1. Temel Kavramlar

Tez kapsamında sıkça kullanılacak olan siber, siber ortam, siber saldırı, siber suç, siber terörizm, siber savaş kavramlarının anlamları müteakip maddelerde sunulmuştur. Buna göre;

### 2.1.1. Siber

Siber sözcüğü "sibernetik" (Cybernetics) kelimesinin bir ön eki olarak kullanılmaktadır. "Siber" sözcüğü aynı zamanda kelimeyi kısaltmak amacıyla da kullanıldığı bilinmektedir.

Türkçede siber kavramının karşılığı olarak "bilişim" kelimesinin kullanıldığı görülmektedir.

“Bilişim” kelimesinin ifade ettiği anlam ise;

“*İnsanların teknik, ekonomik ve toplumsal alanlardaki iletişimlerinde kullandıkları, bilim dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi*” dir (Altunok ve Çakmak, 2009).

Tanımlar incelendiğinde “siber” ile bilgisayar ve buna bağlı elektronik sistemlerden meydana gelen ortam, “bilişim” ile de bu meydana gelen teknolojik ortamlardan faydalanma anlamlarının çıkarılabileceği görülmektedir.

### 2.1.2. Siber Ortam

Günümüzde BİT’ler hayatımızı şekillendirmede çok önemli roller üstlenmektedirler. Diğer taraftan dünya genelinde bilgisayar kullanıcıları internet vasıtasıyla kolayca iletişime geçerek kendi aralarında çok geniş kapsamlı bir elektronik ortam oluşturmuşlardır ki işte buna siber ortam denmektedir. Bu siber ortam interneti, BİT’leri, yazılımları, birbirlerine bağlı bilgi ağları gibi öğeleri kapsamaktadır.

Diğer bir yönden siber ortam; “insanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma durumu” olarak da tanımlanabilmektedir (Hildreth, 2001).

### 2.1.3. Siber Saldırı

Siber ortam yürütülen faaliyetler açısından kapsamlı bir alana sahip olduğu için güvenlik olarak da birçok saldırıya maruz kalmaktadır. Bu sanal saldırılar olabileceği gibi BİT sistemlerine fiziksel saldırı şeklinde de gerçekleşebilmektedir. Yapılan saldırı sonucunda mutlaka hedef bilgi, sistem veya toplum kitlesi üzerinde bozulma, yaygın bir paniğe neden olmaktadır (Vasilescu, 2012).

Bu anlam da siber saldırılar aşağıdaki gibi sınıflandırılabilir;

- E-posta’lar aracılığıyla programlar içine zararlı virüsler yerleştirerek hedef sistemlere gönderme,
- BİT sistemlerine izinsiz ve illegal girişler vasıtasıyla kişisel bilgilerin elde edilmesi,

- Kamu ve ticari kuruluşların prestijlerini sarsmak ve psikolojik zarar vermek maksadıyla web sitelerinin çökertilmesi,
- Kamu hizmeti veren kuruluşların sitelerine aşırı yüklenerek sistemlerin çalışamaz hale getirilmesi,
- Devletlerin kritik altyapılarına internet ağları üzerinden saldırılarak hem maddi hem de psikolojik zararlar verdirilmesi.

Siber saldırılar yukarıda bahsedildiği şekilde verilere ve kontrol sistemlerine yapılmaktadır. Günümüzde verilerin çalınması çok yaygın bir şekilde gerçekleşmektedir. Kritik altyapılara yapılan saldırılarda sistemlerin kumanda ve kontrol mekanizmalarına yapılarak sistemlerin devre dışı kalmalarına sebep olmaktadır. Bu konuda yaşanmış bir olay olarak 2000 yılında Avustralya'da yaşanan bir olay örnek olarak verilebilir. Atık kontrol sistemine giren eski bir çalışan, bir milyon litre katı atığın bir şehrin sahil sularına yayılarak çok ciddi bir surette kirlilik oluşmasına sebep olmuştur. Bu olay sonucunda eski bir personel sistemin çalışma usullerini bilmesinden dolayı kurumuna büyük zararlar vermiştir (Altunok ve Çakmak, 2009).

### 2.1.4. Siber Savaş

Siber savaşla alakalı birçok tanımlamalar mevcuttur ama en popüler olanı, ABD Başkanı Bush'un siber güvenlik danışmanının (cyberwar) adlı kitabında yapmış olduğu tanımlamadır.

"*Bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirilen sızma faaliyetleridir* (Clarke and Knake, 2010).

Özellikle soğuk savaş sonrası dönemde ülkeler birbirleri ile olan mücadelelerini teknoloji ve ekonomi alanlarına çevirmişlerdir. Bir devletin her türlü yeni teknolojiye sahip olması veya ekonomide, endüstride çok iyi konuma gelmesi kendisine düşman olan ülkeler tarafından daima hedef tahtasına oturtulmuştur. Ülkeler hedeflerindeki diğer ülkelere elektronik saldırılarla sistemlerini çökertme, önemli projelere dair bilgilerini sızdırma, alınan şahsi bilgiler neticesinde şantaj maksatlı kullanma gibi birçok saldırı girişimine başvurmaktadırlar. Siber savaş gizlidir, gerçektir, dünyanın her yerini kapsamaktadır ve çok hızlı bir şekilde gerçekleşmektedir (Lupovici, 2011).

### 2.1.5. Siber Suç

Siber suçlar bilgisayar sistemleri ve bilgisayar ağları vasıtası ile işlenebileceği gibi kredi kartı, cep telefonu gibi çok sık kullandığımız araçlarla da bu suçlar işlenebilmektedir.

Siber olaylar özellikle 2000'li yıllardan itibaren gündeme damgasını vurmuş sonuçları itibariyle çok önem arz eden bir konudur. Bu önemini kavrayan ülkeler siber saldırı ve sızdırma yapma konusunda ayrıca birimler kurarak ve yatırımlar yaparak bu pastadan paylarını almaya çalışmaktadırlar. Gerek devlet destekli gerekse bir grubun oluşturduğu siber saldırı takımları yaptıkları saldırılarla hedef ülkelerin ulusal güvenlilerini tehdit eder duruma gelmişlerdir. Bu arada bu saldırıları ticarileştirerek para karşılığı yapan özellikle sanal ortamda kendi reklamını yapmaktan kaçınmayan birçok siber saldırgan da mevcuttur. Ama günümüz de ki gelişmelerde de görülebileceği gibi yapılan bir siber saldırı sonucu saldırganların yeri, menşei ve niteliği saptanamamakta veya ispat edilememektedir. Bu sebepledir ki siber saldırıya başvuran şahıs, grup veya devletler bu konuda çok rahat edebilmektedirler (Tabansky, 2012).

### 2.1.6. Siber Terörizm

Siber terörizm, bilgi ve iletişim teknolojileri sistemlerine zarar vermek, etkisiz hale getirmek, maksadıyla, eylemlerinde en etkili silah olan internet tabanlı bilişim sistemlerini kullanarak yapılan kasıtlı faaliyetlerdir (Stohl, 2006).

Bu alanda ki yapılan saldırılar illegal olarak gerçekleştirildiği için sınırlarının çok geniş boyutlara ulaşabileceği tartışılmazdır. Siber terörizm, terör örgütleri tarafından oldukça fazla rağbet görmektedir. Teröristleri siber saldırılara sevk eden nedenler aşağıda belirtilmiştir (Altunok ve Çakmak, 2009).

- Daha az mali kaynak ve personel ihtiyacı gerektirir,
- Uygulama yöntemi geleneksel terör eylemlerinden daha kolaydır,
- Çok ileri eğitimli olmayı ya da ileri teknolojiyi gerektirmez,
- Tespit edilmeleri ve özellikle kimliklerinin tespit edilmesi oldukça zordur,
- Muhtemel hedeflerinin sayısı ve çeşidi oldukça fazladır,

- Siber terörizm coğrafi engelleri ortadan kaldırmaktadır, uzak mesafelerden saldırılar kolaylıkla gerçekleştirilebilmektedir.

### 2.1.7. Siber Güvenlik

Siber güvenlik (Cyber Security); siber ortamda kurum kuruluş ve kullanıcıların varlıklarını korumak maksadıyla kullanılan araç, politika, güvenlik kavramları, risk yönetim yaklaşımları, güvenlik teminatları, faaliyetler, eğitimler, uygulamalar ve teknolojiler bütünüdür. Bu tanım kurum ve kuruluşların bilgi işlem donanımlarını, personel, altyapı, uygulamalar, hizmetler, elektronik haberleşme sistemleri ve siber ortamda iletilen ve saklanan tüm bilgileri kapsamaktadır (Şimay, 2013).

Siber güvenlik, devlet kurumları, firmalar, şahısların varlıklarını siber saldırılara ve siber terör eylemlerine karşı koruyabilecek niteliklere haiz olmalıdır. Siber tehditler birçok gelişmiş ülke yöneticileri tarafından en tehlikeli tehdit olarak nitelendirilmektedir. ABD Başkanı Obama siber tehdidi,
"*Millet olarak karşı karşıya kaldığımız en ciddi milli ve ekonomik güvenlik tehditlerinden biri*" olarak tanımlamaktadır (Çifci, 2012).

Siber ile ilgili bahsedilen temel kavramların temel özelikleri ve birbirleri arasındaki ilişkiler Tablo-2.1'de özetlenmiştir (Altunok ve Çakmak, 2009).

Tablo 2.1: Siber Suç, Siber Terör ve Siber Savaşın Temel Özellikleri.

| Eylemin | Siber Suç | Siber Terör | Siber Savaş |
|---|---|---|---|
| Niteliği | Doğrudan | Sembolik | Doğrudan, Sembolik |
| Şiddeti | Az Yoğun | Yoğun | En Yoğun |
| Motivasyonu | Kişisel Kazanç | Siyasi | Siyasi, Doğrudan Savaş Kabiliyetini Azaltmak, Casusluk |
| Failleri | Bireyler, Organize Suç Örgütleri, Anonim | Terörist Örgütler, Hangi Örgüt Olduğu Tahmin Edilebilir. | Failin kim olduğu tam olarak bilinmese de hangi devletlerden kaynaklandığı bilinebilir. |

| Tablo 2.1.: Devam. | | | |
|---|---|---|---|
| Hedefleri | Kazanç Sağlanacak Hedefler | Kritik Tesisler, Güvenlik Birimleri, Hükümet Temsilcilikleri | Kritik Tesisler, Ekonomik ve Endüstriyel Altyapılar, Güvenlik Birimleri, Hükümet Temsilcilikleri, Askeri Altyapılar. |
| Kaynağı | Ülke İçinden veya Dışından | Ülke İçinden veya Dışından | Ülke Dışından |

## 2.2. BİT Sistemlerine Karşı Yapılan Siber Saldırılar

Siber saldırılar; Siber saldırganların (bunlar bir devlet organı olabileceği gibi şahıs veya yasa dışı örgüt de olabilir) hedef olarak belirledikleri argümanlara ulaşmak için siber ortamda gerçekleştirdikleri saldırılardır. Siber saldırılar, veri tabanlarını, yazılım ve donanımları hedef almaktadır. Özellikle 2007 yılında Rusya'nın Estonya'nın devlet organlarının çalışmasını hedef alması ile kendini duyuran siber saldırılar günümüzde gerek açıktan gerekse perde arkasından yoğun bir şekilde hedef kitlelere uygulanmaya çalışılmaktadır (Vasilescu, 2012).

Bilişim sistemlerine ve bilgisayar ağlarına çok farklı türden saldırılar düzenlenebilmektedir. Bunlardan bazı önemli olanları;

### 2.2.1. Kabloya Saplama Yapma

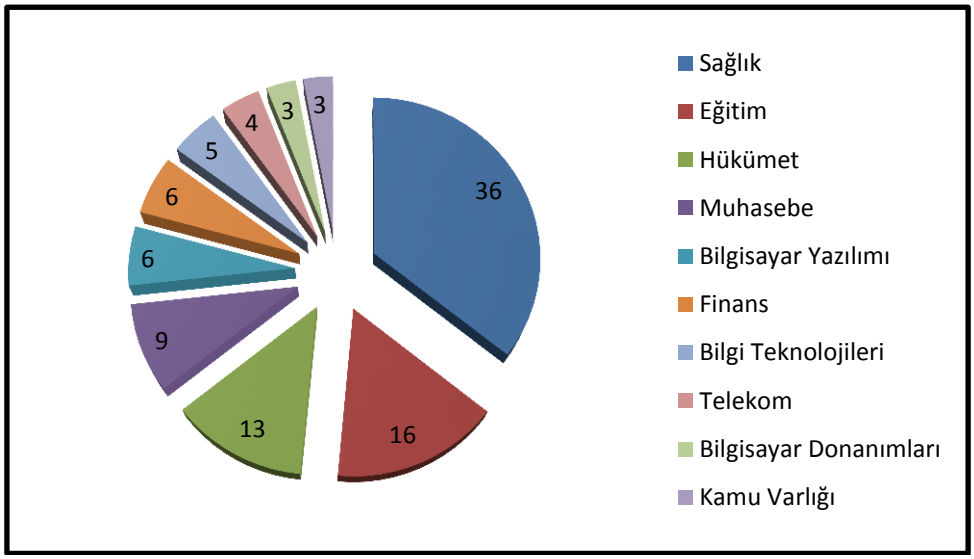
Kabloya saplama yapma (Wire Tapping), özel cihaz ve tekniklerle yeterli güvenlik önlemi alınmamış olan iletişim ağı kablolarına fiziki olarak saplama yapılması ve ilgili iletişim ağı ile bağlantıya geçilmesidir. Bu metotla iletişim faaliyetinde bulunan her iki unsurunda bilgi trafiği ele geçirilmiş bulunmaktadır. Bilgisayar ağları, telefon trafiği ve fiber hatların da bu yöntemle dinlenebilmektedir.

### 2.2.2. Hizmet Dışı Bırakma (Dos, Ddos)

Hizmet dışı bırakma (Denial of service, DOS), bilgisayar sistemlerinin hedef kullanıcılar tarafından kullanılmasını engellemek veya sistemleri çalışamaz hale getirmek maksadıyla gerçekleştirilen saldırılardır. Bu metodu daha etkili kılmak maksadıyla "Dağınık Hizmet Dışı Bırakma" (Distributed Denial of Service-DDOS) saldırıları da yaygın olarak kullanılmaktadır (Altundal, 2012b).

DDOS; DOS saldırısının dağıtık yapıda uygulanmasıdır. Bu saldırı türü, birçok bilgisayar tarafından hedef seçilen bir servisin legal olarak kullanımını engellemek maksadıyla yapılır. Burada amaç sistemlere sızma girişimi değil bilişim sistemlerine erişimi etkisiz kılma çabasıdır (Çifci, 2012).

DDOS saldırılarının, yalnızca bilgisayarlardaki güvenlik programları veya işletim sistemleri tarafından %100 olarak engellenmesi mümkün değildir. Başarılı bir Ddos koruması için sistemin tasarım aşamasından başlanarak Network'ün tüm aşamalarında gerekli güvenlik önlemleri alınmalıdır. Ataktan önce Network Trafiği özenle izlenmesi ve uzman personelden yardım alınması fayda sağlayacaktır. Daha sonra atak algılama ve filtreleme işlemlerinin uygulanması ve ardından atak kaynağının tanımlanması ve izlenmesi uygun olacaktır. Dünya genelinde değişik sektörlere saldırılar düzenlendiği bilinmektedir. Şekil 2.1'de 2012 yılında dünya genelinde saldırı yapılan ve bilgi ihlali ile sonuçlanan saldırı yüzdeleri sunulmuştur (Colesniuc, 2013).




Şekil 2.1: 2012 Yılındaki Sektörel Bilgi İhlalleri.

### 2.2.3. Kriptografik Saldırılar

Kriptografik saldırılar; şifre ile korunmaya çalışılan mesaj veya verilerin şifrelerinin çözülmesi maksadıyla uygulanan saldırılardır. Bu tarz saldırılarda sistemin genel kriptolojisinin zayıf tarafları araştırılarak çözmeye çalışılır. Kriptografik algoritmaların tasarımında temel prensip, güçlü bir algoritmanın güvenliği, bütünüyle anahtar yapısının içindedir, algoritmanın tasarım detaylarında değildir. Bu sebepten dolayı güçlü algoritmaya sahip sistemlere karşı saldırılar, anahtarın tahmin edilmesini ya da ele geçirilmesini ve bilinmeyen algoritmaların anlaşılmasını gerektirir (Çifci, 2012).

### 2.2.4. Yemleme (Phishing)

Bilişim sistemleri kullanıcılarının, kandırılmaları veya ikna edilmeleri neticesinde kişisel bilgilerini alarak kişilerin bilgisayar sitemlerine gönderilen virüsler aracılığıyla sitemi ele geçirme girişimleridir. Bu durumda elde edilen bilgiler dolandırıcılık faaliyetlerinde kullanılabileceği gibi siteme zara vermek maksadıyla da kullanılmaktadır (Patel and Zaveri 2010).

### 2.2.5. Yerine Geçme (Masquerading)

Yerine geçme, bilişim sistemlerinde bir bilgisayarın başka bir bilgisayarın yerine geçerek onun nüfuzunu kazanma eylemidir. Bu eylem, bir ağdaki dâhili bir bilgisayar aracılığı ile diğer bütün bilgisayarları dış dünyaya bağlamak için veya herhangi bir saldırı yapmak içinde kullanılabilir. Yerine geçme saldırısında, kullanıcı hesapları, parola, kişilik bilgilerinin elde edilerek güvenlik zafiyetlerinden faydalanarak sisteme zarar vermeyi amaç edinmektedir (Otuteye, 2013).

### 2.2.6. Köle Bilgisayarlar

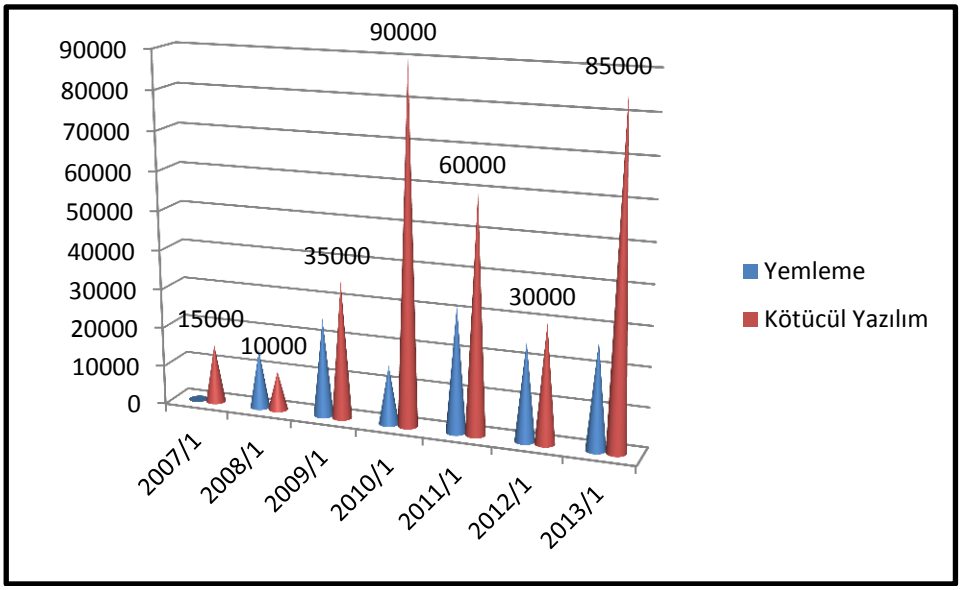
Bilişim sistemleri kendilerine erişen herhangi bir kötücül yazılım veya program vasıtasıyla uzaktan kontrol altına alınabilmektedir. Uzaktan kontrol edilebilen ve kötücül kullanımlara açık olan ve birçok bilgisayardan oluşan yapıya köle bilgisayarlar (zombie) denir.

Bilgisayar sistemlerine gizlice yerleşerek saldırganın bu bilgisayarları internet üzerinden kontrol etme imkânı tanıyan bu programlar, yaklaşık olarak dünya genelinde ev bilgisayarlarının %10'unda aktif oldukları bilinmektedir (Arora, 2012).

### 2.2.7. Kötücül Yazılımlar

Bir diğer saldırı yöntemlerinden birisi de, bilişim sistemlerine zararlı yazılımlar gönderilerek siteme zarar verilmesidir. Kötücül yazılımlar çok değişik metotlarla hedef bilgisayara yerleştirilebilmektedirler. Sistem güvenliğinde açık bir noktanın tespit edilerek (port, servis, v.b.), kullanıcı hatalarından yararlanılarak, güncelleme ve program yükleme sitelerinin taklit edilerek (Phishing) yazılımların hedef bilgisayar sistemlerine yükletilmesi sağlanarak saldırı gerçekleştirilebilmektedir. Dünya genelinde yıllara sarih yemleme ve kötücül yazılım değerleri Şekil-2.2'de gösterilmiştir (Symantec, 2013).

Burada özellikle 2010 ve 2013 yıllarındaki kötücül yazılım artışları oldukça dikkat çekmektedir.




Şekil 2.2: Güvenliği Zayıf Olan, Haftalık Saldırıya Uğrayan İnternet Site Sayıları.

Bilinen başlıca kötücül yazılımlar aşağıda belirtilmiştir;

#### 2.2.7.1. Truva Atı (Trojen Horse)

Truva atı; yararlı gibi görünen fakat arkasında gizli bir kodunda yer alması nedeniyle bilişim sistemlerine zarar veren bir yazılım çeşididir. Truva atları bilgisayarları arkadan yönetmek için arka kapı açan yazılımlardır. Truva atları bilişim sistemlerine eriştiğinde kendi başlarına herhangi bir işlem yapamazlar. Truva atları bilişim sistemlerine yayılsalar bile her bilgisayar sahibinin bu Truva atlarını çalıştırmaları gerekir (Turhan 2010).

#### 2.2.7.2. Solucan (Worm)

Bilişim sistem ağları arasında bağımsız olarak dolaşan, kendi kendini kopyalayabilen ve kendini aktif haline getirebilen, herhangi bir donanım ve yazılıma zara verme zorunluluğu olmayan yazılımlardır. Solucanlar, güvenlik açığını buldukları herhangi bir bilgisayara yerleşir ve daha sonra kendini defalarca kopyalayarak aynı ağa tanımlı tüm bilgisayarlara yayılır. Saniyeler içinde milyonlarca bilgisayara bulaşabilir. Solucanlar genellikle virüsler ile karıştırılmaktadırlar fakat solucanlar virüsler gibi sisteme zarar vermeden de sistem içinde dolaşabilmektedirler (Guinchard, 2011).

#### 2.2.7.3. Virüs

Virüs başka programlara bağımlı olarak çalışabilen, kendi kendini kopyalayabilen, sitem üzerinde yerleşebileceği herhangi bir programa ihtiyaç duyan bir yazılımdır. Yerleştiği bilgisayar kullanıcısı tarafından virüsün yerleştiği programın çalıştırılmasından itibaren virüs aktif hale gelerek başka programlara da bulaşmaya başlar. Zararlı virüsler 1980'li yıllarda ortaya çıkmasından itibaren çok hızlı bir gelişim göstermiştir. Gün geçtikçe virüsler kopyalandıkları program içine çok iyi gizlenmekte ve görünmemektedirler. Buna mukabil kullanıcılarda karmaşık yakalama tekniklerini uygulayabilen anti virüs programlarını kullanmaya başlamışlardır (Giordano and Francesco, 2013).

### 2.2.7.4. Arka Kapılar (BackDoor)

Bilişim sistemi üzerinde normal araştırmalar kapsamında bulunamayacak şekilde normal kimlik kontrol mekanizmalarına takılmayan veya uzaktan bu sisteme erişmeye çalışan kişiye olanak tanıyan yöntemlerdir. Arka kapılar, sistemdeki açıklıklardan faydalanarak meydana gelmektedir. Bu bazen programcının herhangi bir portu gerek bilerek gerekse bilmeden açık bırakması ile olabileceği gibi önceden sisteme sızmış kötü niyetli bir kişinin de açık bırakması ile gerçekleşebilmektedir (Knopová and Knopová, 2014)

### 2.2.7.5. Mantık Bombası (Logıc Bomb)

Belirli bir zamanda veya belirli şartların oluşmasında çalışabilen yazılımlardır. Bu yazılımın bozucu, aldatıcı, yıkıcı etkileri mevcuttur. Mantık bombası sistem içinde çalışacağı günü bekleyebilir veya kullanılan bir program içinde zamanı geldiğinde zararlı girişimlerde bulunmak maksadıyla kendini muhafaza edebilmektedir. Söz konusu kötücül yazılım, kullanacağı bilgileri önceden kodlar, saldırgan tarafından talimat gönderilince de görevini icra eder (Robillard, 2004).

### 2.2.7.6. Kök Kullanıcı Takımı (Rootkit)

Bilişim sistemlerinde çalışmakta olan işlemleri, dosyaları verileri ve sistem bilgilerini işletim sisteminden gizleyerek varlığını gizlice idame ettiren kötücül yazılımlardır. Genellikle işletim sisteminde çekirdek düzeyinde çalıştıkları için tespit edilmeleri zordur (Önal, 2012).

### 2.2.7.7. Klavye Dinleme (KeyLogger)

Klavye dinleme; bilgisayar kullanıcısının klavyede dokunduğu tuşları başka bir kaynak bilgisayar tarafından kaydedilmesine yarayan programlardır. Bu yöntemle kullanıcıların girmiş oldukları şifreler, kullanıcı adları, e-posta adresleri gibi kişisel bilgiler rahatça başkaları tarafından öğrenilebilmektedir (Özdemir, 2007).
Bu programlardan bazıları; Keysnatch, Spyster, Keylogger, Prokeylogger'dır.

# 3. SİBER SAVUNMA

Siber savunma; siber ortamda faaliyet gösteren yazılım, donanım ve ağ tabanlarından meydana gelen bilgi sistemlerini ve bu sistemlere bağlı olarak çalışan araç, teçhizat, sistem ve alt yapıları, oluşabilecek siber tehditlere karşı koruyabilmek için alınabilecek önlemler dizisidir. BİT sistemlerinin zararlı yazılımların olumsuz etkilerine maruz kalmaları nedeniyle yavaşlama veya devre dışı kalma problemi ile karşı karşıya kalmaktadırlar. BİT'ler söz konusu saldırılardan korunmak için alınması gereken bazı tedbirler mevcuttur. Öyle ki bu tedbirler alındığı takdirde sistemler de tutarlı ve sağlam bir şekilde çalışmalarına devam edeceklerdir (Karaarslan vd., 2008).

Bunu sağlamanın yöntemlerinden birisi de saldırı tespit edildiğinde savunma önlemlerinin alınmasının yanında sistemin fiziksel ya da yazılımsal olarak zarar gören bileşenlerinin acilen çalışır hale getirilmesi gerekmektedir. Gizlilik ilkesi siber savunmanın en temel ilkesidir. BİT sistemlerini veya diğer kritik altyapı sistemlerini meydana getiren her türlü yazılım, donanım ve veri tabanlarının gizliliğinin sağlanması gerekmektedir (Çifci, 2012).

## 3.1. Siber Savunma Faaliyetlerinin Temel Nitelikleri

Siber ortamda işlev gören BİT sistemleri ve siber sistemlerin savunma faaliyetlerinin temel özellikleri şu şekilde sıralanabilir (Çifci, 2012),

- Siber saldırı ve tehditlerin analiz edilmesi,
- Siber tehditler ile ilgili uyarı ve ikaz sistemlerinin kurularak merkezi olay yönetiminin desteklenmesi
- BİT sistemlerinin her türlü siber saldırı ve elektronik taarruzlardan korunması,
- BİT sistemlerine izinsiz illegal girişlerin engellenmesi,
- Ağ tabanlarında ya da BİT sistemleri üzerinde meydana gelebilecek zararlı ve izinsiz girişimlerin, işlemlerin engellenmesi,
- BİT sistemlerinin alt yapılarının dışarıdan gelebilecek saldırılara karşı fiziksel olarak da çok dayanıklı olarak inşa edilmesi,

- Siber ortamda faaliyet gösteren her türlü sistem başta olmak üzere, bu sistemi meydana getiren tüm bileşenlere yönelik siber saldırı ve girişimlerin derinlemesine analiz edilmesi,
- Siber savunma sistemleri tarafından saldırı girişimleri tespit ve teşhis edilerek, BİT sistemlerine zarar vermeden yerinde reaksiyonlarla saldırının engellenmesi.

## 3.2. Siber Savunma Sisteminin Unsurları

### 3.2.1. Güvenlik Duvarı

Güvenlik duvarı yazılımları, bilgisayar sisteminin bir parçası olmakla birlikte kuruldukları konumda bir kural kümesi prensibinde çalışan, bilgisayara ve internet ağına gelen giden veri trafiğini kontrol eden ve sisteme yetkisiz erişimleri engelleyen güvenlik sistemleridir (Arora, 2012).

Program birçok filtreleme özelliği ile bilgisayar ve ağın gelen giden tüm veri transferleri olmak üzere tüm internet trafiğini kontrol altında tutmaktadır. Web filtreleme, port filtreleme, içerik filtreleme bunlardan bazılarıdır. Güvenlik duvarı kullanımı ve bağlantı noktası yapılandırma konusunda iyi seviyede yetişmiş personel tarafından son derece güvenli bir şekilde yapılandırma işlemleri tesis edilerek gelebilecek tehlikelere karşı korunma sağlanabilecektir (Kaya ve Öğün, 2009).

### 3.2.2. Antivirüs

Bilgisayar ve ağ sistemlerinin, zararlı programlardan korunmak için programlanmış olan ve aynı zamanda temizleme ve kurtarma işlevlerini yerine getiren güvenlik yazılımlarına denir. Bu kapsamda Antivirüs programı herhangi bir programın veya casus yazılımın korumalı bir dosyaya erişimini engelleyerek veya şüpheli bir yazılım konusunda kullanıcıyı uyararak görevini yerine getirdiği görülmektedir. Antivirüsler tek başlarına yeterli seviyede güvenlik sağlayamazlar, bunların yanında güvenlik duvarı gibi diğer güvenlik yazılımlarının da kullanılması gerekmektedir (Zeltser, 2011).

### 3.2.3. Sayısal İmza

Verinin içeriğinin değiştirme durumu ve gönderen kaynağın gerçekliliğini ispat etme söz konusu olduğunda kullanılır. Sayısal imza kısaca yazılan mesajın özetinin gizli bir anahtar ile şifrelenmesi ve bir sıra numarası verilmesi ile elde edilmektedir. Fakat sayısal imzanın güvenilirliği, el ile atılan imza ya göre daha etkindir. Sayısal imzanın daha güvenilir olmasını sağlayan etken, imzalamada kullanılan matematiksel algoritmalardır. Amaç kimlik doğrulamasının yapılabilmesidir (Gennaro and Rohatni, 2001)

Sayısal imza, imzalanacak belgenin bir özet fonksiyonundan geçirilerek elde edilen özetinin, imzalayan kişinin gizli anahtarıyla şifrelenmesi ile elde edildiği için, imza veya imzalanan belge değişikliğe uğradığında kolayca fark edilir ve belge reddedilir. Bu da belgenin bütünlüğü ve kaynağını güvenilir kılmaktadır.

### 3.2.4. İçerik Filtreleme

İçerik filtreleme, iletişim ağı veya bilgisayara giren ve bilgisayardan çıkan tüm trafiğin incelenmesi sonucunda gerek zararlı olarak nitelendirilen gerekse istenmeyen verileri filtreleyen yazılımlardır. Bu yazılımlar aracılığıyla istenmeyen web siteleri, elektronik postalar, belirli kelimeler, resimler, uygulamalar filtrelenerek engellenebilmektedir (Stark, 2007).

Son yıllarda ailelerin çocuklarını sanal dünyanın zararlı etkilerinden bir nebze olsun koruyabilmek maksadıyla başvurduğu yollardan birisidir.

### 3.2.5. Adli Bilişim

Genel olarak adli bilişim, bilişim sistemlerinden delil elde edilmesi, elde edilen delillerin veri bütünlüğü bozulmadan analiz edilerek gerekli işlemlere tabi tutulmasına denmektedir. Günümüzde birçok suçun yine birçok alanda işlenmesi sonucu suçun ve suçlunun tespiti konusunda önemli derecede zorlanılmaktadır (Boyd and Forster, 2004).

Hiçbir suçlu yoktur ki ardında iz bırakmadan suçunu işlesin prensibinden yola çıkarak özellikle bilişim sistemlerinde işlenen suçlar da adli bilişim teknikleri kullanılarak suçluların tespiti konusunda ciddi surette mesafe alınabilmektedir.

### 3.2.6. Bal Küpü

Bal küpü, bilişim sistemlerine karşı saldırıların tespit edilmesinde kullanılmaktadır. Yani gücünü saldırılabilirliğinden alan bir güvenlik yazılım türüdür. İnternet ağı üzerine yerleştirilen Bal küp'leri saldırganları üzerine çekerek saldırı ve saldırgan konusunda ipucu elde etmeye yarayan yazılım türleridir (Gökırmak vd., 2013)

Bal küpleri birçok saldırı türünü üzerine çektiklerinden dolayı, kullanıldıkları ağ için bir tehdit oluşturabilirler. Bal küpü sistemi üzerinde bilinçli olarak bazı açıklıklar bırakılarak güvenlik sistemlerini aşabilen saldırı girişimleri tespit edilmektedir.

### 3.2.7. Siber Tehditleri Algılama Sistemi

BİT sistemlerine yapılan saldırıların tespit ve teşhis edilmesinde kullanılan bir başka yolda algılama sistemlerinin kullanılmasıdır. Burada güvenliği yalıtılmış bir ortamın içeriği kaydedilip faaliyetleri izlenerek bir saldırı girişiminin tespit edilmeye çalışılması söz konusudur. Bu amaçla üretilen " Siber Tehditleri Algılama Merkezi Projesi" aracılığıyla ağın herhangi bir noktasına yapılmakta olan siber saldırılar anında tespit edilebilmektedir. Ağın kritik noktalarına yerleştirilecek olan bu sitemler ile bütün ağı tehdit etmekte olan saldırılar tek bir noktadan izlenebilmektedir (Karnikis et al., 2013).

### 3.2.8. Şifreleme Sistemleri

Açık anahtarlı şifreleme; şifre ve deşifre işlemlerinin yapılabilmesi için farklı anahtarların kullanıldığı bir şifreleme sistemidir. Haberleşen taraflardan her ikisinde de birer çift anahtar bulunmaktadır. Bu anahtarlardan birisi gizli anahtar olarak, diğeri ise açık (gizli olmayan) anahtar olarak adlandırılmaktadır. Bu anahtarlardan hiç birisi hem şifreleme hem de deşifre işlemlerinin her ikisini beraber yapamamaktadır. Bir evin güvenliğinin alarm sistemi ile sağlanması gibi bir verinin veya bir dosyanın da şifrelenerek korunması sağlanabilmektedir. Bu şekilde izinsiz bir şekilde şahsi veya kurumsal bilgisayara erişim sağlandığında dosyaların şifrelenmesi vasıtasıyla veriye erişim sağlanamayacaktır. (Symantec, 2012).

### 3.2.9. Kimlik Doğrulama Sistemleri

Ağ sistemlerine ve bilgisayarlara kullanıcı maksatlı giriş yapacak şahısların kimlik bilgilerinin güvenli bir şekilde sorgulanması, sistemlere erişim için atılması gereken ilk adımdır. Tablo-3.1'de bilinen bazı kimlik doğrulama sistemleri özetlenmiştir (Çifci, 2012).

Tablo 3.1: Yaygın Olarak Kullanılan Kimlik Doğrulama Sistemleri.

| Doğrulama Ekseni | Doğrulama Sistemi |
|---|---|
| **Personel Bilgisi** | Kullanıcı tarafından bilinen statik şifreler. |
| | Zamana veya sorgu sıralamasına dayalı olarak dinamik bir algoritma tarafından üretilen dinamik (bir defalık) şifreler. Örnek: Bankacılık işlemlerinde cep telefonu aracılığıyla gönderilen tek kullanımlık şifreler. |
| **Personel Konumu** | Sorgulama ve cevap: Doğrulayıcının sorgusuna, tekil bir cevap sağlayan elektronik simge veya akıllı kart cihazı. |
| | Adrese dayalı cevap: Kaynağı doğrulamak için, sistem tarafından daha önce kendisinde kayıtlı olan bilgileri geri çağırarak bağlantıyı kurar. |
| | Konuma dayalı cevap: Kullanıcı, GPS (Global Positioning System) vasıtasıyla dünya üzerindeki fiziksel konumu ile cevap verir. |
| | Kriptoğrafik doğrulama: Elektronik simge veya akıllı kart cihazlarına kriptografik yazılımlar yüklenerek kimlik doğrulaması yapılır. |
| **Personel Özellikleri** | Biyometrik yöntemlerle kimlik doğrulama[1],<br>Retina taraması,<br>Parmak izi,<br>Yüz şekli,<br>Ses, |
| | İnsan vücuduna cihazın fiziksel olarak entegre edilmesi, |

[1]Biyometrik Yöntem: Kullanıcıların önceden deri altı okuyucu sensörler ile parmak, avuç içi gibi organlarının deri altı damar görüntüsünün alınarak veri tabanına kaydedilmesi ve daha sonrada kullanıcının sisteme giriş maksatlı her faaliyetinde kullanıcı kimlik doğrulama yapmak istediğin de ilgili organın damar haritası alınır ve daha önce veri tabanında kayıtlı olan görüntü ile karşılaştırılır.

# 4. SİBER GÜVENLİK KONUSUNDA TÜRKİYE'DE Kİ MEVCUT DURUM

Ülkemizde BİT sistemleri kullanımının hızla yaygınlaşması pozitif faydalar sağladığı gibi güvenlik, bilişim suçları ve gizli bilgilerin ihlali gibi birçok tehlikeyi de beraberinde getirmiştir. BİT sistemlerinin kamu kuruluşları yanında kritik altyapı sektöründe de kullanılması bu konunun güvenlik açısından önemini daha da artırmaktadır. Kritik altyapıların maruz kalabileceği her hangi bir siber saldırının; ülke çapında önemli derecede maddi zarara, can kaybına, ulusal güvenliğin sarsılmasına ve kamu işleyiş düzeninin zedelenmesine sebep olabilecektir.

Siber ortamda meydana gelen her türlü siber saldırı girişimi anonimlik taşıdığı ve inkâr edilebildiği bilinmektedir. Özellikle kritik altyapıların güvenliğine ilişkin yapılan siber saldırıların kaynağının tespit edilmesi oldukça zordur. Bu durum siber saldırılar, risk ve tehditlerin asimetrik bir etkiye sahip olduğunu gözler önüne sermektedir.

Bütün bu bilgiler ışığında, Bakanlar Kurulunun 11 Haziran 2012 tarihli ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararı" 20 Ekim 2012 tarihinde 28447 sayılı resmi gazetede yayınlanmıştır. İlgili bakanlar kurulu kararınca; Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan program rapor usul esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında Siber Güvenlik Kurulu kurulmuştur. Siber Güvenlik Kurulu (SGK)'nu oluşturan üyeler (ResGaz 3, 2012) ;

- Ulaştırma, Denizcilik ve Haberleşme Bakanı (Başkan),
- Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,
- Milli Savunma Bakanlığı Müsteşarı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,
- Kamu Düzeni ve Güvenliği Müsteşarı,
- Milli İstihbarat Teşkilatı Müsteşarı,

- Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,
- Bilgi teknolojileri ve İletişim Kurumu Başkanı,
- Türkiye bilimsel ve Teknolojik Araştırma Kurumu Başkanı,
- Mali Suçları Araştırma Kurumu Başkanı,
- Telekomünikasyon İletişim Başkanı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanıca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır.

Yukarıda bahsedilen bakanlar kurulu kararı ile ulusal siber güvenliğin sağlanmasına ilişkin her türlü politika, eylem planı ve strateji belirleme görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir. Yine aynı karar kapsamında tüm kamu kurum ve kuruluşlar ile gerçek ve tüzel kişiler, Siber Güvenlik Kurulu tarafından belirlenen politika, strateji ve eylem planı çerçevesinde kendilerine tevdi edilen görevleri yerine getirmek ve belirlenen usul ve esaslara uymakla yükümlü hale getirilmiştir (ResGaz 3, 2012).

## 4.1. Ülkemizde Siber Güvenlik Çalışmaları Kapsamında 2013-2014 Eylem Planında Görev Verilen Kurumlar

20 Ekim 2012 tarih ve 28447 sayılı resmi gazete ile yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" kapsamında Siber Güvenlik Kurulu oluşturulmuş, bu kurul üyesi bakanlık ve kuruluşlara "Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı"nda bazı görevler verilmiştir. Bu kurumlar aşağıda sunulmuştur (ResGaz 3, 2012)

Ulaştırma, Denizcilik ve Haberleşeme Bakanlığı

- Bilgi Teknolojileri ve İletişim Kurumu (BTK)
- Ulusal Siber Olaylara Müdahale Merkezi (USOM)
- Siber Olaylara Müdahale Ekipleri (SOME)
- İnternet Geliştirme Kurulu
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
- Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)
- ULAKNET Bilgisayar Olaylarına Müdahale Birimi (Ulak-CSIRT)

- Siber Güvenlik Kurulu (SGK)
- TSK Siber Savunma Merkezi Başkanlığı

## 4.2. Türkiye'de Siber Güvenliğe Yönelik Atılan Önemli Adımlar

Türkiye, siber güvenlik konusunda ki çalışmalarına 2003 yılında başlamıştır. Bu alandaki çalışmaların kronolojik sıralaması (Çifci 2012);

- 2003/10 Sayılı Başbakanlık Genelgesi (2003)
- E-Dönüşüm Türkiye Projesi (2003)
- E-Dönüşüm Türkiye Projesi Eylem Planı (2005)
- Bilgi Toplumu Stratejisi ve Eylem Planı (2006)
- Ulusal Sanal Ortam Güvenlik Politikası (2009)
- MGK Bildirisi (2010)
- Siber Güvenlik Çalıştayı (2011)
- Siber Güvenlik Hukuku Çalıştayı (2012)
- Ulusal Siber Güvelik Strateji Çalıştayı (2012)
- TBMM Meclis Araştırma Komisyonu Raporu (2012)
- Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (2012)
- Siber Güvenlik Kurulunun İlk Toplantısı (2012)
- Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının Kabul Edilmesi (2013)
- USOM (Ulusal Siber Olaylara Müdahale Merkezi) ve Balküpü Sisteminin TİB Tarafından Kurulması ve İşletilmesine Yönelik Kararın Onaylanması (2013)
- SOME'lerin (Siber Olaylara Müdahale Ekipleri) Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esasların Yayınlanması (2013)

## 4.3. Türkiye'de Siber Güvenliğe Yönelik Gerçekleştirilen Yasal Düzenlemeler

Türkiye 2003 yılından itibaren farklı yönleri ile ele almaya çalıştığı siber güvenlik konusunda, siber güvenliğe yönelik hükümler içeren yasal düzenlemeler yapmayı da ihmal etmemiştir (Çifci, 2012).

Yapılan bu düzenlemeler;

- 5070 Sayılı Elektronik İmza Kanunu,
- 5237 Sayılı Türk Ceza Kanunu (TCK) Kapsamında (ResGaz 2, 2004),
  - Hürriyete Karşı Suçlar (Md. 124),
  - Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar (Md.132-136),
  - Bilişim Alanında Suçlar (Md. 242-246).
- 5271 Sayılı Ceza Muhakemesi Kanunu (CMK) (Md. 134) (ResGaz 1, 2004),
- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5809 Sayılı Elektronik Haberleşme Kanunu,
- 5846 Sayılı Fikir ve Sanat Eserleri Kanunu,
- Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik,
- Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin, 20 Ekim 2012 Tarihli Bakanlar Kurulu Kararı,(ResGaz 3, 2012)
- Siber Suçlar Sözleşmesi 2010 yılında imzalanmıştır. (Council Of Europe Convention on Cybercrime)[2] (Europe, 2001),

[2] Siber Suçlar Sözleşmesi (Council of Europe Convention on Cybercrime), Türkiye tarafından 10 Kasım 2010 tarihinde imzalanmış fakat henüz TBMM tarafından onaylanmamıştır.

## 4.4. Türkiye'de İcra Edilen Siber Güvenlik Tatbikatları

Kamu kurum ve kuruluşlarının sahip oldukları bilgi ve bilişim güvenliği yeteneklerinin ve aldıkları önlemlerin ne derece de yeterli olduklarını test etmek maksadıyla siber güvenlik tatbikatları düzenlenmektedir (Tatar 2011).

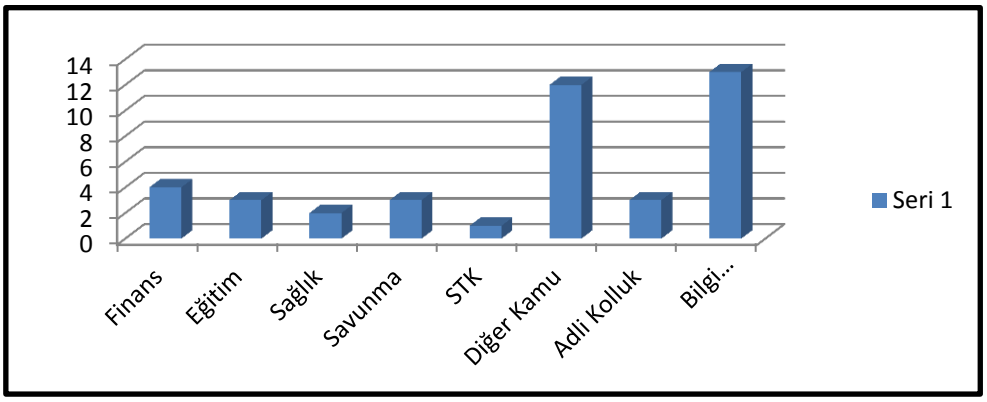
Tüm bu gelişmeler kapsamında Türkiye'de icra edilen siber güvenlik tatbikatları aşağıda sunulmuştur.

- ***BOME 2008 Tatbikatı;***

Türkiye Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME) koordinatörlüğünde, 20-21 Kasım 2008 tarihlerinde ülkemizde ilk defa bilgi sistemleri güvenliği tatbikatı icra edilmiştir. Tatbikatın ismi "BOME 2008 Tatbikatı" olarak belirlenmiştir (Çifci 2012). Tatbikata Cumhurbaşkanlığı, Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Hazine Müsteşarlığı, Merkez Bankası, Sermaye Piyasası Kurulu, Tapu Kadastro Genel Müdürlüğü olmak üzere 8 adet kurum ve kuruluş iştirak etmiştir. BOME 2008 tatbikatı, kurumsal BOME süreçleri ile kurumların dış kaynaklı bir siber saldırıya maruz kalmaları durumunda TR-BOME ile iş birliği süreçlerinin kontrol edilmesi amacıyla yapılmıştır (Tatar 2008).

- ***Ulusal Siber Güvenlik 2011 Tatbikatı (USGT);***

USGT 2011 finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin, adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilciliklerinden meydana gelen 41 kamu kurumu, özel sektör ve sivil toplum kuruluşunun katılımıyla 25-28 Ocak 2011 tarihinde icra edilmiştir. Bu kurumlar Şekil 4.1'de gösterilmiştir (TÜBİTAK-BTK, 2011).




Şekil 4.1: Çalışma Alanlarına Göre Katılımcı Kurum ve Kuruluşlar.

Ülkemizde icra edilen ikinci ulusal siber güvenlik tatbikatı olan USGT 2011'de, katılımcı kuruluşların teknik yeteneklerini tespit etmek ve kuruluşlara karşı olası saldırılara müdahale etme kabiliyeti kazandırmak amacıyla hem gerçek saldırılar hem de yazılı ortamda senaryolar gerçekleştirilmiştir (TÜBİTAK-BTK , 2011).

USGT 2011'de gerçekleştirilen senaryolar sonucunda elde edilen bulgular Şekil 4.2'de gösterilmiştir (TÜBİTAK-BTK 2011).

| S.Nu.: | Açıklama |
|---|---|
| 1 | Bilgi Güvenliği Yönetim Sistemi (BGYS) eksikliği |
| 2 | Sistem yöneticilerinin teknik konularda yetersizliği |
| 3 | Saldırı tespit sistem ve süreçlerinin yetersizliği |
| 4 | Sosyal mühendislik saldırılarına yönelik bilinç yetersizliği |
| 5 | Güncel olmayan antivirüs programları |
| 6 | Sistem yöneticilerinin güvenlik boyutunda yetersiz olmaları |
| 7 | Kurum içi koordinasyon konusunda eksikliklerin olması |
| 8 | Erişim kontrol politikasının bulunmaması |
| 9 | Sistem planlama aşamasında güvenliğin göz ardı edilmesi |
| 10 | Kablosuz ağlardan kaynaklanan risklerin bulunması |
| 11 | İş sürekliliği planlarının eksikliği |
| 12 | Port tarama saldırılarının tespit edilememesi |
| 13 | Dağıtık Servis Dışı Bırakma saldırılarının (DDOS) olumsuz sonuçlar vermesi |
| 14 | Web uygulamalarında açıklıkların bulunması |
| 15 | Kayıt dosyalarının analizinin tam olarak gerçekleştirilememesi |
| 16 | Yasal mevzuata ilişkin bilgi eksikliğinin bulunması |

Şekil 4.2: USGT 2011 Tatbikatında Elde Edilen Sonuçlar.

- ***Siber Kalkan 2012 Tatbikatı;***

BTK tarafından, siber saldırılara karşı önlem alma yeteneğinin kazandırılması amacıyla, 8-29 Mayıs 2012 tarihleri arasında icra edilen Siber Kalkan 2012 Tatbikatına Türkiye'de internet erişim hizmeti sunan ve internete erişim sağlayan elektronik haberleşme sektörünün % 99,9'unu oluşturan 12 firma katılmıştır (TELEKOM, 2013).

Tatbikat sonucunda;

- İnternet servis sağlayıcıları tarafından gerekli önlemlerin alınması durumunda, DDOS saldırılarının büyük ölçüde önlenebildiği,
- Tatbikatın siber saldırılara karşı farkındalık oluşturma anlamında faydalı olduğu, tatbikatta siber saldırılara karşı kurum içi koordinasyonun iyi seviyede sağlandığı (Çifci, 2012),
- Siber saldırılara yönelik tespitlerin genel olarak doğru yapıldığı,
- İnternet servis sağlayıcılarının maruz kaldıkları saldırılar karşısında kendi başlarına aldıkları yöntemler yerine, birlikte koordineli şekilde alınan önlemlerin daha etkili olduğu bulgularına ulaşılmıştır (TELEKOM, 2013).

- ***Ulusal Siber Güvenlik 2013 Tatbikatı;***

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinesinde, TÜBİTAK ve BTK tarafından yürütülen ikinci siber güvenlik tatbikatı, 41 oyuncu, 20 gözlemci olmak üzere toplam 61 kurum ve kuruluşun iştiraki toplamda 194 personel ile 25 Aralık 2012 - 11 Ocak 2013 tarihleri arasında icra edilmiştir.

Siber saldırılara önlem alınması, kurumların bilgi güvenliği sistemlerinin güçlendirilmesi ve kurumlar arası koordinasyonun artırılması amacıyla düzenlenen tatbikat 25 Aralık 2012 tarihinde gerçek saldırılar ile başlamıştır (Çifci, 2012).

Tatbikat, enerji, sağlık, iletişim, ulaştırma gibi kritik altyapıları yöneten ve işleten kurumları kapsamış aynı zamanda adli ve kolluk birimlerinin de katılımı sağlanmıştır (BTK-TÜBİTAK, 2013).

Ulusal tatbikatların sonuçları incelendiğinde faydalarının ne kadar çok olduğu görülmektedir. Özellikle eksikliklerin objektif bir şekilde tespit edilmesinin ileri de

karşılaşılabilecek daha büyük saldırılar karşısında kurumların daha fazla zarar görmemesi açısından oldukça önem arz etmektedir.

# 5. KRİTİK ALTYAPI ve SİSTEMLER

## 5.1. Kritik Altyapılar

Kritik altyapılar (Critical Infrastructure) hakkında, ülkeler ve uluslararası kuruluşlar tarafından farklı kategorilerde tanımlamalar yapılmıştır.

Türkiye'nin ulusal siber güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda, kritik altyapılar;

"*İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır" (*T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2012).

Amerika Birleşik Devletleri (ABD) kongresi tarafından USA PATRIOT ACT of 2001 yasasında kritik altyapılar;

"*Yetersizliği veya tahribi, güvenliğe, milli ekonomik güvenliğe ve kamu sağlığına veya emniyetine zayıflatıcı bir etkisi olan fiziksel veya sanal sistem ve varlıklar*" şeklinde tanımlanmıştır (Public Law 107-56, 2001).

OECD (Organisation for Economic Co-operationand Development) Kritik altyapıları;

"*Fonksiyonelliğini yitirmesi durumunda sağlık hizmetlerine, toplumsal emniyet ve güvenliğe, vatandaşların ekonomik refahına veya hükümetin/ekonominin verimli çalışmasına ciddi yönde tesir eden bilgi ağları ve sistemleri*" olarak tanımlamaktadır (Kara ve Çelikkol, 2011)

Kritik altyapılar tüm ülke ve kuruluşların gündemine gelmelerinden itibaren ülkelerinde bulunan altyapılardan hangilerinin kritik olabileceklerine karar verme süreci başlamıştır. Bu kapsamda ABD kritik altyapılarını Tablo-5.1'de olduğu gibi belirlemiştir (Vasilescu 2012).

Siber ortamı çok daha yaygın olarak kullanan ve sistemlerinin neredeyse tamamını internet tabanlı yöneten ülkeler, siber saldırılara karşı da muazzam bir hedef haline gelmişlerdir. ABD, belirlemiş olduğu 18 adet kritik sektörün işlevlerini sürdürebilmesi için internete bağlı olmasından dolayı açık bir şekilde hedef olduğundan siber saldırılara karşı savunmasız olduğu değerlendirilmektedir (Çifci, 2012).

Tablo 5.1: ABD Kritik Altyapı Sistemleri.

| ABD KRİTİK ALT YAPI SİSTEMLERİ | | |
|---|---|---|
| Tarım ve Gıda | Barajlar | Bilgi Teknolojisi |
| Bankacılık ve Finans | Savunma Endüstrisi | Milli Anıtlar |
| Kimya | Acil Servisler | Nükleer Reaktör, Madde, Atıklar |
| Ticari Tesisler | Enerji | Kargo ve Sevkiyat |
| İletişim | Devlet Tesisleri | Nakliye Sistemleri |
| Kritik Üretim | Halk Sağlığı | Su |

AB yaptığı çalışmalar neticesinde 11 adet altyapının kritik olduğunu değerlendirmiştir (COESS, 2010). Bu kritik altyapılar Tablo-5.2'de sunulmuştur.

Tablo 5.2: AB Kritik Altyapı Sektörleri.

| AB KRİTİK ALTYAPI SEKTÖRLERİ | | |
|---|---|---|
| Enerji | Gıda | Uzay ve Araştırmalar |
| Ulaşım | Nakliye | Kamu Düzeni ve Emniyeti |
| Finans | Su | Kimyasal ve Nükleer Endüstri |
| Sağlık | Bilgi ve İletişim Teknolojileri | |

ABD ve AB ülkelerinin kritik altyapıları incelendiğinde ülkeler arasında farklılıklar olduğu görülmektedir. Bu farklılıklara rağmen genellikle ülkeler finans, ulaşım, enerji, sağlık, iletişim ve haberleşme, bilgi teknolojileri gibi sektörleri kritik altyapı kategorisine almışlardır. Bazı ülkelere ait kritik altyapı sistemleri Tablo-5.3'de özetlenmiştir (OECD, 2008).

Tablo 5.3: Bazı Ülkelere Ait Kritik Altyapı Sistemleri.

| Sektör | Avustralya | Kanada | Hollanda | İngiltere | Türkiye |
|---|---|---|---|---|---|
| Enerji | X | X | X | X | |
| Bit | X | X | X | X | |
| Finans | X | X | X | X | |
| Sağlık | X | X | X | X | |
| Gıda | X | X | X | X | |
| Su | X | X | X | X | |
| Ulaşım | X | X | X | X | |
| Güvenlik | Acil Hizmetler | X | X | Acil Hizmetler | |
| Hükümet | | X | X | X | |
| Kimyasallar | | X | X | | |
| Savunma Sanayi | X | X | X | | |
| Diğer Sektör veya Faaliyetler | Ulusal Anıtlar ve Meydanlar | | Adalet ve Yargı | | |

Bu sektörlerin kritik olarak nitelendirilmesinde, çok çeşitli askeri ve sivil saldırılara hedef teşkil etmelerinin önemli payı vardır. Kritik altyapıların internet ile bağlarının hızla artması ve aralarındaki kontrol ve denetim ilişkilerinin genişlemesinden dolayı güvenlik açıkları her geçen gün artmakta ve gelecekte daha da artacağı düşünülmektedir. Kritik altyapılarda arıza meydana gelmesi diğer altyapıları da etkileyebileceğinden çok önem arz eden bir konudur. Bu alanda problemlerin en aza indirilebilmesi için de sitem dâhilinde kapsamlı bir koordinasyon ve etkin bir kontrol yapılması kaçınılmazdır (Macdonald et al., 2012)

Ülkelerin, kurumların ve şahısların bilgi ve iletişim teknolojilerine bağımlılıkları her geçen gün hızla artmaktadır. ABD Ticaret Bakanlığının sunduğu konuya ilişkin raporda ABD'deki şirketlerin gerçekleştirmiş oldukları yatırım miktarlarının yarısını bilişim teknolojileri yatırımları olduğunu belirtilmektedir (Karabacak, 2010).

Bilgi ve iletişim teknolojilerinin sağlamış oldukları faydalar çok fazladır fakat bunu yanında bu sistemlerin çok fazla kullanılması ile birlikte literatürümüze yeni bir tehdit türü olarak "Sayısal Tehdit" girmiştir. Sayısal tehditlerden korunmak için birey bazından ülke bazına kadar birçok tedbirler alınmalıdır.

İnternetin çok yaygın olarak kullanılmaya başlamasından itibaren kötü niyetli internet kullanıcıları, düşmanlar, diğer ülkeler ya da terör örgütleri kritik altyapılarının bilgi sistemlerine internet üzerinden siber saldırı düzenleyerek zarar vermeye çalışmaktadırlar. Kritik altyapılar karmaşık ve dağınık bir yapıya sahip olduklarından, işletim esnasında sistemin değişik kısımlarının operatörler tarafından uzaktan gözlenmesi, kontrol ve kumanda etmeleri gerekmektedir.

Günümüz network ağ sistemleri, operatörlere veya yetkililere bu şekilde uzaktan kumanda etme olanağı sağlamaktadır. Günümüz teknolojisinde endüstriyel komuta ve kontrol sistemlerinin gelişmiş hali SCADA (Süpervisory Control and Data Acquisition) olarak adlandırılmaktadır. SCADA sistemleri ağlara ve internete kolayca bağlanabilmektedir. Bu bağlanma özelliği, sitemlerin kullanımını ve kontrolünü kolaylaştırmış olsa da ciddi boyutta güvenlik problemlerini de beraberin de getirmiştir. Eğer sistemler internet vasıtasıyla uzaktan kumanda ediliyorsa SCADA sistemlerine yapılabilecek bir saldırı tüm sistemi etkileyebilecektir. Böyle bir saldırı neticesinde maddi zararların olmasının yanında insanlar başta olmak üzere diğer canlılarda zarar görebilecektir (Karakuş, 2013).

SCADA vasıtasıyla kumanda edilen sistemlere günümüze kadar birçok siber saldırı gerçekleştirilmiştir. Bunlardan bazıları (Zhu, 2014);

1992 yılında, yangın ve hırsızlığın engellenmesi amacı için kurulan Chevron alarm sistemi devre dışı bırakılmıştır.

2000 yılında, Gazprom boru hatlarının siber korsanlar tarafından ele geçirilmesi olayı gerçekleşmiştir.

2003 yılında, Ohio'da Davis-Besse nükleer santral emniyet sistemleri Slammer solucanından etkilenmiştir.

2003 yılında, ABD'nin doğu yakası Blaster solucanı nedeniyle elektriksiz kalmıştır.

2004 yılında, "Code red" virüsü nedeniyle ABD'de Amtrak demiryolu hatları kapanmıştır.

2008 yılında, ABD'de Hatch nükleer enerji santrali, yazılım güncellemesi yaptıktan sonra kapanmıştır.

2009-2010 yıllarında, İran'ın nükleer tesisleri Stuxnet solucanından dolayı etkilenmiştir.

2010 yılında, Çin'in dünyada ki internet trafiğinin % 15'ini 18 dakika boyunca kendine yönlendirmesi, olarak gerçekleştirilmiştir.

Kritik altyapılar BT arasındaki ilişki, BT'den oluşan kritik altyapılar, tamamen BT'den oluşan kritik altyapılar ve SCADA ile kontrol edilen ve izlenen kritik altyapılar olmak üzere 3 kategoride yer almaktadır (Karabacak 2011a).

BT'yi Kullanan Kritik Altyapılar;

- Ulaşım
- Bankacılık ve Finans
- Sağlık ve Acil Durum Servisler
- Kritik Kamu Servisleri

Tamamen BT'den Oluşan Kritik Altyapılar,

- Telekomünikasyon

SCADA ile Kontrol Edilen veya İzlenen Kritik Altyapılar;

- Kritik Üretim Tesisleri
- Enerji
- Barajlar
- Sulama Sistemleri
- Elektrik Üretim ve Dağıtım Sistemleri
- Petrol Rafinerileri
- Gaz İletim Sistemleri
- Fabrikalar

## 5.2. Kritik Altyapılara Uygulanan Siber Saldırılar

Siber saldırı; dünyanın herhangi bir yerinden başka bir yerdeki bilgisayar kontrolündeki sistemlere internet ortamından izinsiz erişerek ilgili kritik altyapının yönetimini ele geçirme çabasıdır. Birbirine bağlı olarak ve internet ile irtibatlı olan kritik altyapılar gerek şahıslar gerekse ülkeler tarafından hedef tahtasına oturtulmuşlardır. Saldırganlar bu alanda yapılabilecek saldırılar konusunda birçok model geliştirilebilmektedir.

Özellikle de sistemlerin alt yapılarında ki eksiklikler saldırganlar için çok iyi bir fırsat olarak değerlendirilebilmektedir (Niekerk and Maharaj, 2011).

Siber saldırıya maruz kalan ülkeler; fiziki, finansal, prestij gibi zararlara uğramalarının yanında ciddi surette psikolojik olarak da zarar görmektedirler. Burada amaç hedef sistemin kontrolünü ele geçirerek verileri çalmak, değiştirmek, bozmak, çökertmek ya da yanlış yönlendirmektir. Siber ortamdaki aktivasyonlar;

- Siber saldırı,
- Siber silahlar,
- Siber savaş,
- Siber savunma,

Olmak üzere kısaca 4S olarak tanımlanmaktadır.

Siber ortamda düşman, görünmez, bilinmez, hissedilmez, anlaşılmaz olduğundan diğer tehditlere göre daha sinsidir ve tehlikelidir. Bu sebepten dolayı hedef bilgi sistemlerinin yazılım ve kodlarının devre dışı bırakılması, verilerin çalınması, bozulması veya sistemleri kendi amaçları doğrultusunda çalıştırmaları gibi olaylar günümüzde çokça yaşanmaktadır (Karakuş, 2013).

Son yıllarda dünya genelinde kritik altyapılara yapılan bazı siber saldırı olayları;

Soğuk savaş döneminde, Rusya ile ABD karşılıklı birbirlerinin açıklarını aradıkları bir dönemde casusluk faaliyetleri oldukça hız kazanmıştır. Rusya 1982 yılında Kanada'da bulunan bir şirketten doğalgaz boru hatlarının kontrolü maksadıyla kullanılan bir yazılımı çalmaya başlamıştır. ABD olayın farkına varmasından itibaren çok stratejik bir yol izleyerek operasyonu durdurmak yerine yazılımın içine virüs yerleştirerek kaşı atakta bulunmuşlardır. Rusların çalmış oldukları yazılım bir süre sonra virüs tarafından bozularak doğalgaz borusundan geçen gaz miktarını aşırı seviyede artırarak doğalgaz borusunun patlamasına sebep olmuştur. Sonuç olarak o güne kadar uzaydan görülebilen en büyük (nükleer olmayan) patlama gerçekleşmiştir. Bu olay dünya tarihine ilk siber saldırı olarak geçmiştir (Şenkaya ve Adar, 2014).

ABD 1992 yılında daha savaş başlamadan Irak devletinin tüm telekomünikasyon altyapısını siber saldırı düzenleyerek çökertmiştir. Oysaki Irak devleti saldırıdan önce çok ciddi yatırımlarla en son teknolojik sayısal haberleşme sistemlerini kurmuştu. Yapılan siber saldırı yöntemi ile Irak'ta tüm askeri birliklerin birbirleri ile iletişimleri bir anda kesilmiştir.

2003 yılında ABD Irak'ı işgal etmeyi planlarken, Irak Savunma Bakanlığında çalışan binlerce kişi, işgalden hemen önce bilgisayar ekranlarında ABD Merkez Komutanlığından gelen bir mesaj görmüşlerdir (Yayla, 2013).

Bu mesajın içeriğinde;

"*Yakın bir zamanda Irak'ı işgal edebiliriz. Sizlere zarar vermek istemiyoruz. Başınıza bir şey gelmesini istemiyorsanız, savaş başladığında evlerinize gidin*" deniyordu.

Aralarında askerlerin de bulunduğu birçok kişi bu mesajı aldıktan sonra bırakıp gitmişlerdir ve ABD Irak işgalinde kayda değer bir direnişle karşılaşmamıştır (Karakuş, 2013).

Estonya'nın başkenti Tallin'de Sovyetler Birliğinin dağılmasından sonra etnik Ruslar ve Estonya'lılar arasında gerilimler oluşmaya başlamıştır. Gerilimin sebebi Sovyetler birliği döneminden kalma bronz "Kahraman Kızıl Ordu Askeri" heykeli bulunuyordu. 27 Nisan 2007 yılında iki taraf arasında karşılıklı çatışmalar yaşanmaya başlayınca Estonya hükümeti heykelin kaldırılmasına karar vermiştir. Konu Rusya medyasına ve meclisine yansıyınca çatışmalar siber ortama taşınmıştır. Rusya'nın siber saldırıları neticesinde Estonya'nın bankaları, kamu kurumları, özel sektör kuruluşları çalışamaz hale gelmiştir (Alkan, 2012).

İran'ın nükleer enerji altyapısı, 2010 yılında Stuxnet adı verilen zararlı yazılımın etkisiyle operatörler tarafından santralin kullanılamaz durumuna getirmiştir. Stuxnet SCADA sistemleri için yazılmış etkili bir zararlı yazılımdır. Ağustos 2010 yılından itibaren dünya genelinde bu yazılımdan etkilenen bilgisayarların % 60'ı İran'da olduğu tespit edilmiştir. Stuxnet İran'ın Natanz şehri uranyum işleme merkezindeki santrifuj sistemlerini ve Bashehr şehrindeki nükleer reaktör türbinlerini hedef almıştır.

Yazılım bu sistemlerin kumanda ve kontrol sistemlerini ele geçirmiş ve yerinden kullanımını engellemiştir. Bu olayın hitamında yapılan incelemeler kapsamında stuxnet'in daha önce hiçbir zararlı yazılımda görülmeyen özellikleri tespit edilmiştir. Öncelikle sadece nükleer enerji santrallerinde kullanılan belli marka ve özellikteki cihazları ve SCADA sistemlerini hedef alan bir yazılım olduğu anlaşılmıştır. Bilgi güvenliği uzmanları bu şekilde karmaşık bir yazılımın ancak ulusal düzeyde bir çalışmayla yazılmış olabileceğini, bu yazılımın bağımsız bilgisayar korsanları tarafından başarılamayacağını bildirmişlerdir (Karabacak, 2011b)

Türkiye'nin Suriye sınırından yaklaşık 120 km içeride İsrail uçakları tarafından 06 Eylül 2007 de bir inşaat bombalanmıştır. Bir nükleer tesis inşaatı olduğu tahmin edilen bu tesisin vurulmasından Suriye'nin ancak sabah haberi olabilmiştir. Suriye'nin Rusya'dan almış oldukları hava savunma sistemleri bu kadar etkiliyken nasıl oldu da bu saldırı gerçekleşebilmişti? Yapılan soruşturmanın ardından İsrail'in Suriye'nin savunma ağlarına yerleştirmiş olduğu zararlı bir yazılım sayesinde radarlardaki görüntüyü silerek yerine boş bir hava sahası fotoğrafı yerleştirmiştir. Suriyeli görevliler 06 Eylül 2007 gecesi tertemiz bir radar görüntüsü izlemişler ve sorunsuz bir gece geçirdiklerini düşünmüşlerdir (Clarke and Knake, 2010).

İsrail bu siber saldırıyı başarabilmek için saldırıdan önce Suriye hava sahasına gizlice sokulan insansız hava araçları sayesinde bozuk sinyal gönderimi yaparak hava radarlarında arıza ve karışıklık meydana getirmiştir. Bu arada İsrail tarafından Suriye hava sahasını denetleyen bilgisayar koduna tuzak kapan yazılımı yerleştirilmiştir. Ağ sisteminin kontrolünü tamamen eline geçirmek için kullanılan bu zararlı yazılım radarda ki görüntüyü İsrail'in istediği gibi değiştirmiştir. Netice itibari ile çok dersler çıkarılacak bir siber saldırı sorunsuz olarak gerçekleşmiştir (Turan, 2011)

# 6. UYGULAMA

Kritik altyapıların güvenliğinin aktif ve güncel tutulabilmesi için en önemli unsurlardan birisi de, dâhilin de yer alan açıklıkların tespit edilerek en kısa zamanda problemlerin giderilmesidir. Bu durum ise Sızma Test'i olarak bilinen test faktörünün belirli aralıklarla kritik altyapıya mütecaviz kurum ve firmalara uygulanması ile sağlanmaktadır.

Bu bölümde sızma testlerinin karakteristikleri ve metodolojisi üzerinde durularak, hali hazırda firma ve kurumların söz konusu testleri "GİZLİ" gizlilik dereceye mahsus bilgilerin ifşa edilebileceği gerekçesi ile kabul etmemelerinden dolayı konu hakkında teorik olarak bir model sunulmuş ve ayrıntılı bir şekilde incelenmiştir. Aynı zamanda Türk Standartları Enstitüsü (TSE)'nün bu konuda test yaptıracak firma veya kurum ile testi icra edecek kuruluş arasında "Gizlilik Sözleşmesi"nin imzalanmasını şart koşması, bu alanda bağımsız olarak bir sızma testinin yapılmasını ve yayımının yapılmasını engellemiştir (TSE, 2013).

## 6.1. Kritik Altyapıların Güvenliği Açısından Sızma Testleri

Kritik altyapıların güvenliğinin sağlanması konusunda alınan tedbirlerin nitelikleri önemli olduğu gibi, bu alınan tedbirlerin etkinliğinin güncel tutulması da oldukça önem arz etmektedir. Gerek firmalar gerekse kurumlar bu alandaki güvenlik önlemlerinin tespitini yapmak için sızma testlerini uygulatmaktadırlar. Bu testler ile mümkün olduğu kadar gerçek hayatta karşılaşılabilecek saldırıların modellenerek ilgili kurum veya firmaya gerçekleştirilmesi sağlanır (Ayyüzlü ve Özer, 2013).

Kritik altyapıların güvenliğinin sağlanmasında üçüncü bir gözün etkisi çok önemlidir. Alınan tedbirlerin farklı bir bakış açısıyla kontrol edilerek raporlanması yöneticilerin üzerine titredikleri kurum veya firmalarının güvenliği konusunda kendilerini iyi hissetmelerine katkıda bulunacaktır. Günümüzde hacker'ların uyguladıkları saldırı yöntemlerinin her geçen gün farklı bir bakış açısı kazanmasıyla alınacak tedbirlerin kapsamı ve güncelliği oldukça önem arz etmektedir.

Bankacılık Düzenleme ve Denetleme Kurulu (BDDK) tarafından BİT argümanlarını ihtiva eden sistemlere yönelik siber ortamda gerçekleştirilebilecek saldırıların da değişim göstermesinden dolayı 2011 yılında 4022 sayılı BDDK kararı ile sızma testlerinin belirli aralıklarla yapılması zorunlu hale getirilmiştir.

Bu gelişmelere bağlı olarak artık kurumlar yılda en az bir kere sızma testine tabi tutularak, hazırlanacak raporlara göre açıklıklarını ve eksikliklerini tamamlama yoluna gideceklerdir (BDDK, 2012).

Firma veya kurumların sızma testine tabi tutulması kapsamında çalışma alanlarında tecrübeli kişi veya kurumların tercih edilmesi firmaların lehine olacaktır. Zira bahse konu alan o kadar aktif bir gündeme sahiptir ki, hacker'ların her geçen gün hedefleri üzerinde kendilerine farklı açıklıklar bulmalarına karşın, işin profesyonel uzmanı beyaz yakalı hacker'ları da bu açıklıkları bertaraf edecek yolları bulmak zorundadırlar.

## 6.2. Sızma Test Kategorileri

Sızma testleri uygulanış biçimlerine göre üçe ayrılmaktadır (Önal, 2012).

### 6.2.1. Kapalı Kutu Sızma Testleri

Kapalı kutu sızma test yönteminde testleri yapan kurumla her hangi bir bilgi paylaşılmaz. Şirket firmaya ait sistemlerin domainleri üzerinden test gerçekleştirilir. Burada şirket firmaya ilişkin maksimum bilgi edinmeyi amaç edinir ve bulduğu tüm açıklıkları değerlendirmeye çalışır.

### 6.2.2. Açık Kutu Sızma Testleri

Açık kutu sızma test yönteminde firma maksimum seviyede şirkete kendisine ilişkin bilgileri verir, sızma testi yapanlar bu kategoride firmaya ilişkin bilgilere baştan ulaştığından, firma üzerinde bu bilgiler ışığında testler uygulanır. Burada amaç firmada önceden çalışan bir şahsın firmaya hangi zararları verebileceği ölçülür.

### 6.2.3. Zafiyet Değerlendirme Testleri

Burada testi uygulayanlar tüm enerjilerini açıklık tespiti yapma üzerine harcarlar. Bu kategoride konuya ilişkin özel programlar kullanılır (Nmap, Nessus, v.b.). bu bağlamda firma içinde kısıtlı yetkiye sahip kişilerin firmaya ne kadar zarar verebilecekleri ölçülür.

Sızma testleri yapılırken uygulanacak faaliyet alanları aşağıda sunulmuştur. Bu testlere uygulama yapacak firmalar tarından ekleme veya çıkarma yapılabilmektedir (BDDK 2012).

- İletişim Altyapısı ve Cihazlar
- DNS Servisleri
- Kullanıcı Bilgisayarları
- E-Posta Servisleri
- Veritabanı Sistemleri
- WEB Uygulamaları
- Mobil Uygulamaları
- Kablosuz Ağ Sistemleri
- DDOS Testleri
- Sosyal Mühendislik Testleri

## 6.3. Sızma Testinin Uygulanmasında Takip Edilecek Adımlar

Sızma testlerinin uygulanmasında genel olarak beş basamaktan oluşan bir yol izlenmektedir. Bu basamakların her biri ayrı bir öneme haiz olup, sıralaması da ayrı bir önem arz etmektedir. Öyle ki her biri diğerine zincirin bir halkası gibi bağlı olmakla birlikte ancak tam bir bütün olarak uygulandığı takdirde kayda değer bir sonuca varılabilmektedir. Bu adımlar müteakip maddelerde belirtilmiştir (Yiğit ve Akyıldız 2014).

- **Birinci Adım** : Bilgi Toplama Süreci
- **İkinci Adım** : Keşif Süreci
- **Üçüncü Adım** : Zafiyet Taraması Süreci
- **Dördüncü Adım** : Açıklıkların İstismar Edilmesi Süreci
- **Beşinci Adım** : Sistemin Ele Geçirilmesi Süreci
- **Altıncı Adım** : İzlerin Temizlenmesi Süreci
- **Yedinci Adım** **:** Raporlama Süreci
- **Sekizinci Adım** **:** Önlem Alma Süreci

- **Dokuzuncu Adım** : Kontrol Testi Süreci

Burada ele alınan test basamaklarının her biri ayrı bir öneme sahiptir. Ancak en önemli basamağın raporlama süreci olduğu söylenebilir. Çünkü testi yaptıran firmanın bu uygulama sonucunda elde edeceği en önemli ürün faaliyet sonucunda düzenlenen rapordur. Bu bağlamda düzenlenen raporun çok kapsamlı ve itina ile hazırlanması gerekmektedir. Bir başka önemli unsur ise raporun firma yetkilisine şifreli bir şekilde teslim edilmesi gerekir. Hiç şüphesiz o rapor söz konusu firma için "GİZLİ" bilgileri ihtiva eden bir doküman hükmündedir. Genellikle testi yapan kuruluş veya firmalar test sonucunda iki adet rapor düzenlemektedirler. Bunlardan birisi "Teknik Sonuç Raporu" diğeri ise " Yönetimsel Sonuç Raporu"dur. Birinci raporda teste ilişkin teknik detaylar ayrıntılı olarak belirtilirken, ikinci raporda yöneticilere hitaben teknik detaylara girmeden yüzeysel olarak çözüm önerilerinden bahsedilmektedir (TÜBİTAK BİLGEM, 2011).

Firma ise bu sonuç raporunu güvenlik önlemleri alınmış ortamlarda saklaması gerekmektedir. Bu bilgilerin yetkisiz kişilerin eline geçmesi durumunda firmaya tahmin edilenden daha fazla zarar verebileceği akıldan çıkarılmamalıdır.

Yapılan test sonuçlarının ardından düzenlenen rapor ışığında alınması gereken önlemlerin bir an önce yerine getirilmesi ve açıklıkların kapatılması ayrı bir öneme sahiptir. Tespit edilen eksikliklerin giderilmediği düşünüldüğünde yapılan bu uygulamaların hiçbir önemi bulunmamaktadır. Aksi takdirde müteakip testler sonucunda aynı veya daha kötü bir manzara ile karşılaşılacaktır. Dolayısıyla test sonucunda yapılması gerekenler şu şekilde özetlenebilir (Önal, 2012);

- Test raporları firmanın üst yönetimi ile paylaşılarak destekleri alınmalı,
- Sonuçlar doğurabilecekleri risk faktörleri belirtilerek yönetime arz edilmeli,
- Raporda ki tüm eksik hususların sorumluları belirlenerek bu şekilde yönetime arz edilmeli,
- Sistemlerin hem yazılım hem de donanım uzmanları ile toplantılar yapılması,
- Açıklıkların kapatılmasına ilişkin sürecin yakinen takip edilmesi,

- Bir sonraki sızma testinin tarihinin ve niteliğinin belirlenmesi gerekmektedir.

Tüm bu gelişmeler ışığında testi yapan kuruluşlar genellikle, ilgili firma veya kuruma "Kontrol Testi" uygulamaktadırlar. Burada amaç tespit edilen açıklıkların belirlenen zaman diliminde giderilip giderilmediğinin tespit edilmesidir. Bu test; firma veya kurumun kendini hazır olarak kabul ettiği zaman diliminde gerçekleştirilmektedir.

2006 yılında ülkemizde kurulan Ulak-CSIRT birimi; BİT sistemlerinin güvenlik uygulamalarını ve ağ yönetim merkezine bildirilen bilgisayar olaylarına daha planlı bir şekilde müdahale de bulunmayı amaç edinmiştir. Bu bağlamda Ulak-CSIRT'ün görev envanteri içinde yer alan olaya müdahale, uyarma, açıklıklarla mücadele, sızma testleri, risk analizi, koordinasyon v.b. olayların için de yer alan en önemli görevlerden birisi de sızma testleridir (Soysal v.d. 2006).

Dolayısıyla ülkemizde yer alan kritik altyapıların birçoğunun sızma testleri, Ulak-CSIRT ve TÜBİTAK BİLGEM UEKAE bünyesinde bulunan "Bilişim Sistemleri Güvenliği" bölümü tarafından yapılmaktadır. Bir kısmı ise özel kuruluşlar tarafından icra edilmektedir.

Ülkemizde bu alanda faaliyet yürüten söz konusu kuruluşların, özellikle son yıllarda başarılı sonuçlar elde etmesinin en büyük sebebi, uzmanlık gruplarının kendi alanlarında profesyonelleşmesi ve faaliyetlerini icra ettikleri laboratuarların modern ve efektif olmasıdır (TÜBİTAK BİLGEM, 2011).

## 6.4. Sızma Testinin Uygulanmasında Dikkat Edilecek Hususlar

Sızma testlerinin uygulanmasında birçok araç ve yöntem bulunmaktadır. Bu bağlamda yapılacak testin firma veya kurum üzerine olabilecek etkileri iyi düşünülmelidir. Bu araç ve yöntemlerden bazıları sistemler üzerinde arıza meydana getirebileceği gibi bazıları da faaliyetlerin durmasına, verilen hizmetin sekteye uğramasına sebep olabilmektedir (Duggan, 2005).

Bahse konu problemlerin önüne geçilebilmesinin yollarından birisi; firma ve kurumlar tarafından sızma test uygulamalarının bu iş için oluşturulacak laboratuarlarda yapılmasıdır.

Bu yolla firma ve kuruma ait sistemlerin zarar görmesinin engellenebileceği gibi personel ve çalışma alanlarında meydana gelebilecek tahribat da en aza indirilebilecektir (Stouffer et al., 2011).

Diğer bir taraftan test esnasında tespit edilen çok önemli bir açıklığın testin sona ermesi beklenmeden ivedi bir şekilde firma veya kuruma bildirilmesi gerekmektedir. Sızma testinin uygulama aşamasında mevcut şartlara göre test yöntemine ekleme ve çıkarmaların yapılabileceği de unutulmamalıdır.

Sızma testini yapacak kadronun gerekli uzmanlık seviyesinde olması sağlanmalıdır. Bu kişilerin gerekli donanıma erişmeleri için alacakları eğitimleri de TSE tarafından yetkilendirilmiş kuruluşlardan almaları son derece önemlidir. Bu alanda ki eğitimlerden "Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ile Web Uygulamaları ve Veri tabanı Sızma Testi Uzmanlığı"nın önemi ayrıca vurgulanmaktadır (TSE, 2013).

Sızma testlerine ilişkin düzenlenen raporların gizli tutulması ve diğer kuruluşlara gösterilmemesi, sunumlarda kullanılmaması, bunun yanında testlerde görev alan uzmanların hangi alanlarda görev aldığı ve hangi işlemleri uyguladığı bilgisine haiz kayıtların en az iki yıl saklanması, test sonuç raporlarına erişimin bilmesi gereken prensibine göre yetkilendirilmesi gibi faktörlerin çok önemli olduğu unutulmamalıdır (TSE, 2013).

SCADA sistemlerinde oluşabilecek açıklıkların tespit edilebilmesi için bir çok yöntem denenerek sistemler için en ideal yöntem bulunmaya çalışılmaktadır. Bu yöntemlerin, gerek açıklıkların giderilmesi gerekse firma ve kurumların güvenli bir şekilde verimliliğini artırmaları açısından önemi tartışılmaz bir gerçektir (ISA, 2005).

Kritik altyapılarda yer alabilecek açıklıkların tespit edilmesinde uygulanan yöntemlerden birisi manüel test yöntemi diğeri ise otomatik test yöntemidir. Manüel test yöntemi yukarıda belirtildiği gibi alanında uzman gruplar tarafından laboratuarlarda icra edilen test yöntemidir. Bu yöntem uluslararası akademisyenler

tarafından zaman ve para yönünden dezavantaj meydana getirmekle eleştirilmektedir. Otomatik test yöntemi ise, yine açıklık tespiti yapacak olan WEB tarayıcılarıdır.

Söz konusu test yöntemi konu ile ilgili makalelerde dinamik test yöntemi olarak ele alınmış ve manüel test yöntemine göre daha fazla tercih edilmesinin faydalı olacağı mütalaa edilmiştir (Mirjalili et. al., 2014)

## 6.5. Kritik Altyapılara Uygulanan Sızma Testlerinde Yer Alan Örnek Değerlendirme Anketi

Burada verilecek soru örnekleri, yapılan sızma testinin firma veya kurumun hangi üniteleri ile ilgili olduğunun, teknik ve genel uygulama alanlarının kavranmasının, ayrıca konunun genel hatları ile anlaşılması açısından bir örnek teşkil edeceği hedeflenmiştir.

1. Kurumunuz tarafından çalıştırılan bir sistemin bozulması veya yetkisiz erişimle karıştırılması halinde, **vatandaşın can kaybına uğraması veya diğer olumsuz durumlarla karşılaşılması, Türkiye ekonomisinin zarara uğraması, ulusal güvenliğin sekteye uğraması** gibi sonuçlar oluşur mu?

**Not:** Birinci soruya olumlu cevap verilmesi durumunda test yaptıran kurum "Kritik Altyapı Sistemi" olarak nitelendirilmektedir.

2. Kurumun uyması gereken mevzuat nedir ve bu mevzuatın uygulanmasına dair ne gibi önlemler alıyorsunuz? Mevzuatta siber güvenlik konusuna değiniliyor mu?
3. Kurumunuzun ait olduğu sektörün önemine binaen, çeşitli sektör istatistiklerini bizimle paylaşır mısınız?
4. Kritik altyapı sisteminizin bağımlı olduğu başlıca sistemler (enerji, ulaştırma, iletişim v.b.) hangileridir?
5. Bağımlı olduğunuz kurumlarla iletişim konusunda ne gibi sıkıntılar yaşıyorsunuz?
6. Kritik altyapı sisteminize bağımlı olan başlıca sistemler (enerji, ulaştırma, iletişim v.b.) hangileridir?
7. Kurum bilişim sistemi ile SCADA sistemi arasında bağlantı var mı?
8. Kurum bilişim sisteminin ve SCADA sisteminin birbirleriyle ve Internet'le bağlantı durumunu genel hatlarıyla açıklayabilir misiniz?
9. SCADA sistemine izleme, güncelleme veya bakım için (WEB ara yüzü vb.) uzaktan erişim mümkün mü?

10. Kurum bilişim sisteminin halka veya paydaşlarınıza açık bileşeni var mı? Varsa, sisteme erişen toplam kullanıcı sayısı nedir?

11. Kurum bilişim sistemini kullanan personel sayısı nedir?

12. Kritik altyapı sisteminizde yerel sistemler yer alıyorsa bunların geniş alan ağı iletişimine ve sistem merkezine bağımlılığı nedir?

13. Sistem Merkezinin yedeklenme durumu nedir? Yedek sistem merkezi varsa konumu neresidir?

14. Geniş alan ağı iletişimi için kullanılan hatlara kurum bilişim sistemlerinin ve SCADA sistemlerinin erişimi nasıl düzenleniyor?

15. Kuruma ait bir yönetim sistemi sertifikası var mı? (ISO 27001, BS 25999, ISO 9001, vs)

16. Bilgi güvenliği konusunda yazılı politika ve kurumsal organizasyon var mı?

17. Bilgi sistemleri güvenliği ile ilgili personelin görevleri tanımlı mı? Personel, görevini yapacak yetkinlik düzeyinde mi?

18. Kritik altyapı sisteminizi çalıştıran veya destekleyen bilgisayar sistemlerine yönelik belli başlı riskler nelerdir?

19. Kritik rollere atanan personelin yedeği mevcut mu? İnsan kaynağı yeterli mi? Bilgi güvenliği süreci kurum içinden veya dışından bağımsız makamlar tarafından tetkik ediliyor mu?

20. Personele bilişim hizmetleri kullanım sözleşmesi tarzında bir sözleşme imzalatıyor musunuz?

21. Fiziksel ve çevresel güvenlik önlemleri mevcut mu? Kuruma hafıza kartı ve benzeri varlıkların sokulmaması, sokuluyorsa bunların izlenmesi için önlem var mı?

22. SCADA sisteminin üreticisi ile, sistemin bakımını ve olaylara müdahale konusunda desteği de içeren anlaşma yapılmış mı? Anlaşmada bakımı yapacak personelin ve bakım sırasında sisteme bağlanacak bilgisayarların sağlaması gereken güvenlik kriterlerine ilişkin maddelere yer verilmiş mi?

23. Bilginin yedeklenmesine ilişkin süreç çalıştırılıyor mu? Yedeklerin güvenliği ile ilgili önlemler, yedekleme ve yedekten geri dönme prosedürleri mevcut mu?

24. Kullanıcı kimliği belirlemeye yönelik akıllı kart, biyometrik sistem ve benzeri önlemler mevcut mu? Kullanıcılar eski parolalarından farklı karmaşık

parolalar seçmeye ve düzenli aralıklarla değiştirmeye zorlanıyor mu? Sistemlerin ilk parolaları değiştiriliyor mu?

25. Son beş yıl içinde kritik altyapı sisteminizin bozulması veya yetkisiz erişimle karıştırılması durumları yaşandı mı?

# 7. KONUYA İLİŞKİN ÖNERİLER

Ülkemizde siber ortam güvenliğini sağlamak, kritik altyapıları siber saldırılara karşı korumak ve siber saldırılarla etkin bir şekilde mücadele etmek maksadıyla yapılması gereken temel faaliyetler müteakip maddelerde sunulmuştur.

Siber güvenliğin sağlanmasında günümüzde geçerli olan yasalar çerçevesinde siber güvenliğin tam olarak tesis edilmesi ve siber suçlarla mücadele edilmesi mümkün değildir. Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile değerlendiren bütüncül bir yaklaşımın benimsenmesi ve gerekli yasal mevzuatın oluşturulması gerekmektedir (Çifci, 2012).

Bu konuda yasal mevzuat hazırlanırken tüm kamu kurumlarının yetkileri ve sorumlulukları, birbirleri ile koordinasyon ve ilişkileri açık bir şekilde belirtilmelidir (Çifci, 2012). Yasal mevzuat net bir şekilde oluşturulmadığı takdirde; siber saldırılara karşı konulamayacağı, aktif bir siber savunma gerçekleştirilemeyeceği ve dada da kötüsü bilinçsizce yapılan mukabele girişimleri neticesinde suç teşkil eden girişimlerde bulunabileceği unutulmamalıdır. Bu durumun hem kamu kurumlarını hem özel kuruluşları hem de şahısları kapsadığı düşünüldüğünde olayın önemi daha da artmaktadır (Çifci, 2012).

İlk aşamada hangi eylemlerin suç kapsamına gireceği, suçlar için kapsayıcı bir tanımlama yapılması ve siber alandaki suçlarla ilgili soruşturmaların kim tarafından yapılacağı net bir şekilde ortaya konulmalıdır (Altunok ve Çakmak, 2009).

İkinci olarak, suç teşkil eden olayların ve suç yerinin tespit edilmesi konuları oldukça önem arz etmektedir. Siber ortamda işlenen suçların, suçlunun ve eylem yerinin tespiti oldukça zor olduğundan bu aşamada birkaç kurumun (Emniyet Genel Müdürlüğü, Adalet Bakanlığı, Adli Bilişim vb.) koordinesi neticesinde bazı sonuçlara erişilebilecektir (Altunok ve Çakmak, 2009).

Ülkemizde internet suçları ile mücadele kapsamında hazırlanan "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 22 Mayıs 2007 tarihinde yürürlülüğe girmiştir Buna bağlı olarak "İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik" ise 01 Kasım 2007 tarihinde yayımlanmıştır. Bahse konu yasa ve yönetmelikle, ülkemiz için yasal zemin oluşturulmaya çalışılmış fakat aradan geçen sürede meydana gelen

gelişmeler analiz edildiğinde, kanunun tam olarak uygulanamadığı tespit edilmiştir (Altunok ve Çakmak, 2009).

Ülkemiz için etkili bir şekilde siber tehditlerle mücadele edebilmek maksadıyla ilgili kanun ve yönetmeliğin uygulanabilirliği fazla, kapsama alanı geniş ve her türlü ayrıntıya özellikle yer veren, uluslararası hukuk sistemleri ile uyumlu bir şekle dönüştürülmesi için güncellenmesi ve gerekli olan durumlarda ilave yasaların çıkarılmasının uygun olduğu değerlendirilmektedir. Yasal düzenlemelerde siber suçlar ile siber terörizm ayrı ayrı tanımlanmalı ve bu konuda uluslararası düzeyde bir fikir birliğine ulaşılmalıdır. Uluslararası düzeyde alınmayan tedbirlerin, farklı ulusal stratejilere sahip olacağı ve dolayısı ile bilgisayar suçları için "Zayıf Bölgeler" meydana getireceği değerlendirilmektedir. Ayrıca bu zayıf bölgelerin bilgi alışverişi ve ticarette kısıtlamalara neden olacağı düşünülmektedir (Altunok ve Çakmak, 2009).

Siber suçlar ve siber terörizmle mücadele kapsamında yasal zemin oluşturulurken, her şeye rağmen modern demokrasilerin gerekliliği olan kişisel hakların (kişisel verilerin korunması, iletişimin gizliliği vb.) garanti altına alınması ve söz konusu değerler arasında önemli bir dengenin kurulmasının oldukça önemli olduğu değerlendirilmektedir (Altunok ve Çakmak, 2009).

Günümüzde siber tehditler ile mücadele, bireyden başlayarak uluslararası topluma kadar genişleyen bir alanda etkisini göstermektedir.

Bu konudaki sorumluluk, birey bazından başlamak suretiyle artarak özel sektördeki firmaları daha sonra devlet çapında resmi kurumları ve en sonunda uluslararası toplumu kapsamaktadır (Altunok ve Çakmak, 2009).

BİT'lerin oldukça yaygınlaşması ve hayatımızın her alanında yoğun olarak kullanılıyor olması ve bu baş döndürücü gelişmelere rağmen halkın bu yenilikleri kullanırken oldukça bilgisiz olması, birçok tehlikenin meydana gelmesini kaçınılmaz kılmaktadır. Özellikle sanal ortamda paylaşılan bilgilerden, cihaz ve sistemlerimizi güvenlik önlemlerini sağlamadan kullanmaya, bazı organizasyonlar tarafından dağıtılan veya hediye edilen bedava depolama aygıtlarına yüklenen casus yazılımlara kadar birçok faaliyette aslında ne kadar yanlış yaptığımız ortadadır.

Bu alanda etkili bir mücadele için halkın bu konuda bilgili ve ülkenin yetişmiş uzman personele sahip olması gerekmektedir.

Özellikle tüm vatandaşların siber güvenlik konusunda farkındalığının artırılabilmesi maksadıyla, devlet kurumlarının, özel sektör firmalarının,

üniversitelerin ve diğer organizasyonların bu konuda danışmanlık hizmetleri almaları sağlanmalıdır. Hali hazırda halk tarafından siber saldırı sonuçlarının ne kadar yıkıcı olabileceği ve tehlikenin büyüklüğü tam anlamıyla bilinmemektedir. Bu konunun önemi, geniş kapsamlı, halka açık bir bilinçlendirme kampanyası ile halkın genelinin farkındalığı artırılmaya çalışılmalıdır (Çifci, 2012).

Siber güvenlik konusu, özellikle lise eğitim müfredatlarına, üniversiteler de lisans bölümlerinin müfredatlarına dâhil edilmelidir. Üniversiteler de siber güvenlik bölümü açılmalı, akademik alanda yüksek lisans ve doktora programları açılarak günümüzün en tehlikeli tehditlerinden biri olan siber tehditler alanında halkımızın daha eğitim sürecinde bilinçlenmesi sağlanmalıdır (Çifci, 2012).

Siber saldırılara karşı güvenliğin tesis edilmesinde en büyük faktörün "Zincirin En Zayıf Halkası" insan olduğu hiçbir zaman unutulmamalıdır. Siber savunma ile ilgili görevlendirilecek personel seçiminde, mevcut teknolojiye hâkim, nitelikli, yetişmiş ve özgün güvenlik çözümlerini ve ürünlerini geliştirebilen kişiler tercih edilmelidir (Şenol, 2012).

Ülkemizde tam anlamıyla ulusal güvenliğin sağlanması ancak milli teknolojik ürünlerin yani kaynak kodların kullanımı ile sağlanabilecektir. Buna bağlı olarak işletim ve şifreleme sistemleri (PARDUS, LİNUX vb.) başta olmak üzere, bilgi sistem teknolojilerinde milli ürünlerin üretilmesi çalışmalarına gereken önem verilmelidir (Şenol, 2012).

Kurum ve kuruluşların kullandıkları yazılımların, işletim sistemlerinin güvenli olması kadar saldırı tespit sistemlerinin de güvenilir olması oldukça önem arz etmektedir. TÜBİTAK desteğiyle 2013 yılında üretilen ve DDOS saldırılarını engelleyen, saldırıların kanıtları ile görülmesini sağlayan, raporlama ve analiz etme imkânı veren "DDOS Mitigator" cihazı bu alanda en önemli milli ürünlerden birisidir. "DDOS Mitigator" cihazının ve benzeri yerli ürünlerin başta kamu kurumları olmak üzere özel sektör kuruluşlarında da yaygın olarak kullanılması sağlanmalıdır (TÜBİTAK, 2013).

Ülke genelinde siber savunma faaliyetlerinin dış cephe savunmasında rol sahibi olan organizasyonlar ISS'lerdir. Bu yönüyle ISS'lerin ülke siber savunmasında önemi oldukça büyüktür. Gelişmiş ülkelerin uygulamış oldukları ülke içi ISS trafiğinin değiştirildiği bir genel ağ değişim noktasının (IXP), ülkemizde nüfusu birkaç milyonun üzerinde olan şehirlerde kurulması büyük önem taşımaktadır (Şenol, 2012).

Yurt dışı genel ağ giriş ve çıkışlarının topolojik olarak belirli noktalarda tutulması, siber savunma koordinasyon merkezine bu noktalara ait güncel verilerin sürekli ulaştırılması, kritik kurum ve kuruluşlara yapılabilecek yurt dışı kaynaklı siber saldırılara hedef ve kaynak anlamında filtrelerin hazır bulundurulması, özellikle yurt dışından gelebilecek DDOS saldırıları için etkili bir dış savunma kalkanı oluşturulması açısından önemlidir (Şenol, 2012).

Özellikle teknolojinin geliştirilmesi ve Ar&Ge çalışmaları kapsamında TÜBİTAK başta olmak üzere üniversiteler, teknokentler, bilim ve teknoloji merkezleri ve diğer bütün ilgili kuruluşların başta nitelikli personel yetiştirme olmak üzere milli teknolojik ürünlerin üretilmesine yönelik desteklemelerin faydalı olacağı değerlendirilmektedir.

Siber saldırıların ilk başta, örün tabanlı yapılara yönelik yapılacağı kabul edilse de, otomasyon sistemlerinin gelişmesi ve genel ağ protokolünün (IP) giderek haberleşme platformu olarak kullanılmaya başlanması, ileride meydana gelebilecek siber saldırı niteliklerinin ne kadar kapsamlı olabileceğini göstermektedir. Bu yüzden kurulacak siber savunma konsepti bu geniş yelpazeyi kapsayabilecek şekilde tesis edilmelidir (Şenol, 2012).

Bu yüzden ülke içinde hizmet vermekte olan su, elektrik, havalimanları, gaz iletim ve dağıtım sistemleri de olmak üzere her türlü kritik fiziki altyapıyı da kapsayan bir siber savunma anlayışının mutlaka geliştirilmesi gerekmektedir (Şenol, 2012).

Kritik bilgi sistemlerindeki yaşanabilecek kesinti ve arızalara karşı acil müdahale ve kurtarma planlarının hazırlanmasında ve siber saldırılara karşı emniyetli sistemlerin tesis edilmesinde, bu alanda uzman kurum ve kuruluşlardan destek ve danışmanlık hizmeti alınmalıdır (Çifci, 2012).

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında, bakanlar kurulu kararı ile siber güvenliğin sağlanmasına ilişkin politika, strateji, eylem planı, koordinasyon görevleri Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir (ResGaz 3, 2012).

Koordinasyon sorumlusu ilgili bakanlık tarafından kritik altyapıları işleten hem devlet hem de özel kuruluşların gerçekleştirmesi gereken önleyici çalışmalardan vatandaşı, yapması ve yapmaması gereken birçok konuyu kapsayan bilinçlendirme programı için ulusal medya, sosyal medya ve sanal ortam vb. kaynaklar kullanılmalıdır (Karabacak, 2011b).

Özellikle siber saldırı ve tehditlere karşı tepki yeteneğini geliştirmek için BOME ve SOME'lerin yetenekleri geliştirilmelidir. Kritik altyapıları işleten kurumlarda etkin kendi BOME ekiplerini oluşturmalıdırlar. Bunun yanında farklı BOME ve SOME'ler kendi aralarında koordinasyon ve yardımlaşma yeteneklerini artırmalıdırlar (Karabacak, 2011c).

ABD Şubat 2003'te siber ortamın güvenliğini sağlamak için ulusal strateji belgesini yayınlamıştır. Bu belge, BİT'ler ile kritik altyapıları çok sıkı bir şekilde ilişkilendirmekte ve siber ortamın kritik altyapıların sinir sistemi olduğunu ifade etmektedir. Belgede bunun yanı sıra özel sektörün rolü, kritik altyapıların direnci, kritik altyapılara yapılacak saldırıların engellenmesi, koruyucu önlemler alınması ve olaydan geri dönüş kabiliyetleri gibi hususlar yer almaktadır (Karabacak, 2011b).

Avrupa Birliği'nin bu alanda yaptığı çalışmalar kapsamında Avrupa Komisyonu tarafından 20 Ekim 2004 tarihinde "Kritik Altyapıların Korunması İçin Avrupa Programı-EPCIP" başlıklı bir program açılmıştır. AB üyesi ülkeler bu programda yer alan esaslar çerçevesinde kritik altyapıların korunmasına yönelik tedbirlerini almaktadırlar (Karabacak, 2011b).

OECD bünyesinde yer alan "Bilgi Güvenliği ve Mahremiyeti Çalışma Grubu" üye ülkelerin kritik altyapıların korunmasına ilişkin yol gösterecek dokümanlar hazırlamaktadırlar (OECD 2008). Söz konusu grup "Kritik Bilgi Altyapılarının Korunması Hususunda Konsey Tavsiyeleri" adlı dokümanı Ocak 2008'de yayımlamıştır. Dokümanda yer alan tavsiyeler iki ana kısma ayrılmıştır. Bu kısımlardan birincisi; ülkelerin kendi sınırları içerisinde yer alan kritik altyapıların korunması ile ilgili tavsiyeler, ikincisi ise; ülkeler arasında sağlanması gereken koordinasyon hususlarını içermektedir. Söz konusu grup, üyelik için başvuran ülkelerden temel bilgi güvenliği prensiplerine uyulmasını zorunlu kılmaktadır. OECD üye ülkelerden cevaplamasını istediği sorular şu şekildedir (OECD 2008);

- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili bir siyasa ve strateji oluşturdu mu?
- Hükümetiniz kritik bilgi altyapılarının kamu, özel sektör ve bireyler nezdinde korunması için liderlik ve katılım gösteriyor mu?
- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili rol ve sorumlulukları belirleyip atamaları yaptı mı?

- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili değişik yönleri içine alan bir yönetim yapısı oluşturdu mu?
- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili kamu kurumlarını, özel sektörü ve bireyleri kapsayan bir bilinçlendirme ve eğitim faaliyeti uyguluyor mu?

OECD'nin kurucu ülkelerinden biri olan Türkiye'nin kritik bilgi altyapılarının korunmasına ilişkin hususlara uyumu bulunmamaktadır.

NATO kritik bilgi altyapılarını korunmasına yönelik 20 Aralık 2007'de "NATO Sayısal Savunma Siyasal Belgesi"ni yayımlamıştır (Gardner, 2009). Bu siyasal belgesinde sorumluluklar, stratejiler ve izlenecek yol haritaları yer almaktadır. NATO'da bu alandaki yaklaşım doğrudan teknik ve operasyonel desteğin sağlanmasını da içermektedir. NATO tarafından, sayısal savunma reaksiyon takımını sayısal ataklara maruz kalan üye ülkelere, üye ülkenin talep etmesi durumunda gönderilmektedir (Gardner, 2009).

Ülkemizde de diğer ülkelerde olduğu gibi bilgi ve iletişim teknolojileri ile kesişimi olan kritik altyapıları bulunmaktadır.

Ülkemizde başlangıç seviyesinde olan bu kritik altyapıların korunmasına yönelik program uygulanırken ve geliştirilirken izlenen süreçte yukarıda bahsedilen özellikle NATO, OECD, AB ve ABD'de ki bu alanda yapılan çalışmaların ve yayımlanan strateji ve siyasa belgelerinin dikkate alınması oldukça önem arz etmektedir.

Ülkemiz için bu konuda alınacak tedbirler kapsamında; üst seviyede devlet desteğinin sağlanması, çalışmalar için yeterli seviyede bütçenin ayrılması, yasal mevzuatın tamamlanması ve yürürlülüğe girmesi, kritik altyapıların korunması ile ilgili politika belgesinin hazırlanması, özel sektör ile iş birliği ve koordinasyon sağlanması, kritik altyapılarla ilgili çalışmaları koordine edecek bir merkezin tesis edilmesi, OECD ilkelerine uyum sağlanması, açıklıkların belirlenebilmesi maksadıyla periyodik olarak güvenlik testleri ve siber tatbikatların düzenlenmesi, araştırma ve geliştirme faaliyetlerinin desteklenmesi, güçlü ve alternatifli internet altyapısının oluşturulması, internet servis sağlayıcısının etkin yönetimi ve koordinasyonu gibi çok önem arz eden tedbirlerin ivedilikle yerine getirilmesi gerekmektedir.

Kritik altyapıların güvenliğinin sağlanmasında insan faktörü ve güvenlik bilinci en önemli öğelerin başında gelmektedir. Bilgi ve iletişim sistemlerinin güvenlik

önlemleri göz önüne alınarak yönetilmesi ve temel güvenlik önlemlerinin alınması durumunda siber güvenliğin büyük oranda sağlanacağı ve sistemlerin siber saldırılara karşı güvenli duruma gelecekleri değerlendirilmektedir.

Bu çerçevede ülkemizde bulunan bütün kritik altyapı olarak nitelendirilebilecek kurum, kuruluş ve firmalar özellikle alanında uzman kuruluş veya şahıslara başta sızma testleri olmak üzere SWOT analizi v.b. açıklıkları tespit etme yöntemlerini uygulamalarının faydalı olacağı, diğer taraftan söz konusu testler ile ilgili yasal mevzuatın geliştirilerek tüm kritik altyapıların yılda bir kez teste tabi tutulmasının ve ülkemizin bu konudaki genel durumunun ortaya çıkarılmasının faydalı olacağı değerlendirilmektedir.

# 8. SONUÇ

Tüm bu gelişmeler göz önüne alındığında ülkemizde 2003 yıllarında temelleri atılmaya başlanan siber güvenlik kapsamında ki çalışmalarda, özellikle 2008 yılı sonrası çok hızlı gelişmeler sağlanmıştır. Gerek yasal gerekse teknik ve sosyal boyutta yapılmaya çalışılan iyileştirmeler ülkemizi bu konuda belli bir seviyeye getirse de bunun yeterli olmadığı açıkça görülmektedir.

Hiç zaman kaybetmeden özellikle NATO, OECD, AB ve ABD'de ki bu alanda yapılan çalışmalar ile örtüşecek bir devlet politikasının belirlenmesi çok önem arz etmektedir. Uluslararası kamuoyunda öneminin ve sakıncalarının sıkça vurgulandığı siber tehditler ülkemiz için de geçerlidir. Kritik altyapıların her geçen gün çoğalması ve insanlarında bu teknolojilere bağımlı hale gelmesi, muhtemel gerçekleşebilecek siber saldırıların riskini artırdığı görülmektedir.

Siber güvenlik konusunda alabileceğimiz tedbirler ve yapılabilecek yasal ve teknik çalışmalar ışığında uluslararası aktörlerin gerisinde kalmayacak şekilde çalışmaların büyük bir azimle sürdürülmesi tartışılmaz bir gerçektir.

# KAYNAKÇA


Aksal, F., (2011), "Bilgisayar Teknolojilerinin Kullanımında Etik ve Karşılaşılan Sorunlar." Akademik Sosyal Bilimler İndeksi, 2, (3), 5.

Alena B. and Libor G. (2012), "Green ICT Adoption Survey Focused on ICT Lifecycle from the Consumer's Perspective (SMEs)." Journal of Competitiveness, 4, (4),109–122.

Alkan, M. (2012), "Siber Güvenlik ve Siber Savaşlar." Siber Güvenlik Siber Savaşlar TBMM İnternet Komisyonu, Bilgi Güvenliği Derneği, 15.

Altundal Ö. F., (2012a), "Bilgi Güvenliği ve Risk Yönetimi." Siber Güvenlik Derneği, Ağ Güvenliği Çalışma Grubu, 3-5.

Altundal Ö. F., (2012b), "DDoS Nedir, Ne Değildir?" Siber Güvenlik Derneği, Ağ Güvenliği Çalışma Grubu, 1-4.

Altunok T., Çakmak, H. (2009), Suç Terör ve Savaş Üçgeninde Siber Dünya. Edited by Prof. Dr. Haydar ÇAKMAK ve Prof. Dr. Taner ALTUNOK, 1. ed., Ankara,

Arora M., (2012), "E-Security Issues." International Journal of Computers & Technology, 3, (2), 301–305.

Ayyüzlü E., Özer E. (2013), "Bukalemun-Bilişim Güvenliğinde Yeni Bir Sızma Test Platformu", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 310. Ankara.

BDDK, (2012), "Bilgi Sistemlerine İlişkin Sızma Testleri" 24.07.2012 tarih ve B.02.1.BDK.0.77.00.00/010.06.02-1 sayılı Bankacılık Düzenleme ve Denetleme Kurulu Kararı, Anakara.

BTK-TÜBİTAK, (2013), "İkinci Siber Güvenlik Tatbikatı", Bilişim Dergisi,:148-150.

Boyd C., Forster P., (2004), "Time and Date Issues in Forensic Computingda Case Study", Science Direct 1, 18–23.

Clarke R., Knake R., (2010), "Siber Savaş", İstanbul Kültür Üniversitesi, Yayın Nu.: 148, Çeviri: Murat ERDURAN. İstanbul.

CoESS (2010), “Kritik Altyapıların Güvenliği ve Korunması”, Avrupa Güvenlik Hizmetleri Konfederasyonu-CoESS, Kritik Altyapıların Güvenliği Çalışma Komitesi, Belçika, 5-6.

Colesniuc D., (2013), “Cyberspace and Critical Information Infrastructures.” Informatica Economica, 17, (4), 124.

Çalıkuşu F., Karamehmet B., Mert Denizci Ö., (2007), “Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetimi Modeli”, Risk Yönetimi Modeli Risk Management Model Within İnformation Security Management System, 3-4.

Çifci, H. (2012), “Her Yönüyle Siber Savaş”, TÜBİTAK Popüler Bilim Kitapları 537, 1’inci Basım, Ankara, 134-135.

Dardick S.G., (2007), “The Journal of Digital Forensics Security and Law.” The Journal of Digital Forensics, 2, (4).

Duggan D. P., (2005) Penetration Testing of Industrial Control Systems, Sandia National Laboratories, Report No SAND 2005-2846P, USA.

Europe Council Of. (2001), “Convention on Cybercrime Report”, Convention Committee on Cybercrime, Budapest.

Gardner F. (2009), “Nato’s Cyber Defence Warriors”, Security correspondent, 26-28.

Gennaro R., Rohatni P., (2001), “How to Sign Digital Streams.” Information and Computation, 165, (1), 100–116.

Gharibi W., Shaabi M., (2012), “Cyber Threats in Social Networking Websites” İnternational Journal of Distrubuted and Paralel Systems 3 (1): 119–126.

Giordano F., Francesco G., Schiraldi M., (20139, “From Business Continuity to Design of Critical Infrastructures- Ensuring the Proper Resilience Level to Datacentres.” International Journal of Engineering and Technology, 5, (4), 3552.

Gökırmak Y., Yüce E., Bektaş O., Soysal M., Orcan S., (2013), “IPv6 Balküpü Tasarımı”, TÜBİTAK-ULAKBİM, 1–3.

Grance T., Jonsen W., (2011), “Guidelines on Security and Privacy in Public Cloun Compiting.” NIST Special Publication, 800-144, 4–6.

Guinchard A., (2011), “Between Hype and Understatement- Reassessing Cyber Risks as a Security Strategy.” Journal of Strategic Security, 4, (2), 87.

Hamiti M., Reka B., Baloghova A., (2014), “Ethical Use of Information Technology in High Education.” Procedia - Social and Behavioral Sciences 116 , doi:10.1016/j.sbspro.2014.01.957, 4411–4415.

Hildreth Steven A., (2001), “Cyberwarfare”, CRS Report for Congress, Congressional Research Service, Order Code RL30735, 2.

Hostland K., Enstad Arne P., Eilertsen O., Boe G., (2010), “Information Security Policy”, GEANT, 7.

ISA, (2005), “Presented at 15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference”, U.S. Department of Energy under DOE Idaho Operations Office, The Instrumentation, Systems and Automation Society, Contract No. DE-AC07-05ID14517.

Kağnıcıoğlu H. (1998), “Bilişim Teknolojisinin Önemi”, Açıköğretim Fakültesi Yayınları,13.

Kara M., Çelikkol S., (2011), “Kritik Altyapılar : Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği”, 4 . Ağ ve Bilgi Güvenliği Sempozyumu, 2–6. Kocaeli: TÜBİTAK-BİLGEM-UEKAE.

Karaarslan E., Akın G., Feath V., (2008), “Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Klavuzu”, Ulusal Akademik Ağ ve Bilgi Merkezi, Döküman Kodu: ULAKCSIRT-2008-01, 1, 2.

Karabacak B., (2010), “İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları”, TÜBİTAK-UEKAE, 2.

Karabacak B., (2011a), “Kritik Bilgi Altyapıları ve Siber Güvenlik”, Siber Güvenlik Konferansı, “Bilişim Sistemleri Güvenliği Bölümü”,9.

Karabacak B., (2011b), “Kritik Altyapılar” , TÜBİTAK BİLGEM, 29.

Karabacak B., (2011c), “Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri”, 4.

Karakuş C., (2013), "Kritik Altyapılara Siber Saldırı", İstanbul Kültür Üniversitesi, 11.

Karnikis K., Thoompson E., Ivanov I., Graham M., Hickey M., 2013. "Systems and Methods for Cyber-Threat Detection", 2.

Kaspersky (2013), "Global IT Security Risks:2012", Kaspersky Lab ZAO, 5-8.

Kaya A., Öğün N. M., (2009), "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri 18, 8–27.

Knopova M., Knopova E., (2014), "The Third World War? In The Cyberspace. Cyber Warfare in the Middle East", 3, (1), 23–32.

Lupovici A., (2011), "Cyber Warfare and Deterrence- Trends and Challenges in Research", Military and Strategic Affairs, 3, (3), 49.

Macdonald C., Oldreive M., Pegalo E., (2012), "Managing Current Complexity : Critical Energy Infrastructure Failures in North America", Dalhousie Journal of Interdisciplinary Management, 8, (3), 7.

Markauskaite L., (2006), "Towards an Integrated Analytical Framework of Information and Communications Technology Literacy: From Intended to Implemented and Achieved Dimensions", İnformation Research, 11, 3–5.

Mirjalili M., Nowroozi A., Alidoosti A., (2014), "A Survey On Web Penetration Test", ACSIJ Advances in Computer Science: an International Journal, 3, (6), No.12 , ISSN : 2322-5157.

Niekerk B. V., Maharaj M. S., (2011), "Relevance of Information Warfare Models To Critical Infrastructure Protection", Scientia Militaria - South African Journal of Military Studies, doi:10.5787/39-2-114, 39, (2), 52–75.

OECD (2008), "Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Secutiy", 5.

Oracle, Pro-G. 2003. "Bilişim Güvenliği", Sürüm 1.1, 6.

Otuteye E., (2004), "Framework for E-Business Information Security Management", 506.

Önal H., (2012), "Hedef Odaklı Sızma Testleri", Bilgi Güvenliği Akademisi, BGA Bilgi Güvenliği, Anakara, 10.

Önal H., (2012a), "Bilgi Güvenliği Açısından Sızma Testleri", Bilgi Güvenliği Akademisi,11.

Özdemir B., (2007), "Zararlı Yazılıma Karşı Korunma Kılavuzu", TÜBİTAK UEKAE, 12.

Patel S., Zaveri J., (2010), "A Risk-Assessment Model for Cyber Attacks on Information Systems", Journal of Computers, doi:10.4304/jcp.5.3.352-359, 5 (3), 352–359.

Pervan G., (1998), "A Ceo View of the Key Issues in Australian Information Systems Management-1997" doi: AJIS, 5, (2), 51–59.

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

Rastogi A., Malhotra S., (2013), "ICT Skills and Attitude as Determinants of ICT Pedagogy Integration", European Academıc Research, 1, (3), 6.

Reis A., Pedrosa A., Dourado M., Reis C., (2013), "Information and Communication Technologies in Long-Term and Palliative Care", Science Direct, 1303–1312.

ResGaz 1, (2004), Ceza Muhakemesi Kanunu, 17 Aralık 2004 tarih ve 25673 sayılı Resmi Gazete.

ResGaz 2 (2004), Türk Ceza Kanunu, 26 Eylül 2004 tarih ve 25611 sayılı Resmi Gazete.

ResGaz 3, (2012), Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı, 20 Ekim 2012 tarih ve 28447 sayılı Resmi Gazete.

Robillard N., (2004), "Global Information Assurance Certification Paper", 1, (4), 2.

Saint R., (2005) "Information Security Management Best Practice Based on ISO/IEC 17799", The Information Management Journal, 60.

Soysal M., Karaarslan E., Eryol G., Yüce H., (2006), "Ulak-NET Bilgisayar Olaylarına Müdahale Ekibi (ULAK-CSIRT) Deneyimi", 2.

Stark P. B., (2007), "The Effectiveness of Internet Content Filters", Department Of Statistics, University Of California, 1–2.

Stohl M., (2006), "Crime, Law and Social Change", 46, (4-5), 223–225.

Stouffer K., Falco J., Scarfone K., (2011), "Guide to Industrial Control Systems (ICS) Security" National Institute of Standards and Technology Special Publication 800-82, Department of Commerce-USA: D3

Symantec (2012), "How Endpoint Encryption Works", Security and IT administrators, USA,1-2.

Symantec (2013), "İnternet Security Threat Report 2013", Symantec Corporation, (18), 15-18, USA.

Şenkaya Y., Adar U. G., 2014. "Siber Savunmada Yapay Zeka Sistemleri Üzerine İnceleme." Akademik Bilişim 2014, 4–5.

Şenol M., (2012), "Silahlı Kuvvetler Dergisi." ATASE, July, 50.

Şimay M. M., (2013), "Siber Tehdit", Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi.

Tabansky L., (2012), "Cybercrime- A National Security Issue?" Military and Strategic Affairs, 4, (3), 117.

Tatar Ü., (2008), "BOME 2008 Bilgi Sistemleri Güvenliği Tatbikatı, Tatbikat Sonuç Raporu", Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Tatar Ü., (2011), "Altıncı Kamu Kurumları Bilgi Teknolojileri Konferansı", Dünya'da ve Türkiye'de Siber Güvenlik Tatbikatları, TÜBİTAK, 2.

TELEKOM (2013), "Bilgi Güvenliği" Telekom Dünyası Dergisi Özel Ek, Bilgi Güvenliği Derneği, 5.

TSE, (2013), "Sızma Testi Hizmeti Veren Personel Ve Firmalar İçin Yetkilendirme Programı" Türk Standartları Enstitüsü, ANKARA

Turan Y., (2011), "İsrail 2011", Sakarya Üniversitesi Uluslararası İlişkiler Bölümü, Ortadoğu Yıllığı-2011.

Turhan M., (2010), "Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri", Bilgi Teknolojileri ve İletişim Kurumu, 42.

TÜBİTAK (2013), "TÜBİTAK Temmuz Ayı Bülteni", 24.

TÜBİTAK-BTK (2011), "Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu", ISBN: 978-605-62506-1-3.

TÜBİTAK BİLGEM, (2011), "Sızma Testleri ve Güvenlik Denetlemeleri İş Tanımlama Dokümanı Şablonu" Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi-TÜBİTAK.

Ünver M. ve Canbay C., (2010), "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik." E-Akademi 438, 95.

Ünver M., Canbay C., Mirzaoğlu A. G., (2011), "Siber Güvenliğin Sağlanması: Türkiye'de ki Mevcut Durum ve Alınması Gereken Tedbirler", Bilgi Teknolojileri ve İletişim Kurumu, 1. Basım, ISBN: 978-9944-0189-6-8, 22-24.

Üzmez İ., (2010), "Bilgi Toplumuna Dönüşüm Sürecinde Türkiye", Silahlı Kuvvetler Dergisi, January.

Vasilescu C., (2012), “Cyber Attacks-Emerging Threats to the 21st Century Critical Information Infrastructures”, Pobrana a Strategıe/Defence & Strategy 1/2012 (10.3849/1802-7199.12.2012.01.053-062), 55.

Xiao-yan G., Yu-qing Y., Li-Lei L., (2011), “An Information Security Maturity Evaluation Mode”, Procedia Engineering 24, 335-336.

Yayla M., (2013), “Hukuki Bir Terim Olarak ‘Siber Savaş’ ”, TBB Dergisi, 186.

Yiğit T., Akyıldız M. A., (2014), “Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi”, Suleyman Demirel University Journal of Natural and Applied Science, 18, (1), 15.

Yılmaz ve Sağıroğlu, (2013), “6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı”, Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri, 162.

Zeltser L., (2011), “Understanding Anti-Virus Software”, Securing The Human, 2.

Zhu B. X., (2014), Resilient Control and Intrusion Detection for SCADA Systems, Electrical Engineering and Computer Sciences University of California at Berkeley, Technical Report No. UCB/EECS-2014-34, 3-4.

# ÖZGEÇMİŞ

UŞAK ilinin Banaz ilçesinde 1981 yılında dünyaya geldim. 1999 yılında Sakarya Üniversitesi Eğitim Fakültesi Fen Bilgisi Öğretmenliği bölümünde lisans eğitimine başladım. 2003 yılında eğitim fakültesinden mezun olarak yine 2003 yılı Ağustos ayında Deniz Astsubay Sınıf Okulu'na giriş yaptım. 2004 yılı Ağustos ayında buradan mezun olarak Deniz Kuvvetleri Komutanlığı'nda Astsubay olarak görev yapmaya başladım. 2012 yılında Astsubaylıktan Subaylığa geçiş sınavını kazanarak 2012 yılından beri Deniz Kuvvetlerinde Güvenlik Subaylığı görevini deruhte etmekteyim. Hali hazırda 2013 yılı bahar döneminde başlamış olduğum Gebze Teknik Üniversitesi Sosyal Bilimler Enstitüsü Strateji Biliminde Akademik eğitimine devam etmekteyim.