ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI

# ULUSAL SİBER GÜVENLİĞİN SAĞLANMASI VE TÜRKİYE İÇİN KAMU GÜVENLİ AĞI MODEL ÖNERİSİ

**Mehtap ŞEN**

**Ulaştırma ve Haberleşme Uzmanlığı Tezi**

**2014**

**Ankara**

ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI

# ULUSAL SİBER GÜVENLİĞİN SAĞLANMASI VE TÜRKİYE İÇİN KAMU GÜVENLİ AĞI MODEL ÖNERİSİ

Mehtap ŞEN

Ulaştırma ve Haberleşme Uzmanlığı Tezi

2014

Ankara

## KABUL VE ONAY

Mehtap ŞEN tarafından hazırlanan "Ulusal Siber Güvenliğin Sağlanması ve Türkiye için Kamu Güvenli Ağı Model Önerisi" adlı bu tezin Ulaştırma ve Haberleşme Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Daire Başkanı Gündüz ŞENGÜL
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Ulaştırma ve Haberleşme Uzmanlığı Tezi olarak kabul edilmiştir.

Başkan :_____

Üye :_____

Üye :_____

Üye :_____

Üye :_____

Bu tez, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tez yazım kurallarına uygundur.

## İÇİNDEKİLER

# ÖZET


| ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI | |
|---|---|
| Tezin Adı | Ulusal Siber Güvenliğin Sağlanması ve Türkiye için Kamu Güvenli Ağı Model Önerisi |
| Türü | Ulaştırma ve Haberleşme Uzmanlığı Tezi |
| Yazar | Mehtap ŞEN |
| Teslim Tarihi | 2014 |
| Anahtar Kelimeler | Siber güvenlik, Strateji, Eylem planı, Kritik altyapılar, Kamu güvenli ağı |
| Tez Danışmanı | Daire Başkanı Gündüz ŞENGÜL |
| Sayfa Adedi | 184 |

Bu çalışmada, siber güvenliğin sağlanması konusunda dünya ülkelerinin ve uluslararası kuruluşların hukuki, idari ve uygulamaya yönelik çalışmaları, siber güvenlik stratejileri ve kamu güvenli ağı konusu ele alınmıştır. Siber saldırgan profilleri, saldırı türleri, yaşanan siber saldırılar, siber suçlar ve en çok bilinen zararlı yazılımlar detaylı olarak incelenmiş, kategorilere ayrılarak tez içerisinde sunulmuştur. Türkiye'nin siber tehditler alanında Dünya'da ve Avrupa'daki yerini gösteren güncel raporlar incelenmiş ve konuya ilişkin somut rakamlara, yüzdelik oranlar içeren şekillere tez içerisinde yer verilmiştir. Kamu güvenli ağı konusunda dünya ülkeleri çalışmaları incelenmiş ve Türkiye için bir model önerilmiştir. Türkiye'de siber güvenlik konusunda çalışmalarda bulunan kurum, kuruluşların rol ve sorumlulukları, bu alanda yapılan hukuki, idari ve uygulamaya yönelik çalışmalar ile Türkiye'nin siber güvenlik strateji belgesi ve eylem planı incelenmiş, mevcut durum değerlendirilmiş ve diğer ülkeler ile uluslararası kuruluşların yaptığı çalışmalar göz önünde bulundurularak Türkiye için önerilerde bulunulmuştur.

## ABSTRACT


| MİNİSTRY OF TRANSPORT, MARİTİME AFFAİRS AND COMMUNİCATİONS | |
|---|---|
| Thesis | Ensuring National Cyber Security and Public Safety Network Model Proposal for Turkey |
| Type | Transport and Communications Expert Thesis |
| Author | Mehtap ŞEN |
| Submission Date | 2014 |
| Keywords | Cyber security, Strategy, Action plan, Critical infrastructures, Public safety network |
| Advisor | Head of Department Gündüz ŞENGÜL |
| Total Page | 184 |

In this study, legal, administrative and practical works, cyber security strategies and public safety network issues of world countries and the international organizations about ensuring cyber security is discussed. Cyber attacker profiles, the types of cyber attacks, cyber crimes and the most known malwares are examined in detail and divided up into categories in this thesis. Turkey's up-to-date reports regarding its position about the cyber threats around the world and Europe were researched and concrete figures and percentage rates about the topic are presented. Studies of world countries about public safety network are examined and a model for Turkey has been suggested. Studies of institutions on cyber security, their roles and responsibilities, works of organizations concerning legislative and administrative implementations, Turkey's cyber security strategy document and action plan has been examined, our current situation has been reviewed and by taking the works of other countries and international organizations into consideration, suggestions have been made for Turkey.

## TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Daire Başkanı Sn. Gündüz ŞENGÜL'e, tez yazma sürecinde desteklerini eksik etmeyen mesai arkadaşlarıma, bu süreçte hep yanımda olup beni destekleyen sevgili aileme teşekkürü bir borç bilirim.

# TABLOLAR LİSTESİ

# ŞEKİLLER LİSTESİ

# KISALTMALAR LİSTESİ

| | |
|---|---|
| **AB** | Avrupa Birliği (European Union (EU)) |
| **ABD** | Amerika Birleşik Devletleri |
| **ANSSI** | Ağ ve Bilgi Güvenliği Ajansı (Network and Information Security Agency) |
| **APCERT** | Asia Pasific Computer Emergency Response Team Asya Pasifik Bilgisayar Olaylarına Müdahale Ekibi |
| **BİLGEM / SGE** | Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi / Siber Güvenlik Enstitüsü |
| **BİT** | Bilgi ve iletişim teknolojileri |
| **BM** | Birleşmiş Milletler (United Nations(UN)) |
| **BTK** | Bilgi Teknolojileri ve İletişim Kurumu |
| **CCD COE** | Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence) |
| **CCIRC** | Kanada Siber Olaylara Müdahale Merkezi (Canadian Cyber Incident Response Centre) |
| **CDMB** | Siber Savunma Yönetim Kurulu (Cyber Defense Management Board ) |
| **CERT** | Bilgisayar Olaylarına Acil Müdahale Ekibi (Computer Emergency Response Team) |
| **CPNI** | Ulusal Altyapının Korunması Merkezi (Centre for the Protection of National Infrastructure) |
| **CS&C** | Siber güvenlik ve İletişim Ofisi (The Office of Cybersecurity and Communications) |
| **CSIRT** | Bilgisayar Güvenlik Olaylarına Müdahale Ekibi (Computer Security Incident Response Team) |
| **CSOC** | Siber Güvenlik Operasyon Merkezi (Cyber Security Operations Center) |
| **DoS** | Hizmetin engellenmesi (Denial of Service) |
| **DDoS** | Dağıtık Hizmetin Engellenmesi (Distributed Denial of Service) |

| | |
|---|---|
| **DHS** | İç Güvenlik Bakanlığı (Department of Homeland Security) |
| **DKS** | Dağıtık Kontrol Sistemi |
| **DoD** | Savunma Bakanlığı (Department of Defence) |
| **DOJ/FBI** | Adalet Bakanlığı / Federal Soruşturma Bürosu (Department of Justice/ The Federal Bureau of Investigation) |
| **EGC** | Avrupa Hükümet CERT'leri (European Government CERTs) |
| **ENISA** | Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency) |
| **ETSI** | Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute) |
| **FCC** | Federal İletişim Komisyonu (Federal Communication Commission) |
| **FIRST** | Olay Müdahale ve Güvenlik Ekipleri Forumu (Forum of Incident Response and Security Teams) |
| **FIRSTNET** | First Responders Network Authority |
| **FISMA** | Federal Bilgi Güvenliği Yönetimi Yasası (Federal Information Security Management Act) |
| **FNR** | Federal Ağ Dayanıklılığı (Federal Network Resilience) |
| **FSB** | Federal Güvenlik Servisi (Federal Security Service) |
| **GCSB** | Hükümet İletişim Güvenliği Bürosu (The Government Communications Security Bureau) |
| **GNET** | Hükümet Omurga Ağı (Government Backbone Network) |
| **GovCertUK** | İngiltere Bilgisayar Olaylarına Müdahale Ekibi (Computer Emergency Response Team (CERT) for UK Government) |
| **HGM** | Haberleşme Genel Müdürlüğü |
| **ICCP** | Bilgi, Bilgisayar ve İletişim Politikaları Komitesi (Committee for Information, Computer and Communications Policy) |
| **ICS** | Endüstriyel Kontrol Sistemleri (Industrial Control Systems) |
| **Interpol** | Uluslararası Kriminal Polis Teşkilatı (International Criminal Police Organization) |

| | |
|---|---|
| **ISPC** | Bilgi Güvenliği Siyaseti Konseyi (Information Security Policy Council) |
| **ISO** | Uluslararası Standardlar Organizasyonu (International Organization for Standardization) |
| **IC3** | İnternet Suçları Şikayet Merkezi (Internet Crime Complaint Center) |
| **IEC** | Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission) |
| **IMPACT** | Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık (International Multilateral Partnership Against Cyber Threats) |
| **LTE** | Long-Term Evolution |
| **NASA** | Ulusal Havacılık ve Uzay Dairesi (National Aeronautics and Space Administration) |
| **NATO** | Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization) |
| **NCAZ** | Milli Siber Savunma Merkezi (National Cyberdefence Centre) |
| **NCCIC** | Ulusal Siber ve Haberleşme Entegrasyon Merkezi (The National Cybersecurity and Communications Integration Center) |
| **NCIRC** | Bilgisayar Olaylarına Müdahale Yeteneği (Computer Incident Response Capability) |
| **NCSC** | Ulusal Siber Güvenlik Merkezi (The National Cyber Security Centre) |
| **NISAC** | Ulusal Altyapı Simülasyon ve Analiz Merkezi (National Infrastructure Simulation and Analysis Center) |
| **NISC** | Ulusal Bilgi Güvenliği Merkezi (National Information Security Center) |
| **NISCC** | Ulusal Altyapı Güvenlik Koordinasyon Merkezi (National Infrastructure Security Coordination Centre) |
| **NSA** | Ulusal Güvenlik Teşkilatı (National Security Agency) |
| **NSC** | Milli Güvenlik Konseyi (National Security Council) |

| | |
|---|---|
| **NSD** | Ağ Güvenliği Kurulumu (Network Security Deployment) |
| **NTIA** | Ulusal Telekomünikasyon ve Bilgi Yönetimi Dairesi (The National Telecommunications and Information Administration) |
| **NW3C** | Ulusal Beyaz Yakalı Suç Merkezi (National White Collar Crime Center) |
| **NZSIS** | Yeni Zelanda Güvenlik İstihbarat Birimi (New Zealand Security Intelligence Service) |
| **OCLCTIC** | Bilgi ve İletişim Teknolojileri ile ilgili Suçla Mücadele Merkez Ofisi (Central Office for the Fight against Crime related to Information and Communication Technology) |
| **OCSIA** | Siber Güvenlik ve Bilgi Güvencesi Ofisi (Office of Cyber Security and Information Assurance) |
| **OEC** | Acil Durum Haberleşme Ofisi (Office of Emergency Communication) |
| **OECD** | Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Cooperation and Development) |
| **OGCIO** | Hükümet Bilişim Kurulu Başkanı Ofisi (The Office of the Government Chief Information Officer) |
| **OSCE** | Avrupa Güvenlik ve İşbirliği Teşkilatı (Organization for Security and Cooperation in Europe) |
| **SCADA** | Veri Tabanlı Merkezi Kontrol ve Gözetleme Sistemi (Supervisory Control and Data Acquisition) |
| **SE / CIR** | Paydaş Katılımı ve Siber Altyapı Esnekliği (Stakeholder Engagement and Cyber Infrastructure Resilience) |
| **SOME** | Siber Olaylara Müdahale Ekipleri |
| **TİB** | Telekomünikasyon İletişim Başkanlığı |
| **TSE** | Türk Standardları Enstitüsü |
| **TÜBİTAK** | Türkiye Bilimsel ve Teknolojik Araştırma Kurumu |
| **UDHB** | Ulaştırma, Denizcilik ve Haberleşme Bakanlığı |
| **US-CERT** | ABD Acil Durum Hazırlık Ekibi (United States Computer Emergency Readiness Team) |

| | |
|---|---|
| **USCYBERCOM** | ABD Siber Komutanlığı (United States Cyber Command) |
| **USOM** | Ulusal Siber Olaylara Müdahale Merkezi (TR-CERT) |
| **VPN** | Sanal Özel Ağ (Virtual Private Network) |

# GİRİŞ

Bilgi ve iletişim teknolojileri günlük hayata her geçen gün daha fazla nüfuz etmektedir. Bu teknolojiler aracılığıyla işlenmekte olan verilerin paylaşımı ise hızla yaygınlaşmakta olan internet üzerinden gerçekleştirilmektedir. Bilişim sistemleri üzerinde kullanılan ve internet üzerinden paylaşılan bu veriler, çok önem arz etmeyen bir bilgi olabileceği gibi, devlete ait güvenlik, askeri, mali, enerji gibi önemli alanları kapsayacak kadar kritik de olabilmektedir. Bu nedenle, bazı durumlarda, bilginin gizliliğini, bütünlüğünü, erişilebilirliğini korumak, ülkenin güvenliğini korumakla eş değer kabul edilmektedir.

Teknolojinin gelişmesi ile birlikte, bilişim sistemlerine yapılan siber saldırıların sayıları ve türleri hızla artmaktadır. Bu siber saldırılar kişisel ağlara, uygulamalara, mobil ağlara veya ülkelerin kritik altyapılarına yönelik olarak gerçekleştirilebilmektedir. Siber saldırıların karmaşıklığı ve çeşitliliği, özellikle mobil veri trafiğinin artması ve bulut bilişimin büyümesi ile orantılı olarak artmaktadır.

Dünya çapında gerçekleştirilmekte olan siber saldırılar, bilgilere hasar verme, gizliliğini ifşa etme, değiştirme, yok etme amacıyla yapılabilmekte ve yaratılan ekonomik zararın yanı sıra, insan hayatınına zarar verebilecek kadar tehlikeli olabilmektedir. Bu durum, teknolojinin ulaştığı noktanın, getirdiği avantajların yanı sıra onun doğrudan bir silah olarak da kullanılabildiğini göstermektedir. Bu nedenle, günümüzde, kara, deniz, hava ve uzayın yanı sıra siber uzay da ulusal güvenlik açısından yeni bir mücadele alanı olarak kabul edilmektedir.

Sadece internet ile sınırlı olmayan siber uzay alanı, bilgi ve iletişim teknolojilerini kullanan kapalı ağlar, scada sistemleri, uydu sistemleri gibi birçok sistem ve donanımı kapsamaktadır.

Siber saldırıların çok düşük bütçelerle yapılabiliyor olması ve kaynağının bulunması konusundaki zorluklar da, siber uzayda yaşanabilecek tehlikenin büyüklüğünü gözler önüne sermektedir. Üstelik siber saldırılar neticesinde oluşabilecek yıkımın tahmin edilmesinin oldukça güç olduğu değerlendirilmektedir.

Bu öneme binaen, dünya ülkeleri kendi altyapılarını korumak için siber güvenlik stratejileri belirlemekte, savunma yöntemleri geliştirmekte hatta kendi siber ordularını oluşturmaktadırlar. Ülkeler, özellikle kritik altyapılarının korunması ve kamunun güvenli bir ağ üzerinden iletişim kurması konularında daha etkin rol almaktadırlar. Türkiye'de de bu alanda yapılan ve yapılması gerekenler bu tez çalışması içerisinde değerlendirilecektir.

Bu çalışma, ulusal siber güvenliğin sağlanması konusunda dünya ülkelerinin ve uluslararası kuruluşların hukuki, idari ve uygulamaya yönelik çalışmalarının incelenerek Türkiye için önerilerde bulunulması açısından önem arz etmektedir. Çalışma kapsamında, bilgi güvenliği ve siber güvenlik kavramları, siber saldırılar, siber saldırgan profilleri, siber saldırı türleri, en çok yankı uyandıran siber saldırılar, siber suçlar, en çok bilinen zararlı yazılımlar ile ulusal siber güvenliğin sağlanması konusunda dünya örnekleri ve uluslararası kuruluşların mevcut çalışmaları, siber tehditlere ilişkin güncel raporlar ve kamu güvenli ağı oluşturulması konuları incelenecektir.

Çalışmanın yöntemi olarak, ilk aşamada literatür taraması yapıldıktan sonra dünya ülkeleri yapılanma modelleri ve hukuki uygulamaları değerlendirilecektir. Sonraki aşamada, dünya ülkeleri ile Türkiye arasında mukayese yapılarak, Türkiye için önerilerde bulunulacaktır.

Çalışmanın birinci bölümünde, bilgi güvenliği ve siber güvenlik kavramlarının ne olduğu, aralarındaki ilişki, bilgi güvenliğine ilişkin standartlar, siber güvenliğe yönelik başlıca risk unsurları ve ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler incelenecektir.

İkinci bölümde, siber saldırıların neler olduğu, saldırgan profilleri, siber saldırı türleri, dünya çapında en çok yankı uyandıran siber saldırılar, siber suçlar, en çok bilinen zararlı yazılımlar ele alınacaktır.

Üçüncü bölümde, ülkelerin ve uluslararası kuruluşların, siber güvenlik alanındaki mevcut idari, teknik ve hukuki düzenlemeleri/çalışmaları ile siber tehditlere ilişkin güncel raporlar incelenecektir.

Dördüncü bölümde, Türkiye'de siber güvenlik alanında yapılan çalışmalar, mevzuatta siber güvenliğin yeri, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın amacı ve kritik altyapıların önemi değerlendirilecektir.

Beşinci bölümde, Amerika Birleşik Devletleri, Birleşik Krallık ve Çin Halk Cumhuriyeti Hong Kong Özel İdari Bölgesi'nde kamu güvenli ağı oluşturulmasına ilişkin idari yapılanma ve altyapı çalışmaları değerlendirilecektir.

Altıncı bölümde, Türkiye'de kamu güvenli ağı oluşturulmasına için yapılan çalışmalar, Türkiye için önerilen kamu güvenli ağı modeli ve dünya ülkelerinin kritik altyapı olarak belirlenen sektörleri ile ulusal çaptaki yapılanmaları incelenerek Türkiye için kritik altyapı olarak belirlenmesi önerilen alanlar incelenecektir.

Sonuç ve öneriler bölümünde ise; tez içerisinde ele alınan konular değerlendirilecek ve Türkiye'de idari, teknik ve hukuki açıdan yapılması gereken hususlar ile ilgili önerilerde bulunulacaktır.

# 1. BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK

Bu bölümde, temel kavramlar, bilgi güvenliği ve siber güvenlik tanımları ile aralarındaki ilişki, bilgi güvenliği standartları, siber güvenliğe yönelik başlıca risk unsurları ve ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler değerlendirilmektedir.

## 1.1. Temel Kavramlar

**Bilişim sistemleri:** Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri ifade etmektedir. (Bakanlar Kurulu Kararı, 2013).

**Siber ortam:** Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı ifade etmektedir. (Bakanlar Kurulu Kararı, 2013).

**Kamu bilişim sistemleri:** Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan ve/veya kamu kurum ve kuruluşları tarafından işletilen bilişim sistemlerini ifade etmektedir. (Bakanlar Kurulu Kararı, 2013).

**Gerçek ve tüzel kişilere ait bilişim sistemleri:** Türkiye Cumhuriyeti kanunlarına tabi olarak gerçek ve tüzel kişilere ait olan ve/veya gerçek ve tüzel kişilerce işletilen bilişim sistemlerini ifade etmektedir. (Bakanlar Kurulu Kararı, 2013).

**Ulusal siber ortam:** Kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortamı ifade etmektedir. (Bakanlar Kurulu Kararı, 2013).

**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 altyapıları ifade etmektedir. (Bakanlar Kurulu Kararı, 2013).

**Siber olay**: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulması olarak ifade edilmektedir (Tebliğ, 2013).

**Siber olaya müdahale:** Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemlerde tutulan veya işlenen verilerin gizlilik, bütünlük ve erişilebilirliğinde meydana gelme riski bulunan veya meydana getiren siber olayın kaynağını, nedenlerini ve sonuçlarını tespit ederek siber olayın devam etmesini, tekrarını veya zarar vermesini önleyen çalışmaları ifade etmektedir (Tebliğ, 2013).

**Endüstriyel kontrol sistemi:** Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan bilgi sistemleridir. Bu sistemler Veri Tabanlı Merkezi Kontrol ve Gözetleme Sistemi (SCADA) ile coğrafi olarak Dağıtık Kontrol Sistemleri (DKS) şeklinde gruplanmaktadır (Tebliğ, 2013).

**Siber suç:** Bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan, bilişim sistemi kullanılarak işlenen ve hukuka aykırı olan suçlar siber suç olarak adlandırılır (İEM, 2014).

**Siber saldırı:** Hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan, planlı ve koordineli saldırılara denilmektedir. Aynı saldırıların ülke veya ülkelere yönelik yapılmasına ise 'Siber Savaş' denilmektedir (Bilgi Güvenliği Derneği, 2012).

## 1.2. Bilgi Güvenliği

**Bilgi güvenliği:** Bilgileri izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemine denir. Bilginin güvenliğinin sağlanabilmesi için "Gizlilik, Bütünlük, Erişilebilirlik" parametrelerinin sağlanması, korunması gerekmektedir (Bakanlar Kurulu Kararı, 2013).

Gizlilik: Bilişim sistem ve verilerine sadece yetkili kişi veya sistemlerce erişilebilmesini,

Bütünlük: Bilişim sistemlerinin ve bilginin sadece yetkili kişilerce veya sistemlerce değiştirilebilmesi,

Erişilebilirlik: Yetkili kişilerin ve işlemlerin ihtiyaç duyulan zamanda ve kalitede bilişim sistemlerine ve bilgiye erişebilmesi olarak tanımlanmaktadır (Bakanlar Kurulu Kararı, 2013).

Bilgi Güvenliğine İlişkin Standartlar:

ISO (Uluslararası Standartlar Organizasyonu) 1947 yılında kurulmuş olup merkezi İsviçre, Cenevre'dir. Amacı, uluslararası ticareti kolaylaştırmak ve desteklemek için standartlar geliştirmektir. ISO, elektrik, elektronik ve benzer teknolojiler alanlarında standart ve terminoloji geliştirmek için IEC (Uluslararası Elektroteknik Komisyonu) ile ortak komiteler oluşturmuştur. ISO 27000 standartları da, ISO'nun ve IEC'nin

ortaklığında geliştirilmektedir (Wikipedia, 2014g).

BGYS (Bilgi Güvenliği Yönetim Sistemi) kurum/kuruluşun hassas bilgilerini yönetebilmek, korunmasını sağlamak amacıyla benimsenen sistematik bir yaklaşımdır. BGYS'nin kuruma uygulamasında Planla, Uygula, Kontrol Et, Önlem Al (PUKÖ) modelinin kullanılması tavsiye edilmektedir. Bilgi güvenliği yönetimi konusunda en yaygın kullanılan standartlar, ISO 27002 ve ISO 27001'dir. ISO 27002 standardı, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek amacıyla genel prensipleri ve yönlendirici bilgileri ortaya koymaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002'de ortaya konulan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ise ISO/IEC 27001'de belirlenmektedir (MARTTİN Vedat, PEHLİVAN İhsan, 2010). ISO 27001 standardı dünya çapında kabul görmüş ve en ideal uygulamaları bir araya getiren uluslararası bir modeldir ve bilgi güvenliği yönetim sistemi oluşturmada güvenlik için gereken 11 kontrol alanı, 39 kontrol hedefi ve 133 kontrolü tanımlayan bir uygulama kılavuzudur (ICS SERT, 2012).

Bu kontrol alanları aşağıda 11 madde halinde yer almaktadır:

A5- Güvenlik Politikası
A6- Bilgi Güvenliği Organizasyonu
A7- Varlık Yönetimi
A8- İnsan Kaynakları Güvenliği
A9- Fiziksel ve Çevresel Güvenlik
A10- Haberleşme ve İşletim Yönetimi
A11 Erişim Kontrolü
A12- Bilgi Sistemleri Edinim, Geliştirme ve Bakım
A13- Bilgi Güvenliği İhlal Olayı Yönetimi
A14- İş Sürekliliği
A15- Uyum

Genel olarak, ISO 27001 standardı aşağıdaki yer alan amaçları gerçekleştirmektedir (ICS SERT, 2012):

- Kurumun / kuruluşun bilgi güvenlik risklerini, bilgi varlıklarına yönelik tehditleri, varlıkların açıklıklarını sistematik olarak denetlemek,
- Risk işleme planları, artık risklerin transferleri ile tutarlı bilgi güvenliği kontrollerini tanımlamak ve gerçekleştirmek, riskleri kabul edilebilir seviyelere çekmek,
- Bilgi güvenliği kontrollerinin sürekliliğini bilgi güvenliği esaslarına göre sağlamak amacıyla yönetim süreçlerini kabul etmek ve uygulamaktır.

<u>ISO/IEC 27001 Standardının Madde Başlıkları (ICS SERT, 2012):</u>

Genel
Proses yaklaşımı
Diğer yönetim sistemleriyle uyumluluk
1 Kapsam
  1.1 Genel
  1.2 Uygulama
2 Atıf yapılan standardlar ve/veya dokümanlar
3 Terimler ve tarifler
  3.1 Varlık
  3.2 Kullanılabilirlik
  3.3 Gizlilik
  3.4 Bilgi güvenliği
  3.5 Bilgi güvenliği olayı
  3.6 Bilgi güvenliği ihlal olayı
  3.7 Bilgi güvenliği yönetim sistemi
  3.8 Bütünlük
  3.9 Artık risk
  3.10 Riskin kabulü
  3.11 Risk analizi
  3.12 Risk değerlendirme
  3.13 Risk derecelendirme
  3.14 Risk yönetimi
  3.15 Risk işleme
  3.16 Uygulanabilirlik bildirgesi
4 Bilgi güvenliği yönetim sistemi

### 1.3. Siber Güvenlik

> Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi "Siber güvenlik" kavramını ifade etmektedir (Bakanlar Kurulu Kararı, 2013).

Bakanlar Kurulu Kararı (2013)'na göre Türkiye'de bulunan bilgi ve iletişim sistemleri ile ilişkili siber güvenliğe yönelik <u>başlıca risk unsurları</u> aşağıda sıralanmıştır:

- ✓ Siber ortamın bilişim sistemlerine ve veriye yapılan saldırılar için anonimlik ve inkâr edilebilirlik fırsatları sunması, saldırı için gerekli araç ve bilginin çoğu zaman ucuz ve kolay elde edilebilir olması, dünyanın herhangi bir yerindeki kişi

veya sistemlerin kasıtlı ya da kasıtsız olarak siber saldırılara iştirak edebilmeleri nedeniyle tehdidin asimetrik olması.

- ✓ Siber ortamın bütünleşik ve kesintisiz iletişime açık yapısı ve siber ortamda bulunan kötücül yazılım ve benzeri tehdit ajanları nedeni ile siber ortamda yer alan tüm bilişim sistemlerinin birbirlerine zarar verebilmesi.
- ✓ Günümüzde büyük kitlelere sunulan kritik hizmet ve servislerin birçoğunun bilişim sistemleri tarafından sağlanıyor ya da kontrol ediliyor olması.
- ✓ Kritik altyapılara ait bilişim sistemlerinin çoğunun internete bağlı olması.
- ✓ Siber güvenliğin ulusal düzeyde bütün vatandaşlarca topyekûn sağlanabileceği gerçeğine rağmen bu konudaki ulusal bilincin yetersiz olması.
- ✓ Siber güvenlik alanında paydaş kurumların arasında ulusal koordinasyon eksikliği.
- ✓ Kişi ve kurumların kamuoyu önünde saygınlıklarını kaybetmemek amacıyla veya başka sebeplerle kendilerine yönelik saldırıları gizlemesi.
- ✓ Siber güvenlik olaylarının araştırma ve soruşturulmasında ulusal ve uluslararası mevzuat yetersizliklerinin işbirliğini güçleştirmesi.
- ✓ Kritik altyapı hizmet ve servislerinin, gerçekleştirilen siber saldırılara ek olarak bilişim sistemlerinin kendi hatalarından, kullanıcı hatalarından ya da doğal afetlerden de olumsuz olarak etkilenmesi ve bu tür olaylara yönelik alınabilecek tedbirler açısından gerekli yeterliliğe sahip olunmaması.
- ✓ Kurumlarda bilgi güvenliği yönetimi altyapılarının yeterli düzeyde olmaması.
- ✓ Siber güvenlik konusunda kurumsal ve kişisel seviyede yeterli bilgi ve bilinç seviyesine ulaşılamamış olması.
- ✓ Siber güvenlik konusunda kurumların üst düzey yöneticilerinin yeterli bilince sahip olmamaları veya siber güvenlik konusunu yeterince sahiplenmemeleri.
- ✓ Siber güvenlik konusunda kurumların yapılanmalarının yetersiz olması ve siber güvenliğin, kurumların sadece bilgi işlem birimlerinin sorumluluğunda görülmesi.
- ✓ Bilgi işlem birimlerinde çalışanların siber güvenlik konusunda yeterli bilgi seviyesine ve tecrübeye sahip olmaması.
- ✓ Siber güvenlik olaylarının detaylı araştırılması ve ihlal ile ortaya çıkan suçun soruşturulması alanlarında az sayıda yeterli personel bulunması.

- ✓ Kurumsal iç denetim süreçlerinde siber güvenliğe ilişkin denetim adımlarının yeterli seviyede ele alınmaması.
- ✓ Siber güvenliğin, geliştirilen veya tedarik edilen bilişim sistemlerinin vazgeçilmez bir unsuru olarak ele alınmaması, buna bağlı olarak kamu kurumlarının bilgi ve iletişim teknolojileri alanındaki ürün ve hizmet tedariklerinde siber güvenliğin yeterli seviyede göz önünde bulundurulmaması.
- ✓ Donanım ve yazılım alanında yerli üretimin yeterli düzeyde olmamasıdır.

Bakanlar Kurulu Kararı (2013)'na göre ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler ise şunlardır:

- ✓ Siber güvenlik, risk yönetimini esas alan, etkin ve sürekli iyileştirmeye dayalı yöntemler aracılığıyla sağlanır.
- ✓ Siber güvenlik için teknik boyutun yanı sıra, hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım benimsenir.
- ✓ Risk yönetiminde, teknik zaafların giderilmesi, saldırı ve tehdidin önlenmesi ile muhtemel zararın en aza indirgenmesi unsurları esas alınır.
- ✓ Siber güvenliğin sağlanmasında birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumluluklarını yerine getirmesi esas kabul edilir.
- ✓ Kritik altyapıların güvenliğinin sağlanması için, özel sektörle, karar mekanizmalarına katılımı da içeren tam bir işbirliği yapılır.
- ✓ Siber ortam güvenliğinin sağlanması ve sürdürülmesinde kamu, özel sektör, üniversiteler ve sivil toplum örgütleri işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir.
- ✓ Uluslararası işbirliği ve bilgi paylaşımı için diplomatik, teknik ve kolluk iletişim kanallarının sürekli ve etkin kullanımı esas alınır.
- ✓ İhtiyaç duyulan mevzuat geliştirilirken uluslararası anlaşma ve düzenlemeler göz önünde bulundurulur.
- ✓ Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir.

- ✓ Siber ortamda şeffaflık, hesap verilebilirlik, etik değerler ve ifade özgürlüğü desteklenir.
- ✓ Güvenlik ile kullanılabilirlik arasında denge kurulur.
- ✓ Düzenleyici ve denetleyici kurumlar sorumlu oldukları alanlarda siber güvenliğin sağlanmasını gözetirler.
- ✓ Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, inovasyon (yenileşim) anlayışı esas kabul edilir.

Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi veya teşebbüste bulunulması olarak ifade edilen siber olayın, odak noktasına göre yaşanan olayın etkisi değişebilmektedir. Siber olayın etkisi ve odak noktası Şekil 1.1'de gösterilmektedir.

Şekil 1.1. Siber Olayın Etkisi ve Odak Noktası


Kaynak: HGM Görev Raporu, 2014

### 1.4. Bilgi Güvenliği ve Siber Güvenlik Arasındaki İlişki

Korunması gereken bilgilere/sistemlere gelebilecek tehditler, güvenlik açıklıkları, bu sistemlere erişilebilme yöntemleri bakımından bilgi güvenliği ve siber güvenlik farklılık gösterebilmektedir. Şekil 1.2'de görüldüğü üzere, siber güvenlik, bilgi güvenliğinin bir alt kümesi olarak değerlendirilmektedir.

Şekil 1.2. Bilgi Güvenliği ve Siber Güvenlik


Kaynak: Nova Infosec, 2014

# 2. SİBER SALDIRGAN PROFİLLERİ, SALDIRI TÜRLERİ VE SİBER SUÇLAR

Bu bölümde, siber saldırgan profilleri, günümüzde sıkça duyulan siber saldırı türleri ve siber suçlar değerlendirilmektedir.

## 2.1. Siber Saldırgan Profilleri

Siber saldırgan profilleri, aşağıda 4 başlık altında incelenmektedir (HGM Görev Raporu, 2014):

### I. Profesyonel Saldırganlar

Profesyonel saldırganlar, hedefli ve bilinçli olarak hareket etmektedirler. Arkalarında devlet veya büyük bir işletmeninin gücü olabilmektedir. Amaç, saldırı yapılan ülkenin siyasi duruşunu zedeleyerek politik anlamda zarar vermek olabileceği gibi, ekonomik anlamda bir yıkım yaratmak da olabilmektedir. Tecrübeli ve bilgi seviyesi yüksek olan bu saldırganların yapacağı siber saldırının kimler tarafından finanse ve organize edildiğinin tespitinin oldukça zor olduğu değerlendirilmektedir.

### II. Organize Suç Örgütleri

Organize suç örgütleri, kişiden/kurumdan kâr elde etmek amacıyla satılabilecek ya da dolandırıcılık, ihaleye fesat karıştırma, şantaj için kullanılabilecek veri ve bilgileri toplamak amacıyla saldırı yapmaktadırlar.

### III. Teknoloji Casusları

Teknoloji casusları olarak isimlendirilen bu saldırganlar, rakip kurumlardaki güncel durumu, yapılan çalışmaları öğrenebilmek ve kendi çıkarları adına kullanmak

amacıyla saldırı yapmaktadırlar. İletişim hırsızlığı bu başlık altında değerlendirilmektedir. Bu durum haksız rekabete neden olmaktadır.

IV. Genç Kuşak Saldırganlar

Genç kuşak saldırganlar, genellikle hedefsiz ve bilinçsiz olarak hareket etmektedirler. Bu kişiler tarafından yapılan saldırılar, büyük zararlar vermemekle birlikte kişisel verilerinizin çalınmasına, gizliliğinin ihlal edilmesine neden olabilmektedir. Bu saldırganlar, sosyal çevresindeki bazı insanlar tarafından övgüyle karşılandığından, bu davranışı tekrarlama ihtiyacı hissederler. Başka kişilerin özel hayatının gizliliğini ifşa ederek, var olduklarını ispat etmekte, kişisel tatmin sağlamaktadırlar.

Dünya çapında yapılan tehditlerin, hangi tehdit kaynağı tarafından gerçekleştirildiği ve hangi amaçla yapıldığı konusu örneklerle desteklenerek Tablo 2.1'de gösterilmiştir.

Tablo 2.1. Dünya Çapında Tehditler

| **Tehdit Kaynağı** | **Motivasyon** | **Tehdit Eylemi/İşlemi** |
|---|---|---|
| Hacker (Bilgisayar Korsanı)<br>İnternet korsancılığı | Meydan Okuma<br>Ego<br>Ayaklanma | Web sitesi saldırıları<br>DoS<br>Sistem saldırıları/izinsiz giriş<br>Yetkisiz sistem erişimi |
| Kurum çalışanları (Az eğitimli, kötü niyetli, ihmalkâr, sahtekâr çalışanlar) | Merak<br>Parasal Kazanç<br>İntikam<br>Kasıtsız Hatalar | Dolandırıcılık ve Hırsızlık<br>Sahte Giriş<br>Bozulmuş Veri<br>Kişisel Bilgilerin Satışı<br>Sistem Hataları<br>Sistem Sabotajı |
| Bilgisayar Suçluları<br>Örgütlü/Organize Suçlar | Parasal Kazanç<br>Yasadışı Bilginin Açığa Çıkması<br>Bilgilerin İmha Edilmesi<br>Yetkisiz Veri Değiştirme | Gasp, Şantaj<br>Kimlik Hırsızlığı<br>Rüşvet<br>Sistem Saldırıları/İzinsiz Giriş |
| Teröristler | Şantaj<br>İmha<br>İstismar<br>İntikam | Bomba / Terörizm<br>Bilgi Savaşı<br>Sisteme Saldırı, Hizmetin Engellenmesi (Dos)<br>Sisteme Nüfuz Etme |
| Dış Devletler | Küresel Güç<br>Hedef Tanımlama<br>Teknoloji ve Savunma<br>Faaliyetlerin Finansmanı<br>Geniş Çaplı Aksaklıklar | Bilgi Savaşı<br>Bilgi Sistemlerini Haritalama<br>Casusluk<br>Sisteme Saldırı<br>Sisteme Nüfuz Etme |

Kaynak: HGM Görev Raporu, 2014

## 2.2. Siber Saldırılar ve Türleri

Bu bölümde, siber saldırıların tanımı, dünya ülkelerinde yaşanan ve en çok bilinen siber saldırılar ile siber saldırı türleri detaylı olarak incelenmiştir.

### 2.2.1. Siber saldırılar

Hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılara denilmektedir (Bilgi Güvenliği Derneği, 2012).

Siber Saldırılar; iki kategoriye ayrılmaktadır (Wikipedia, 2014e):

1. Sözdizimsel saldırılar

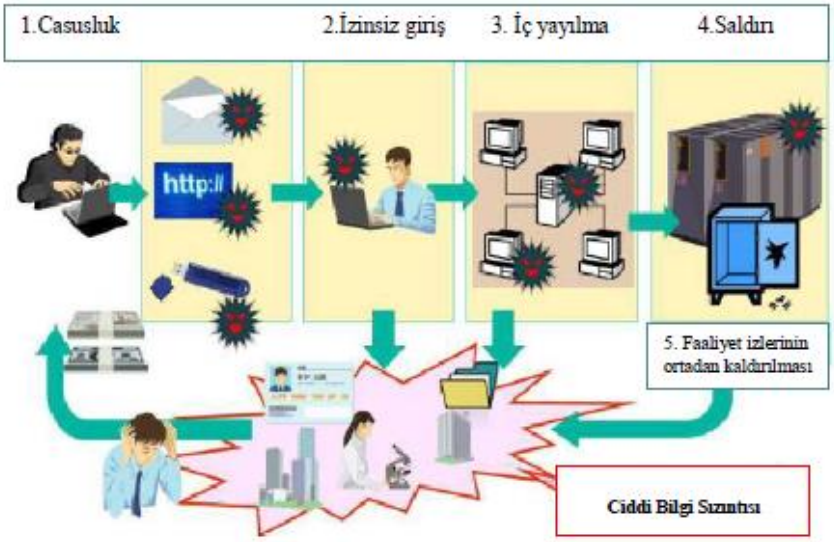
Sözdizimsel saldırılar yalındır. Virüs, solucan, truva atı gibi zararlı yazılımlar bu kapsamda değerlendirilmektedir.

2. Anlambilimsel saldırılar

Anlambilimsel saldırılar ise, bilgilerin değiştirilmesi ve dağıtılmasına neden olan zararlı yazılımlar aracılığıyla yapılan saldırılar olarak değerlendirilmektedir.

Siber saldırılarda kullanılan yöntem hakkında genel işleyiş Şekil 2.1'de gösterilmektedir.

Şekil 2.1. Hedeflenen Siber Saldırılarda Kullanılan Yöntemin Genel İşleyişi




Kaynak: NEC, 2013

Şekil 2.1'de görüldüğü üzere, tipik bir saldırı 5 aşamadan oluşmaktadır (NEC, 2013):

1. Casuslık (Espionage)

2. İzinsiz Giriş (Intrusion)

3. İç yayılma

4. Saldırı

5. Faaliyet izlerinin ortadan kaldırılması

Yapılan siber saldırılar ciddi bilgi sızdırmalarına neden olabilmektedir.

NATO (2013)'ya göre dünya çapında en çok yankı uyandıran, maddi veya politik açıdan zarar veren siber saldırılar zaman sıralamasına göre aşağıda yer almaktadır:

- Morris Solucanı, Yıl: 1988

Dünyanın yeni oluşmaya başlayan siber altyapısını etkileyen ve dünyada bilinen ilk solucan olan Morris büyük ölçüde ABD'deki bilgisayarlara yayılmıştır. Solucanın yaratıcısı olan Robert Tappan Morris ABD'de "Bilgisayar Dolandırıcılığı ve Kötüye Kullanma" yasasının ilk mahkûmu olmuştur (NATO, 2013). Solucan UNIX sistemindeki zayıflıkları kullanmış ve düzenli olarak kendini çoğaltmıştır. 6000 bilgisayarın etkilendiği ve tahminen $10-$100 milyon dolar zararın oluştuğu raporlanmıştır (ARNNET).

- NASA, Yıl: 2006

NASA (National Aeronautics and Space Administration, Ulusal Havacılık ve Uzay Dairesi) 2006 yılı Aralık ayında, ekleri ile birlikte gönderilen mail saldırısına maruz kalmıştır. Saldırganlar tarafından ABD uzay fırlatma araçları planlarının ele geçirildiği raporlanmıştır (NATO, 2013).

- Estonya, Yıl: 2007

Estonya 2007 yılı nisan ayında saldırganlar tarafından hizmetin engellenmesi (DoS) saldırısına maruz kalmıştır. Devlette bazı çevrimiçi hizmetler kesintiye uğramış ve çevrimiçi bankacılık işlemleri durdurulmuştur. Zarar vermekten çok kargaşa, isyan çıkarma amacıyla yapıldığı değerlendirilmektedir (NATO, 2013).

- ABD, Yıl: 2007

2007 yılı haziran ayında ABD Savunma Bakanı'nın tasnif dışı e-mail hesabı hacklenmiştir (NATO, 2013).

- Çin, Yıl: 2007

Çin Uzay Bilimleri ve Endüstri Kurumu'nun(CASIC) intranet ağında bir araştırma yapılmıştır ve gizli birimlerdeki bilgisayarlar ile kurumsal liderlerin bilgisayarlarında spyware zararlı yazılımı bulunmuştur (NATO, 2013).

- Gürcistan, Yıl: 2008

2008 yılı ağustos ayında, Gürcistan Rusya ile çatışma içerisindeyken, Gürcistanın bilgisayar ağları bilinmeyen saldırganlar tarafından hacklenmiştir. Gürcistan hükümetinin web sitelerinde birtakım yazılar görünmüştür. Hacklenme sonucunda bazı hizmetlerde kısa süreli kesinti olmuş veya hiç olmamıştır ancak yaşanan olayın Gürcistan üzerinde siyasi anlamda bir baskı yaptığı değerlendirilmektedir (NATO, 2013).

- İsrail, Yıl: 2009

2009 yılı Ocak ayında, Gazze Şeridindeki askeri harekât sırasında, hackerlar İsrail'in internet altyapısına saldırmıştır. Saldırı en az 5.000.000 bilgisayar tarafından yürütülmüş olup hükümet web sitelerine odaklanmıştır (NATO, 2013).

- Çin, Yıl: 2010

2010 yılı Ocak ayında, "İran Siber Ordusu" olarak adlandıran bir grup, Çin'in popüler arama motoru olan Baidu'nun hizmetinin kesintiye uğramasına yönelik saldırıda bulunmuştur. Baidu'yu kullanmak isteyen kullanıcılar İran'a özgü siyasi bir mesaj gösteren sayfaya yönlendirilmiştir (NATO, 2013).

- İran Stuxnet, Yıl: 2010

Stuxnet, Siemens endüstriyel kontrol sistemlerini etkileyebilecek şekilde tasarlanmış ve İran'ın nükleer programlarına yönelik yapılmış olan karmaşık bir zararlı yazılım

parçasıdır (NATO, 2013). Stuxnet, endüstriyel kontrol sistemlerinin ve dış dünyaya kapalı sistemlerin de siber saldırılara hedef olabileceğini göstermesi, uzun süre sistemde gizlenerek hiçbir virüs programı tarafından tespit edilmeden değişiklikler yapabilmesi ve çözümlenememesi açısından siber güvenlik konusunda büyük öneme sahiptir ve yankı uyandırmıştır. Kaspersky, Siemens, Symantec, F-Secure gibi birçok firma, Stuxnet'in tespit edilmesi ve etkileri üzerinde çalışma yürütmüştür. Zero day (sıfır gün) açıklığını kullanan dijital olarak imzalanmış yazılımlar kullanan Stuxnet, virüslü bilgisayara takılan usb bellek aracılığıyla Tablo 2.2'de göründüğü üzere birçok ülkeye yayılmıştır (Wikipedia, 2014f).

Tablo 2.2. Stuxnet Yazılımından Etkilenen Ülkeler ve Bilgisayarların Oranı

| Ülke | Etkilenen Bilgisayarların Oranı |
|---|---|
| İran | 58.85% |
| Endonezya | 18.22% |
| Hindistan | 8.31% |
| Azerbaycan | 2.57% |
| ABD | 1.56% |
| Pakistan | 1.28% |
| Diğer | 9.2% |

Kaynak: Wikipedia, 2014f

- Kanada, Yıl: 2011

2011 yılı Ocak ayında, Kanada hükümeti; Milli Savunma Dairesinin araştırma kuruluşu olan "Savunma Araştırma ve Geliştirme" kuruluşu da dâhil olmak üzere kurumlarına büyük bir siber saldırı bildirmiştir. Saldırı; Kanada'nın başlıca ekonomik kuruluşları olan Maliye Bakanlığı ve Hazine Kurulu'nu, internet bağlantısını kesmeye zorlamıştır (NATO, 2013).

- ABD, Yıl: 2011

2011 yılı Temmuz ayında, ABD Savunma Bakanlığı'nın siber stratejisinin açıklandığı bir konuşmada, ABD savunma bakan yardımcısı hacklenmiştir ve Savunma Bakanlığı'ndan 24.000 dosya çalındığı belirtilmiştir (NATO, 2013).

- Red October Saldırısı, Yıl: 2011

Bir Rus firması olan Kaspersky, en az 2007 yılından beri faaliyette olan ve " Red October (Kızıl Ekim)" olarak adlandırılan dünya çapında bir siber saldırı keşfetmiştir. Hackerların, microsoft'un word ve excel programlarının açıkları üzerinden bilgi topladığı belirtilmiştir. Saldırının öncelikli hedefinin, Doğu Avrupa, Eski Sovyetler Birliği ve Orta Asya ülkeleri olduğu görünmektedir. Virüsün; hükümet büyükelçiliklerinden, araştırma firmalarından, askeri tesislerden, enerji sağlayıcılardan, nükleer ve diğer kritik altyapılardan bilgi topladığı belirtilmiştir (NATO, 2013).

- Kore, Yıl: 2013

Güney Kore finans kuruluşlarının yanı sıra Koreli yayın kuruluşu YTN'nin ağları 2013 yılında gerçekleşen bir siber olaydan dolayı zarar görmüştür (NATO, 2013).

### 2.2.2. Siber saldırı türleri

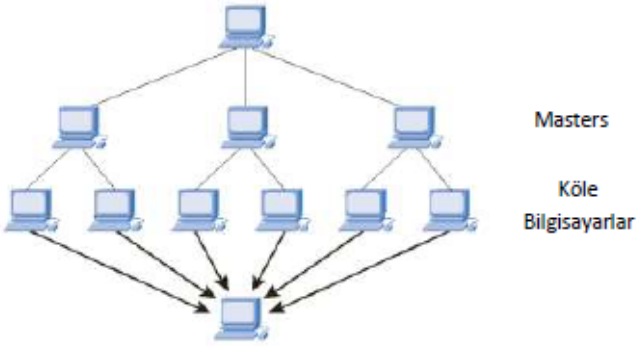
Bilgisayar kullanıcısının izni olmadan bir bilgisayar sistemine yasa dışı saldırı yapılmasına hackleme (hacking) denilmektedir. Siber saldırı türleri şu başlıklar altında değerlendirilmektedir:

**I. Hizmetin Engellenmesi (Hizmet Dışı Bırakma) Saldırısı (Denial of Service (DoS) Attack)**

Mağdurun kaynaklarını tüketme amaçlı yapılan saldırı çeşididir.

Mağdurun ağının bant genişliğini aşarak, disk alanı veya işlemci zamanını tüketerek, istenmeyen e-postalar ile e-posta kutusunu doldurarak, işletim sistemi veri yapılarını tüketerek, mağduru servislerden yoksun bırakma amaçlı tek bir bilgisayardan yapılan saldırıdır. DDOS (Distributed Denial of Service, Dağıtık hizmetin engellenmesi) ise saldırıların daha etkili olması için kullanılan bir yöntemdir. Çünkü saldırgan, öncelikle gerekli trafik hacmini üretmek için kullanacağı bir bilgisayar ağı kurmaktadır. Daha fazla sistem kullanıldığından saldırı trafiği çok daha yüksek olmaktadır (Çifci, 2013, s.393). Şekil 2.2'de DDOS saldırılarının genel işleyişi gösterilmektedir.

Şekil 2.2. DDOS Saldırıları




Kaynak: CISCO, 2013

### II. Bilgi Sızdırma/Yanıltma Sinyali (Spoofing)

Ağdaki diğer bilgisayarlara erişim sağlamak amacıyla genellikle özel erişim ayrıcalıklarına sahip başka bir bilgisayarın kimliğini, kullanarak oynuş gibi hareket etme işlemine denilmektedir. Yani; başka bir ağa atak yapan saldırgan kendisini atak yaptığı sistemin yetkilisi olarak göstermektedir. **IP spoofing** (IP aldatmacası) olarak da adlandırılan bu saldırı yönteminde IP paketlerinin içeriğinin değiştirilmesi ile ya da Proxy/Socks sunucularının kullanılması ile bu saldırı gerçekleştirilebilmektedir (Çifci, 2013, s.145).

### III. Kriptografik Saldırılar

Şifrelenmiş mesaj veya verinin şifresinin çözülebilmesi amacıyla yapılan saldırılara kriptografik saldırılar denilmektedir. Bu saldırı türünde, saldırgan kriptografik sistemin açıklıklarını kullanarak şifreyi çözmeye çalışmaktadır (Çifci, 2013, s.141).

### IV. Hattı Dinleme (Wire Tapping)

Gerekli güvenlik önlemleri alınmamış sistemlerde, özel teçhizatlar kullanılarak, iletişim ağı kablolarına bağlanılabilmekte ve tüm trafik dinlenebilmektedir. Bu saldırı türü hattı dinleme (Wire Tapping) olarak adlandırılmaktadır.

### V. Yığın e-posta Gönderimi/İstenmeyen e-posta (Spam e-mail, Junk e-mail)

Birbirine benzer içeriğe sahip mesajın, yüksek sayıdaki kopyasının, internet üzerinden bu tip bir mesaji alma talebinde bulunmamış kişilere gönderilmesi işlemine denilmektedir (AKU, 2013).

Bu tür istenmeyen e-postalar, kredi teklifleri gibi ticari kazanç içerikli konular da içerebilmekte olup, kullanıcının tek bir e-postaya yanıt vermesi ya da eklentileri açması halinde tehlikeli sonuçlar doğurabilmektedir.

### VI. Virüs Yayılması (Virus Dissemination)

Bilgi ve iletişim teknolojileri üzerinde bulunan diğer yazılımlara tutunan ve mağdurun sistemine zarar veren kötü amaçlı yazılımlar (virüs, solucan, Truva Atı, time bomb (zaman bombası), logic bomb (Mantık Bombası) vb.) bu başlık altında değerlendirilmektedir. Bir virüsün kasıtlı olarak yayılması/serbest bırakılması virüs yayılması olarak adlandırılmaktadır (VirtualPone, 2013).

### VII. Veri Sahteciliği (Data Diddling)

Bu tür saldırılar, ham bir verinin, bilgisayar tarafından işlenmeden önce değiştirilmesi ve işlendikten hemen sonra geri değiştirilmesi işlemine denilmektedir. Hindistan'da elektrik panoları, eklenen veri diddling programlarının kurbanı olmuştur. 1996 yılında gerçekleşen NDMC Elektrik Fatura Dolandırıcılık Vakası, bu durumun tipik bir örneğidir (Fayfoundation, 2013, s.3).

### VIII. Salam Saldırısı (Salami Attacks)

Bu suç, küçük değişiklikler yapıp farkedilmeden sistemden ayrılma işlemine denilmektedir. Örneğin, saldırgan bir bankanın tüm müşterilerinin hesabından ayda 20 kuruş gibi küçük bir rakamı kendi hesabına çekmekte ancak böyle bir durumda hesap sahipleri bu küçük rakam için bankayla iletişime geçme ihtiyacı duymamaktadır, suçlu ise büyük miktarda kazanç elde etmektedir (VirtualPone, 2013).

### IX. Ağ Tarama (Network Scanning)

Bir ağ üzerinden geçen verilerin gözlenmesi veya bu ağ üzerinde bulunan donanımların zaafiyetlerinin araştırılması işlemine denilmekte olup, ağ güvenlik değerlendirmesinin yanı sıra saldırı amaçlı da yapılabilmektedir (Çifci, 2013, s.148).

## X. Sosyal Mühendislik Saldırısı (Social Engineering Attack)

Sosyal mühendislik, insanlar arasındaki iletişim modellerini açıklıklar olarak tanıyıp, bunlardan faydalanarak güvenlik bariyerlerini aşan yönteme verilen isimdir (Çifci, 2013, s.147).

Genellikle e-posta üzerinden gerçekleşen bir yöntemdir. Saldırgan, amacına ulaşabilmek için mağdura güvenilir ya da doğruluğu sorgulanamaz bir kaynaktan geldiğine inandırmaktadır. Saldırgan, mağduru bilgi vermeye zorlamak ya da hatalı bir hareket yapmaya (sahte web sitesine tıklamak, virüslü yazılım kurmak vb.) yönlendirmektir.

## XI. Oltalama (Phishing)

Sosyal mühendisliğin uygulama alanlarından biridir. Aldatıcı yollarla, kişilerin bankadaki kurumsal hesap sahiplerinin kişisel gizli bilgilerini çekme tekniği, phishing saldırılarının uygulanma yöntemlerinden birisini oluşturmaktadır.

Örneğin; saldırgan, mağdura, resmi bir kurumdan gelmiş gibi göstererek bir e-mail göndermekte ve bu yolla mağduru aldatıp banka hesap bilgilerini ve kredi kartı şifrelerini çalabilmektedir (VirtualPone, 2013). Oltalama yöntemi kullanılarak, Fatura Zararlı Yazılımı (FatMal) ile 2012 yılında başlayan ve özellikle Türkiye'deki kullanıcıları hedef alan saldırılar gerçekleştirilmiştir.

## XII. Kredi Kartı Dolandırıcılığı

Güvenli olmayan ortamda yapılan elektronik işlemlerde; kullanım dışı olan web sayfasının içerisine mağdurun kredi kartı bilgilerini girmesi ile birlikte, saldırganın bu kart bilgilerini çalıp, mağdurun kimliğine bürünerek, kötü amaçlı kullanmasına neden olmaktadır. Bu tür saldırılar kredi kartı dolandırıcılığı olarak adlandırılmaktadır.

## XIII. Zararlı Yazılım (Malware) Kullanımı

Herhangi bir sisteme saldırmanın en kolay yollarından biri, zararlı bir yazılımın yüklenmesi veya mağdurun hatalarından faydalanarak mağdur tarafından yüklenmesini sağlamaktır.

Zararlı yazılımların en çok bilinen türleri aşağıda sıralanmıştır (Malwaretruth, 2014):

- **Virüs:** Başka programlara veya yazılımlara bağımlı çalışan, yazılım çalıştırıldığı zaman kendi kendine çoğalma özelliği olan ve yerleşebileceği bir programa ihtiyaç duymakta olan bir programdır.

- **Solucan (Worm):** Kendi kendine çoğalabilen ve ağ üzerinde bir bilgisayardan diğerine yayılma yollarını bulan ve yayılan, sistem işletim dosyaları ve veri dosyalarını yok eden bir programdır.

- **Truva atı (Trojan):** En tehlikeli zararlı yazılımlardan birisidir. Hedeflerine ulaşmak amacıyla tespit edilmeden, silinmeden ve kapatılmadan çalışmayı sürdürebilen zararlı yazılımlardır.

- **Mantık Bombası (Logic Bomb):** Bilgisayarda belirlenmiş bir zaman diliminde çalışabilen ve sistemde o zamanı bekleyerek kalabilen, belirlenen zaman geldiğinde ise istenen faaliyeti gerçekleştiren programlardır.

- **Arka Kapı (Back Door):** Arka kapı, normal kimlik doğrulama işlemlerini atlayarak, sisteme gizli bir yoldan ulaşmayı sağlayan yöntemdir. Genellikle bazı portları açarak başka bir yazılımın sisteme sızmasını sağlayan yazılımlardır.

- **Adware (Advertising-Supported Software):** En az tehlikeye sahip olan ve en kârlı zararlı yazılımdır. Adware bilgisayardaki reklamları görüntülemektedir.

- **Casus Yazılım (Spyware):** Adından da anlaşılacağı gibi, casus yazılım, internet üzerindeki hareketleri izlemekte, merkezi bir bilgisayara göndermekte ve sonrasında mağduru reklamlar (adware) ile hedef almaktadır.

- **Rootkits:** Sistemde yüklü olan ve tespitinin önlenmesi amacıyla gizli olarak sistemde kalan kötü amaçlı bir programdır. Bilgisayardaki sistem bilgilerini veya dosyaları, işletim sisteminden gizleyebilme yeteneğine sahiptir.

- **Ransomware (Fidye Yazılım):** Mağdurun ekranda, siber suç için ödeme yapılana kadar bilgisayarının kitlendiğine dair uyarı alması durumuna neden olan zararlı yazılımdır.

- **Browser Hi-jacker (Tarayıcı Korsanı):** Mağdurun anasayfasındaki görünümünü eklenen görüntüler ile değiştiren bu tehlikeli zararlı yazılım, normal arama faaliyetini yönlendirmekte ve geliştiricilerin görmek istedikleri sonuçları vermektedir.

### 2.3. Siber Suçlar

Siber suç, bir bilişim sistemine izinsiz ve hukuka aykırı olacak şekilde girilmesi ve sonrasında yapılan eylemlere denilmektedir. Bu suçta hedef bir kişi olabileceği gibi kişinin malvarlığı veya bir sistemin kendisi de olabilmektedir. Örneğin, bir sisteme girerek, zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilmektedir (İEM, 2014).

Avrupa Konseyi Siber Suçlar Sözleşmesi (2008)'ne göre, siber suçlar 4 başlık altında değerlendirilmektedir:

i. Bilgisayar sistemlerinin ve verilerin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar,

ii. Bilgisayarlarla ilgili suçlar,

iii. İçerikle ilgili suçlar,

iv. Telif hakları ve bağlantılı haklarının ihlali ile ilgili suçlar.

Avrupa Konseyi Siber Suçlar Sözleşmesi, Uluslararası Kuruluşlar başlığı altında detaylı olarak incelenmiştir.

Ayrıca, Türkiye Cumhuriyeti Hükümeti ile Gürcistan Hükümeti arasında "Suçla Mücadelede İşbirliği" konulu mutabakat zaptı imzalanmıştır. İşbirliği alanları içerisinde siber suçlarla mücadele de bulunmaktadır (Bakanlar Kurulu Kararı, 2012a).

# 3. DÜNYA'DA SİBER GÜVENLİK ÇALIŞMALARI

Bu bölümde, ülkelerin ve uluslararası kuruluşların, siber güvenlik alanındaki mevcut idari, teknik ve hukuki düzenlemeleri/çalışmaları incelenmektedir.

## 3.1. Ülke Örnekleri

Bu bölümde, ülkelerin siber güvenlik konusunda yaptığı mevzuat çalışmaları ve siber güvenlik stratejileri yer almaktadır. Siber güvenlik alanındaki çalışmaları/yapılanmaları web ortamından erişilebilir olan ülke örnekleri incelendiğinde, ülkelerin çoğunun, siber güvenlik alanındaki çalışmaları bir yasa ile değil, strateji ya da Başkanlık Emri gibi resmi yazılarla yürüttüğü görülmektedir.

### 3.1.1.Amerika Birleşik Devletleri (ABD)

ABD'de siber güvenlik; İç Güvenlik Bakanlığı (Department of Homeland Security, DHS) tarafından sağlanmaktadır. Bakanlık bünyesinde bulunan US-CERT, siber olayları koordine etmek amacıyla görev yapmaktadır.

Amerika Birleşik Devletleri'nin siber güvenlik alanında çalışan başlıca kurumları şunlardır:

- DHS
- FBI
- USCYBERCOM
- Ulusal Güvenlik Teşkilatı (National Security Agency, NSA)

ABD İç Güvenlik Bakanlığı, ülkenin siber güvenlik duruşunu geliştirmek, siber alanda yapılacak bilgi paylaşımını koordine etmek ve ABD vatandaşlarının anayasal haklarını korurken; proaktif olarak siber riskleri yönetmek için de çaba harcamaktadır. Dinamik ve karmaşık bir ortamda yanıt verebilen ve işbirliğine önem veren US-CERT'ün, güvenilir, küresel bir siber lider olmayı hedeflediği belirtilmektedir. Siber güvenlik alanında yapılan önemli çalışmalar aşağıda sıralanmıştır:

- 2003 yılı şubat ayında "Ulusal Siber Uzay Güvenliğini Sağlama" stratejisi yayımlanmıştır (US-CERT, 2003).
- 2007 yılında Siber Komutanlığı (Cyber Command) kurulmuştur.
- 2008 yılında "Kapsamlı Ulusal Siber Güvenlik Girişimi (Comprehensive National Cybersecurity Initiative (CNCI))" direktifi hazırlanmıştır (White House, 2008).
- 2011 yılında ABD Siber Güvenlik Stratejisi yayımlanmıştır. Siber Güvenlik Stratejisinde üç temel öncelik bulunmaktadır (ENISA, 2011):
    - ABD'nin kritik altyapılarına karşı olabilecek siber saldırıları önlemek,
    - Siber saldırılara karşı ulusal güvenlik açıklarını azaltmak,
    - Siber saldırılardan kaynaklanan zararı ve toparlanma sürecini minimuma indirmektir.

ABD'de siber güvenliğin yürütüldüğü İç Güvenlik Bakanlığı'nın yapılanması, bu alanda görev yapan bazı önemli birimleri ve sorumlulukları bölüm içerisinde detaylı olarak incelenmiştir. İç Güvenlik Bakanlığı'nın siber güvenliğe ilişkin organizasyon yapısı Şekil 3.1'de gösterilmektedir.

Şekil 3.1. İç Güvenlik Bakanlığı'nın Siber Güvenliğe İlişkin Organizasyon Yapısı


Kaynak: HGM Görev Raporu, 2014

Ulusal Güvenlik Teşkilatı, ülke sınırları dışındaki siber tehdit istihbaratını yürütmekten sorumlu birimdir. ABD İç Güvenlik Bakanlığına bu alanda destek vermektedir.

Ulusal Altyapı Simülasyon ve Analiz Merkezi (NISAC) ise İç Güvenlik Bakanlığı içinde bulunan, simülasyon ve analiz programı konusunda bir modellemedir. NISAC, "kritik altyapıları koruma amaçlı ulusal uzmanlık kaynağı" olarak hizmet vermektedir. NISAC uzmanları, modelleme ve simülasyon yeteneklerini kullanarak, kritik altyapıların karmaşıklığı, güvenlik açıklıkları, birbirine bağımlılıklarını analiz etmektedir. NISAC, ulusal, bölgesel ve yerel düzeyde 16 kritik altyapı sektöründe, altyapı kesintilerin sonuçlarını sunmaktadır (NISAC, 2013).

ABD'nin *kritik altyapıları* aşağıda yer almaktadır (DHS, 2014b).

- Enerji
- İletişim
- Kimyasal atık
- Barajlar
- Sosyal tesisler
- Finansal Hizmetler
- Kritik üretim
- Devlet olanakları
- Sağlık hizmetleri ve halk sağlığı
- Bilgi teknolojileri
- Nükleer reaktörler, malzemeler ve atık
- Su ve atık su sistemi
- Ulaşım sistemi
- Gıda ve tarım
- Acil durum hizmetleri
- Savunma sanayi

#### 3.1.1.1. Siber güvenlik ve iletişim ofisi

Siber Güvenlik ve İletişim Ofisi (CS&C), ABD'nin siber güvenliğinin ve iletişim altyapısı güvenliğinin, olası saldırılara karşı dayanıklılığının/esnekliğinin sağlanmasından sorumlu olan İç Güvenlik Bakanlığı'nın en önemli birimlerinden birisidir (DHS, 2014a).

**Hedefleri:**

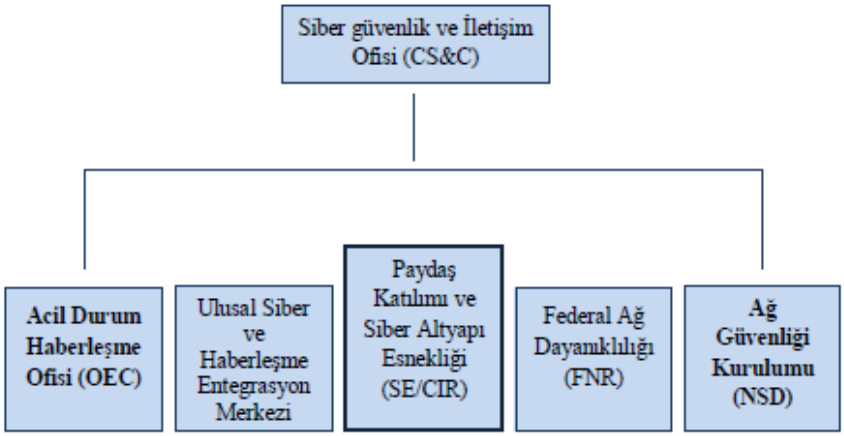
- Karşı karşıya gelinen siber güvenlik ve iletişim riskleri anlayışını artırmak,
- En çok zarar veren olayların oluşumunu önlemek ve etkilerini azaltmak,
- Tüm paydaşların kapasitesini genişletmek,
- CS&C 'de dünya çapında yetenek ve faaliyet oluşturmak.

**Sorumlulukları:**

- Acil durum haberleşme yetenekleri,
- dot-gov'ları güvence altına almak,
- dot-com'ları korunmasına yardımcı olmak,
- Kritik altyapıların güvenliği konusunda yardımcı olmak,
- Ulusal haberleşme güvenliğini sağlamak,
- Siber ve iletişim olaylarına yanıtı koordine etmek.

Siber Güvenlik ve İletişim Ofisi'nin organizasyon yapısı Şekil 3.2'de detaylı olarak incelenmiştir.

Şekil 3.2. Siber Güvenlik ve İletişim Ofisi Organizasyon Yapısı




Kaynak: HGM Görev Raporu, 2014

Acil Durum Haberleşme Ofisi (Office of Emergency Communications, OEC)

11 Eylül 2001 tarihinde yaşanan trajik olayların ardından, 9/11 Komisyonu ülke çapında acil bir durum ile karşı karşıya kalındığı zaman, iletişim sorunlarını çözmek için, birlikte çalışabilen ulusal kamu güvenliği haberleşme ağının kurulmasını tavsiye etmiştir.

O zamandan bu yana, kamu güvenliği topluluğu, gelişmiş koordinasyon, yönetim yapıları, planlama, eğitim ve ekipman aracılığıyla acil iletişim yeteneklerini geliştirmede ilerleme kaydetmiştir. Aynı zamanda, yüksek hızlı, kablosuz iletişim teknolojisindeki gelişmeler ile özel sektörde, acil ve günlük işlemler sırasında bilgi paylaşımı ve iletişimi geliştiren bir platform ile kamu güvenliğini sunmuştur. Genişbant teknolojisi sayesinde, kamu güvenliği kullanıcıları, devam etmekte olan bir suçun video görüntülerine erişebilme, yanan bir binanın planını yükleyebilme, ya da diğer toplumlardan personeli ile hızlı ve güvenli bir şekilde bağlantı kurma imkânına sahip olmaktadır (HGM Görev Raporu, 2014).

22 Şubat 2012 tarihinde, ABD Başkanı Barack Obama, Ulusal Kamu Güvenliği Geniş Bant Ağını finanse etmek ve yönetmek için hükümler içeren, HR3630 sayılı yasayı imzalamıştır. Ulusal Kamu Güvenliği Genişbant Ağı, acil durumlarda iletişim kurmak amacıyla, yalnızca bunun için tahsis edilmiş olan sağlam, güvenilir bir şebeke sağlayacaktır (DHS, 2013a).

Ağ Güvenliği Kurulumu (NSD)'nun girişimleri ve sorumlulukları aşağıda belirtilmiştir (HGM Görev Raporu, 2014):

<u>Girişimler</u>

- Ulusal Siber Koruma Sistemi
  - Saldırı Tespit
  - Saldırı Önleme
  - Bilgi Paylaşımı
  - Analiz Araçları

- Özel sektör kuruluşları için yönetilen hizmet çözümleri
  - Gelişmiş Siber Güvenlik Hizmetleri

- Siber bilgi alışverişinin standardizasyonu ve birlikte çalışabilirlik.

Sorumluluklar

- Ulusal siber güvenlik koruma sistemi tasarlamak, geliştirmek, dağıtmak, sürdürmek ve müşteri desteği sağlamak,

- Hükümet ve endüstri sektörü ortakları ile siber bilgi alışverişinin standardizasyonu ve birlikte çalışabilirliği geliştirmek, iyileştirmek.

Federal Ağ Dayanıklılığı (FNR), çalışmanın beşinci bölümünde detaylı olarak incelenmiştir.

### 3.1.1.2. Ulusal siber güvenlik operasyon ekibi

ABD Ulusal Siber Güvenlik Operasyon Ekibi; DOJ/FBI (Adalet Bakanlığı/FBI), DHS (İç Güvenlik Bakanlığı) ve DoD (Savunma Bakanlığı) kurumlarından oluşmaktadır. Kurumların rolleri ve sorumlulukları aşağıda detaylı olarak açıklanmaktadır (HGM Görev Raporu, 2014).

Şekil 3.3. ABD Ulusal Siber Güvenlik Operasyon Ekibi


Kaynak: HGM Görev Raporu, 2014

**Ulusal Rolleri ve Sorumlulukları**

I. DOJ/FBI (Department of Justice (Adalet Bakanlığı) / FBI)

- Siber suçları araştırmak, özelliklerini çıkarmak, soruşturmak,
- Yerli ulusal güvenlik operasyonlarına liderlik etmek,
- Siber tehdit soruşturmalarını koordine etmek,
- Siber olaylardan ulusal korunma, önleme, azaltılma ve kurtarma desteği sağlamaktır.

II. İç Güvenlik Bakanlığı

Siber olaylardan ulusal olarak korunma, önleme, azaltılma ve kurtarma konusunda;

- Koordinasyonu sağlamak,
- Yurtiçi siber tehdit ve güvenlik açığı analizlerinin yayılımını yapmak,
- Federal sivil sistemlerin güvenliğini sağlamak,
- DHS yetkisi altındaki siber suçları soruşturmak,
- Kritik altyapıları korumaktır.

III. DoD (Savunma Bakanlığı)

- Saldırılara karşı ulusu savunmak,
- Ulusal güvenlik ve askeri sistemlerinin güvenliğini sağlamak,
- Askeri yargı kapsamında bilişim suçlarını soruşturmaktır.

### 3.1.1.3. Siber güvenlik alanındaki mevzuat

Ülkede siber güvenlik alanındaki mevcut düzenlemelerin en önemlileri şunlardır:

I. "Kamuda Bilgi Güvenliğinin Yönetilmesi Kanunu" (Federal Information Security Management Act (FISMA)) / 2002

Federal Bilgi Güvenliğinin Yönetilmesi Kanununun amacı aşağıda yer almaktadır (FISMA, 2002):

- Federal faaliyet ve varlıkları destekleyen bilgi kaynakları üzerindeki bilgi güvenlik kontrollerinin etkinliğini sağlamak için kapsamlı bir çerçeve oluşturmak,
- Ülke çapında, tüm paydaşlarla işbirliği ve koordinasyon halinde, güvenlik riskleri konusunda etkili yönetim ve gözetim sağlamak,
- Federal bilgi ve bilgi sistemlerini korumak için gerekli asgari kontrollerin geliştirilmesi ve bakımı için destek sağlamak,
- Federal bilgi güvenliği programlarının gözetimi için altyapı oluşturmaktır.

II. "Siber Güvenlik Yasa Tasarısı" (Cyber Security Act of 2012) (Siber Güvenlik Yasa Tasarısı, 2012)

Siber Güvenlik Yasa Tasarısı'nın içeriğindeki genel başlıklar aşağıda yer almaktadır (Siber Güvenlik Yasa Tasarısı, 2012) :

- Kritik altyapının korunması
- Hükümet ağlarının korunması
  - FISMA Reformu
  - Bilgi teknolojilerinin yönetimi
  - Tasarruf hükümleri
- Mevcut rollerin ve otoritelerin açıklığa kavuşturulması ve güçlendirilmesi
- Eğitim, istihdam ve işgücünün geliştirilmesi
- Araştırma ve geliştirme
- Federal kazanım risk yönetim stratejisi
- Bilgi paylaşımı
- Kamuoyu bilinçlendirme raporları
- Uluslararası işbirliği

Mevzuata ilişkin yapılan diğer çalışmalar şunlardır (Çifçi, 2013):

- 2003 yılında "Siber uzayın güvenliği için ulusal strateji" isimli belge yayımlanmıştır.
- 2009 yılında "Siber uzay politikasının gözden geçirilmesi" isimli belgede, siber güvenlik ile ilgili mevcut yapı ve politikalara ilişkin değerlendirmelerde bulunulmuştur.
- "Güvenilir ve Esnek bir Bilgi ve İletişim Altyapısı Sağlanması" konulu bir rapor yayınlanmıştır.
- 2011 yılında ABD Milli Savunma Bakanlığı'nın siber ortamda harekât stratejisi dokümanı yayımlanmıştır.

ABD Başkanı Barack Obama imzalı "Kritik Altyapılarda Siber Güvenliğin İyileştirilmesi" başlıklı Başkanlık Kararnamesi (Executive Order) 12 Şubat 2013 tarihinde yürürlüğe girmiştir. Kararname, toplam 12 kısımdan oluşmaktadır. Kararnamenin içeriği detaylı olarak aşağıda yer almaktadır (White House, 2013):

**Kritik Altyapılarda Siber Güvenliğin İyileştirilmesi, Başkanlık Kararnamesi**

Kritik altyapılarda siber güvenliğin öneminini anlatan bu kararname, temel olarak, özel sektörle bilgi paylaşımına ve siber güvenlik alanında gönüllülük esaslı programlar kurulmasına değinmiştir. ABD yayınladığı kararnamede, kritik altyapıların önemini şu ifadeyle göstermiştir:

Bu sistemlerin zarar görmesi, iş göremez hale gelmesi, ulusal sağlık ve emniyet, ulusal ekonomik güvenlik ya da bu gibi maddelerin bir araya gelmesinden oluşan herhangi bir şeyin, güvenlik üzerindeki zayıflatıcı etkileri Amerika Birleşik Devletleri için hayati önem taşımaktadır (White House, 2013).

**Kısım 1: Politika**

Kritik altyapılara karşı tekrarlanan siber saldırılar siber güvenliğin geliştirilme ihtiyacını ortaya çıkarmıştır. Kritik altyapılara yapılan bu siber tehditler büyümeye devam etmekte ve çok ciddi ulusal güvenlik mücadelelerinden biriyle yüzleşmemiz gerektiğini göstermektedir. Amerika Birleşik Devletleri'nin ulusal ve ekonomik güvenliği, ulusun bu tür tehditlerle yüzleştiği kritik altyapılarının işleyişine bağlıdır.

Ulusun kritik altyapı güvenliğini ve direncini artırmak, sivil haklar, gizlilik, iş mahremiyeti, güvenlik, emniyet, ekonomik refah, yenilik ve verimliliği teşvik eden bir siber ortam sağlamak Amerika Birleşik Devletlerinin politikasıdır.

**Kısım 2: Kritik Altyapı**

Kritik altyapı kavramı, sanal ya da gerçek tüm sistem ve varlıkları ifade etmektedir.

Bu yüzden, bu sistemlerin zarar görmesi, iş göremez hale gelmesi, ulusal sağlık ve emniyet, ulusal ekonomik güvenlik ya da bu gibi maddelerin bir araya gelmesinden oluşan herhangi bir olayın, güvenlik üzerindeki zayıflatıcı etkileri Amerika Birleşik Devletleri için hayati önem taşımaktadır.

**Kısım 3: Politika Koordinasyonu**

Politika koordinasyonu, rehberlik, anlaşmazlıkların çözümü, fonksiyonlar ve programlar ile ilgili gelişen görüşler 13 Şubat 2009 tarihli Başkanlık Politikası Direktifi-1 (Milli Güvenlik Kurulu Sistemi Organizasyonu) ya da herhangi bir ardıl içinde var olan kuruluşlar arası işleyiş aracılığıyla burada belirlenebilir ve tanımlanabilir.

**Kısım 4: Siber Güvenlik Bilgi Paylaşımı**

a) ABD özel sektör kuruluşları ile paylaşılan siber tehdit bilgilerinin hacmini, güncelliğini ve kalitesini artırmak; Amerika Birleşik Devletleri Hükümeti'nin politikasıdır. Böylelikle bu kuruluşlar da siber tehditlere karşı kendilerini daha iyi savunabilmekte ve koruyabilmektedirler.

b) Adalet Bakanı, İç Güvenlik Bakanı ve Milli İstihbarat Direktörü bu emrin yayım tarihinden itibaren 120 gün içerisinde, bu emrin 12 (c) kısmındaki gereksinimleri ve kendi yetkileri ile tutarlı, ABD' de yapılan siber tehditlerin özel olmayan raporlarının zamanında üretimi ve sağlanması ile ilgili tüm konuları içeren talimatlar hazırlayacaktır.

c) Bu talimatlar, istihbarat ve kolluk kaynakları, yöntemleri, operasyon, soruşturma ve koruma ihtiyacını ele alacaktır.

d) İç Güvenlik Bakanı ve Adalet Bakanı, Ulusal İstihbarat Direktörü ile koordinasyon içinde, hedef işletme için kısım 4 (a) uyarınca üretilen bu raporların hızla yayılacağı bir süreç oluşturacaktır.

e) Bu süreç, aynı zamanda, ulusal güvenlik bilgilerini koruma gereksinimine uygun olarak, bunları almaya yetkili kritik altyapı kuruluşları için gizli (sınıflandırılmış) raporların yayılması konusunu içerecektir. İç Güvenlik Bakanı ve Adalet Bakanı, Ulusal İstihbarat Direktörü ile koordinasyon içinde, bu raporların üretilmesi, yayılması ve kullanma yetkisinin izlenmesi için bir sistem kuracaktır.

f) İç Güvenlik Bakanı, 6 USC 143 (Federal Olmayan Siber Güvenlik Yapısının Güçlendirilmesi) ile tutarlı ve Savunma Bakanı ile işbirliği içinde, sömürü, zarar ya da yetkisiz erişimden kendi sistemlerini korumak için kritik altyapı sahipleri ve işletmecilerine yardımcı olmak ve bu kararnamenin yayım tarihi itibariyle 120 gün içinde, tüm kritik altyapı sektörleri için Geliştirilmiş Siber Güvenlik Hizmetleri programını yaymak amacıyla prosedürler oluşturacaktır.

g) İç Güvenlik Bakanı, 18 Ağustos 2010 tarihli 13549 kararnamesi (Sınıflandırılmış Ulusal Güvenlik Bilgi Programı) altında oluşturulan Gizli Ulusal Güvenlik Programı adına icra yetkilisi olacaktır.

h) Bu kararnamenin 9. kısmında tanımlanan kritik altyapılara öncelik verilerek, kritik altyapıların sahipleri ve işletmecileri tarafından, istihdama uygun bulunan personelin güvenlik açıklıklarının işlenmesini hızlandırmak zorundadır.

i) Özel sektör ile siber tehdit bilgi paylaşımından alınan faydayı maksimize etmek amacıyla, İç Güvenlik Bakanı geçici olarak federal hizmete özel sektörden konunun uzmanı kişileri getirerek programların kullanımını yaygınlaştırmak zorundadır. Konunun uzmanlarının, siber riskleri azaltmak amacıyla kritik altyapı sahipleri ve işletmecileri için oldukça kullanışlı olan bilginin içeriği, yapısı ve çeşitleri ile ilgili tavsiyelerde bulunmaları gerekmektedir.

**Kısım 5: Mahremiyeti (Gizliliği) ve Sivil Hakları (İnsan Hakları) Koruma**

a) Kurumlar, bu kararname doğrultusunda, mahremiyet ve sivil haklar için kendi üst düzey kurum yetkilileri ile faaliyetlerini koordine edecek ve mahremiyet ve sivil hak koruyucularının bu tür faaliyetler içerisine dâhil olmasını sağlayacaktır. Adil Bilgi Uygulama İlkeleri, diğer mahremiyet ve sivil haklar politikaları, ilkeleri ve her bir kurumun faaliyetlerine uygulanacak çerçeveler baz alınacaktır.

b) İç Güvenlik Bakanlığı'nın Sivil Haklar ve Sivil Özgürlükler Ofisi görevlisi ve gizlilik kurulu başkanı, bu kararname çağrısı ile İç Güvenlik Bakanlığı tarafından üstlenilen programların ve fonksiyonların mahremiyet ve sivil haklar risklerini değerlendirmeli ve bu kararnamenin yayım tarihinden itibaren 1 yıl içinde piyasaya sürülmüş olacak olan ve halka açık olması gereken bir raporda, bu riskleri en aza indirmek veya azaltmanın yollarını İç Güvenlik Bakanına önermelidir.

c) Bu kararname altındaki faaliyetlerde bir araya gelen diğer kuruluşlar için, kıdemli kurumlardaki mahremiyet ve sivil hak yetkilileri, kurumlarının faaliyetlerini değerlendirmeli ve rapora dâhil etmek için İç Güvenlik Bakanlığı bu değerlendirmeleri gözden geçirecektir.

d) Rapor gerektiğinde yıllık bazda revize edilecektir.

e) (b) bendi altında raporun hazırlanmasında, ihtiyaç olması halinde İç Güvenlik Bakanlığı'nın, Sivil Haklar ve Sivil Özgürlükler Görevlisi ve Gizlilik Kurulu Amiri, Bütçe ve Yönetim Ofisi (OMB) ile koordineli olarak Gizlilik ve Sivil Özgürlükler Gözetim Kurulu'na danışılmalıdır.

f) Bu kararname altında özel kuruluşlar tarafından 6 USC 133 uyarınca gönüllü olarak verilen bilgiler yasaların izin verdiği ölçüde korunmalıdır.

**Kısım 6: Danışma Süreci**

İç Güvenlik Bakanı kritik altyapıların siber güvenliğindeki gelişmeleri koordine etmek amacıyla bir istişare (danışma) süreci belirleyecektir. İstişare sürecinin bir parçası olarak, İç Güvenlik Bakanı, bu kararname altında Kritik Altyapı Ortaklık Danışma Konseyi tarafından belirtilen konularda önerileri dikkate alacak; sektör koordinasyon konseyleri; kritik altyapı sahipleri ve operatörler; sektöre yönelik kurumlar; diğer ilgili kurumlar, bağımsız düzenleyici kurumlar, devlet, üniversiteler ve dış uzmanlardan alınacak tavsiyeleri değerlendirecek ve iç içe geçirecektir.

**Kısım 7: Kritik Altyapılarda Siber Riski Azaltmak için Temel Çerçeve**

a) Ticaret Bakanı, kritik altyapılara ("Siber Güvenlik Çerçevesi") yapılan siber riskleri azaltmak amacıyla, bir çerçevenin gelişmesine öncülük etmek üzere Standartlar ve Teknoloji Ulusal Enstitüsü Müdürünü ("Yönetici") bu konuda yönlendirecektir.

b) Siber Güvenlik Çerçevesi, standardlar, metodolojiler, prosedürler ve politika uyum süreçleri, iş ve siber riskleri adresleyen teknolojik yaklaşımları kapsayacaktır. Siber Güvenlik Çerçevesi mümkün olan en geniş ölçüde mutabakat sağlanmış standartları ve endüstrideki en iyi uygulamaları içerecektir.

c) Siber Güvenlik Çerçevesi kritik altyapı sahipleri ve işletmecilerine yardımcı olmak için siber riski tanımlamak, değerlendirmek, yönetmek ve bilgi güvenliği tedbirleri ve kontrolleri konuları da dâhil olmak üzere, esnek, tekrarlanabilir performansa dayalı maliyet-etkin bir yaklaşım sağlayacaktır. Siber Güvenlik Çerçevesi sektörler arası güvenlik standartları ve kritik altyapıları için geçerli kurallar belirlenmesi üzerine odaklanmalıdır. Siber Güvenlik Çerçevesinde, aynı zamanda, belli sektörlerde ve standartları gelişmekte olan kuruluşlar ile gelecekteki iyileştirme için tanımlı alanların belirlenmesi konusu işbirliği içerisinde ele alınmalıdır.

d) Siber Güvenlik Çerçevesi, bu çerçevesinin uygulanmasında bir işletmenin performansını ölçmek için bir rehber içerecektir.

e) Siber Güvenlik Çerçevesi, sivil haklar ve bireysel mahremiyetini korumak, ilişkili bilgi güvenliği önlemleri veya iş gizlilik kontrollerinin etkilerini belirlemek ve azaltmak için yöntemler içermelidir.

f) Siber Güvenlik Çerçevesini geliştirirken, Yönetici açık bir kamu inceleme ve yorum sürecini birleştirmektedir.

Yönetici ayrıca bu emrin 6. kısmında tanımlanan danışma süreci doğrultusunda İç Güvenlik Bakanı, Ulusal Güvenlik Kurumu, Sektörel Özgü Kurumları ve OMB 'nin kapsadığı diğer ilgili kuruluşlar, kritik altyapı sahipleri ve işletmeciler ve diğer paydaşlar ile istişarede bulunur. İç Güvenlik Bakanı, bu kararnamenin 9. bölümü altında işlenen Siber Güvenlik Çerçevesi için performans hedefleri sağlayacaktır.

g) Bu kararnamenin yayım tarihinden itibaren 240 gün içinde, Yönetici, Siber Güvenlik Çerçevesinin bir ön sürümünü ("Ön Hazırlık Çerçevesi") yayımlayacaktır. Bu emrin yayım tarihinden itibaren 1 yıl içinde ve bu emrin 8. kısmı altında uygunluğunu sağlamak için İç Güvenlik Bakanı ile koordinasyon sonrası, Direktör Siber Güvenlik Çerçevesinin ("Nihai Çerçeve") son sürümünü yayımlayacaktır.

**KISIM 8: Gönüllü Kritik Altyapı Siber Güvenlik Programı**

a) İç Güvenlik Bakanı, Sektöre Yönelik Kurumlar ile koordineli olarak, kritik altyapı sahipleri ve işletmecileri ve diğer ilgili kuruluşlar tarafından Siber Güvenlik Çerçevesinin benimsenmesini desteklemek için gönüllü bir program ("Program") kuracaktır.

b) Sektöre Yönelik Kurumlar, İç Güvenlik Bakanı ve diğer ilgili kuruluşlar ile istişare içinde, Siber Güvenlik Çerçevesini gözden geçirmek amacıyla Koordinasyon Kurulu Sektörü ile koordine içinde olmalı ve gerekli olduğu durumlarda, sektöre özel riskleri ve çalışma ortamlarında ele alınan uygulama rehberliği veya tamamlayıcı malzemeleri geliştirmek zorundadır.

c) Sektöre Yönelik Kurumlar, bu emrin 9. kısmında bildirilen sahipleri ve işletmecileri Programa katıldıkları ölçüde, İç Güvenlik Bakanı aracılığıyla, Başkan'a yıllık raporlar sunacaktır.

d) İç Güvenlik Bakanı, Programa katılımı teşvik etmek için tasarlanmış bir dizi teşvik tespit edilmesini koordine edecektir. Bu emrin yayım tarihinden itibaren 120 gün içinde, İç Güvenlik Bakanı ile Hazine ve Ticaret Bakanı, İç Güvenlik ve Terörle Mücadele Başkanı ve Ekonomik İşlerden Sorumlu Başkan Yardımcısı aracılığıyla, Başkana ayrı ayrı tavsiyelerde bulunur.

e) Bu emrin yayım tarihinden itibaren 120 gün içinde, Savunma Bakanı ve Genel Hizmetler Yöneticisi, İç Güvenlik Bakanı ve Federal Tedarik Düzenleme Konseyi ile istişare içinde, İç Güvenlik Başkan Yardımcısı, Terörle Mücadele Başkan Yardımcısı ve Ekonomik İşlerden Sorumlu Başkan Yardımcısı aracılığıyla fizibilite, güvenlik yardımları, satın alma planlama ve kontrat idaresi içine güvenlik standartları geçişi ile ilgili konularda Başkana tavsiyelerde bulunmak zorundadır.

f) Bu rapor, siber güvenlik ile ilgili tutarlı mevcut tedarik şartları oluşturmak ve harmonize etmek için ne tür adımlar atılması gerektiğini göstermelidir.

**KISIM 9: En Fazla Risk Altında olan Kritik Altyapıların Tanımlanması**

a) Bu emrin yayım tarihinden itibaren 150 gün içinde, İç Güvenlik Bakanı, Ulusal Güvenlik ya da ekonomik güvenlik, halk sağlığı ya da emniyeti üzerinde ulusal ya da bölgesel felaket etkileriyle sonuçlanabilecek bir siber güvenlik vukuatının gerçekleştiği yerde kritik altyapıları tanımlamak için risk-tabanlı bir yaklaşım kullanmalıdır. Bu amaç için kritik altyapı tanımlarken, İç Güvenlik Bakanı bu kararname içinde 6. kısımda bahsedilen danışma sürecini kullanmalı ve Sektöre Yönelik Kurumların uzmanlarından faydalanmalıdır.

b) Başkan, bu tip kritik altyapılar belirlenirken tutarlı, objektif kriterler uygulamalıdır. İç Güvenlik Bakanı bu bölüm altında herhangi bir ticari bilgi teknolojisi ürünleri veya tüketici bilgi teknolojisi hizmetlerini tanımlamayacaktır. İç Güvenlik Bakanı, bu bölüm altında belirlenen kritik altyapı listesini İç Güvenlik, Terörle Mücadele ve Ekonomik İşlerden Sorumlu Başkan Yardımcısı aracılığıyla yıllık bazda gözden geçirmeli, güncellemeli ve bu listeyi Başkana sunmalıdır.

c) Sektöre Yönelik Kurumlar ve diğer ilgili kuruluşların başkanları, bu bölüm altında sorumluluklarını yürütmek için gerekli bilgileri İç Güvenlik Bakanı'na

sunacaklardır. İç Güvenlik Bakanı, bu bölümün (a) alt başlığında gerekli tanımlamanın yapılmasına yardımcı olmak amacıyla diğer ilgili paydaşlar için bilgi gönderimi ile ilgili bir süreç geliştirmek zorundadır.

**KISIM 10: Çerçevenin Kabulü**

a) Kritik altyapıların güvenliğini düzenleyen sorumlu kurumlar, Ön Siber Güvenlik Çerçevesini gözden geçirmek ve mevcut Siber Güvenlik mevzuat şartlarının mevcut ve öngörülen riskler açısından yeterli olup olmadığını belirlemek amacıyla DHS, OMB ve Ulusal Güvenlik Çalışanlarını bir danışma süreci içinde birleştirmelidir.

b) Bu kararı almak için, söz konusu kurumlar, bu emrin 9. bölümü içinde yer alan gerekli kritik altyapının belirlenmesini dikkate alacaktır.

c) Ön Çerçevenin halka açılmasından sonraki 90 gün içinde, bu kurumlar, Ekonomik İşlerden Sorumlu Başkan Yardımcısı ve İç Güvenlik ve Terörle Mücadele Başkan Yardımcısı aracılığıyla Başkana bir rapor sunacaktır.

d) Eğer mevcut düzenleyici gereksinimleri yetersiz olarak kabul ediliyorsa, nihai çerçevenin yayımlanmasından sonraki 90 gün içinde, bu bölümün (a) fıkrasında tanılanan kurumlar, öncelikli, risk esaslı, verimli eylemleri önerecektir.

e) Son Çerçevenin yayım tarihinden itibaren 2 yıl içinde, 13563 ve 10 Mayıs 2012 tarihli Başkanlık Kararı 13610 (Tanımlama ve Düzenleme Yükler azaltılması) ile tutarlı olarak, bu kısmın (a) bendinde belirlenen kurumların, kritik altyapı işletmecileri ve sahipleri ile istişare içinde, verimsiz, birbiriyle çelişen veya aşırı külfetli siber güvenlik gereksinimleri gerektiren herhangi bir kritik altyapıyı OMB'ye bildirmelidir, rapor etmelidir.

f) Bu rapor kurumlar tarafından yapılan çalışmaları tanımlayacak, bu tür gereksinimleri en aza indirmek veya ortadan kaldırmak için ileriye yönelik tavsiyelerde bulunacaktır.

g) İç Güvenlik Bakanı, kendi siber güvenlik işgücü ve programlarının geliştirilmesi üzerine bu bölümün (a) bendinde belirlenen kuruluşlara teknik yardım sağlanmasını koordine eder.

h) Kritik altyapıların güvenliğini düzenleyen sorumlu bağımsız düzenleyici kurumlar, İç Güvenlik Bakanı ile istişare süreci içerisinde, ilgili Sektöre Yönelik Kurumlar ve diğer etkilenen tarafların yetkileri ile tutarlı olarak kritik altyapılarda siber riskleri azaltmak için öncelikli faaliyetleri dikkate alma konusunda teşvik edilmelidir.

**KISIM 11: Tanımlar**

Kurum: Amerika Birleşik Devletleri'nin herhangi bir otoritesi anlamına gelmektedir.

**KISIM 12: Genel Hükümler**

a) Bu kararname, kullanılabilir ödeneğe bağlıdır ve geçerli yasa ile tutarlı olarak uygulanacaktır.

b) Bu kararname altında bulunan hiçbir madde, mevcut kanunlar içerisinde var olan bir kurumun yetkisinden daha büyük ya da kritik altyapıların güvenliğini düzenleyen yetkiye sahip kurum sağlamak amacıyla yorumlanmayacaktır.

c) Bu kararname altında bulunan hiçbir madde, mevcut yasa altında bir kurumun sorumluluk ve yetkisini sınırlandıracak ya da değiştirecek şekilde yorumlanmamalıdır.

d) Bu kararname altında bulunan hiçbir madde, yasama önerileri, idare ya da bütçe ile ilgili OMB'nin Direktörünün görevlerini etkileyecek ya da bozacak şekilde yorumlanmamalıdır.

e) Bu kararname uyarınca alınan tüm eylemler, istihbarat ve kolluk kaynakları ile bilgiyi korumakla görevli yetkili kurumlar ve gereksinimler ile tutarlı olacaktır.

f) Bu kararname altında bulunan hiçbir madde, istihbarat ve kolluk işlemleri doğrudan desteği altında belirli etkinlikler ve dernek güvenliğinin bütünlüğünü korumak için kanun yetkisi altında kurulan tedbirlerin yerini alacağı şeklinde yorumlanmamalıdır.

g) Bu kararname ABD'nin uluslararası yükümlülükleri ile uyumlu uygulanacaktır.

### 3.1.2. Kanada

Kanada'da Siber Güvenlik Hizmetleri, Kanada Kamu Güvenliği Bakanlığı altında çalışmakta olan; Kanada Siber Olaylara Müdahale Merkezi (CCIRC) tarafından yürütülmektedir. Siber Saldırılara karşı ulusal bir yanıt mekanizmasının olması amacıyla kurulmuştur. Merkez, aynı zamanda kritik altyapıların korunması üzerinde 7/24 esasına dayalı çalışmaktadır (Kanada Kamu Güvenliği, 2010).

Kanada Ceza Kanununun 342. maddesinin içeriğinde bilgi güvenliğine ilişkin hükümler yer almaktadır (Justice Laws, 2014). Ayrıca Kişisel Gizlilik Kanunu bulunmaktadır.

Kanada Hükümeti tarafından belirlenen *kritik altyapılar* şunlardır (Kanada Kamu Güvenliği, 2014);

- Enerji ve Kamu Hizmetleri
- Haberleşme ve Bilgi Teknolojileri
- Gıda
- Su
- Üretim
- Sağlık Hizmetleri
- Ulaştırma
- Güvenlik
- Yönetim
- Finans

Kanada'nın *Siber Güvenlik Stratejisi,* 3 Ekim 2010 yılında yayımlanmıştır. 2010-2015 yıllarını kapsamakta olan Eylem Planı temel olarak üç ana hedef içermektedir (ENISA Kanada, 2010) :

1. Hükümet sistemlerinin güvenliği,
2. Federal Hükümet dışında olan ve hayati önem taşıyan siber sistemlerin güvence altına alınması için işbirliği,
3. Güvenli olarak çevrimiçi olmak için Kanada halkına yardımcı olmak.

### 3.1.3. Japonya

Japonya'da, Ulusal Bilgi Güvenliği Merkezi (NISC), 2005 yılı Nisan ayında Bakanlar Kurulu Sekreterliği içerisinde kurulmuştur. Bilgi Güvenliği Siyaseti Konseyi (ISPC) ise, bilgi güvenliği sorunlarıyla ilgili tedbirlerin önemli ölçüde güçlendirilmesi amacıyla, aynı yılın Mayıs ayında, Gelişmiş Bilgi ve

Telekomünikasyon Ağ Toplumu Geliştirme Strateji Genel Merkezinde (BT Stratejik Merkez) kurulmuştur.

2000 yılı şubat ayında "Bilgisayara Yetkisiz Erişim Kanunu" çıkarılmıştır.

Savunma Bakanlığı tarafından 2012 yılı Eylül ayında yayımlanan "Siber Uzayın İstikrarlı ve Etkin Kullanımına Doğru" başlıklı dokümanda, siber alanın daha verimli ve güvenli kullanılması amacıyla uygulanacak politikanın çerçevesi çizilmektedir. SDF C4 (Komuta, Kontrol, İletişim ve Bilgisayar) birimi siber saldırılara müdahale için askeri ve güvenlik alanındaki tüm iletişim ağını sürekli olarak izlemektedir. 2012 yılında, siber saldırıların yaratacağı tehlikeyle uygun şekilde mücadele edilebilmesi için Savunma Bakanlığı ve SDF yapısal ve organizasyonel bazı değişikliklere gitmiş, bu kapsamda "Siber Savunma Grubu" kurulmuştur. Savunma Bakanlığı ve SDF'nin operasyonel altyapının geliştirilmesi konusundaki çalışmaları devam etmektedir. Ayrıca, 2013 yılı şubat ayında Savunma Bakan Yardımcısı'nın başkanlık ettiği "Siber Siyaset Komitesi" kurulmuştur (MGK, 2013).

Japonya'nın 2010-2013 dönemini kapsayan, *Siber Güvenlik Stratejisi* yayımlanmıştır. Stratejinin temel politikaları şunlardır (ENISA Japonya, 2013):

- Yanıt(tepki) organizasyonun/kuruluşunun kurulması ve olası siber saldırıların mihrakları göz önünde bulundurularak politikaların güçlendirilmesi,

- Bilgi güvenliği ortamındaki değişikliklere karşı adapte olabilecek politikaların oluşturulması,

- Pasif bilgi güvenliği önlemleri yerine daha aktif bilgi güvenliği önlemleri oluşturulmasıdır.

Ayrıca Japonya'nın siber güvenlik stratejisinde, Amerika Birleşik Devletleri, İngiltere, Fransa, Almanya, Kore ve Avrupa Birliğinin siber güvenlik alanında yapmış olduğu temel çalışmalara değinilmiştir (ENISA Japonya, 2013).

Japonya'da siber güvenlik alanında;

- Kişisel bilginin korunmasının teşvik edilmesi,
- Siber saldırı bilgi toplama ve paylaşım sisteminin kurulması ve kullanılması,
- Olası büyük bir siber saldırıya karşı hazırlık ve karşı koyma planları,
- Bilgi güvenliği kampanyası yapılması,
- Uluslararası işbirliğinin güçlendirilmesi,
- Bilgi güvenliği alanında insan kaynağının iyileştirilmesi,
- Kritik altyapı sağlayıcılarının rollerinin belirlenmesi,
- Bilgi güvenliğine ilişkin yasal altyapının düzenlenmesi çalışmaları mevcuttur.

Japonya Savunma Bakanlığı tarafından yıllık bazda hazırlanan "Japonya'nın 2013 yılı Savunması" başlıklı Beyaz Kitap 9 Temmuz 2013 tarihinde yayımlanmıştır. "Japonya'nın Etrafındaki Güvenlik Ortamına Genel Bakış", "Japonya'nın Savunma Politikası ve ABD Japonya Güvenlik Düzenlemeleri" ve "Japonya'nın Savunmasına Yönelik Tedbirler" başlıkları altında 3 ana kısımdan ve 350 sayfadan oluşan Beyaz Kitapda diğer ülkelerce gerçekleştirilen bilgi ve iletişim ağlarına yönelik sızmaların istihbarat toplama maksatlı olduğuna dikkat çekilmektedir (Japan White Paper, 2013).

### 3.1.4. Almanya

Almanyada siber güvenliğe ilişkin "Dışişleri Bakanlığı, İçişleri Bakanlığı, Savunma Bakanlığı, Ekonomi ve Teknoloji Bakanlığı, Adalet Bakanlığı, Finans Bakanlığı, Eğitim ve Araştırma Bakanlığı" üyelerinden oluşan "Ulusal Siber Güvenlik Konseyi" oluşturulmuştur (ENISA Almanya, 2011, s.5).

Almanya, 2009 yılında, Federal Bilgi Teknolojilerinin Güvenliğinin Güçlendirilmesi Yasası (Act to Strengthen the Security of Federal InformationTechnology)'nı yayımlamıştır (BSI, 2009).

Ayrıca 2011 yılı şubat ayında Almanya'nın Siber Güvenlik Stratejisi (Cyber Security Strategy for Germany) yayımlanmıştır. Strateji içerisinde, Federal Hükümet, özellikle on stratejik alana odaklanacaktır (ENISA Almanya, 2011):

1. Kritik bilgi altyapılarının korunması,
2. Almanya'da bilişim sistemlerinin güvence altına alınması,
3.Kamu yönetiminde bilgi teknolojilerinin güvenliğinin güçlendirilmesi,
4. Ulusal Siber Müdahale Merkezi,
5. Ulusal Siber Güvenlik Konseyi,
6. Siber uzayda etkin suç denetimi,
7. Avrupa'da ve dünya çapında siber güvenliği sağlamak için etkin koordine eylemi,
8. Güvenilir ve sağlam bilgi teknolojilerinin kullanımı,
9. Federal makam ve mercilerde personel gelişimi,
10. Siber saldırılara yanıt vermek için araçlar.

Federal düzeyde, Almanya'nın *kritik altyapıları* olarak aşağıdaki alanlar tespit edilmiştir (BMI, 2009):

- Enerji
- Bilgi teknolojileri ve telekomünikasyon
- Ulaşım
- Sağlık
- Su
- Gıda
- Finans ve sigorta sektörü
- Devlet ve yönetim
- Medya ve kültür

Siber Güvenlik Stratejisi"nin sonuçlarından biri olan Milli Siber Savunma Merkezi (NCAZ) 2011 yılı Mayıs ayında açılmıştır. Federal Almanya Polisi, Federal Anayasa Koruma Dairesi ve Federal Haber Servisi ile işbirliği içinde çalışacak olan NCAZ'ın temel görevi elektrik, su, iletişim ve lojistik gibi kamusal yaşam için önemli olan altyapı merkezlerini hedef alan olası siber saldırıları erken uyarı ve anında müdahele ile önlemektir.

Almanya'nın olabilecek siber saldırılara karşı almakta olduğu önlemler Federal İçişleri Bakanlığı tarafından hazırlanan "Enformasyon Altyapısı Savunması için Ulusal Plan" dokümanında yer almaktadır (Meral, 2008).

### 3.1.5. Fransa

Fransa'da siber güvenlik ile ilgili temel kurum olan Fransız Ağ ve Bilgi Güvenliği Ajansı (ANSSI) 2009 yılı Temmuz ayında kurulmuştur. ANSSI Başbakanın yetkisi altında faaliyet gösteren bir kurumdur. Bu kurumun görev alanları arasında siber saldırıları tespit ve siber saldırılara karşı cevap yeteneği, araştırma ve geliştirme faaliyetleri aracılığıyla siber saldırıların önlenmesi ve hükümete bilgi sağlanması hususları bulunmaktadır.

2011 yılında, Savunma Bakanlığı'ndaki siber savunma yeteneklerinin güçlendirilmesi çerçevesinde, bir siber kriz durumunda ana arayüz olarak hareket etme ve Bakanlığın siber savunma faaliyetleri koordinasyon sorumluluğunun gerçekleştirilmesi amacı ile Siber Savunma Genel Görevlisi (Cyber Defence General Officer) oluşturulmuştur.

Ayrıca, Fransa'da Siber Güvenlik alanındaki çalışmaları yürütmek amacıyla, Bilgi ve İletişim Teknolojileri ile İlgili Suçla Mücadele Merkez Ofisi (Central Office for the Fight against Crime related to Information and Communication Technology, OCLCTIC) kurulmuştur.

Mevzuat'da Siber Güvenlik:

- Fransa'da veri işleme, veri dosyaları ve kişisel özgürlükleri konuları üzerine; veri koruma alanını düzenleyen temel "Veri Koruma Kanunu", 6 Ocak 1978 tarihinde yürürlüğe girmiştir. 2004 yılında bazı maddeler değişikliğe uğramıştır (Fransa Veri Koruma Kanunu, 2014).
- "Sayısal Ekonomide Güveni Güçlendirme Kanunu" 2004 yılında yürürlüğe girmiştir (Fransa Sayısal Ekonomide Güveni Güçlendirme Kanunu, 2014).

Fransa aynı zamanda uluslararası örgütlerde siber güvenlik politikalarının oluşturulması konusunda aktif çalışmalarda bulunmaktadır. Birleşmiş Milletler ve Avrupa Güvenlik ve İşbirliği Teşkilatının (Organization for Security and Cooperation in Europe, OSCE) yanı sıra özellikle NATO ve Avrupa Birliği içinde siber güvenlik çalışmaları yürütülmektedir.

Fransa, 2011 yılında ulusal bilgi sistemlerinin güvenliği ve savunması ile ilgili Ulusal Strateji Planını yayımlamıştır.

Strateji Planı 4 ana hedef üzerine odaklanmıştır (ENISA Fransa, 2011):

1. Siber savunma alanında dünya gücü olma,
2. Fransa'nın egemenliği ile ilgili bilgilerin korunmasını sağlamadaki yeteneği,
3. Kritik öneme haiz ulusal altyapıların siber güvenliğinin güçlendirilmesi,
4. Siber uzayda güvenliğin sağlanmasıdır.

Eylemler ise 7 alandan oluşmaktadır (ENISA Fransa, 2011):

1. Tahmin ve analiz
2. Tespit, uyarı ve yanıt
3. Bilimsel, teknik, endüstriyel ve insan yeteneklerini sürdürmek ve geliştirmek
4. Devletin bilgi sistemleri ve kritik altyapı işletmecilerini korumak

5. Fransanın mevzuatına uyum
6. Uluslararası işbirliğini geliştirmek
7. Bilgilendirme ve ikna etme için iletişim kurmak.

### 3.1.6. Avusturya

Avusturya'nın siber güvenlik stratejisi 2013 yılı Mart ayında yayımlanmıştır. Strateji'de, ilkeler belirlenmiş olup, bu ilkelere dayanarak, Avrupa ve uluslararası düzeydeki tüm önlemleri içeren kapsamlı ve tutarlı bir siber güvenlik politikasının geliştirildiği belirtilmiştir (ENISA Avusturya, 2013).

Strateji belgesinde genel hatlarıyla şu konular yer almaktadır (ENISA Avusturya, 2013):

- Siber uzaydaki riskler ve fırsatlar
- İlkeler
- Stratejik hedefler
- Faaliyet alanları ve tedbirler
- Yönetim
- Hükümet, ekonomi ve toplum arasındaki işbirliği
- Yapılar ve süreçler
- Kritik altyapıların korunması
- Bilinçlendirme ve eğitim
- Araştırma ve geliştirme
- Uluslararası işbirliği konularına yer verilmiştir.

Avusturya'nın Siber Güvenlik Stratejisi, Güvenlik Stratejisi temelinde geliştirilmiş olup kritik altyapıların korunmasına ilişkin Avusturya Programının ilkeleri tarafından yönlendirilmektedir.

Strateji belgesinde şu hususlar dikkat çekmektedir (ENISA Avusturya, 2013):

- 11 Mayıs 2012 tarihinde, Bakanlar Kurulu kararına dayalı olarak, Siber Güvenlik Yönlendirme Grubu kurulmuştur. Yönlendirme Grubu, Milli Güvenlik Konseyi'nin irtibat görevlileri ve Milli Güvenlik Konseyi'nde temsil edilen bakanlıkların siber güvenlik uzmanlarından oluşmaktadır.

- Avusturya'nın "Siber Kriz Yönetimi" devlet temsilcilerinden ve kritik altyapıların operatörlerinden oluşmaktadır.

- Kritik altyapı operatörleri, kamu kurumları ile işbirliği içerisinde, risk bazında hazırlanmış kriz yönetimi ve sürekliliği planları ile düzenli olarak güncellenen sektöre özgü ve sektörler arası siber tehditleri analiz etmektedir.

- Mevcut siber güvenlik yapılarının güçlendirilmesi ile ilgili bir hususa değinilmiştir. GovCERT'ün (Hükümetin Federal idaresi tarafından işletilmektedir) rolünün geliştirileceği ve güçlendirileceği belirtilmiştir. İçişleri bakanlığının "Siber Suç Yetkinlik Merkezi" nin de geliştirilmesi planlanmaktadır.

- Siber Güvenlik Yönlendirme Grubu'nun "Avusturya'da Siber Güvenlik" başlıklı yıllık raporu hazırlayacağı belirtilmiştir.

- Kamu idarelerinin görev ve sorumlulukların birçoğu; ekonomi, nüfus, bilgi ve iletişim teknolojilerine dayandığından, hükümet, ekonomi ve toplum arasındaki işbirliğinin önemi vurgulanmıştır.

- Tüm paydaşların devam etmekte olan iletişimini kolaylaştırmak için, kamu-özel ortaklığını içeren "Avusturya Siber Güvenlik Platformu"nun kurulacağı belirtilmiştir.

- Bugün hemen hemen tüm altyapıların bağlı olduğu bilişim sistemlerinin, işlemleri giderek daha düzgün, güvenilir ve mümkün olduğunca kesintisiz yapmasının garanti altına alınmasının beklendiği belirtilmiş ve kritik altyapıların önemi, dayanıklılığını artırılması konuları vurgulanmıştır.

- Avusturya'nın ülkelerarası siber tatbikatların planlama ve uygulanmasına aktif olarak katıldığı belirtilmiştir.

### 3.1.7. Çek Cumhuriyeti

Çek Cumhuriyeti'nin 2011-2015 dönemini kapsayan Siber Güvenlik Stratejisi'nde, bilgi ve iletişim teknolojilerinin gelişmiş toplumların işleyişi ve ekonomileri üzerinde önemli bir etkiye sahip olduğu, bilgi ve iletişim teknolojilerine bağımlı olan toplumların saldırı veya tenkide açık olduğu belirtilmiştir (ENISA Çek Cumhuriyeti, 2011).

2011 - 2015 dönemi için hazırlanan Çek Cumhuriyeti'nin siber güvenlik stratejisi başlıca şu konuları içermektedir (ENISA Çek Cumhuriyeti, 2011):

- Toplumdaki tüm sektörler arasında işbirliğinin güçlendirilmesi
- Bireysel sorumluluk
- İş sektörünün sorumluluğu
- Bölümler arası işbirliği

  15 Mart 2010 tarihli 205 sayılı Hükümet Kararı uyarınca; siber güvenlik konuları alanında sorumlu ve ulusal otorite olan kurum Çek Cumhuriyeti'nin *İçişleri Bakanlığı*'dır. Bu bağlamda, önemli bir rolü olan "Siber Güvenlik alanında bölümler arası Koordinasyon Kurulu" yetkili kurum ve kuruluşlar arasında işbirliği yapacaktır.

Strateji belgesinde, Kurul'un, siber güvenlik konularının ele alınacağı, kamu sektörü, özel sektör, enerji sağlayan vb. kurumların ilgili uzmanlarından oluşan çalışma grupları kuracağı belirtilmiştir.

- Uluslararası işbirliği
- Tedbirlerin yeterliliği
- Kamu Yönetimi ve kritik altyapıların bilgi ve iletişim teknolojilerinin siber güvenliğinin güçlendirilmesi
- Ulusal CERT ajansı kurulması
- Devlet, özel sektör ve akademik işbirliği
- Artan siber güvenlik bilinci.

### 3.1.8. Birleşik Krallık

Birleşik Krallık hükümetinin 2010 yılı Ekim ayında yayımlanan "Ulusal Güvenlik Stratejisi Raporu", Birleşik Krallık'ın karşılaşabileceği riskleri gruplara ayırmış ve siber saldırıyı en yüksek risk grubunda değerlendirmiştir (Birleşik Krallık Ulusal Güvenlik Stratejisi Raporu, 2010).

Rapor, diğer ülkeler tarafından yönlendirilecek siber saldırıları ve terörist gruplar ile organize örgütler tarafından yönlendirilecek siber saldırıları da siber saldırı kapsamına almıştır. Ulusal Güvenlik Stratejisi Raporu, açık bir şekilde, farklı ülkelerin Birleşik Krallık'a siber saldırılar düzenlediğini belirtmekte ve siber güvenliğin, raporun düzenlendiği yıl ve onu izleyen beş yıl boyunca en yüksek dereceli ulusal güvenlik risklerinden biri olarak değerlendirilmesi gerektiğinin altını çizmektedir. Ulusal Güvenlik Stratejisi ile dört yıllık Ulusal Siber Güvenlik Programı hazırlanmış ve siber güvenlik için 650 milyon poundluk bir bütçe belirlenmiştir (Bilişim ve Teknoloji Hukuku Enstitüsü, 2012).

Ulusal Siber Güvenlik Programı, Kabine Ofisi'ne bağlı olan Siber Güvenlik ve Bilgi Güvencesi Ofisi (Office of Cyber Security and Information Assurance, OCSIA) tarafından yönetilmektedir.

Yeni Ulusal Siber Güvenlik Programı ile birlikte, Birleşik Krallık, siber güvenlik alanında köklü değişikliklere gitmiş ve birçok yeni kurumun kurulma çalışmalarına başlamıştır. Birleşik Krallıktaki siber güvenlik birimleri, Siber Güvenlik ve Bilgi Güvencesi Ofisi, Siber Güvenlik Operasyon Merkezi (Cyber Security Operations Center, CSOC), İngiltere Bilgisayar Olaylarına Müdahale Ekipleri (GovCertUK)'nden oluşmaktadır.

Ulusal Siber Güvenlik Programı ve ayrıntıları, 2011 yılı Kasım ayında yayımlanan "Siber Güvenlik Stratejisi" raporunda belirtilmektedir.

Siber Güvenlik Stratejisi raporu, internetin gelişimi ile tehditlerin de değiştiğini belirtmekte ve tehditleri dört gruba ayırmaktadır (ENISA Birleşik Krallık, 2011):

i. Bilişim sistemlerine yönelen ve/veya bilişim sistemlerini kullanan suçlular,
ii. Diğer ülkeler,
iii. Terörist gruplar,
iv. Kamu ve özel sektöre saldırılarda bulunan ve genelde politik amaçlar doğrultusunda hareket eden "Hacktivist" gruplardır.

İngiltere'nin ulusal altyapısı, hükümet tarafından, "İngiltere'deki günlük yaşamın devam edebilmesi amacıyla ihtiyaç duyulan temel hizmetlerin verilmesi için gerekli ağlar, sistemler, tesisler" olarak tanımlanmaktadır.

*Ulusal kritik altyapılar*, Birleşik Krallık'ta dokuz sektör içerisinde sınıflandırılmaktadır:

- Acil Durum Hizmetleri
- Enerji
- Su
- Ulaşım
- Sağlık
- Hükümet/ Kamu Hizmetleri
- Finans
- Gıda
- İletişim

Altyapılar, "kritikliğine" veya zarar görmesi halinde oluşabilecek etkilerine göre sınıflandırılmaktadır. Bu sınıflandırma, etkinin şiddetine göre farklı derecelerdeki kategorilere atanan Hükümet'in "Kritiklik Skalası" kullanılarak yapılır.

Kritiklik Skalası; ülkenin temel hizmetlerin dağıtımı üzerinde etkisi, ekonomik etkisi (temel hizmet kaybından kaynaklanan) ve yaşam üzerindeki etkisi (temel hizmet kaybından kaynaklanan) olmak üzere üç etki boyutunu kapsamaktadır.

Ulusal altyapı sektöründe her altyapı "kritik" olarak değerlendirilmemektedir. Sektörler içinde bir altyapının "kritik" olarak belirlenmesi için temel hizmetlerin bütünlüğü veya kullanılabilirliği üzerinde önemli derecede olumsuz bir etkiye neden olabilecek kayıp veya ödünler, ciddi ekonomik ve sosyal sonuçlara veya yaşam kaybına yol açan unsurlar gibi temel öğelerin var olması gerekmektedir.

Bu "kritik" varlıklar, ülkenin kritik ulusal altyapısını (CNI) oluşturur ve "altyapı varlıkları" olarak olarak adlandırılır. Altyapı varlıkları fiziksel (örneğin siteler, tesisler, ekipmanlar) ya da (örneğin bilgi ağları, sistemler) mantıksal olabilmektedir (CPNI).

### 3.1.9. Rusya Federasyonu

Federal Güvenlik Servisi (FSB) Rusya Federasyonunun iç güvenliğinden ve kritik altyapıların korunmasından sorumlu birimidir. Ayrıca, aynı konuya ilişkin, İçişleri Bakanlığı'nda Siber Suçlar İdaresi bulunmaktadır.

9 Eylül 2000 tarihinde Rusya Federasyonu Cumhurbaşkanı tarafından "Rusya Federasyonu Bilgi Güvenliği Doktrini" onaylanmıştır (Rusya Federasyonu Bilgi Güvenliği Doktrini, 2000). Rusya Federasyonu Doktrini, Rusya Federasyonu'nda bilgi güvenliğinin sağlanması için, amaçlar, hedefler, ilkeler ile ilgili resmi görüşlerin bütününü temsil etmektedir.

Mevcut Doktrin aşağıdaki konulara esas teşkil etmektedir (Rusya Federasyonu Bilgi Güvenliği Doktrini, 2000):

- Rusya Federasyonu'nda bilgi güvenliğiyle ilgili hükümet politikasını şekillendirmek,
- Rusya Federasyonu'nda bilgi güvenliğinin sağlanması için yasal, prosedürel, bilimsel-teknik ve örgütsel çerçeveyi geliştirmek için öneriler hazırlamak,
- Hedeflenen ulusal bilgi güvenliği programlarının oluşturulması.

Rusya Federasyonu'nda bilgi güvenliğine yönelik tehditler genel hatlarına göre aşağıdaki alanlara bölünmüştür:

- Bölgedeki vatandaşların anayasal hak ve özgürlüklerine yönelik tehditler,
- Rusya Federasyonu devlet politikası bilişim desteğine yönelik tehditler,
- Rus bilişim sektörüne (bilgi, telekomünikasyon ve haberleşme tesisleri dâhil) yönelik tehditler,
- Rusya toprakları üzerinde kurulmakta olan ya da önceden konuşlandırılmış tesislerin ve bilgi ve telekomünikasyon sistemlerinin güvenliğine yönelik tehditler.

Rusya Federasyonu'nun bilgi güvenliğini sağlamak için genel yöntemler aşağıdaki başlıklar altında sıralanmaktadır:

1. Bilgi güvenliğini sağlamak için yasal yöntemler (Hukuki eylemlerin gerçekleştirilmesini içermektedir)
2. Bilgi güvenliğini sağlamak için organizasyonel-teknik yöntemler (Rusya Federasyonu'nun bilgi güvenliğinin sağlanması için bir sistem kurulması ve geliştirilmesi konusunu içermektedir)
3. Bilgi güvenliğini sağlamak için ekonomik yöntemler.

2001 yılında Rusya, Voronezh'da profesyonel siber korsanlık eğitimi veren Voronezh Askeri Telsiz-Elektrik Elektronik Enstitüsü kurulmuştur (Wikipedia, 2014ç).

### 3.1.10. Çin

Çin Halk Cumhuriyeti, 2011 yılında Mavi Ordu isimli siber savaş biriminin varlığını açıklamıştır (Wikipedia, 2014ç).

Çin Askeri Stratejisi'nde siber güvenlik, Çin Halk Kurtuluş Ordusu'nun (Peoples Liberation Army – PLA) üzerine büyük yatırımlar ve çalışmalar yapması gereken çok önemli bir alan olarak tanımlanmıştır. Çin Halk Cumhuriyeti, siyasi organizasyonu ve ideolojisi sebebiyle ülkenin güvenliği yanında siber güvenliği de büyük oranda ordunun denetimine bırakmış durumdadır. PLA'nın GSD (General Staff Department) 3. ve 4. birimleri, ülkenin bilişim altyapısının korunmasından sorumludur. Bu birimler hava, kara, deniz kuvvetleri ve milis kuvvetlerin ilgili siber güvenlik birimleriyle birlikte Çin sınırları içerisindeki tüm iletişim trafiğini izlemektedir. PLA GSD 3. birimi ayrıca, Çin ordusunun sahip olduğu bilişim altyapısının ve ağların da güvenliğinden sorumludur. 3. birim altında 12 adet operasyonel büro bulunmaktadır. Bunun yanında 3 adet araştırma enstitüsü de ülkenin siber güvenliğinin geliştirilmesi amacıyla aralıksız AR&GE faaliyetleri

yürütmekte ve Çin'in önde gelen üniversitelerinin de desteği alınmaktadır (Bilişim ve Teknoloji Hukuku Enstitüsü, 2012).

2010 yılında veri hırsızlığına ilişkin yönetmelik çıkarılmıştır. Ayrıca, Küresel Çatışma ve İşbirliği Enstitüsü'nün (Institute on Global Conflict and Cooperation, IGCC); "Siyasal, Ekonomik ve Stratejik Boyutlar'da Çin ve Siber Güvenlik" konulu raporu 2012 yılı Nisan ayında yayımlanmıştır (IGCC, 2012).

18 Şubat 2013 tarihinde, New York Times gazetesinde, Çin'in Shangai şehrinde yer alan 12 katlı ofis binasının Çin ordusuna ait siber savaşçıların karargâhı olduğu yönünde haberler çıkmıştır (SANGER E. David, BARBOZA David, PERLROTH Nicole, 2013).

### 3.1.11. Estonya

2007 yılında Estonya'ya yapılan siber saldırının ardından, ülkede siber güvenliğe ilişkin stratejiler, çalışmalar, mevzuat gereksinimleri ortaya konmuş ve konuya ilişkin çalışmalar hız kazanmıştır. 2007 yılından bu yana yürürlükte olan, "Bilgi Güvenliği Birlikte Çalışabilirlik Çerçevesi", ulusal ve kurumsal olarak her iki düzeyde de dikkate alınacak bilgi güvenliği konusundaki temel açıklıkları tanımlamaktadır.

Estonya'da siber savunma çalışmaları, Savunma Bakanlığı tarafından gerçekleştirilmektedir.

Siber Güvenlik Strateji komitesi oluşturulmuştur.

*Üyeleri:*

- Başkan: Savunma Bakanlığı
- Dışişleri Bakanlığı

- İçişleri Bakanlığı
- Eğitim ve Araştırma Bakanlığı
- Ekonomi Bakanlığı
- Adalet Bakanlığı'ndan oluşmaktadır.

Siber Güvenlik Strateji komitesi karar almakla yükümlüdür. Alınan kararların uygulamasını ise bir alt oluşumu olan *Siber Güvenlik Konseyi* yürütmektedir. Estonya, Siber Savunma Mükemmeliyet Merkezi'nin destekçileri arasında yer almaktadır.

Estonya'nın *Siber Güvenlik Stratejisi* 2008 yılında yayımlanmıştır. Strateji belgesinde siber güvenliğin artırılması için belirlenen politikalar şunlardır (ENISA Estonya, 2008):

- Güvenlik önlemleriyle sisteminin geliştirilmesi ve geniş çaplı olarak uygulanması,
- Siber güvenlikte artan yetkinlik,
- Siber güvenliğin desteklenmesi için yasal çerçevenin iyileştirilmesi,
- Uluslararası işbirliğini pekiştirmek,
- Siber güvenlik bilincinin artırılmasıdır.

### 3.1.12. İspanya

İspanya'nın Ulusal Siber Güvenlik Stratejisi 2013 yılında yayımlanmıştır.

Strateji belgesinde Siber Saldırıların özellikleri şu şekilde ifade edilmiştir:

- Düşük maliyet

  Saldırganlar tarafından kullanılan araçların çoğu ücretsizdir ya da çok düşük maliyetle elde edilebilmektedir.

- Her yerden yapılabilmesi ve uygulama kolaylığı

  Saldırıların uygulanması saldırganın yerinden bağımsız olarak yapılabilmekte ve birçok durum için önemli ölçüde teknik bilgiye ihtiyaç duyulmamaktadır.

- Etki ve tesirleri

  Saldırı iyi tasarlanmış ise, istenen hedeflere ulaşılabilmektedir. Siber güvenlik politikalarının olmaması, yetersiz kaynaklar, farkındalığın oluşmamış olması ve yetenek eksikliği, bu olumsuz sonucu kolaylaştırabilmektedir.

- Saldırganlar için düşük risk

  Bir siber saldırıda, olayın gerçek fail veya faillerinin bulunması kolay değildir.

**Yol Gösterici İlkeler**

- Ulusal liderlik ve çalışmaların koordinasyonu
- Sorumluluğun paylaşılması (tüm özel sektör ve kamu kuruluşları)
- Orantısallık, rasyonellik ve verimlilik (Teknolojinin dinamik bir şekilde kullanımından kaynaklanan riskleri yönetmek, fırsatlar ve tehditleri dengelemek)
- Uluslararası işbirliği.

**Amaçlar** (ENISA İspanya, 2013)

- Kamu yetkilileri tarafından kullanılan bilgi ve iletişim sistemlerinin siber güvenliğinin ve dayanıklılığın uygun bir seviyede olmasını sağlamak,
- Kritik altyapı operatörlerinin ve iş sektörünün bilgi ve iletişim sistemlerinin güvenlik ve dayanıklılığının geliştirilmesi,
- Siber uzaydaki suç ve terörist faaliyetleri için; algılama, önleme, reaksiyon, analiz, kurtarma, müdahale, araştırma ve koordinasyon yeteneklerini geliştirmek,
- Siber uzaydaki riskler konusunda; vatandaşlar, işin profesyonelleri, şirketler ve kamu idarelerindeki farkındalığı arttırmak,
- İspanya'nın siber güvenlik hedeflerine dayanak oluşturmak için ihtiyaç duyulan bilgi, beceri, deneyim ve teknolojik yetenekleri kazanmak ve korumak,
- Uluslararası alanda siber güvenliğin iyileştirilmesi konusunda katkıda bulunmaktır.

İspanya, Ulusal Siber Güvenlik Stratejisinde, siber güvenlik organizasyonunun, Başbakanın başkanlığında, aşağıdaki birimlerden oluşacağı belirtilmiştir (Şekil 3.4):

1. Milli Güvenlik Kurulu (National Security Council (NSC));
2. Uzman Siber Güvenlik Kurulu;
3. Uzman Durum Komitesi, (Tüm Milli Güvenlik Sistemi'ne özgü).

Şekil 3.4. İspanya'nın Siber Güvenlik Organizasyon Yapısı


### 3.1.13. Yeni Zelanda

Hükümet İletişim Güvenliği Bürosu (The Government Communications Security Bureau, GCSB) merkez ofisi Yeni Zelanda'da olan bir kamu hizmeti bölümüdür. GCSB, hükümetin bilgi bütünlüğünü ve gizliliğini sağlamakta, Yeni Zelanda'nın kritik altyapılarına karşı yapılan siber olayları soruşturmakta ve analiz etmektedir. GCSB, Yeni Zelanda'nın ilgi alanı dâhilindeki konularda dış istihbaratlardan bilgi toplamakta ve yasal yönden zorunlu işlevlerin yerine getirilmesinde hükümetin diğer devlet kurumlarına yardımcı olmaktadır.

Ulusal Siber Güvenlik Merkezi (The National Cyber Security Centre, NCSC) 2011 yılından bu yana GCSB içerisinde yer almaktadır. NCSC, siber kaynaklı tehditlere karşı savunma yapmak ve devlet kurumları ile kritik altyapı sağlayıcıları için gelişmiş hizmetler ve danışmanlık hizmetleri sunmaktadır. GCSB'nin; iletişim ve kriptografi uzmanları, mühendisler, teknisyenler, yabancı dil uzmanları ve destek

personeli dâhil olmak üzere 300 personeli bulunmaktadır. GCSB'e 2012/2013 yılları için tahsis edilen ödenek 63 milyon dolardır.

*Konuya ilişkin mevzuatlar:*

- Kamu Finansmanı Kanunu, 1989
- Telsiz Kanunu, 1989
- Gizlilik Kanunu, 1993
- Kamu Kayıtları Kanunu, 2005

2011 yılında Yeni Zelanda'nın *Siber Güvenlik Stratejisi* yayımlanmıştır (ENISA Yeni Zelanda, 2011). Ayrıca, konuya ilişkin olarak, 2002 yılında "hükümet sektöründe güvenlik" konulu rapor yayımlanmıştır.

Yeni Zelanda Güvenlik İstihbarat Birimi (New Zealand Security Intelligence Service, NZSIS), Yeni Zelanda'nın güvenlik ile ilgili konularda hükümete tavsiyelerde bulunan bir devlet kurumudur ve birimde yaklaşık 200 personel görev yapmaktadır (NZSIS, 2013).

### 3.2. Uluslararası Kuruluşlar

Bu bölümde, uluslararası kuruluşların, siber güvenlik alanında yaptıkları mevzuat çalışmaları, kararlar ve sözleşmeler detaylı olarak incelenmiştir.

#### 3.2.1. Birleşmiş Milletler

Birleşmiş Milletler (BM), 24 Ekim 1945'te kurulmuş dünya barışını, güvenliğini korumak ve uluslararasında ekonomik, toplumsal ve kültürel bir iş birliği oluşturmak için kurulan, 193 üyeye sahip uluslararası bir örgüttür. Birleşmiş Milletler kendini "adalet ve güvenliği, ekonomik kalkınma ve sosyal eşitliği uluslararasında tüm

ülkelere sağlamayı amaç edinmiş küresel bir kuruluş" olarak tanımlamaktadır (Wikipedia, 2014d).

BM Güvenlik Kurulu, siber güvenlikle ilgili şu kararları kabul etmiştir;

- BM Sosyal ve Ekonomik Komisyonu çerçevesinde 56/121 sayılı "Bilgi Teknolojisinin Suç Amaçlı Suistimaliyle Mücadele"

- 57/239 sayılı "Küresel Siber Güvenlik Kültürü Oluşturulması"
  Karara göre; küresel siber güvenlik kültürü oluşturulması için, tüm katılımcılar aşağıdaki dokuz tamamlayıcı unsuru ele almalıdır:
  (1)Farkındalık
  (2)Sorumluluk
  (3)Müdahale
  (4)Etik
  (5)Demokrasi
  (6)Risk değerlendirmesi
  (7)Güvenlik tasarımı ve uygulanması
  (8)Güvenlik yönetimi
  (9)Ürünlerinin yeniden değerlendirilmesi (ITU, 2003).

Her iki karar da uluslararası işbirliğinin önemi, siber suçlular için güvenli sığınakların ortadan kaldırılması, emniyet uygulamalarında işbirliği ve siber güvenlik konularında genel farkındalığın artırılması ihtiyacını vurgulamaktadır.

### 3.2.2. Uluslararası Telekomünikasyon Birliği (ITU)

ITU, 17 Mayıs 1865 tarihinde kurulmuş olan, merkezi Cenevre'de bulunan ve telekomünikasyon dalında birçok standardı belirleyen bir Birleşmiş Milletler kuruluşudur. 193 ülke ve 700'den fazla özel sektör ve akademik kurum bu birliğe üyedir (ITU, 2014).

8 Eylül 2011 tarihinde, "Siber Tehditlere Karşı Uluslararası Çok taraflı Ortaklık Birimi" (International Multilateral Partnership Against Cyber Threats, IMPACT), Birleşmiş Milletler'in resmi olarak siber güvenlik yürütme kolu haline gelmiştir.

ITU-IMPACT bünyesinde çalışan merkezler şunlardır (IMPACT, 2014):

- Küresel Müdahale Merkezi (Global Response Centre)
- Güvenlik Güvencesi ve Araştırmalar Merkezi (Centre For Security Assurance &Research)
- Politika ve Uluslararası İşbirliği Merkezi (Centre For Policy &International Cooperation)
- Eğitim ve Beceri Geliştirme Merkezi (Centre For Training & Skills Development)

Şekil 3.5. ITU-IMPACT Organizasyon Yapısı


Kaynak: IMPACT, 2014

ITU Genel Sekreterliği, 2007 yılı Mayıs ayı içerisinde, Küresel Güvenlik Gündemi (Global Security Agenda) dokümanını yayımlamış ve üye ülkeler tarafından onaylanmıştır.

Küresel Güvenlik Dokümanının temel hatları,

- Hukuki tedbirler,
- Teknik ve süreçsel tedbirler,
- Siber güvenlik araçları,

- Ulusal siber güvenlik programında bulunması gereken hususlar, ana başlıklarından oluşmaktadır.

Uluslararası Telekomünikasyon Birliği tarafından 2007 yılında "Gelişmekte Olan Ülkeler için Siber Güvenlik Rehberi" dokümanı yayımlanmıştır. Genel hatlarıyla şu konuları içermektedir (ITU, 2007):

- Siber tehditlerin doğası gereği sürekli bir değişim içerisinde olması
- Düşük giriş engellemeleri ve artan çok yönlü siber suçlar
- Mevcut yasal çerçevedeki boşluklar
- Yazılım uygulamalarının güvenlik açıklıkları
- Uygun/ilgili bir organizasyon yapısının olmaması
- İnsanların nelerden zarar geleceğini bilmemesi
- Uluslararası işbirliği: Siber tehditler küresel bir sorundur ve küresel bir çözüm gerekmektedir.
- Siber Güvenlik kavramının herkes için ne anlama geldiğinin anlaşılması gerekmektedir.

ITU, siber güvenliğe ilişkin bilinci artırmak ve üye devletlerin bu alandaki çalışmalarına katkıda bulunmak amacı ile çok sayıda rehber doküman ve kılavuz hazırlamakta ve resmi web sitesi üzerinden yayımlamaktadır.

Bunlardan bazıları aşağıda sıralanmıştır (ITU Cybersecurity, 2014):

1. "2013 Yıllık Güvenlik Özeti/Genel Bakışı" dokümanı hazırlanmıştır.
2. ITU tarafından, üye devletlere siber saldırı eğilimlerine ilişkin bir öngörü sunabilmek amacı ile 2014 yılı siber tehdit öngörüleri üzerine "2014 yılı ve sonrası için bilinen Mikro Güvenlik Tahminleri" isimli bir rapor yayımlanmıştır.
3. Mobil cihazlarda veri korumanın önemini anlatan bir e-kılavuz yayımlanmıştır.
4. Yine mobil cihazlardaki mahremiyeti siber saldırılardan korumak için öneriler getiren bir rehber yayımlanmıştır.

### 3.2.3. Avrupa Birliği (AB)

AB yirmi sekiz üye ülkeden oluşan ve yirmi dört resmi dili bulunan siyasi ve ekonomik bir örgütlenmedir.

Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA), AB'nin bir kuruluşudur. ENISA 460/2004 sayılı AB Tüzüğü ile 2004 yılında oluşturulmuş ve 1 Eylül 2005 yılından bu yana tam olarak faaliyete geçmiştir. ENISA'nın amacı Avrupa Birliği'nin ağ ve bilgi güvenliği geliştirmek, iyileştirmektir. AB bünyesinde siber güvenlik konusunda tavsiyelerde bulunma, risk analizi, risk yönetimi ve bilgi güvenliği alanında farkındalık ve siber güvenlik politikaları konusunda uluslararası paydaşlarla işbirliği yapma gibi çalışmalar gerçekleştirmek amaçları arasındadır.

ENISA, 2012 yılı mayıs ayında, "Ulusal Siber Güvenlik Stratejileri" dokümanını yayınlamıştır. Doküman, AB üye ülkelerindeki siber güvenlik çalışmalarına ait son durumu ve genel değerlendirmeler ile öneriler kısmından oluşmaktadır.

Ulusal Siber Güvenlik Stratejisinde; **kısa vadade** yapılması gerekenler şu şekilde sıralanmıştır (GNS, 2012):

- ✓ Ulusal Siber Güvenlik Stratejisini geliştirmek, yeniden değerlendirmek,
- ✓ Stratejinin yanı sıra siber güvenlik tanımı kapsamı ve hedefleri net olarak belirlemek,
- ✓ Kamu dairelerinin dört bir yandan gelen endişerinden haberdar olmak ve ele almak,
- ✓ Sanayi, akademi temsilcileri ve vatandaşdan gelecek katılımı sağlamak,
- ✓ Diğer üye devletler ve Avrupa Komisyonu ile işbirliği yapmak,
- ✓ Stratejilerin tanınmasını sağlamak.

Ulusal Siber Güvenlik Stratejisinde; **uzun vadade** yapılması gerekenler şu şekilde sıralanmıştır (GNS, 2012):

- ✓ AB genelinde ortak hedefler tanımını desteklemek üzere yeterince hassas olan ve yaygın olarak kabul görmüş olan siber güvenlik tanımının kabul edilmesi.
- ✓ AB ve AB üyesi devletlerin siber güvenlik stratejilerinin, uluslararası toplumun hedefleri ile çakışmamasını ve küresel olarak değerlendirilen siber güvenlik sorunlarını çözmek için çalışmaları desteklemesini sağlamaktır.

Ayrıca ENİSA, 2012 yılında, kolluk kuvvetleri ve SOME'ler arasındaki ilişki ve işbirliğini anlatan, "The Fight against Cybercrime - Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime (Siber suçlarla mücadele-Siber suçlarla mücadelede SOME ve Kolluk kuvvetleri arasındaki işbirliği) dokümanını yayımlamıştır.

### 3.2.4. Avrupa Konseyi

1949 yılında Avrupa çapında insan hakları, demokrasi ve hukukun üstünlüğünü savunmak amacıyla Avrupa çapında kurulmuş hükümetlerarası bir kuruluştur. 5 Mayıs 1949 tarihinde kurulan kuruluşa 47 ülke üyedir ve merkezi Fransa'da bulunmaktadır.

2001 yılında imzaya açılan ve 2004 yılında Avrupa Konseyi tarafından yürürlüğe alınan Siber Suçlar Sözleşmesi, konuyla ilgili yayımlanmış uluslararası bağlayıcılığı olan tek antlaşmadır. Sözleşme, siber suçlarla ilgili mevzuat geliştirmek isteyen ülkeler için rehber niteliğindedir. Amacı; gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi yoluyla siber suçlara karşı toplumun korunmasını amaçlayan ortak bir ceza politikasının izlenmesidir (Siber Suçlar Sözleşmesi, 2001).

Ülkelerin gerekli iç mevzuatlarını geliştirmesini ve siber suçlarla mücadelede uluslararası işbirliği yapılmasını amaçlayan Sözleşme şu ana kadar 46 ülke tarafından imzalanmıştır. Türkiye ise sözleşmeyi 2010 yılında imzalamıştır. Türkiye'de, Siber Suçlar Sözleşmesi, "6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanunu" adıyla yasalaşmış olup, 2 Mayıs 2014 tarihli ve 28988 sayılı resmi gazete'de yayımlanmıştır (Kanun, 2014b)

Sözleşme, toplam 48 maddeden oluşmaktadır. Özellikle telif haklarının ihlalleri, bilgisayarlarla ilgili sahtekârlık eylemleri, çocuk pornografisi, ağ güvenliğine ilişkin suçları tanımlamakta ve bu suçlarla mücadele etmede işbirliğini öngörmektedir (Siber Suçlar Sözleşmesi, 2001).

Ayrıca, Avrupa Konseyi tarafından 2010 yılı Mayıs ayında, "Avrupa için Sayısal Gündem" (Digital Agenda for Europe) girişimi hayata geçirilmiştir. Sayısal Gündem yedi öncelikli alanda gruplanan 132 adet eylem içermektedir. AB siber güvenlik stratejisi ve direktifinin önerilmesi de yedi öncelikli alan içerisinde yer almaktadır. Sayısal Gündem'de siber güvenliğin geliştirilmesi ile ilgili 14 adet eylem maddesi bulunmaktadır (European Commission, 2014).

Türkiye'de de, Türkiye Bilişim Derneği önderliğinde, ülkenin kendi sayısal gündeminin oluşturulması maksadı ile gönüllülük esasına dayalı olarak "Sayısal Gündem 2020 Uzmanlık Grupları" oluşturulmuştur (TBD, 2013).

### 3.2.5. Kuzey Atlantik Paktı (NATO)

2007 yılında Estonya'ya yapılan siber saldırının ardından, NATO 2007 yılı Mayıs ayında, Bakanlar için bir rapor hazırlamıştır. 2008 yılı Ocak ayında NATO siber savunma politikası onaylanmıştır. Siber saldırılara karşı koordine edilmiş bir mukabelede bulunmayı amaçlayan bu politika temel ilkeleri belirlemekte ve gerek

NATO'nun sivil ve askeri unsurlarına gerek müttefik ülkelere rehberlik etmektedir.

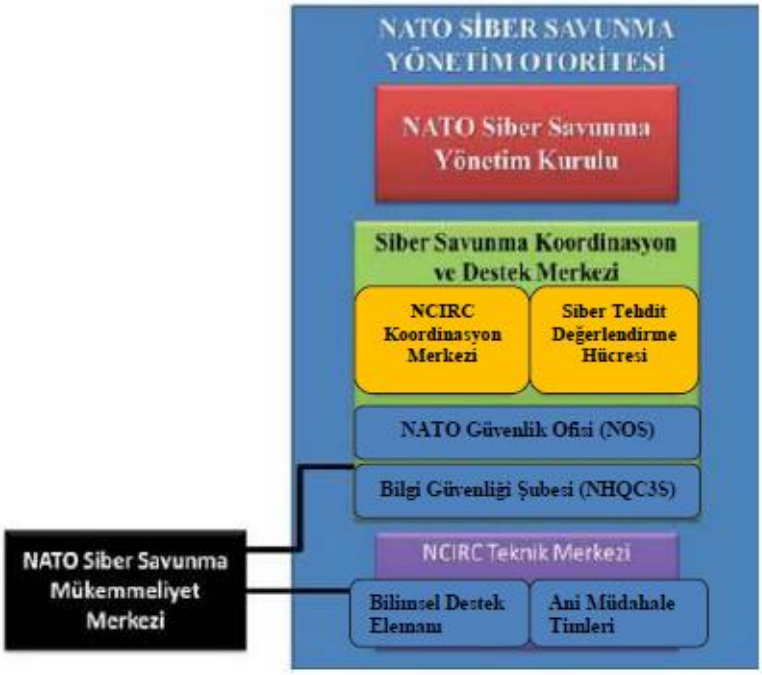
Talin, Estonya'daki İşbirliğine dayalı Siber Savunma Mükemmeliyet Merkezi 2008 yılında bir NATO Mükemmeliyet Merkezi olarak akredite edilmiştir. Merkez, siber savunma ile ilgili farkındalık yaratmak ve standart oluşturmak amacı ile araştırmalar yapmak ve eğitim vermekle görevlidir. NATO Siber Savunma Mükemmeliyet Merkezi Uluslararası Bağımsız Uzmanlar Grubu tarafından hazırlanan "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı" 2013 yılı mart ayında yayımlanmıştır (Tallinn El Kitabı, 2013). Söz konusu el kitabı; siber güvenlik konusundaki hukuk, savaşa girmek için haklı nedenler, savaş sırasında uyulması gereken kurallar), uluslararası hukuk, konularını kapsamaktadır. Hukuki boşluğun nasıl doldurulacağı konusunda bir rehber niteliği taşımakta ancak resmi bir nitelik taşımamaktadır (MGK, 2013).

2010 Lizbon zirvesi, siber güvenliği, NATO'nun ileriki yıllarda ele alması gerekecek olan yeni güvenlik tehditlerinin en ön sırasına oturtmuştur. Lizbon görev tanımı çerçevesinde, 2012 yılı nisan ayı içerisinde NATO Savunma Planlama Süreci (NDPP) içine siber savunma entegrasyonu başlamıştır.

2011 yılı Haziran ayında, NATO'nun müttefikleri ile ilişkilerinde, siber savunma çabalarını güçlendirme planları konusunda net bir vizyon ortaya koyan, yeni bir siber savunma politikası ve eylem planı kabul edilmiştir.

Bilgisayar Olaylarına Müdahale Yeteneği (Computer Incident Response Capability, NCIRC); NATO'nun kendi çerçevesi içerisinde siber savunma hizmetlerinin geliştirilmesi, uygulanması ve devam ettirilmesinin sağlanmasından sorumludur. NCIRC Koordinasyon Merkezi Brüksel, Belçika NATO Karargâhında yer almaktadır.

Şekil 3.6. NATO Siber Savunma Yönetim Otoritesi

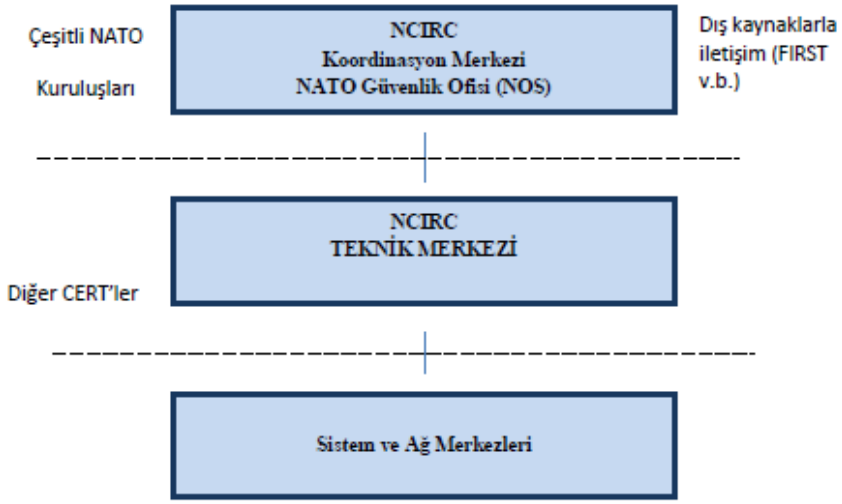



Kaynak: 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2013

NCIRC'nin Görevleri:

- Bir olay sırasında NATO çapında yanıt, koordinasyon
- Yerel sistem yöneticilerini desteklemek için merkezi bilgi tabanı
- Merkezi, online ve yerinde hizmetler
- Kaynakların optimizasyonu
- Dış CERTs / CSIRTs ile iletişim.

Şekil 3.7. NCIRC Yapısı




Kaynak: ANIL, 2004

NATO'nun siber güvenlik alanındaki çalışmalarını yürüten Bilgisayar Olaylarına Müdahele Yeteneği birimi ile üye ülkeler arasında siber güvenlikle ilgili faaliyetlerin koordinasyonu, bilgi paylaşımı ve işbirliği sağlamak amacıyla mutabakat muhtıraları imzalanmıştır. Türkiye Cumhuriyeti adına söz konusu muhtıra, TÜBİTAK tarafından 2007 yılında imzalanarak yürürlüğe girmiştir.

NATO siber savunma faaliyetlerini koordine etmek maksadıyla 2008 yılında NATO Siber Savunma Yönetim Kurulu (CDMB) kurulmuştur. Mevcut muhtıranın; CDMB ile üye ülkeler arasında imzalanmak üzere hazırlanan standart bir mutabakat muhtırası şablonuna uygun hale gelmesi maksadı ile güncelleme ihtiyacı doğmuş olup buna ilişkin çalışmalar devam etmektedir.

Sivil Olağanüstü Hal Planlama Komitesi (Civil Emergency Planning Committee, CEPC) ise; sivil halkın korunması ve NATO'nun hedeflerinin desteklenmesinde sivil kaynakların kullanımı konularında, NATO'nun üst danışma organıdır. CEPC, danışman uzmanlık sağlanması yoluyla ve eğitim desteği ile NATO'nun siber

yeteneklerinin geliştirilmesini desteklemektedir. CEPC, enerji güvenliği ile ilgili konularda, özellikle kritik altyapının korunmasında, uluslararası deneyim alışverişi yoluyla yardımcı olmaktadır (NATO, 2011).

### 3.2.6. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)

OECD, 1961 yılında kurulan, merkezi Fransa, Paris'de bulunan ve 34 tam üyeye sahip olan uluslararası bir ekonomi örgütüdür.

OECD bünyesinde siber güvenlik konusunda çalışmaların yürütüldüğü birim, Bilim, Teknoloji ve Sanayi Müdürlüğüne (Directorate for Science, Technology and Industry, STI) bağlı olarak çalışan Bilgi, Bilgisayar ve İletişim Politikaları Komitesidir (Committee for Information, Computer and Communications Policy, ICCP).

Şekil 3.8. OECD ICCP Genel Yapısı


Kaynak: OECD ICCP, 2010

OECD'nin siber güvenliğe ilişkin yayımlamış olduğu raporlar aşağıda yer almaktadır:

- ✓ 2007 yılında "Kritik Bilgi Altyapılarının Korunmasına İlişkin Politikaların Geliştirilmesi" raporu yayımlanmıştır.
- ✓ 2008 yılında "Kritik Bilgi Altyapılarının Korunmasına İlişkin OECD Tavsiyeleri" raporu yayımlanmıştır.
- ✓ 14 Ocak 2011 tarihinde yayımlanan "Sistemsel Siber güvenlik Riskini Azaltmak" konulu rapor şu konuları içermektedir (SOMMER Peter, BROWN Ian, 2011):

  - Internet'in ortaya çıkışı
  - E-Devlet
  - Akıllı şebekeler ve SCADA
  - Kaynak kodlar/ programdaki hatalar (bugs)
  - Kritik altyapılar
  - Belirli sistemsel tehditler
  - Geniş çaplı suç teşkil eden saldırılar
  - Rekreasyonel hackleme
  - İnternet korsanlığı (Hactivism)
  - Büyük ölçekli devlet ve sanayi casusluğu
  - Risk analizi
  - Hazırlık düzeyi
    - Askeri alandaki yanıtlar/responses
    - Sivil yükümlülükler
    - Özel sektör
    - Polis ve terörle mücadele alanındaki yanıtlar
    - Yasal ve düzenleyici yaklaşımlar
  - Sonuç ve öneriler
    - Ulusal stratejiler
    - Kamu özel sektör ortaklıkları
    - Uluslararası stratejiler

Olası yeni teknik önlemler

Araştırma

Eğitim.

- ✓ "Dönüm Noktasında Siber Güvenlik Politikası oluşturma/İnternet Ekonomisi için Ulusal Siber Stratejilerin Yeni Nesil Analizi" konusunda 16 Kasım 2012 tarihinde bir rapor yayımlanmıştır. Bu rapor, ilk 10 OECD ülkesindeki yeni nesil "Siber Güvenlik Stratejilerindeki" ortak noktaları ve farklılıkları tespit etmekte ve tanımlamaktadır (OECD, 2012).
- ✓ 21 Kasım 2012 tarihinde, OECD "2002 güvenlik yönergeleri değerlendirmeleri" raporu yayımlanmıştır.
- ✓ Bilgi Güvenliği, Gizlilik ve Çocukların Online ortamda Korunması ile ilgili Fırsatlar ve Sorunların anlaşılması konusunda "Bilgi Güvenliği ve Gizlilik Politikaları Veri Tabanı Geliştirilmesi" konulu rapor 20 Aralık 2012 tarihinde yayımlanmıştır.
- ✓ "Kritik Bilgi Altyapısının Korunması için Politikalar Geliştirilmesi" konulu rapor 2007 yılında yayımlanmıştır.

OECD'nin bir alt çalışma grubu olan; Bilgi Güvenliği ve Gizlilik Çalışma Grubu (Working Party on Information Security and Privacy, WPISP), siber güvenlik ve gizliliğin, ekonomik ve sosyal yönlerine odaklanmakta ve bu konuda çalışmalar yürütmektedir (OECD, 2013).

## 3.3. Siber Tehdit Raporları

Bu bölümde, dünya çapında bilinen teknoloji firmalarının güncel tehdit raporları incelenmektedir.

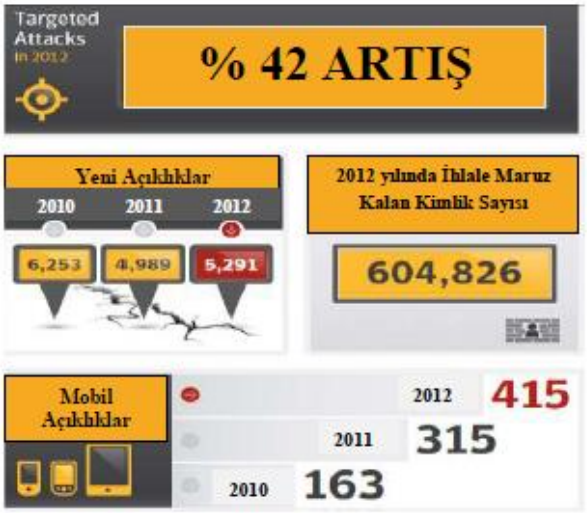
### 3.3.1. Symantec internet güvenlik tehdidi raporu 2013

Symantec yazılım şirketinin 2013 yılında yayımlamış olduğu, İnternet Güvenlik Tehdidi Raporu 2012 yılı dünyadaki internet tehdit verileri ile ilgili en kapsamlı

kaynaklardan birini oluşturmaktadır. Rapor hazırlanırken 157'den fazla ülke ve 30 terabyte'dan fazla veri incelenmiştir (Symantec, 2013).

Şekil 3.9'da görüldüğü üzere, 2012 yılında gerçekleşen siber saldırılar bir önceki yıla göre %42 oranında artmış durumdadır. 5291 adet yeni güvenlik açığı tespit edilmiş olup bunlardan 415 tanesi mobil işletim sistemlerine aittir. Önceki yıllara oranla artış gözlemlenmektedir. 2012 yılında ihlale maruz kalan kimlik sayısı ise ortalama 604.826 adettir (Symantec, 2013, s.10).

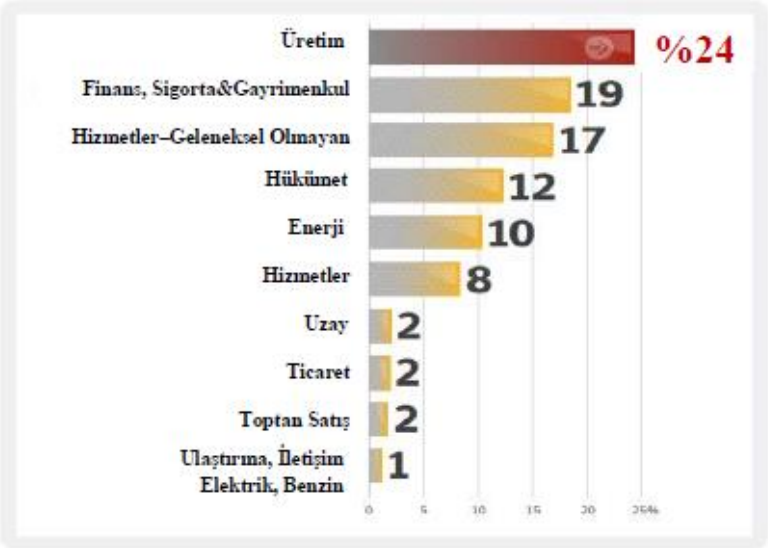
Şekil 3.9. Siber Saldırılar ve Güvenlik Açıklıkları




Kaynak: Symantec, 2013

Şekil 3.10'da görüldüğü üzere, gerçekleştirilen saldırılarıların hedefleri arasında yer alan üretim sektörü, 2012 yılında, yüzde 24'lük oranla ilk sırada yer almaktadır(Symantec, 2013, s.15).

Şekil 3.10. Saldırıların hedefleri




Kaynak: Symantec, 2013

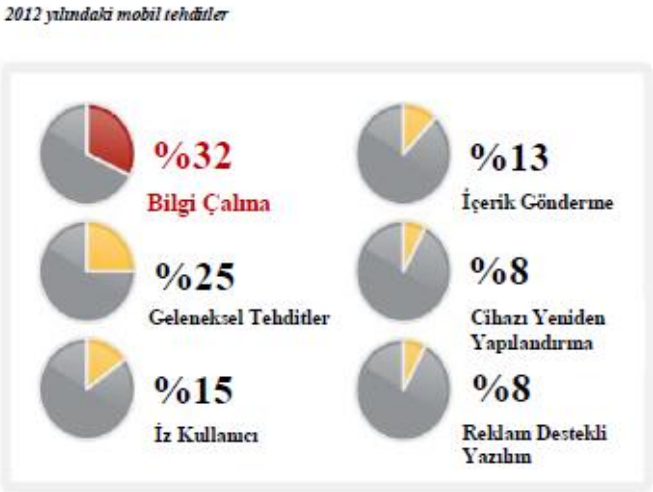
Şekil 3.11'de, İnternet Güvenlik Tehdidi Raporu'na göre; 2009 yılı ile 2012 yılı arasında yapılan saldırılar görülmektedir. Bu saldırılardan en çok dikkat çeken, İran'ın nükleer santrallerine yönelik olarak yapılan "Stuxnet" saldırısıdır (Symantec, 2013, s.20).

Şekil 3.11. Yapılan Saldırılara Ait Zaman Çizelgesi


Kaynak: Symantec, 2013

Şekil 3.12'de görüldüğü üzere; mobil cihazlara yapılan tehditlerin en büyüğü %32'lik oranla bilgi çalma amaçlı yapılan tehditlerdir (Symantec, 2013, s.33).

Şekil 3.12. Mobil Tehditlerin Hedefleri




Kaynak: Symantec, 2013

Tablo 3.1'de görüldüğü üzere, mobil işletim sistemleri üzerindeki güvenlik açıklıklarında Apple İOS, 387 güvenlik açığıyla ilk sırada yer almasına rağmen Android tabanlı cihazlara yapılan tehditler daha fazladır. Tablo 3.1'de yer alan 2 tablo kıyaslandığında, güvenlik açığı sayısının fazla olması daha yüksek seviyede tehdite uğranacağı anlamına gelmediği görülmektedir. Çünkü mobil tehditlerin çoğu, yazılım açıklıklarını kullanmamaktadır (Symantec, 2013, s.34-35).

Tablo 3.1. Mobil İşletim Sistemi Güvenlik Açıklıkları ve Cihaz Tabanlı Tehditler

*İşletim Sistemine göre Mobil Güvenlik*

| Cihaz Türü | Tehdit Sayısı |
|---|---|
| Android malware | 103 |
| Symbian malware | 3 |
| Windows Mobile malware | 1 |
| iOS malware | 1 |

*Cihaz Türüne göre Mobil Tehditler*

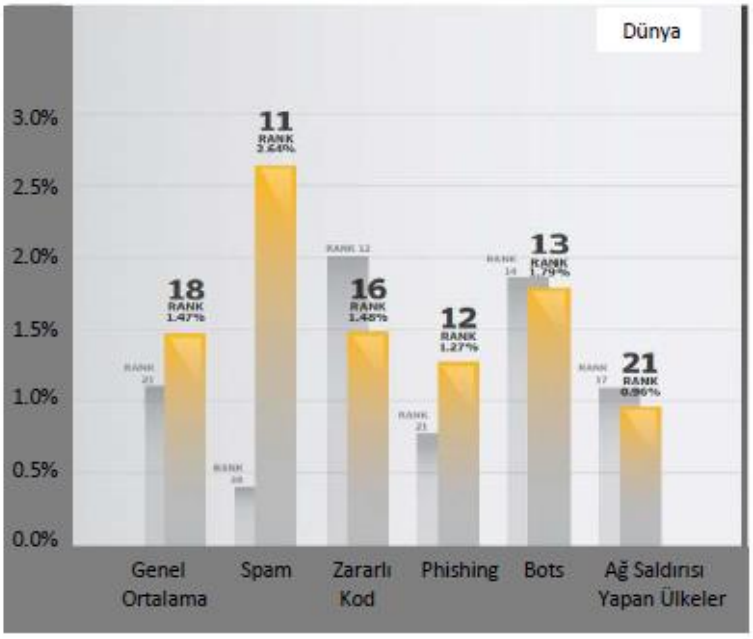
| Platform | Belgelenmiş Güvenlik Açığı |
|---|---|
| Apple iOS | 387 |
| Android | 13 |
| BlackBerry | 13 |
| Nokia | 0 |
| LG Electronics | 0 |
| Windows Mobile | 2 |

Kaynak: Symantec, 2013

Raporun ekinde, gelen tehditlerin sayısı, türü, alanı bakımından, Türkiye'nin Dünya'da ve Avrupa'daki yerini gösteren grafiklerde yer almaktadır.

Şekil 3.13'de görüldüğü üzere, Dünya çapında Türkiye istenmeyen posta içerikleri alanında 11. sırada yer almaktadır. Avrupa sıralamasında ise 5. sırada bulunmaktadır (Symantec-Appendix, 2013).

Şekil 3.13. Türkiye'nin Dünya'daki ve Avrupa'daki yeri


Kaynak:Symantec-Appendix,2013

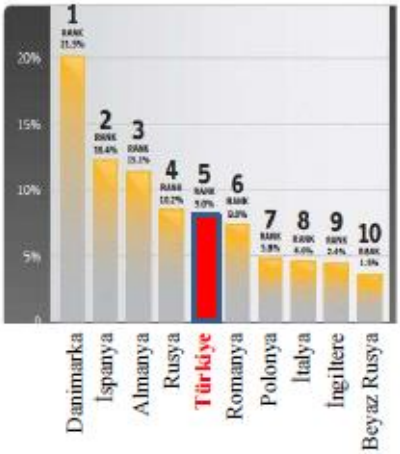
Şekil 3.14'de görüldüğü üzere, Avrupa ülkeleri sıralamasında, Türkiye gelen tehditler sıralamasında 9.sırada yer almakta iken, istenmeyen posta içeriklerinde 5, phishing saldırılarında 8, virüs tehditlerinde ise 5.sırada yer almaktadır (Symantec-Appendix, 2013).

Şekil 3.14. Gelen Tehditler Sıralamasında Türkiye'nin Avrupa'daki Yeri

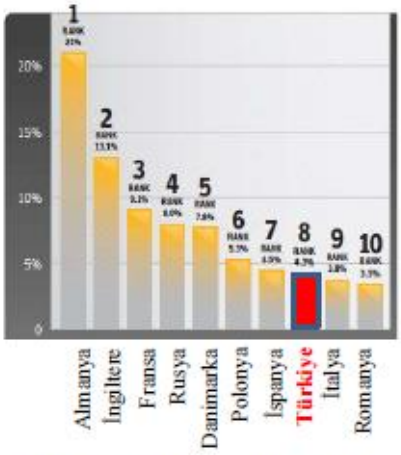
Genel ilk 10

| Top Ten Overall | Rank |
|---|---|
| Almanya | 1 |
| Danimarka | 2 |
| İtalya | 3 |
| İngiltere | 4 |
| Rusya | 5 |
| İspanya | 6 |
| Polonya | 7 |
| Fransa | 8 |
| Türkiye | 9 |
| Macaristan | 10 |

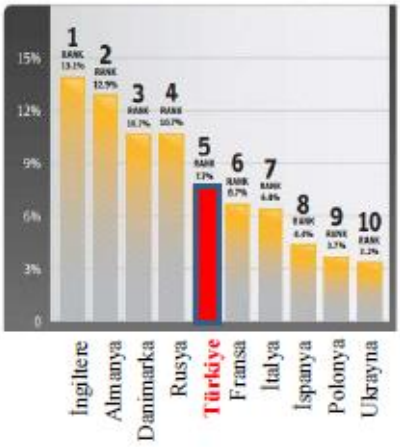
Spam ilk 10




Phishing ilk 10




Virüs ilk 10



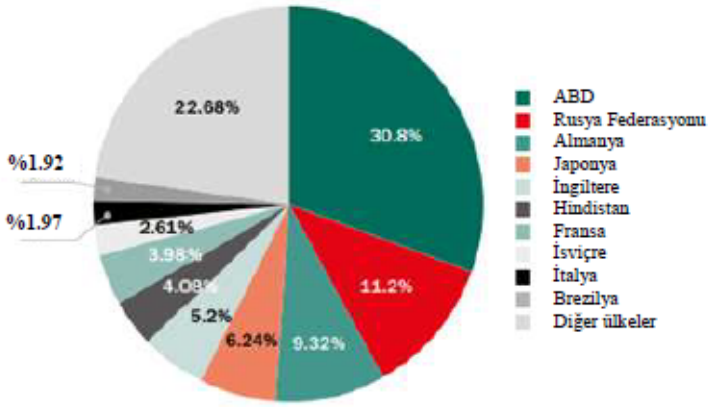

Kaynak: Symantec-Appendix, 2013

### 3.3.2 Kaspersky '2013 finansal siber tehditler' raporu

Kaspersky Lab, 1997 yılında kurulan ve bilgisayar ve internet güvenliği üzerine çözümler sunan Rusya merkezli bir güvenlik şirketidir. Kaspersky Lab tarafından yürütülen '2013 Finansal Siber Tehditler' çalışmasına göre; siber suçluların, kişisel çevrimiçi hesaplara erişimi giderek artmaktadır. 2013 yılında, kötü amaçlı finansal yazılımların kullanıldığı siber saldırıların sayısı bir önceki yıla göre %27,6 artışla 28,4 milyona yükselmiştir.

Türkiye, finansal siber suç oranının en fazla olduğu ülkeler arasında yer almaktadır. Türkiye ile birlikte Afganistan, Bolivya, Kamerun, Moğolistan, Myanmar, Peru ve Etiyopya'da yaşanan vakalar, toplam rakamın %12'sinden fazlasını oluşturmaktadır. Kullanıcıların banka hesaplarından para çalmaya yarayan mobil uygulamaların sayısında 2013 itibarıyla görülen patlama ile kötü amaçlı mobil yazılımlar segmentinde de oldukça fazla faaliyet göze çarpmaktadır. Saldırıların büyük çoğunluğu ise Android akıllı telefon kullanıcılarını hedef almaktadır. Şekil 3.15'de en sık saldırıya uğrayan ülkeler yüzdelik değerler verilerek gösterilmektedir (Kaspersky, 2013).

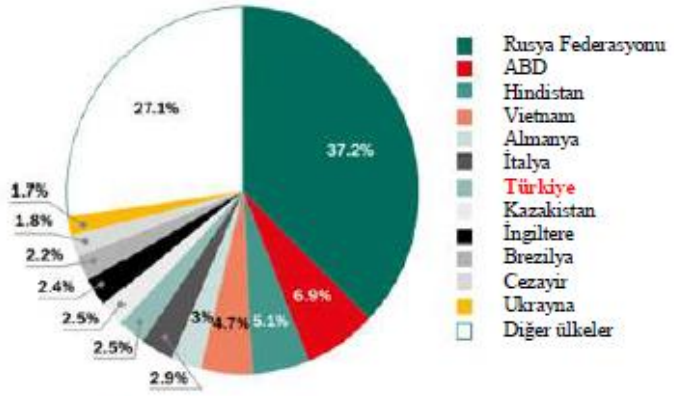
Şekil 3.15. 2013 Yılında En Sık Saldırıya Uğrayan Ülkeler




Kaynak: Kaspersky, 2013

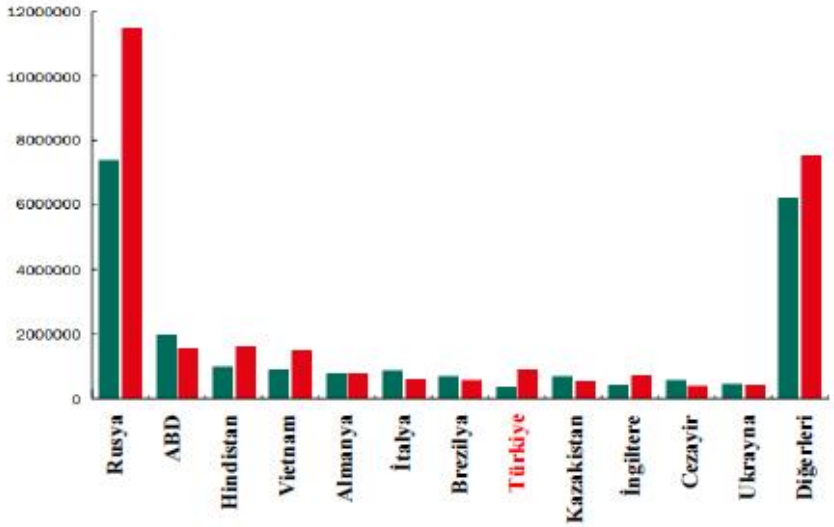
Şekil 3.16'da da görüldüğü üzere, Türkiye %2,5 lik bir yüzdeyle finansal anlamda en çok saldırıya uğrayan ülkeler arasında yer almaktadır.

Şekil 3.16. Finansal Olarak En Çok Saldırıya Uğrayan Ülkeler




Kaynak: Kaspersky, 2013

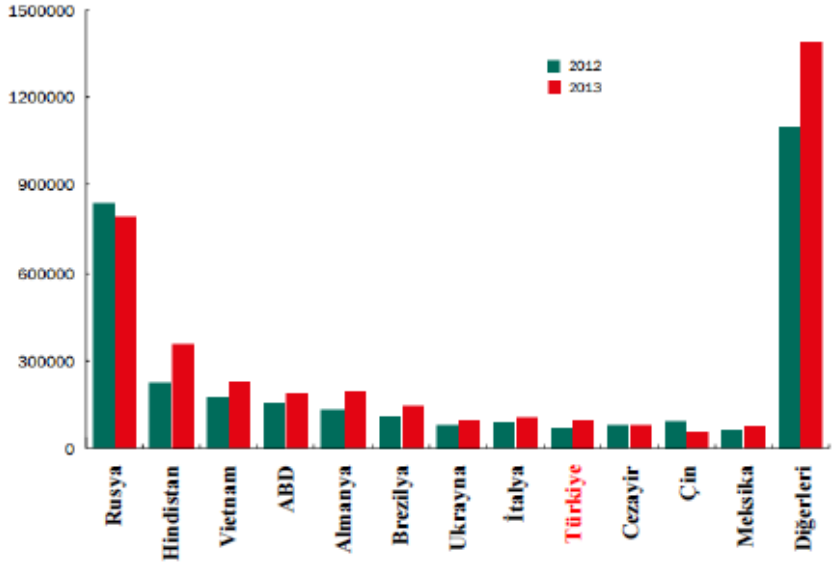
Şekil 3.17. Dünya Çapında Finansal Kötü Amaçlı Yazılım Saldırıları




Kaynak: Kaspersky, 2013

Şekil 3.18'de görüldüğü üzere, bir yıl içerisinde, finansal kötü amaçlı yazılım saldırılarına uğrayan kullanıcı sayılarında en yüksek oranların görüldüğü 10 ülkenin, 8'inde artış yaşanmıştır.

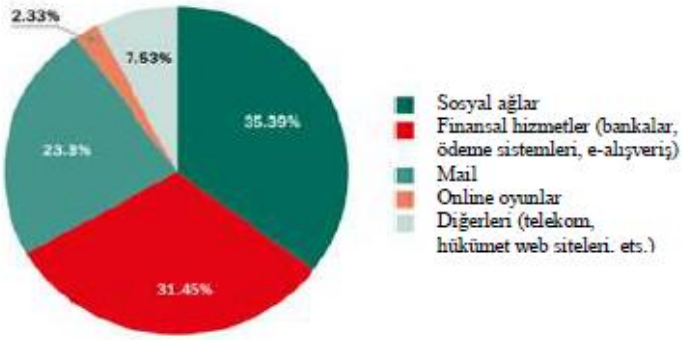
Şekil 3.18. Ülkelere göre Finansal Kötü Amaçlı Yazılımlar Tarafından Hedeflenen Kullanıcı Sayıları




Kaynak: Kaspersky, 2013

Şekil 3.19'da 2013 yılında phishing (e-dolandırıcılık) saldırılarının hedef alanları gösterilmektedir. En fazla phishing saldırısı, sosyal ağlar üzerinden yapılmaktadır.

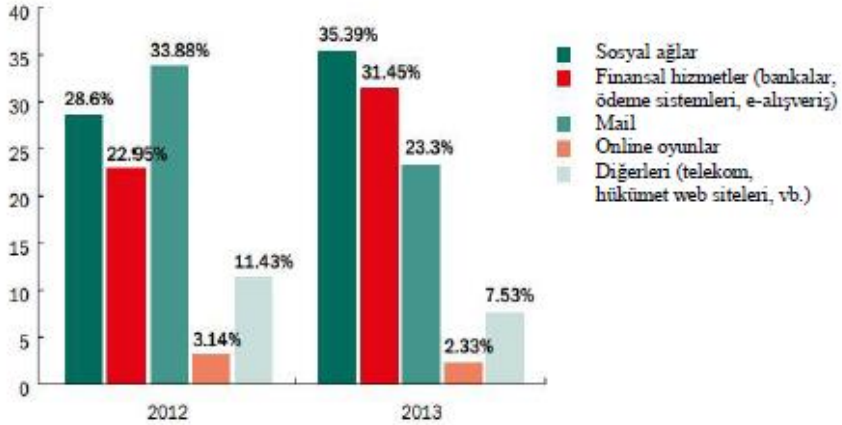
Şekil 3.19. 2013 Yılında Phishing (e-dolandırıcılık) Saldırılarının Hedef Alanları




Kaynak: Kaspersky, 2013

Şekil 3.20'de görüldüğü üzere; finansal saldırılar, 2012 yılına kıyasla, 2013 yılında, en çok artış gösteren saldırı alanıdır.

Şekil 3.20. 2012 ve 2013 Yıllarında Phishing (e-dolandırıcılık) Saldırılarının Hedef Alanları

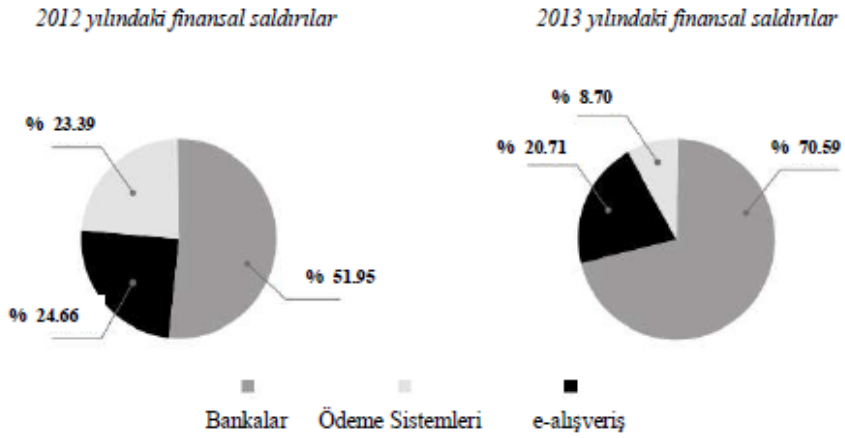



Kaynak: Kaspersky, 2013

Türkiye'de; 2013 yılında, finansal kötü amaçlı yazılım içeren saldırıların sayısı; 899,000+ olarak tespit edilmiştir. Yıllık bazda değişim %156.41, kullanıcı başına düşen saldırıların ortalama sayısı ise 9.22 olarak hesaplanmıştır. Türkiye'de; 2013 yılında, finansal kötü amaçlı yazılımlar (malware) tarafından hedeflenen Kullanıcı sayıları; 97,000+ olarak tespit edilmiştir. Yıllık bazda değişim %37,05, finansal kötü amaçlı yazılımın herhangi bir türünden etkilenen kullanıcı sayısı ise yüzde 12.01 olarak hesaplanmıştır. Türkiye ve Brezilya bu alanda birinci sırada yer almaktadır (Kaspersky, 2013, s.20).

Yalnızca finansal saldırıların, 2012 ve 2013 yıllarındaki artışı, şekil 3.21'de daha ayrıntılı olarak gösterilmiştir.

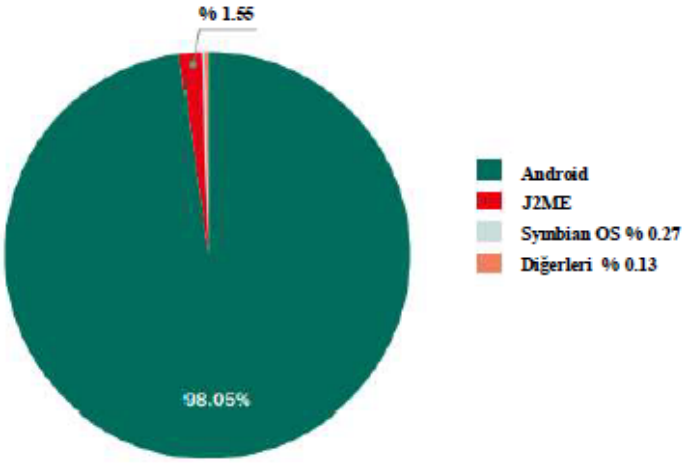
Şekil 3.21. 2012 ve 2013 Yıllarındaki Finansal Saldırıların Hedef Alanları




Kaynak: Kaspersky, 2013

Şekil 3.22'de görüldüğü üzere, 2013 yılında mobil zararlı yazılımlarda, Android %98.05'lik oldukça büyük bir oranla birinci sırada bulunmaktadır.

Şekil 3.22. 2013 Yılında Mobil Zararlı Yazılımlar



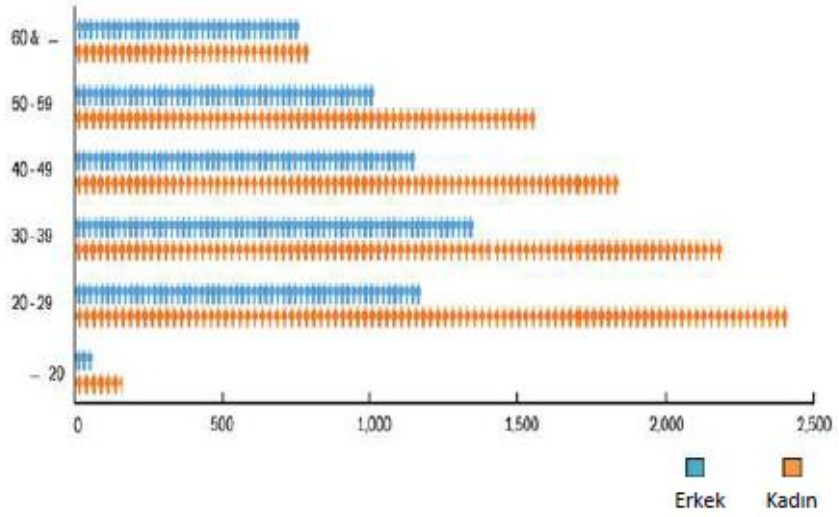

Kaynak: Kaspersky, 2013

### 3.3.3. IC3 "2012 yılı internet suç raporu"

IC3 (Internet Crime Complaint Center), internet ile ilgili suç duyuruları almak ve daha kapsamlı araştırmalar yapmak, geliştirmek amacıyla FBI ve Ulusal Beyaz Yakalı Suç Merkezi (NW3C) ortaklığıyla 8 Mayıs 2000 tarihinde kurulmuştur (IC3, 2014).

IC3 (2012)' e göre İnternet Suç Raporu'nda; 2012 yılında alınan 289.874 şikâyetin % 39.64'ünün (114908) finansal zarara neden olduğu bildirilmiştir. Şekil 3.23'de; internet dolandırıcılığı kategorisi için dikey gösterilen rakamlar yaş grubunu, yatayda gösterilen rakamlar ise bildirilen toplam şikâyet sayısını göstermektedir.

Şekil 3.23. İnternet Dolandırıcılığı Alanında Toplam Şikâyet Sayısı



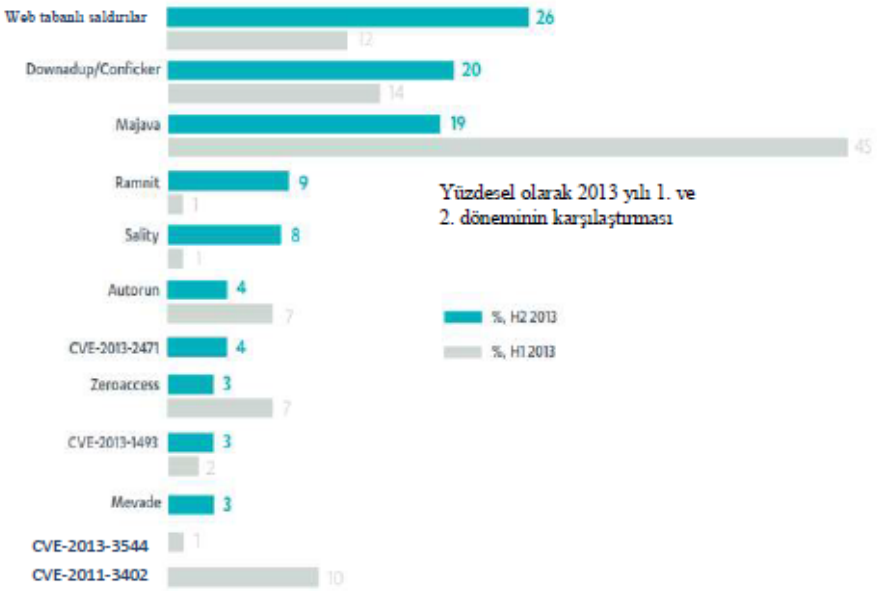

Kaynak: IC3, 2012

Raporda ülkelere göre gösterilen ilk 50 şikâyet istatistiklerinde, Türkiye, IC3'e şikâyet bildiren ülke sıralamasında 0.05 lik bir yüzde ile 41. sırada yer almaktadır (IC3, 2012, s.25).

### 3.3.4. F-Secure 2013 yılı tehdit raporu

F-Secure, Finlandiya merkezli bir bilgisayar güvenlik şirketidir. Günlük yaşantımızda internet ve hizmetlerine bağımlılığımız arttıkça tehditler de ister istemez eşdeğer şekilde artmaktadır. Genellikle web tarayıcıyı kötü amaçlı sitelere yönlendiren teknikler veya kötü amaçlı yazılımları içeren web tabanlı saldırılar için derlenen istatistikler (masaüstü ve mobil istemciler bizim bulut tabanlı uzaktan izleme sistemlerini gönderilen anonimleştirilmiş verilere dayanarak), yılın ilk yarısına kıyasla, 2013 yılı 2. Yarısında iki katına çıkmıştır. F-Secure 2013 yılı 2. yarısı tehdit raporu; en çok tespit edilen tehditleri, ülkelere göre tespit edilen yüzde rakamları, kâr amacı olup olmaması kıstasına göre tespit edilen mobil tehditlerin sayısı gibi önemli verileri kapsamaktadır. Şekil 3.24'de en çok tespit edilen ilk 10 tehdit gösterilmektedir. (F-Secure H2, 2013, s.8-9).

Şekil 3.24. En Çok Tespit Edilen İlk 10 Tehdit




Kaynak: F-Secure H2, 2013

Şekil 3.25'de görüldüğü üzere, Türkiye; Ramnit, Sality ve Autorun isimli tehditlerin en aktif olarak görüldüğü ülkeler arasında yer almaktadır.

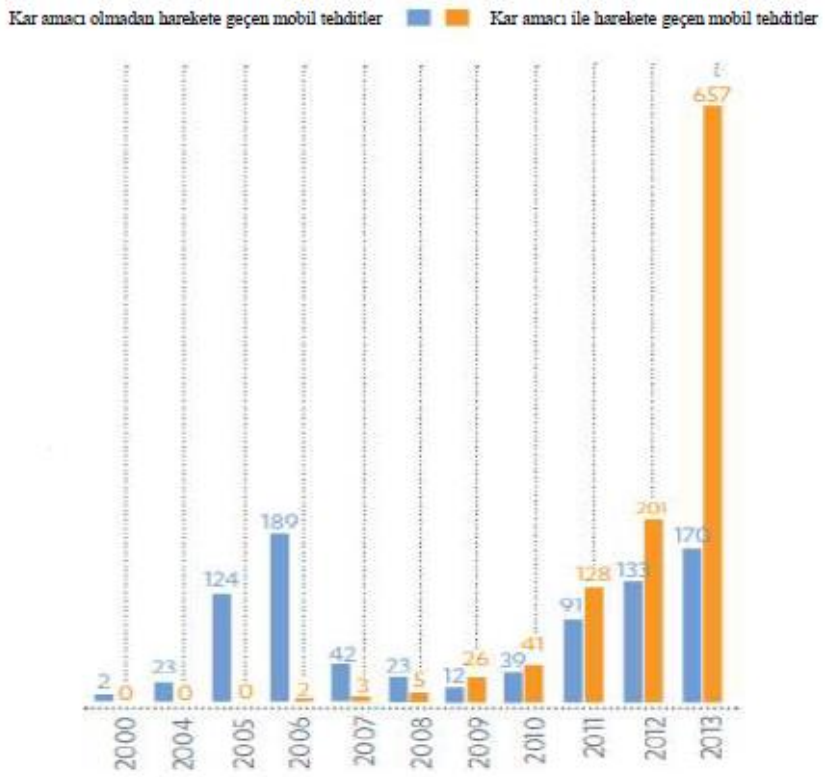
Şekil 3.25 En Çok Tespit Edilen 10 Tehditin Ülkelere Göre Tespit Edilen Yüzde Rakamları

| | Fransa | ABD | İsveç | Brezilya | Finlandiya | Almanya | Hollanda | İtalya | Britanya | Polonya | Danimarka | Malezya | Tunus | Hindistan | Türkiye | Vietnam | Belçika | Mısır | Pakistan | Romanya | Japonya | Tayvan | Bulgaristan | Kanada | Kolombiya | Endonezya | Meksika | Slovenya | Norveç | Birleşik Arap Emirlikleri | Diğer tüm Ülkeler |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Web Tabanlı Saldırılar** | 12 | 7 | 18 | | 9 | 9 | 6 | 4 | 3 | | 4 | | | | | | 3 | | | | | | | | | | | | | | 25 |
| Downadup/Conficker | 6 | | | 18 | | | | 7 | | | | 6 | | | | | | | | | 3 | 2 | 4 | | 3 | | | 4 | | 16 | 32 |
| Majava | 12 | 20 | 9 | | 10 | 9 | 7 | 3 | 5 | 3 | 3 | | | | | | | | | | | | | | | | | | | | 17 |
| Ramnit | | | | 3 | | | | | | | | 4 | 6 | 12 | 7 | 19 | | 6 | 4 | 3 | | | | | | 4 | | | | | 33 |
| Sality | | | | 13 | | | | | | 3 | | 9 | 3 | 13 | 12 | 8 | | 4 | 2 | 2 | | | | | | | | | | | 30 |
| Autorun | 12 | | | 7 | | | | | | 4 | | 10 | 3 | 8 | 5 | | | | | | 4 | 3 | | | | | 4 | | | | 41 |
| CVE-2013-2471 | 9 | 10 | 13 | | 15 | 11 | 7 | 3 | 4 | 5 | 5 | | | | | | | | | | | | | | | | | | | | 17 |
| Zeroaccess | 22 | 23 | 6 | | 4 | 4 | 3 | 3 | 7 | | 3 | | | | | | | | | | | | | 3 | | | | | | | 22 |
| CVE-2013-1493 | 10 | 17 | 13 | | 9 | 14 | 7 | | 4 | | 4 | | | | | | 3 | | | | | | | | | | | | | | 27 |
| Mevade | 32 | 3 | 6 | 5 | 5 | 4 | 6 | 4 | 3 | 5 | | | | | | | | | | | | | | | | | | | 4 | | 16 |

Kaynak: F-Secure H2, 2013

Asya'nın hızla gelişmesi ile birlikte rapor edilen kötü amaçlı yazılım tespitlerinde de artış görülmektedir. Japonya, Malezya, Tayvan, Hong Kong, Filipinler ve Hindistan gibi ülke ve bögelerden 2013 yılında bildirilen kötü amaçlı yazılım tespitleri derlenmiş ve raporda ayrıntılı olarak yer almaktadır.

Şekil 3.26. 2000-2013 Yılları Arasında Kar Amacı Olup Olmaması Durumuna Göre Mobil Tehditlerin Sayısı




Kaynak: F-Secure, 2013

### 3.3.5. F-Secure mobile tehdit 2013 yılı 3. çeyrek raporu

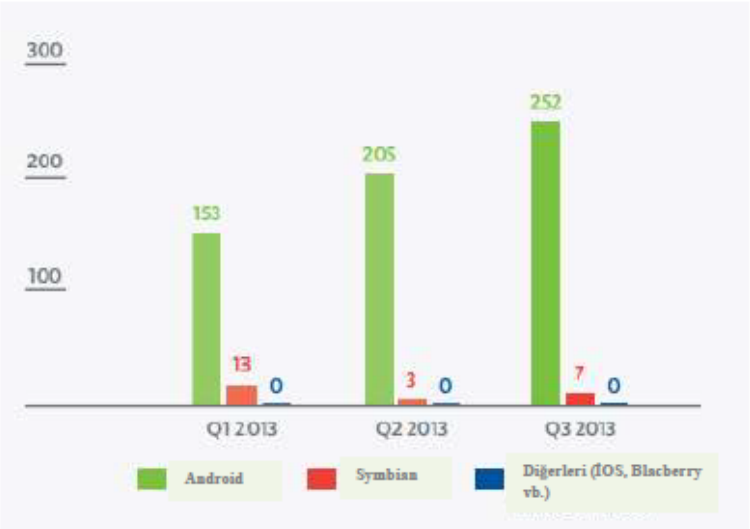
Mobil tehditlerde, zararlı yazılım kodlayıcıları; Android platformu üzerinde yoğunlaşmaya devam etmektedir. Cep telefonları ve tablet cihazlarda % 79,3 pazar payına sahip olan Android için bu durumun olağan kabul edilmesi gerektiği değerlendirilmektedir. 2013 yılı 3. çeyreğinde android üzerinde tespit edilen tehdit

sayısı 252 iken, bu rakam symbian'da 7'dir. Diğer platformlarda ise (Blackberry, iOS Windows) 2013 yılı için henüz kaydedilen bir rakam bulunmamaktadır.

Bu tehditlerin çoğu, 'kötü niyetli' programlar ya da zararlı yazılım (Malware) kategorileri altında yer almaktadır. Trojan örneklerin büyük bir yüzdesini oluşturmaktadır.

Şekil 3.27. Farklı Platformlarda Keşfedilen Mevcut Tehditler ve Mevcutların Yeni Varyasyonlarının 2013 Yılı 1. Çeyrek ve 3.Çeyrek Arasında Keşfedilen Rakamları

Yeni Mobile Tehdit Çeşitleri




Kaynak: (F-Secure)

### 3.3.6. ENISA tehdit raporu 2013

ENISA (Ağ ve Bilgi Güvenliği Avrupa Birliği Ajansı) AB, Üye Devletler, özel sektör ve Avrupa vatandaşları için ağ ve bilgi güvenliği uzmanlık merkezidir. Mevcut ve gelişmekte olan siber tehditlere genel bir bakış sunan "ENİSA Tehdit Raporu 2013" 11 Aralık 2013 tarihinde yayımlanmıştır (ENISA İnternet Tehdit Raporu, 2013).

Bilindiği üzere Avrupa Birliği'nin Siber Güvenlik Stratejisi tehdit analizi ve siber güvenlik alanında ortaya çıkan eğilimlerin önemini vurgulamaktadır. ENISA, mevcut tehdit analizi raporu için 250'den fazla kaynak analiz etmiştir. Toplanan kaynaklar, özel sektörden ve kamu sektöründen gelen raporlar, bloglardan alınan bilgiler, tartışmalar, sunumlar v.b. kaynaklardan edinilmiştir. Kaynaklar, açık kaynak istihbarat (Open Source Intelligence, OSINT) yöntemleri kullanılarak toplanmıştır (ENISA İnternet Tehdit Raporu, 2013).

Bu rapor gelişmekte olan teknoloji alanındaki tehdit eğilimleri ile ilgili tahminler sunmaktadır.

Tablo 3.2'de, gelişmekte olan teknoloji alanındaki, ilk 15 mevcut tehdit ve tehdit eğilimleri değerlendirilmiştir.

Tablo 3.2. Tehditler ve Gelişen Trendlere Genel Bakış

| Top Tehditler | Güncel Eğilimler | Kritik Altyapılar | Mobil Bilgisayar | Sosyal Ağ | Bulut Bilişim | Güvenli Altyapılar | Büyük Veri | İnternet Üzerindeki Konular |
|---|---|---|---|---|---|---|---|---|
| 1. Drive-by Downloads | ↑ | ↑ | ↑ | ↑ | | ↑ | ↑ | |
| 2. Worms/Trojans | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ |
| 3. Code Injection | ↑ | ↑ | ↑ | ↻ | ↑ | ↑ | ↑ | |
| 4. Exploit Kits | ↑ | ↻ | ↑ | ↑ | ↑ | ↑ | ↑ | |
| 5. Botnets (Zombi PC Ağı) | ↻ | ↑ | ↑ | ↑ | ↑ | | | |
| 6. Fiziksel Zarar/ Hırsızlık/Kayıp | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ |
| 7. Kimlik Hırsızlığı/ Dolandırıcılık | ↑ | | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ |
| 8. Hizmetin Engel-lenmesi(DoS) | ↑ | ↑ | | | ↑ | | | ↑ |
| 9. Phishing (Oltalama) | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ |
| 10. İstenmeyen e-posta | ↻ | | | ↑ | | | | ↑ |
| 11. Rogueware/ Ransomware/ Scareware | ↑ | | | | | | | |
| 12. Veri İhlali | ↑ | | ↑ | | ↑ | ↑ | ↑ | ↑ |
| 13. Bilgi Sızıntısı | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ |
| 14. Hedefli Saldırılar | ↑ | ↑ | | | | ↻ | ↑ | ↑ |
| 15. Watering Hole | ↑ | | | | | | | |

Trends: ↓ Azalan ↻ Sabit ↑ Artan

Kaynak: ENISA İnternet Tehdit Raporu, 2013

2013 yılındaki mevcut tehdit analizleri, 2012 yılı sonuçları ile karşılaştırıldığında, aşağıdaki tabloda da görüldüğü üzere epeyce değişiklik olmuştur. Buna ek olarak, tehdit sıralamasında değişiklikler de tablo 3.3'de gösterilmektedir.

Tablo 3.3. 2012 ve 2013 Yılı Güncel Tehditlerin Karşılaştırılması

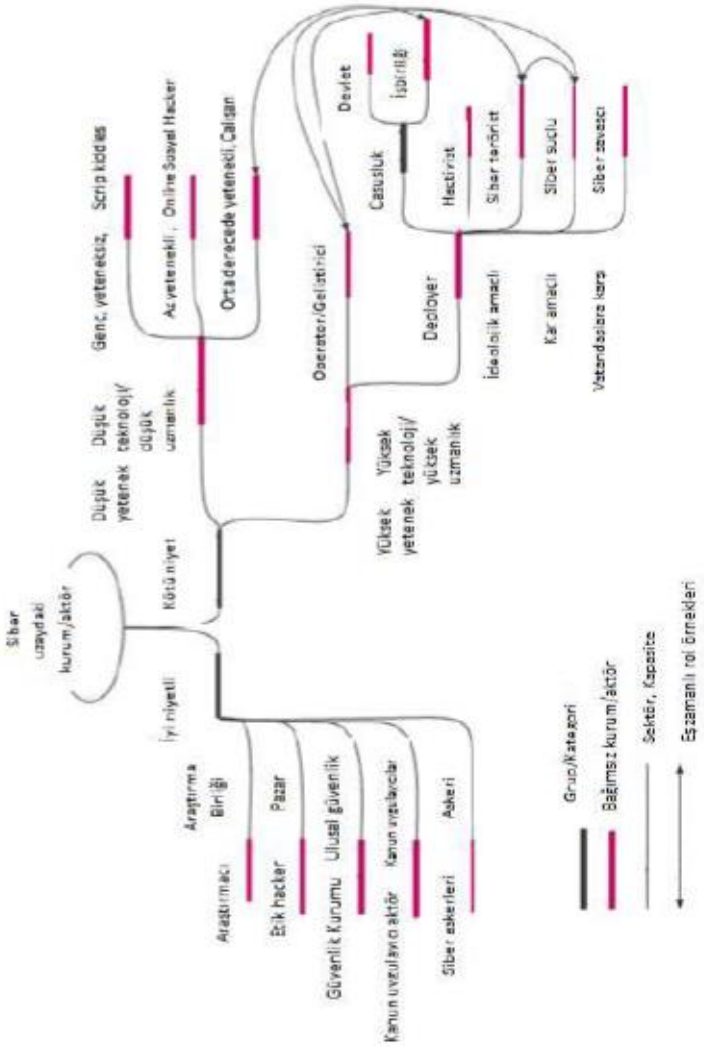
| Top Tehditler 2012 | 2012 yılı Eğilimleri Değerlendirilmesi | Top Tehditler 2013 | 2013 yılı Eğilimleri Değerlendirilmesi | Sıralamadaki Değişiklikler |
|---|---|---|---|---|
| 1. Drive-by Exploits (Drive-by download) | ↑ | 1. Drive-by downloads | ↑ | → |
| 2. Worms/Trojans | ↑ | 2. Worms/Trojans | ↑ | → |
| 3. Code Injection | ↑ | 3. Code Injection | ↑ | → |
| 4. Exploit Kits | ↑ | 4. Exploit Kits | ↑ | → |
| 5. Botnets (Zombi PC Ağı) | ↑ | 5. Botnets (Zombi PC Ağı) | ⊃ | → |
| 6. Hizmetin Engellenmesi (DoS) | ⊃ | 6. Fiziksel Zarar/Hırsızlık/Kayıp | ↑ | ↑ |
| 7. Phishing (Oltalama) | ⊃ | 7. Kimlik Hırsızlığı/ Dolandırıcılık | ↑ | ↑ |
| 8. Gizli Bilgiyi Riske Atma (Veri İhlali) | ↑ | 8. Hizmetin Engellenmesi (DoS) | ↑ | ↓ |
| 9. Rogueware/Ransomware /Scareware | ⊃ | 9. Phishing (Oltalama) | ↑ | ↓ |
| 10. İstenmeyen e-posta | ↓ | 10. İstenmeyen e-posta | ⊃ | → |
| 11. Hedefli Saldırılar | ↑ | 11. Rogueware/Ransomware /Scareware | ↑ | ↓ |
| 12. Fiziksel Zarar/Hırsızlık/Kayıp | ↑ | 12. Veri İhlali | ↑ | ↓ |
| 13. Kimlik Hırsızlığı | ↑ | 13. Bilgi Sızıntısı | ↑ | ↑ |
| 14. Bilgi Sızıntısı | ↑ | 14. Hedefli Saldırılar | ↑ | ↓ |
| 15. Arama Motoru Zehirlenmesi (Delil olmadığından tehdit listeden kaldırılmıştır.) | ⊃ | 15. Watering Hole | ↑ | ↑ |
| 16. Sahte Sertifikalar (Worms/trojan ile bütünleşiktir) | ↑ | | | |

↓ Azalan ⊃ Sabit ↑ Artan
↑ Yükselişte → Aynı ↓ Azalışta

Kaynak: ENISA İnternet Tehdit Raporu, 2013

Siber uzaydaki aktörlerin genel görünümü (saldırganın niyeti, yeteneği, amacı vb.) şekil 3.28'de detaylı olarak gösterilmektedir.

Şekil 3.28 Siber Uzaydaki Kurumların/Aktörlerin Genel Görünümü




Kaynak: ENISA İnternet Tehdit Raporu, 2013

Tablo 3.4 ise; en çok görünen tehditlerin tehdit aktörleri ile ilişkisini göstermektedir.

Tablo 3.4 En Çok Görünen Tehditlerin Tehdit Aktörleri ile İlişkisi

| | Tehdit Aktörleri | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Kurum | Ulus Devlet | Hactivist | Siber Terörist | Siber Suçlu | Siber Savaşçı | Script Kiddies | Online Sosyal Hacker | Çalışan |
| Drive-by Exploit | | ✓ | | | ✓ | | | | |
| Worms/Trojans | | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Code Injection | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Exploit Kits | | | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Botnets | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| Fiziksel Zarar/ Hırsızlık/Kayıp | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kimlik Hırsızlığı/ Dolandırıcılık | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Denial of Service | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Phishing-Oltalama | ✓ | ✓ | | | ✓ | | | ✓ | |
| Spam | ✓ | | | | ✓ | | | ✓ | |
| Rogueware/Ransomware/Scareware | | | | | ✓ | | | | |
| Veri İhlali | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Bilgi Sızıntısı | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Hedefli Saldırılar | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Watering hole | ✓[178] | ✓ | | | ✓ | ✓ | | | |

Kaynak: ENISA İnternet Tehdit Raporu, 2013

Kritik altyapılar ve ana bileşenlerinden olan Endüstriyel Kontrol Sistemleri (ICS) hâla potansiyel tehdit hedefi olarak görülmektedir. Tablo 3.5 kritik altyapılarda yaşanan tehditleri ve tehdit eğilimlerini göstermektedir.

Tablo 3.5 Kritik Altyapılar Alanındaki Tehditler ve Yükselen Trendler

| | Gelişen tehditler | Tehdit eğilimleri |
|---|---|---|
| 1. | Worms/Trojans (ICS gibi şebeke altyapısının önemli kısmını etkilemektedir.) | ↑ |
| 2. | Code Injection | ↑ |
| 3. | Drive-by Downloads | ↑ |
| 4. | Exploit Kits | → |
| 5. | Fiziksel Hırsızlık/ Kayıp/ Zarar görme | ↑ |
| 6. | Hizmetin Engellenmesi | ↑ |
| 7. | Botnets (Zombi PC Ağı) | ↑ |
| 8. | İstenmeyen e-posta | ↑ |
| 9. | Bilgi Sızıntısı | → |
| 10. | Hedefli Saldırı | → |

↓ Azalan → Sabit ↑ Artan

Tablo 3.6. Mobil Bilişim Alanında Tehditler ve Yükselen Trendler

| | | |
|---|---|---|
| 1. | Worms/Trojans | ↑ |
| 2. | Fiziksel Hırsızlık/ Kayıp/ Zarar görme | ↑ |
| 3. | Drive-by Downloads | ↑ |
| 4. | Exploit Kits | ↑ |
| 5. | Code Injection | ↑ |
| 6. | İstenmeyen e-posta | ↑ |
| 7. | Kimlik Hırsızlığı | ↑ |
| 8. | Bilgi Sızıntısı | ↑ |
| 9. | Botnets (Zombi PC Ağı) | ↑ |
| 10. | Veri İhlali | ↑ |

↓ Azalan → Sabit ↑ Artan

Kaynak: ENISA Internet Tehdit Raporu, 2013

Çevrimiçi sosyal faaliyetlerin artırması ve mobilleşmesi, eğlence, eğitim ve meslek hayatı ile ilgili faaliyetlerin sosyal medya üzerinden yapılması sonucunda, sosyal medya; toplama, bilginin yaygınlaştırılması ve pazarlama konusunda iletişimin ana kanalı olmuştur. Sosyal medyanın kullanımı ile birlikte artan kimlik hırsızlığı, sahte haberler, sahte sosyal hesapları gibi olgular sonucu, sosyal medya hackleme alanlarında en ön sıralarda yerini almıştır. Bu konularda sosyal medyanın çok hızlı yayılım alanı olduğu gözlemlenmektedir.

Sosyal ağlarda en çok ortaya çıkan tehditler Tablo 3.7'de gösterilmektedir.

Tablo 3.7. Sosyal Ağlardaki Tehditler ve Yükselen Trendler

| | | |
|---|---|---|
| 1. | Worms/Trojans | ↑ |
| 2. | Bilgi Sızıntısı | ↑ |
| 3. | Phishing (Oltalama) | ↑ |
| 4. | İstenmeyen e-posta | ↑ |
| 5. | Kimlik Hırsızlığı | ↑ |
| 6. | Exploit Kits | ↑ |
| 7. | Fiziksel Hırsızlık/ Kayıp/ Zarar görme | ↑ |
| 8. | Drive-by Downloads | ↑ |
| 9. | Code Injection | ⇄ |
| 10. | Botnets (Zombi PC Ağı) | ↑ |

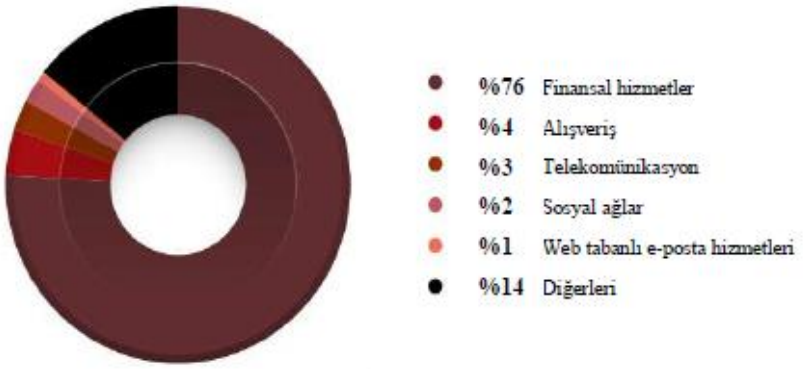
↓ Azalan ⇄ Sabit ↑ Artan

Kaynak: ENISA İnternet Tehdit Raporu, 2013

### 3.3.7. ITU "2013 yıllık güvenlik özeti/genel bakışı" raporu

ITU "2013 Yıllık Güvenlik Özeti/Genel Bakışı" raporu, siber suçların değerlendirilmesine ilişkin yararlı bilgiler sağlamaktadır. Rapor'da 2013 yılı en popüler mobil güvenlik tehditleri şekil 3.29'da gösterildiği üzere %76'lık bir oranla finansal hizmetler alanına yönelmiştir.

Şekil 3.29. 2013 Yılı En Popüler Mobile Güvenlik Tehditleri




Kaynak: ITU, 2013

Şekil 3.30'da görüldüğü üzere, 2013 yılında endüstri alanına yönelik hedeflerde ise; hükümet web sitelerinin, hedeflenen saldırılardan en fazla zarar gören alan olduğu gözlemlenmiştir.

Şekil 3.30. 2013 Yılı Endüstri Alanına Yönelik Hedefler

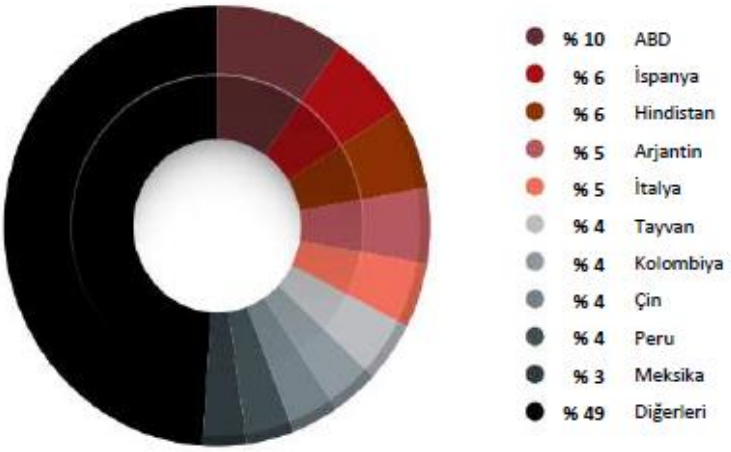

Kaynak: ITU, 2013

2013 yılında hedeflenen saldırılardan en çok etkilenen 20 ülke arasında Türkiye'de yer almaktadır. Şekil 3.31, 2013 yılı boyunca izlenmekte olan hedefe yönelik saldırılara ilişkin ITU'nun bulgularını göstermektedir. Asya'da özellikle Japonya ve Tayvan'a yönelik çok saldırı olmuştur.

Şekil 3.31. 2013 Yılı Boyunca İzlenmekte Olan Hedefe Yönelik Saldırılarda ITU'nun Bulguları


Kaynak: ITU, 2013

Şekil 3.32 En Çok Spam Gönderen Ülkeler




Kaynak: ITU, 2013

### 3.3.8. CISCO 2014 yıllık güvenlik raporu

CISCO merkezi San Jose, California'da olan Amerikan çok uluslu bir ağ teknolojileri şirketidir. Dünyada internet altyapısında ve kurumsal ağlarda kullanılan aktif cihazların çoğu CISCO firması tarafından üretilmektedir (Wikipedia, 2014a).

CISCO 2014 Yıllık Güvenlik Raporunda, CISCO tarafından günlük olarak tespit edilen tehditler aşağıda belirtilmiştir (CISCO 2014, 2014):

• 4.5 milyar e-posta engellenmektedir,

• 80 milyon web istekleri engellenmektedir,

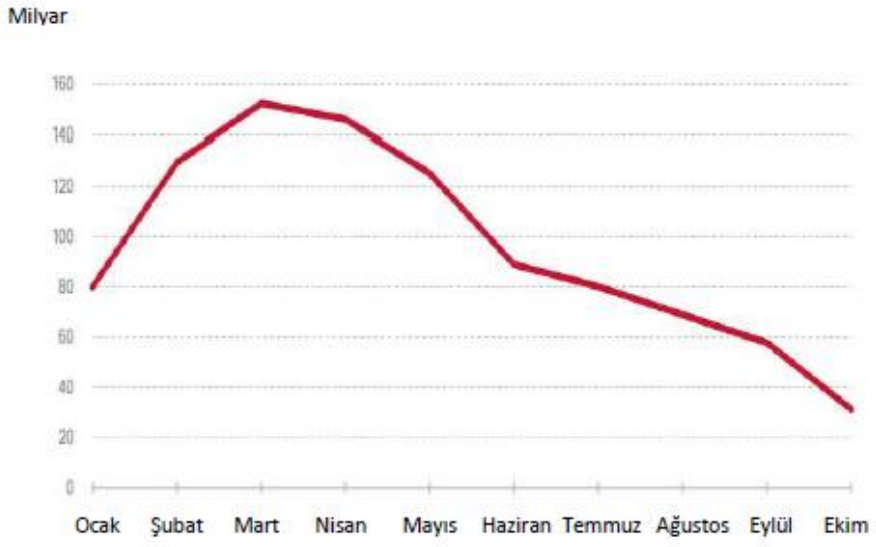
• 6450 uç nokta dosya tespiti ortaya çıkmaktadır,

• 3186 uç nokta ağ tespiti ortaya çıkmaktadır,

• 50,000 ağa izinsiz girme durumu tespit edilmektedir.

CISCO Tehdit Araştırma Analiz ve Haberleşme (TRAC) tarafından toplanan verilere göre, şekil 3.33'de de görüldüğü üzere, 2013 yılında küresel spam hacminde düşüş gözlemlenmektedir.

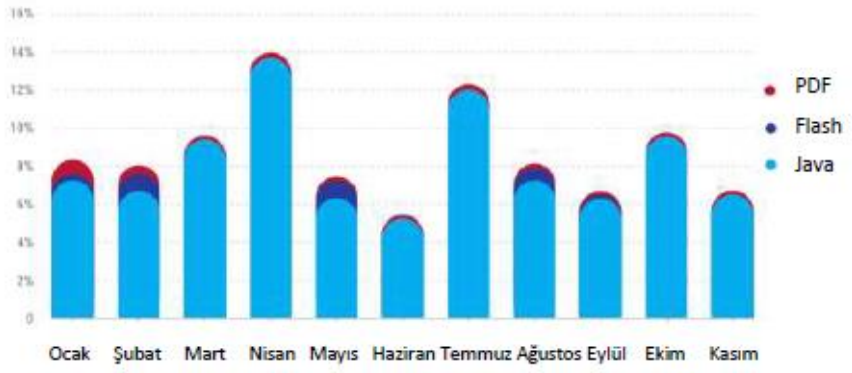
Şekil 3.33. Küresel Spam Hacmi 2013




Kaynak: CISCO 2014, 2014

Güvenliği zayıflatmaya yönelik web tabanlı tehditlerde, CISCO verilerine göre, Java programlama dili açıkları, çevrimiçi suçlular tarafından en sık kullanılan hedef olmaya devam etmektedir.

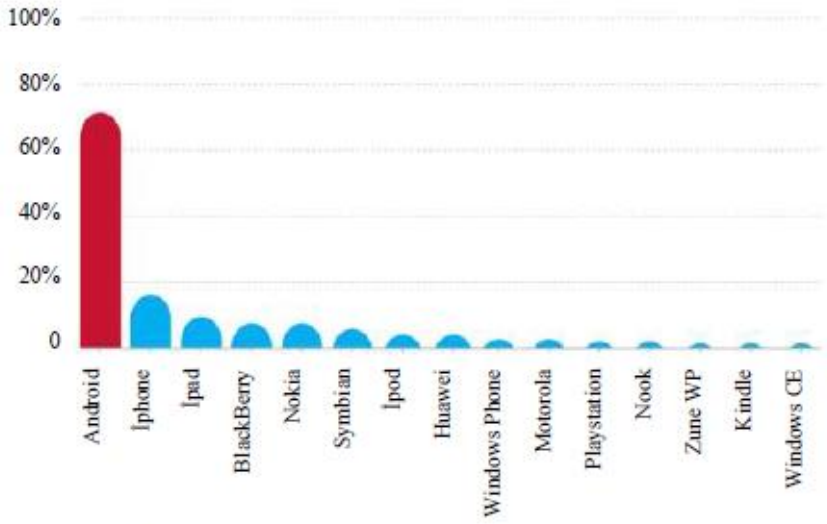
Şekil 3.34 PDF, Flash ve Java ile Oluşturulan Kötü Amaçlı Saldırılar 2013




Kaynak: CISCO 2014, 2014

Şekil 3.35'de, mobil ağlarda karşılaşılan web zararlı yazılımları görülmektedir. Görüldüğü üzere, bir mobile zararlı yazılım uzmanlaşmak için bir cihaza yerleşmek istediğinde, büyük oranda Android cihazları hedef almaktadır.

Şekil 3.35. Mobil Ağlarda Karşılaşılan Web Zararlı Yazılımları




Kaynak: CISCO 2014, 2014

En yaygın zararlı yazılım %64'lük oranla Trojan'dır

Şekil 3.36. En Yaygın Zararlı Yazılım Kategorileri


Kaynak: CISCO 2014, 2014

Raporda, ilaç ve kimya sanayi ve elektronil üretim gibi yüksek kar getiren şirketlerin web zararlı karşılaşmada yüksek oranlara sahip olduğu görülmektedir. Rapor'da, nispeten düşük riskli olan tarım ve madencilik endüstri sektöründe kötü amaçlı yazılım ile karşılaşmada olağanüstü büyüme gözlemlendiği belirtilmiştir (CISCO 2014, 2014).

# 4. TÜRKİYE'DE SİBER GÜVENLİK ÇALIŞMALARI

Bu bölümde, diğer ülke örnekleri ve uluslararası kuruluşlarda siber güvenlik alanında yapılan çalışmaların incelenmesinin ardından, Türkiye'de bu alanda ne tür çalışmalar yapıldığı, mevzuatta siber güvenliğin yeri, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nın amacı ve kritik altyapıların önemi değerlendirilmektedir.

## 4.1. Türkiye'deki Mevcut Durum

Türkiye'de siber güvenlik faaliyetleri Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinasyonunda ilgili kamu kurum ve kuruluşları, özel sektör, üniversiteler ve dernekler ile birlikte yürütülmektedir.

Siber güvenliğe ilişkin görev ve sorumlulukları bulunan ve bu alanda aktif çalışmalar yapan *başlıca kurumlar* aşağıda sıralanmıştır:

- Bilgi Teknolojileri ve İletişim Kurumu (BTK)

  BTK tarafından yürütülen siber güvenlik ile ilgili çalışmaların en önemlileri arasında siber güvenlik tatbikatları yer almaktadır. Siber güvenliğin sağlanmasına yönelik girişimler içerisinde uzmanlık seviyesinin geliştirilmesi, bilgi güvenliği standartlarının uygulanması ve kullanıcı eğitimlerinin yanı sıra, siber güvenlik konusunda farkındalığın arttırılmasına yönelik çalışmalarda siber güvenlik tatbikatları önemli bir yer tutmaktadır. Ayrıca; BTK bünyesinde doğrudan kurum başkanına bağlı olarak faaliyet göstermekte olan TİB (Telekomünikasyon İletişim Başkanlığı), siber güvenliğe ilişkin önemli çalışmaların yapıldığı bir kurumdur (BTK, 2014a).

- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)

  Ulusal siber güvenlik kapasitesinin arttırılmasına yönelik çalışmalar gerçekleştirmek amacıyla kurulan SGE (Siber Güvenlik Enstitüsü)'nin faaliyetleri

1997 yılında Bilişim Sistemleri Güvenliği (BSG) birimi adı ile TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) altında başlamıştır. 2012 yılından bu yana ise TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak faaliyetlerini sürdürmektedir. SGE; siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte; askeri kurumlara, kamu kurum ve kuruluşlarına ve özel sektöre çözüme yönelik projeler gerçekleştirmektedir (TÜBİTAK BİLGEM, 2013).

- TSK Siber Savunma Merkezi Başkanlığı

  Gelişmiş siber savunma ikaz ve tepki sistemlerine sahip güçlü bir merkezi siber savunma yeteneği kazanmak amacıyla 2012 yılında Genelkurmay Başkanlığında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur (Çifci, 2010).

- Emniyet Genel Müdürlüğü / Siber Suçlarla Mücadele Daire Başkanlığı

  Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli daire başkanlıklarının ve taşra teşkilatındaki birimlerin dağınık yapısının tek bir çatı altında toplanması, mükerrer yatırımların önüne geçilmesi, siber suçlarla mücadelenin etkin ve verimli olarak yürütülmesini sağlamak amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. 28/02/2013 tarih ve B.05.1.EGM.0.65.35539/31772 sayılı Bakanlık Oluruna istinaden Bilişim Suçlarıyla Mücadele Daire Başkanlığının ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir (EGM, 2013).

Bilgi güvenliği ve siber güvenliğe ilişkin aktif çalışmaların yapıldığı *sivil toplum kuruluşları* aşağıda sıralanmıştır:

- Bilgi Güvenliği Derneği

  Bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, üyelerinin

mesleki gelişimini arttırmak ve kamu yararına faaliyet gösteren dernek olmak amacı ile kurulan bir sivil toplum kuruluşudur (BGD, 2013).

Bilgi güvenliği ve siber güvenliğe ilişkin konferans, sempozyum, seminer, kurs ve benzeri etkinlikler düzenlenmekte, bilgi dokümanları hazırlanmakta ve çalışma grupları oluşturulmaktadır.

- Siber Güvenlik Derneği

  Siber Güvenlik Derneği 2011 yılında kurulmuş bir sivil toplum kuruluşudur. Amaçları aşağıda sıralanmıştır (Çifci, 2013, s.377):

  - Ulusal siber güvenlik kültürünün oluşturulmasına ve kritik bilgi altyapılarının korunmasına katkıda bulunmak,
  - Sektörler arasında siber güvenlik konusunda gerçekleşen bilgi alışverişini sağlamak amacıyla teknik, bilimsel, sosyal ve kültürel faaliyetleri yürütmek,
  - Üyelerin mesleki gelişimini artırmak,
  - Türkiye'yi yurtdışında ilgili kurullarda ve toplantılarda temsil etmektir.

20 Ekim 2012 tarihli ve 28447 sayılı resmi gazete'de yayımlanarak yürürlüğe giren, Bakanlar Kurulu'nun 3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Karar" ile siber güvenliğe ilişkin çalışmalara yasal dayanak oluşturulmuştur. 2012 yılı öncesinde, bilgi güvenliği ve siber güvenlik alanında Türkiye'de temel teşkil edecek önemli çalışmalar şunlardır:

- 24/03/2005 tarih ve sayılı Yüksek Planlama Kurulu kararı ile tebliğ olarak resmi gazete'de yayımlanan "e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı"

  Eylem Planı'nın içerisinde; bilgi güvenliği ve siber güvenliğe ilişkin eylem maddeleri ana başlıkları aşağıda sıralanmıştır (Tebliğ, 2005):

  • Kamu kurumlarına ait bilgi güvenliği risk analizi,

  • Kamu kurum ve kuruluşlarında açık kaynak kodlu yazılımların uygulanabilirliği,

• Güvenli internet kullanımı konusunda toplumda farkındalık yaratılması,
• Bilişim suçları kanunu,
• İstenmeyen elektronik iletişimle mücadeledir.

- 11/7/2006 tarih ve 38 sayılı Yüksek Planlama Kurulu kararı ile 28 Temmuz 2006 tarihli ve 26242 sayılı resmi gazete yayımlanan "Bilgi Toplumu Stratejisi (2006-2010)" ve "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)"

2006-2010 yıllarını kapsayan eylem planında 7 temel stratejik öncelik olduğu belirtilmiştir ve gerçekleşmesi hedeflenen toplam 111 adet eylem maddesi bulunmaktadır. Eylem planında, bilgi toplumu stratejisi yaklaşımı şekil 4.1'de özetlenmiştir (Kurul Kararı, 2006).

Şekil 4.1. Bilgi Toplumu Stratejisi Yaklaşımı


Kaynak: Kurul Kararı, 2006

Bilgi Toplumu Stratejisi Eylem Planı'nın içerisinde; bilgi güvenliği ve siber güvenliğe ilişkin eylem maddeleri 6 ana başlık altında aşağıda sıralanmıştır (Kurul Kararı, 2006):

- İnternet Güvenliği (Eylem maddesi numarası: 10)

**Açıklama**

• Bireylerin BİT kullanımına yönelik motivasyonlarının artırılması amacıyla İnternet ortamını güvenli hale getirecek yasal düzenlemeler gerçekleştirilecektir.

• İnternet üzerinde çeşitli denetim ve yasakların düzenlenmesi, gereklilik ve ölçülülük kriterlerine bağlı kalınması şartıyla, çocukların zihinsel ve bedensel sağlığının, kişilik haklarının, ailenin ve kamu düzeninin korunması sağlanacaktır.

**10 numaralı eyleme İlişkin Gelişmeler/Değerlendirme**

Eylem ile, internet ortamında yapılan her türlü yayının denetiminin sağlanarak konusu suç teşkil eden yayınlarla mücadele amacıyla etkin bir yasal koruma sisteminin geliştirilmesi hedeflenmiştir. Eylemin amacına ulaşması için internet ortamında güvenliğin sağlanmasına ilişkin yasal mevzuat oluşturulmasından sorumlu kurum Adalet Bakanlığı tarafından yapılan Ağustos 2006'da Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı adlı bir taslak çalışma kamuoyuyla paylaşılmış ancak söz konusu taslağın yasalaşma süresinin uzaması nedeniyle 2007 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 23.05.2007 tarihli Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. "Bilgi toplumu stratejisi ve eylem planı nihai değerlendirme raporu"nda, söz konusu Kanuna, getirdiği yükümlülükler ve site kapatma kararları sebebiyle kamuoyundan bir takım eleştirilerin gelmesi üzerine, 5651 sayılı Kanunda tadilat yapılması amacıyla mülga İnternet Kurulu bünyesinde çeşitli çalışmalar yürütüldüğü belirtilmektedir (Bilgi Toplumu, 2013).

- Kamu internet siteleri standardizasyonu ve barındırma hizmeti (Eylem maddesi numarası: 27)

  **Açıklama**:

  • Kamu kurumları internet siteleri için görsel, hizmet kalitesi, içerik, güvenlik, kimlik yönetimi ve kullanılabilirlik standardizasyonu sağlanacaktır.

  • Kamu İnternet sitelerinin özürlüler tarafından da kullanılabilmesine yönelik geliştirmeler yapılacaktır.

  • Talep eden kamu kuruluşlarının internet siteleri merkezi olarak barındırılacaktır.

  **27 numaralı eyleme İlişkin Gelişmeler/Değerlendirme**

  Eylem kapsamında yürütülen çalışmalar sonucunda, kamu kurumlarının internet sitelerinin tasarımında uymaları gereken kuralları ve prensipleri tanımlayan Kamu İnternet Siteleri Standartları ve Önerileri Rehberi hazırlanmış ve bu rehber www.kakis.gov.tr internet adresinden yayınlanmıştır. Ayrıca aynı adreste, hazırlanan internet sitelerinin Rehberdeki kurallara uygunluğunu test etmek amacıyla kullanılabilen bir site değerlendirme aracı bulunmaktadır. Diğer taraftan, 2007/4 sayılı Başbakanlık Genelgesi ile TÜBİTAK koordinasyonunda hazırlanan Kamu Kurumları İnternet Siteleri Kılavuzuna (Sürüm 1.0) kamu kurum ve kuruluşlarının uyumu zorunlu hale getirilmiştir. Birlikte Çalışabilirlik Esasları Rehberinde (Sürüm 2.1), 2007/4 sayılı Başbakanlık Genelgesi ile yürürlüğe konulan kılavuza uyum zorunluluğu getirilirken, TÜRKSAT tarafından hazırlanan Kamu İnternet Siteleri Standartları ve Önerileri Rehberinin geliştirilmesi öngörülmüştür. Ayrıca, Birlikte Çalışabilirlik Esasları Rehberinde (Sürüm 2.1) W3C Erişilebilirlik Kılavuzu 2.0 (2008) isimli standarda kamu kurumlarının internet sitelerinin erişilebilirliği için önerilen standart olarak yer verilmiştir. "Bilgi toplumu stratejisi ve eylem planı nihai değerlendirme raporu"nda, kamu kurumlarının internet sitelerinin barındırılması açısından TÜRKSAT tarafından bir altyapı kurulmuş olsa da, TÜRKSAT'ın kamu kurumlarına bu eylemde kurgulanan şekilde hizmet sağlayamadığı ifade edilmektedir. Raporda, hali hazırda çeşitli kamu kurumlarının internet sitesi

barındırma, felaket kurtarma merkezi, iş sürekliliği merkezi gibi isimlerle farklı yatırımlara yöneldiği belirtilmektedir (Bilgi Toplumu, 2013).

- Kamu Güvenli Ağı (Eylem maddesi numarası: 70)

  **Açıklama**:

  Kamu kurumlarının farklı geniş alan ağ altyapısı yatırımları yerine kamunun bu yöndeki ihtiyaçları ve internet çıkışları için ortak bir güvenli iletişim altyapısı kurulacak, e-devlet mimarisinin omurgası oluşturulacaktır.

  Tez çalışmasının 6. bölümünde bu konu detaylı olarak incelenmiştir.

- Kamuda Açık Kaynak Kodlu Yazılım Kullanımı (Eylem maddesi numarası: 74)

  **Açıklama**:

  Kamuda açık kaynak kodlu yazılım kullanımı için örnek oluşturmak üzere bir kurumda pilot uygulama yapılacak ve bu uygulamada elde edilen tecrübelere göre açık kaynak kod kullanımının uygulanabilirlik analizi geliştirilecektir.

  **74 numaralı eyleme İlişkin Gelişmeler/Değerlendirme**

  2009 Aralık itibarıyla eylemin sorumlu kurumu olan TÜBİTAK ile Enerji Piyasası Düzenleme Kurumu (EPDK) arasında kurumsal tümleşik bilişim sistemi çözümleri, açık kaynak kodlu yazılım göçü planlaması ve gerçekleştirme konularında bir sözleşme imzalanmış ve çalışmalara başlanmıştır. Ancak, gelinen aşamada, proje kapsamında elde edilen bilgi birikiminin değerlendirildiği bir uygulanabilirlik analizi gerçekleştirilememiştir (Bilgi Toplumu, 2013).

- Bilgi Güvenliği ile İlgili Yasal Düzenlemeler (Eylem maddesi numarası: 87)

  **Açıklama**:

  • Ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal altyapıyla ilgili düzenleme yapılacak ve uygulamaya konulacaktır.

• Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Taslağı yasalaştırılacaktır.

**87 numaralı eyleme İlişkin Gelişmeler/Değerlendirme**

Milli Savunma Bakanlığı tarafından yürütülen Ulusal Bilgi Güvenliği Kanun Tasarısı Taslağı çalışmaları 24.07.2008 tarihinde Kalkınma Bakanlığında yapılan toplantıda alınan karar neticesinde Adalet Bakanlığına devredilmiştir. Adalet Bakanlığı Kanunlar Genel Müdürlüğünün 2009-2010 yılları arasında yaptığı hazırlık çalışmaları neticesinde söz konusu taslak belirli bir olgunluğa ulaşmıştır (Bilgi Toplumu, 2013). Söz konusu taslak, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda yer alan 2 numaralı eylem maddesi kapsamında "Siber Güvenlik Kanunu" tasarısına dönüştürülmüş olup, çalışmaları Adalet Bakanlığı koordinasyonunda devam etmektedir. "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik", 24 Temmuz 2012 tarih ve 28363 sayılı Resmi Gazete'de yayımlanmıştır (Bilgi Toplumu, 2013).

- Ulusal Bilgi Sistemleri Güvenlik Programı (Eylem maddesi numarası: 88)

**Açıklama:**

• Siber âlemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "bilgisayar olaylarına acil müdahale merkezi (CERT)" kurulacaktır.

• Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır.

**88 numaralı eyleme İlişkin Gelişmeler/Değerlendirme**

Eylem kapsamında, TÜBİTAK-UEKAE bünyesinde Türkiye Bilgisayar Olaylarına Acil Müdahale Ekibi (TR-BOME) koordinatörlüğü kurulmuştur. Bazı

kanu kurumlarında yürütülen ortak çalışmalar sonucunda, bu kurumlarda da BOME oluşturulmuştur. Yine bu eylem kapsamında bilgi güvenliğine ilişkin en iyi uygulamaların paylaşıldığı bir platform olarak Ulusal Bilgi Güvenliği Kapısı www.bilgiguvenligi.org.tr hayata geçirilmiştir. Bilgi Güvenliği Yönetim Sistemi (BGYS) pilot uygulamaları kapsamında, Başbakanlık, Adalet Bakanlığı, Maliye Bakanlığı Muhasebat Genel Müdürlüğü ve Sayıştay Başkanlığında risk analizi çalışmaları tamamlanmıştır (Bilgi Toplumu, 2013).

### 4.2. Mevzuatta Siber Güvenlik

Siber güvenlik konusu ile ilişkilendirilebilen, birincil ve ikincil mevzuatlar bu başlık altında değerlendirilmektedir.

#### 4.2.1. Birincil mevzuatlar

Siber güvenlik kapsamında değerlendirilebilecek, birincil mevzuat düzenlemeleri (mevcut kanunlar) aşağıda listelenmiştir:

**I. 5809 sayılı "Elektronik Haberleşme Kanunu"**

Bu Kanunun amacı; elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesidir (Elektronik Haberleşme Kanunu, 2008).

19 Şubat 2014 tarih ve 28918 sayılı resmi gazete'de yayımlanan "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik

Yapılmasına Dair Kanun" ile 5809 Sayılı Elektronik Haberleşme Kanunu'na şu maddeler eklenmiştir (Kanun, 2014a):

- 5809 sayılı Elektronik Haberleşme Kanununun "Bakanlığın görev ve yetkileri" başlıklı 5 inci maddesinin birinci fıkrasına aşağıdaki bent eklenmiştir.

  h) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, Siber Güvenlik Kurulunun sekretaryasını yapmak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.

- 5809 sayılı Kanunun "Kurumun görev ve yetkileri" başlıklı 6 ncı maddesinin birinci fıkrasının (ü) bendinden sonra gelmek üzere aşağıdaki (v) bendi eklenmiş ve diğer bent buna göre teselsül ettirilmiştir.

  v) Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek.

- 5809 sayılı Kanuna aşağıdaki ek madde eklenmiştir.

  Siber Güvenlik Kurulu

  EK MADDE 1 – (1) Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını

ve koordinasyonunu sağlamak amacıyla; Bakanın başkanlığında Siber Güvenlik Kurulu kurulmuştur. Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir.

(2) Kurulun görevleri şunlardır:

- Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak.
- Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak.
- Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.
- Kanunlarla verilen diğer görevleri yapmak.

(3) Siber Güvenlik Kurulunun çalışma usul ve esasları Başbakanlıkça çıkartılacak yönetmelikle belirlenir.

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

Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir (Kanun, 2007).

19 Şubat 2014 tarih ve 28918 sayılı Resmi Gazete'de Yayımlanan "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname İle Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun" ile 5651 sayılı kanunun 10. maddesine siber güvenliğe ilişkin şu fıkra eklenmiştir:

"(6) Başkanlık, ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve

kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar (Kanun, 2007).

### III. 5237 sayılı "Türk Ceza Kanunu"

5237 sayılı "Türk ceza kanunu" içerisinde yer alan "Bilişim Alanında Suçlar" başlıklı 10. bölümde, bu kapsam da değerlendirilebilecek 4 madde bulunmaktadır.

"Bilişim Alanında Suçlar" bölümünde yer alan madde başlıkları ve kapsamı aşağıda yer almaktadır (Türk Ceza Kanunu, 2004):

- Bilişim sistemine girme

**MADDE 243.**

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

- Sistemi engelleme, bozma, verileri yok etme veya değiştirme

**MADDE 244.**

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

- Banka veya kredi kartlarının kötüye kullanılması

**MADDE 245.**

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

- Tüzel kişiler hakkında güvenlik tedbiri uygulanması

**MADDE 246.**

(1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

### 4.2.2. İkincil mevzuatlar

Siber güvenlik kapsamında değerlendirilebilecek, ikincil mevzuat düzenlemeleri (yönetmelik tebliğ v.b ) aşağıda listelenmiştir:

### I. Elektronik Haberleşme Güvenliği Yönetmeliği

Bu yönetmeliğin amacı, elektronik haberleşme güvenliğine ilişkin usul ve esasları düzenlemektir. Bu yönetmelik, işletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması için tehditlerden ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesi veya azaltılmasına ilişkin olarak alacakları tedbirlere yönelik usul ve esasları kapsar. Kişisel bilgilerin işlenmesi ve gizliliğinin korunması, bu yönetmelik kapsamı dışındadır (Elektronik Haberleşme Güvenliği Yönetmeliği, 2008).

### II. Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulamasına İlişkin Tebliğ

Bu Tebliğin amacı; yukarıda belirtilmiş olan Elektronik Haberleşme Güvenliği Yönetmeliği'nin "Elektronik Haberleşme Güvenliğini Sağlama Yükümlülüğü" başlıklı 11 inci maddesinin birinci fıkrasının uygulanmasına ilişkin usul ve esasları düzenlemektir (Tebliğ, 2010).

### III. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

Bu Yönetmeliğin amacı, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemektir. Haberleşmenin içeriğine ilişkin verilerin saklanması bu yönetmeliğin kapsamına dâhil değildir (Yönetmelik, 2010).

## IV. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı

20 Ekim 2012 tarih ve 28447 sayılı resmi gazete'de yayımlanarak yürürlüğe giren bu Kararın amaç ve kapsamı, kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemektir (Bakanlar Kurulu Kararı, 2012b).

2012/3842 sayılı bakanlar kurulu kararı ile kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğin korunmasına yönelik tedbirlerin alınması ve bilgi-iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasların düzenlenmesi görevi, Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir (Bakanlar Kurulu Kararı, 2012b).

Ulaştırma Denizcilik ve Haberleşme Bakanı başkanlığında,

Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları müsteşarları, 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 Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur (Bakanlar Kurulu Kararı, 2012b).

Bu karar kapsamında, Ulaştırma Denizcilik ve Haberleşme Bakanlığına verilmiş olan görevler şunlardır (Bakanlar Kurulu Kararı, 2012b):

a) Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak,
b) Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak,
c) Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak,
ç) Ulusal bilgi teknolojileri ve iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik altyapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmaları yapmak,
d) Ulusal Siber Güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak,
e) Ulusal Siber Güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek,
f) Bu Karar çerçevesinde diğer ülkeler ve uluslararası kuruluşlarla işbirliği yapmak,
g) Ulusal Siber Güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek,
ğ) Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek,
h) Siber Güvenlik Kurulunun sekretarya hizmetlerini yürütmek.

**IV. Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usül ve Esaslar Hakkında Tebliğ**

11 Kasım 2013 tarih ve 28818 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Tebliğ'in amacı, Siber Olaylara Müdahale Ekiplerinin kuruluş, görev ve çalışmalarına ilişkin usul ve esaslarını belirleyerek, hizmetlerin etkin ve verimli bir şekilde yürütülmesini sağlamaktır (Tebliğ, 2013).

### 4.3. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı"nın, "Bakanlığın Görev ve Yetkileri" başlıklı 5. Maddesi (a) fıkrası uyarınca, ilgili kurum/kuruluşların katkıları ile hazırlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013/4890 sayılı bakanlar kurulu kararı ile, 20 Haziran 2013 tarihli ve 28683 sayılı resmi gazetede yayımlanarak yürürlüğe girmiştir.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının **Amacı** (Bakanlar Kurulu Kararı, 2013):

- Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına, yönelik bir altyapı oluşturmaktır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, kamu bilişim sistemlerini ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerini kapsamaktadır.

2013-2014 döneminde gerçekleştirilmesi planlanan stratejik eylemler aşağıdaki 7 başlık altında gruplanmıştır (Bakanlar Kurulu Kararı, 2013):

1 Yasal Düzenlemelerin Yapılması

2 Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi

3 Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması

4 Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

5 Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri

6 Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi

7 Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

Eylem planında yer alan eylem ve alt eylemlerin bir kısmı için bitirilme tarihi belirlenmiş, periyodik olarak tekrarlanması ve sürekli olarak yürütülmesi öngörülen eylemler ise ayrıca belirtilmiştir. 2013-2014 döneminde, gerçekleştirilmesi planlanan toplam 29 adet eylem maddesi ve 86 adet alt eylem maddesi bulunmaktadır (Bakanlar Kurulu Kararı, 2013).

Eylem Planı kapsamında değerlendirilebilecek çalışmalar aşağıda sıralanmıştır:

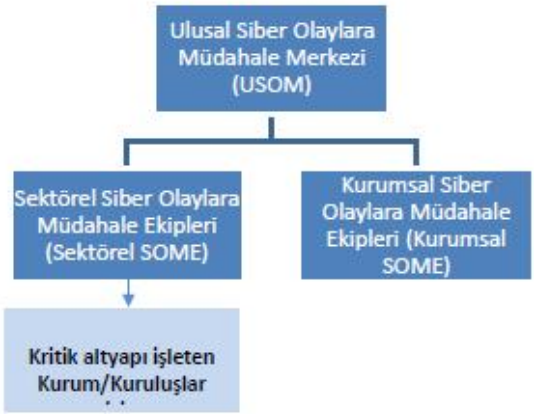
**I. Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması**

2013 yılı öncesi: Devlet Planlama Teşkilatı tarafından hazırlanan "2006-2010 Bilgi Toplumu Strateji ve Eylem Planı" 88 nolu eylem maddesi kapsamında TÜBİTAK bünyesinde, TR-BOME kurulmuştur.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı sorumluluğunda bulunan "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması" başlıklı 4 numaralı eylem maddesi kapsamında USOM, 27 Mayıs 2013 tarihinde TİB bünyesinde kurularak faaliyete başlamıştır.

USOM, Türkiye'de siber güvenlik olaylarına müdahale konusunda ulusal ve uluslararası koordinasyonun sağlanması ve siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetlerini gerçekleştirmek amacıyla kurulmuştur.

Şekil 4.2. USOM ve SOME'lerin ilişkisi




Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı, USOM'un ulusal temas noktası olarak diğer ülkelerin eşdeğer makamlarıyla ve uluslararası kuruluşlarla yakın işbirliği halinde olması gerektiğini ifade etmektedir. USOM, kamu kurum kuruşuluşları, özel sektör kuruluşları ve internet aktörleri ile işbirliği yapmakta, yine kamu kurum kuruluşları, uluslararası kuruluşlar, internet aktörleri, ilgili sektör kuruluşları, araştırma merkezleri, adli makam ve kolluk birimleri ile birlikte siber güvenlik faaliyetlerini yürütmektedir.

22.05.2013 tarih ve 2013/DK-TİB/278 sayılı Bilgi Teknolojileri ve İletişim Kurulu Kararı ile USOM görevleri, çalışma usul ve esasları belirlenmiştir. Söz konusu usul ve esaslara göre USOM'un görevleri şunlardır (USOM, 2013):

- Siber olaylara müdahale konusunda ulusal ve uluslararası koordinasyon çalışmaları yürütür.
- Siber tehditlerle ilgili olarak alarm, uyarı, duyuru faaliyetlerini yürütür. Yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesini sağlar.
- Siber güvenlik olaylarına maruz kalan kamu bilişim sistemlerine yönelik koruyucu tedbirlerin alınması konusunda koordinasyon sağlar.
- Çalışmaları esnasında, konusu suç teşkil eden veriler ile karşılaşması halinde, adli makamlar ve kolluk kuvvetleri ile koordinasyon içinde hareket eder.
- Güvenli bir iletişim kanalı üzerinden sektörel ve kurumsal SOME'ler ile bilgi paylaşımı yapar. Acil olarak alınması gereken tedbirleri bu iletişim kanalı vasıtasıyla çevrimiçi paylaşır.
- Zararlı yazılımları analiz eder, gerekmesi durumunda TÜBİTAK veya diğer kuruluşlara analiz etmek üzere gönderir.
- 7/24 esasına göre çalışır.
- Eylem planı çerçevesinde Kurulun verdiği diğer görevleri yerine getirir.
- USOM, siber güvenlik olaylarına ilişkin olarak aşağıdaki adımları takip eder;
    - Siber güvenlik olayının tespit edilmesi halinde ilgililere bilgi verir.
    - İlgililerden talep edilmesi halinde uzaktan müdahale desteği sağlar.
    - Talep edilmesi halinde kritik altyapılarda ortaya çıkan siber güvenlik zafiyetlerinin giderilmesi için yerinde müdahale desteği sağlar.
- Ayrıca USOM belirli periyotlarda kendisine bildirilen siber tehditler, gelen ihbarlar, yurtiçi ve yurtdışı kaynaklı siber saldırılar ile ilgili olarak istatistik ve rapor hazırlar.

## II. Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usül ve Esaslar Hakkında Tebliğ'in Resmi Gazete'de Yayımlanması

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda Ulaştırma, Denizcilik ve Haberleşme Bakanlığı sorumluluğunda bulunan "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması" başlıklı 4 numaralı eylem maddesi kapsamında "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usül ve Esaslar Hakkında Tebliğ" 11 Kasım 2013 tarih ve 28818 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmşitir.

Tebliğ, Sektörel ve Kurumsal SOME'lerin Kuruluşu, Yapısı, Görev ve Yükümlülükleri, USOM'la İlişkileri konularını içermektedir.

Tebliğ'e göre, Kurumsal SOME'ler, Bakanlıkların bünyesinde, hizmet gereklerine göre, Bakanlık birimlerini, bağlı, ilgili ve ilişkili kurumlarını kapsayacak şekilde kurulur. Sektörel SOME'ler ise düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulur. İhtiyaç duyulması halinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan diğer sektörlerde ilgili olduğu Bakanlık bünyesinde sektörel SOME kurulabilir.
Kurumsal ve Sektörel SOME'lerin görev ve sorumlulukları aşağıda yer almaktadır (Tebliğ, 2013):

**Kurumsal SOME'lerin görev ve sorumlulukları:**

1 Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler.

2 Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar.

3 Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini varsa birlikte çalıştığı sektörel SOME ile eşgüdüm içerisinde yürütürler. Durumdan gecikmeksizin USOM'u haberdar ederler.

4 Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar. Bunun mümkün olmaması halinde varsa birlikte çalıştığı sektörel SOME'den ve/veya USOM'dan yardım talebinde bulunabilirler.

5 Kurumsal SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.

6 Kurumsal SOME'ler kurumlarına yapılan siber olayları raporlar ve gecikmeksizin USOM ve birlikte çalıştığı sektörel SOME'ye bildirirler.

7 Kurumsal SOME'ler USOM ve/veya birlikte çalıştığı sektörel SOME tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirleri alırlar.

8 Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler.

**Sektörel SOME'lerin görev ve sorumlulukları:**

1 Sektörel SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütürler.

2 Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olayları gecikmeksizin USOM'a bildirirler.

3 Sektörel SOME'ler siber olaylara ilişkin USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları SOME'lerde gerekli tedbirlerin alınmasına yönelik çalışmaları yürütürler.

4 Sektörel SOME'ler birlikte çalıştıkları SOME'lerin yapılanması konusunda düzenleyici faaliyetleri yürütürler.

5 Sektörel SOME'ler ilgili oldukları sektörde, bilgilendirme, bilinçlendirme ve eğitim faaliyetleri ile siber güvenlikle ilgili kabiliyetlerinin geliştirilmesi ve önlemlerin alınması konusunda gerekli düzenleyici faaliyetleri yürütürler.

6 Sektörel SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştıkları SOME'lere ve USOM'a bildirirler.

7 SOME'ler 7/24 erişilebilir olan iletişim bilgilerini Sektörel SOME'lere ve USOM'a bildirirler.

8 Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olaylarda imkânları ölçüsünde gerekli desteği sağlarlar. Sektörel SOME'ler, imkânlarının yetersiz olması durumunda USOM'dan destek alırlar.

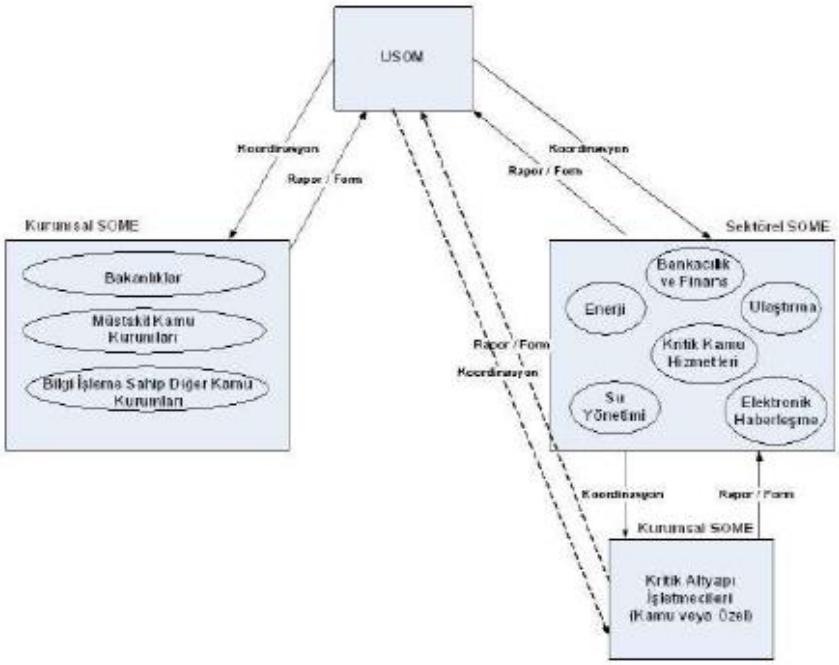
9 Sektörel SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.

10 Sektörel SOME'ler gerekmesi durumunda birlikte çalıştıkları SOME'ler arasındaki işbirliğini koordine ederler (SOME Tebliği, 2013).

**USOM ve SOME'lerin İlişkisi**

SOME'lerin USOM ile ilişkilerini varsa birlikte çalıştıkları sektörel SOME'ler üzerinden yürütmesi esastır. Birlikte çalıştıkları bir sektörel SOME olmayan kurumsal SOME'ler, faaliyetlerini doğrudan USOM ile koordineli yürütürler. USOM'un SOME'ler ile ilişkisi şekil 4.3'de detaylı olarak anlatılmaktadır.

Şekil 4.3. USOM ve SOME'lerin ilişkisi




Kaynak: BTK, 2014b

## III. Üniversitelerde Siber Güvenlik Eğitimlerinin Yaygınlaştırılması

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda "Üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması" başlıklı 20. Eylem maddesi kapsamında değerlendirilen; "Bilgi güvenliği/ Siber güvenlik konularında" aşağıda adı geçen üniversitelerde yüksek lisans ve doktora programları açılmıştır:

Tablo 4.1. Üniversitelerde Siber Güvenlik/Bilgi Güvenliği konularında Yüksek Lisans/Doktora Programları

| Üniversite | Enstitü | Program | YLS/ DR | Tezli/ Tezsiz | Eğitim Dili |
|---|---|---|---|---|---|
| Bahçeşehir Üniversitesi | Fen Bilimleri Enstitüsü | Siber Güvenlik | YLS | Tezli-Tezsiz | İngilizce |
| İstanbul Ticaret Üniversitesi | Fen Bilimleri Enstitüsü | Siber Güvenlik | YLS | Tezli-Tezsiz | Türkçe |
| Sakarya Üniversitesi | Fen Bilimleri Enstitüsü | Siber Güvenlik | YLS | Tezli | Türkçe |
| Gazi Üniversitesi | Fen Bilimleri Enstitüsü | Bilgi Güvenliği | YLS | - | Türkçe |
| İstanbul Şehir Üniversitesi | Fen Bilimleri Enstitüsü | Bilgi Güvenliği Mühendisliği | YLS | Tezli-Tezsiz | Türkçe |
| TOBB Ekonomi ve Teknoloji Üniversitesi | Fen Bilimleri Enstitüsü | Bilgi Güvenliği | YLS | Tezli | Türkçe |
| TOBB Ekonomi ve Teknoloji Üniversitesi | Fen Bilimleri Enstitüsü | Bilgi Güvenliği | YLS | Tezsiz | Türkçe |
| Hacettepe Üniversitesi | Bilişim Enstitüsü | Bilgi Güvenliği | YLS | Tezsiz | Türkçe |
| Gazi Üniversitesi | Fen Bilimleri Enstitüsü | Bilgi Güvenliği | DR | - | Türkçe |

Kaynak: Üniversitelerin web sayfalarından derlenmiştir, 2014

### IV. Siber Güvenlik Yaz Kampı

TÜBİTAK BİLGEM SGE ve Bilgi Güvenliği Akademisi işbirliğiyle üniversite öğrencilerine yönelik Siber Güvenlik Yaz Kampları düzenlenmektedir (TÜBİTAK, 2013).

### V. Sızma Testi Uzmanlığı (Beyaz Şapkalı Hacker) Eğitimleri

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda, 2. alt eylemi TSE'nin sorumluluğunda olan "Siber Güvenlik Konusunda Ürünlerin ve Hizmet Sağlayıcıların Belgelendirilmesi" başlıklı 12 numaralı eylem maddesi kapsamında çalışmalar yürütülmektedir.

Sektörden uzmanlarla beraber TSE bünyesinde oluşturulan Siber Güvenlik Özel Komiteleri bu konuda çalışmalar yürütmüş ve özel sektörün de katkısıyla 'Sızma Testi, Eğitim ve Danışmanlık Hizmeti Veren Personel ve Firmalar için Yetkilendirme Programı' ile 'Sızma Testi Teknik Kriterleri Programı' adları altında iki çalışma ortaya çıkmıştır. "Sızma Testi, Eğitim ve Danışmanlık Hizmeti Veren Personel ve Firmalar İçin Yetkilendirme Programı" ile sızma testi yapan firmaların ve kişilerin ne gibi şartları sağlaması gerektiği belirlenmiştir. Program, güvenlik testi yapan firmaların ve kişilerin belirli bir uzmanlık seviyesine ulaşmalarını ve bu uzmanlıklarını belgelendirmelerine imkân tanırken, güvenlik testi yaptıracak kurumlara da çalışacakları kişi ve firmaları belirlerken temel alacakları kriterlerin neler olması gerektiği bilgisini sunacaktır. Beyaz Hacker'ların temel görevi sistemin açıklarını tespit etmek ve bunları sistem yöneticisine bildirmek olarak tanımlanmaktadır. Böylece güvenlik testi yaptıran kurumlar sistemlerinde açıkların ve risklerin, yasadışı sızmalar olmadan tespit edilmesi imkânına kavuşacaktır. Programda Beyaz Hacker'lar için tanımlı "Stajyer Sızma Testi Uzmanı", "Kayıtlı Sızma Testi Uzmanı", "Sertifikalı Sızma Testi Uzmanı" ve "Kıdemli Sızma Testi Uzmanı" olmak üzere 4 farklı uzmanlık seviyesi belirlenmiştir (TSE, 2014).

Sızma Testi Uzmanlığı (Beyaz Şapkalı Hacker) Eğitimleri 2014 yılı Mayıs ayında başlamıştır. Teorik ve uygulamalı eğitim ve sınavlar Capture the Flag (CTF) laboratuvar ortamında gerçekleştirilecektir (TSE, 2014).

### 4.4. Kritik Altyapıların Önemi

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 altyapıları ifade etmektedir (Bakanlar Kurulu Kararı, 2013).

Günümüzde bilişim teknolojileri kritik altyapılarda yoğun bir şekilde kullanılmaktadır. Kritik altyapıların bir bölümü kurumsal ve iletişim sistemlerini kapsayan bilişim sistemlerini oluşturmakta bir kısmı ise Endüstriyel Kontrol Sistemleri tarafından yönetilen sistemleri oluşturmaktadır. Endüstriyel Kontrol Sistemleri, SCADA(Supervisory Control And Data Acquisition) ve dağıtık kontrol sistemleri olarak ikiye ayrılmaktadır. SCADA olarak adlandırılan endüstriyel kontrol sistemleri, kritik altyapıların yönetimi ve izlenmesinde uzun yıllardan bu yana kullanılmaktadır. Geçmişte başka ağlar ile bağlantısı olmayan, bilgi ve iletişim teknolojileri içermeyen veya altyapıya özel olarak geliştirilmiş teknolojileri içeren SCADA sistemleri, günümüzde yaygın olarak kullanılan ve bilinen yazılım, donanım ve ağ protokollerini barındırmaktadır. Ayrıca, kritik altyapıları yöneten ve izleyen birçok SCADA sistemi kurumsal ağlara ve internete bağlantılı hale gelmeye başlamıştır. Bu durum internet üzerinde hızla artan siber risk ve tehditlerle karşı karşıya bulunulduğu gerçeğini gözler önüne sermektedir. Kritik altyapılara yönelik olası bir siber saldırı ekonomik, politik hatta can kaybı gibi ciddi kayıp ve hasarlara neden olabilmektedir. Özellikle SCADA sistemlerine sızmak için tasarlanmış bilinen ilk özel yapım virüs olan Stuxnet bunun en büyük örneğidir. Bu nedenle Türkiye'deki kritik altyapıları, her türlü siber tehdit/saldırıdan korumak büyük önem arz etmektedir (Bilgi Güvenliği, 2010).

ABD'nin Siber Güvenlik Yasa Tasarısına göre kritik altyapılar şu şekilde tanımlanmaktadır:
Bir sistem, zarar görmesi ya da yetkisiz erişime maruz kalması durumunda, enerji su, ulaşım, acil servis, gıda dâhil olmak üzere yaşamı idame ettiren hizmetlerin kesintiye uğramasına neden oluyorsa, bu sistem ya da varlık kritik altyapı kapsamına girmektedir.

ABD'de Kasım ayı " Kritik Altyapı Güvenliği ve Dayanıklılığı Ayı" olarak kabul edilmektedir. Ulusal güvenliğin sağlanmasında kritik altyapıların önemi konusunda farkındalık yaratmak adına çalışmalar yapılmaktadır.

### 4.5. Ulusal ve Uluslararası Siber Tatbikatlar

Eylem Planı'nda, "Siber güvenlik tatbikatları düzenlenmesi" başlıklı 8 numaralı eylem maddesi kapsamında; Türkiye'de geniş çapta 2 ulusal, 1 uluslararası siber güvenliğe ilişkin tatbikat gerçekleştirilmiştir.

Siber güvenlik tatbikatlarının amaçları şunlardır (Bilişim Dergisi, 2013):

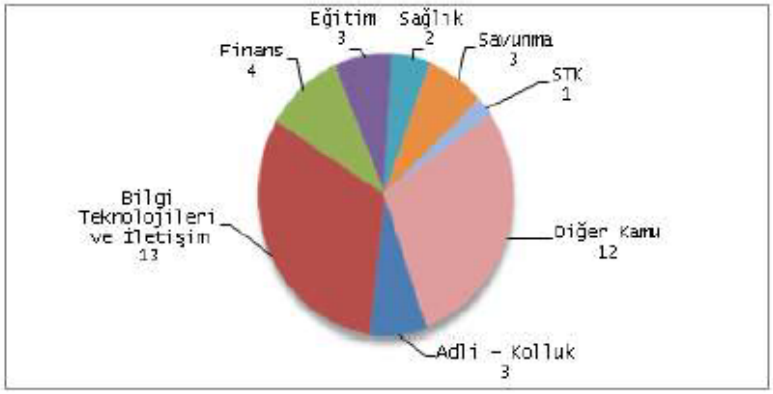
- Bilgi sistemlerini hedef alabilecek saldırılara karşı hazırlıklı olmak,
- Saldırılara karşı kurum içi politikaları ve karar destek mekanizmalarını değerlendirmek,
- Kurumlar arası bilgi paylaşımını, haberleşmeyi ve koordinasyonu test etmek,
- Olası bir saldırıdan sonra geri kurtarma planlarını test etmek, tehditlere ve açıklıklara karşı farkındalık oluşturmak,
- Personeli eğitmektir.

### 4.5.1. Türkiye'nin koordinasyonunda yapılan ulusal ve uluslararası siber tatbikatlar

#### I. Ulusal Siber Güvenlik Tatbikatı 2011

Ulusal Siber Güvenlik Tatbikatı (USGT) 2011; finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumunun, özel sektör kuruluşunun ve sivil toplum kuruluşunun katılımıyla 25-28 Ocak 2011 tarihlerinde gerçekleştirilmiştir. Söz konusu kurum/kuruluşların 6'sı tatbikata gözlemci statüsünde katılmıştır. Tatbikatta, katılımcı kurum/kuruluşlardan bilgi teknolojileri ve iletişim, hukuk ve halkla ilişkiler uzmanı statüsündeki 200'e yakın personel görev almıştır. Katılımcı kurumların siber saldırı durumunda verecekleri tepkilerin gerçek ortamdaki ve simülasyon ortamındaki saldırılarla ölçülmesiyle, kurumların hem teknik kabiliyetleri hem de kurum içi ve kurumlar arası koordinasyon yetenekleri değerlendirilmiştir (BTK USGT, 2011).

Şekil 4.4. USGT 2011 Katılımcılarının Sektörel Profili




Kaynak: BTK USGT, 2011

## II. Siber Kalkan Tatbikatı 2012

2012 yılı Mayıs ayında BTK koordinasyonunda elektronik haberleşme sektöründe faaliyet gösteren 12 işletmecinin (sektörde en fazla pazar payına sahip olan erişim sağlayıcı işletmecilerin ve mobil internet hizmeti sunan 3. Nesil (3G) işletmecilerinin) katılımı ile "Siber Kalkan Tatbikatı 2012" gerçekleştirilmiştir. Erişim sağlayıcıların test sistemlerine 8-22 Mayıs 2012 tarihleri arasında gerçek Dağıtık Hizmeti Engelleme Saldırıları (DDoS - Distributed Denial of Service) yapılmış ve her bir işletmeciye ayrı ayrı uygulanan bu saldırılar boyunca toplamda 100 terabit'in üzerinde trafik hedef sistemlere gönderilmiştir. Söz konusu trafik yurtiçi ve yurtdışından 150 farklı kaynaktan hedef sistemlere yöneltilmiştir. 23-28 Mayıs 2012 tarihleri arasında ise katılımcılara yazılı senaryolar gönderilerek, bu senaryolara verdikleri tepkiler analiz edilmiştir (BTK, 2012).

## III. Ulusal Siber Güvenlik Tatbikatı 2013

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın koordinasyonunda BTK ve TÜBİTAK tarafından birlikte yürütülen ve siber saldırılara karşı hazırlıklı olunmasını amaçlayan Ulusal Siber Güvenlik Tatbikatı 2013, 61 kamu ve özel sektör kuruluşunun katılımıyla 24 Aralık 2012 - 11 Ocak 2013 tarihleri arasında gerçekleştirilmiştir. Katılımcıların çoğu kamu kurumu olmakla birlikte, içlerinde özel sektör ve sivil toplum kuruluşları da bulunmaktadır.

Tatbikat; elektronik haberleşme, enerji, savunma, finans ve sağlık gibi kritik altyapıları yöneten ve işleten kurum ve kuruluşları kapsamaktadır. Aynı zamanda adli ve kolluk birimlerinden de katılım gerçekleşmiştir. Tatbikat katılımcılarının, sadece teknik değil, aynı zamanda hukuk ve iletişim birimlerinden de personeller tatbikatta görev yapmıştır. Tatbikatta gerçek saldırılar (DDoS, Web güvenliği taraması, Port taraması, Log analizi, Web uygulama testi, Sosyal mühendislik) ve 6 adet yazılı senaryo gerçekleştirilmiştir. Ayrıca, 4 farklı takım ile birlikte, siber güvenlik yarışması düzenlenmiştir (BTK 2. USGT, 2013).

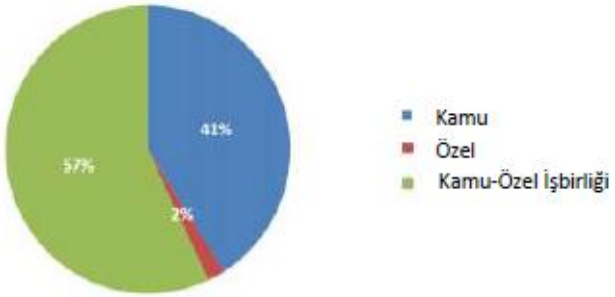
### IV. Uluslararası Siber Kalkan Tatbikatı 2014

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın koordinasyonunda, ITU, Bilgi Teknolojileri ve İletişim Kurumu ile ITU-IMPACT işbirliğinde siber güvenlik konusunda farkındalığın arttırılması, yeteneklerin geliştirilmesi ve uluslararası koordinasyonun sağlanması amacıyla 15-16 Mayıs 2014 tarihinde İstanbul'da, 19 ülkeden temsilcilerin katılımıyla "Uluslararası Siber Kalkan Tatbikatı 2014" gerçekleştirilmiştir. Ülkelerin siber olaylara müdahale ekipleri tarafından yazılı mesajlarla iletilen siber senaryolara cevaplar verilmesi şeklinde uygulamalar gerçekleştirilerek ekiplerin siber saldırılara cevap verme yetenekleri test edilmiştir. Senaryoların konusu sisteme yetkisiz erişim sonucunda sistemin değiştirilmesinin ve mobil cihazda andorid sistemin incelenmesi konularından oluşmaktadır. İki farklı senaryodan oluşan tatbikatta, her bir senaryo için 120 dakika süre verilmiştir (BTK Tatbikat, 2014).

### 4.5.2. Dünya ülkelerinde yapılan siber tatbikatlar

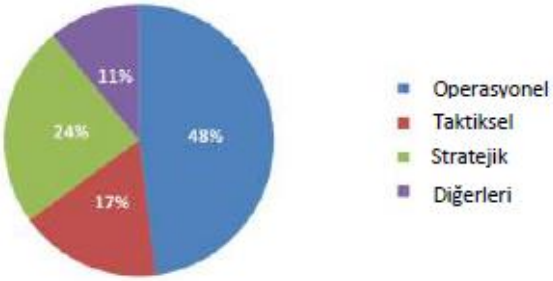
ENİSA'nın 2012 yılı Ekim ayında "On National and International Cyber Security Exercises – Survey, Analysis and Recommendations (Ulusal ve Uluslararası Siber Güvenlik Tatbikatları / Araştırma, Analiz ve Öneriler)" raporu yayımlanmıştır. 2002-2012 yılları arasını kapsayan 85 tatbikat ENİSA tarafından incelenmiştir. Bu raporda, dünya çapında toplam 84 ülkenin katılım sağladığı uluslararası tatbikatlar incelenmiştir. Toplamda 22 Avrupa ülkesi, ulusal siber tatbikatları yürütmüştür. Tatbikata katılan sektörlerin ve tatbikatların odaklandığı alanların yüzdesel oranları şekil 4.5 ve şekil 4.6'da gösterilmiştir. Siber kriz işbirliği alanında özel sektör temsilcileri önemli rol oynadığından dolayı, tatbikatların yarısından fazlasını kamu-özel sektör işbirliği oluşturmaktadır. Siber tatbikatlarda, kamu-özel sektör işbirliğinin önümüzdeki yıllarda daha da artması muhtemel görünmektedir (ENISA Tatbikatlar, 2012, s.12).

Şekil 4.5. Tatbikatlara Katılan Sektörler




Kaynak: ENISA Tatbikatlar, 2012

Şekil 4.6. Tatbikatların Odak Noktaları




Kaynak: ENISA Tatbikatlar, 2012

**Dünyadaki önemli siber tatbikatlar aşağıda sıralanmıştır:**

**Cyber Storm:** Cyber Storm (Siber Fırtına), ABD İç Güvenlik Bakanlığı tarafından, 2006 yılından itibaren çift yıllarda düzenlenen, yazılı senaryo ve simülasyonlarla icra edilen, siber güvenlik tatbikatlarıdır. Tatbikat temel olarak ABD kurum ve kuruluşlarını kapsamakta ancak İngiltere, Kanada, Avustralya ve Yeni Zelanda gibi ülkelerden de katılım olmaktadır (Çifci, 2013).

**APCERT Drill:** Asya Pasifik Bilgisayar Olaylarına Müdahale Ekibi (Asia Pasific Computer Emergency Response Team, APCERT), Asya Pasifik bölgesindeki ülkeler arasında işbirliğini geliştirmek amacıyla kurulmuş olup, 19 ülkeden toplam 25 CSIRT operasyonel üyesidir. APCERT Drill'in 2013 yılında gerçekleştirdiği "Geniş Kapsamlı Hizmetin Engellenmesi Saldırısına (Denial Of Service Attack) Karşı Mücadele" konulu tatbikatta, internet üzerinde var olan gerçek olaylar ve sorunlar yansıtılmıştır (APCERT, 2013).

**Cyber Europe:** ENISA, Avrupa'nın siber kriz işbirliği tatbikatlarını, planlama, yürütme ve değerlendirme sürecini iyileştirmektedir. Avrupa çapında yapılan siber güvenlik tatbikatının ilki 2010 yılında, ikincisi 2012 yılında gerçekleştirilmiştir. ENISA şu anda AB Üye Devletleri ve EFTA ülkeleri ile üçüncü "Siber Avrupa Tatbikatı 2014" ü planlanmaktadır (ENISA Siber Avrupa Tatbikatı, 2014).

**NATO Cyber Coalition (Siber Koalisyon):** 2008 yılından bu yana, NATO üyesi ülkelerin ve NATO siber sistemlerinin güvenliğini sağlamak için gereken işbirliğini sağlamak ve uygulanan politikaları sınamak amacıyla, NATO üyesi olan ve işbirliği kapsamında bulunan ülkelerin katılımıyla, NATO siber savunma tatbikatları düzenlenmektedir. 2009 yılından itibaren tatbikatlara Türkiye'den de katılım sağlanmaktadır.

"Siber Koalisyon 2013" tatbikatı, ağları etkin bir biçimde test etmek amacıyla, sistemleri ve prosedürleri test etme imkânı sağlamaktadır. 30'dan fazla ülke ve 300 uzmanın katılımı ile büyük çapta gerçekleştirilmiş bir tatbikattır. 28 NATO üye ülkesinin yanı sıra, NATO üyesi olmayan Avusturya, Finlandiya, İrlanda, İsveç ve İsviçre katılmıştır. Yeni Zelanda ve Avrupa Birliği ise tatbikatta gözlemci statüsüne sahiptir (Çifci, 2013).

NATO Siber Savunma ve Mükemmeliyet merkezi tarafından yürütülen "Uluslararası Siber Savunma Tatbikatı Kilitli Kalkan 2014", 17 ülkeden 300 katılımcıyı bir araya getiren, 12 savunma ekibiyle hayata geçirilen, gerçek zamanlı bir ağ savunma tatbikatıdır. 12 savunma ekipi; Estonya, Finlandiya, NATO CIRC, İtalya, İspanya, Almanya&Hollanda, Türkiye, Letonya ve Çek Cumhuriyeti, Macaristan, Fransa, Polonya, Avusturya ve Litvanya ülkelerinden oluşmaktadır. Takımlar tatbikata kendi ülkelerinden katılmış olup ve tatbikatın kontrolü ise Tallinn, Estonya'dan yapılmıştır (CCDCOE, 2014). Türkiye'den TÜBİTAK ve TSK temsilcileri tatbikata savunma ekibi olarak katılmış olup, UDHB, Dışişleri Bakanlığı, Milli Savunma Bakanlığı ve TSK'nın ilgili birimleri gözlemci statüsünde katılmıştır.

"Siber Koalisyon Tatbikatı 2014"ün 2014 yılı kasım ayında Tartu, Estonya'da yapılması planlanmaktadır.

# 5. DÜNYA'DA KAMU GÜVENLİ AĞI OLUŞTURULMASINA İLİŞKİN ÇALIŞMALAR

Bu bölümde, ABD, Birleşik Krallık ve Çin Halk Cumhuriyeti Hong Kong Özel İdari Bölgesi'nde kamu güvenli ağı oluşturulmasına ilişkin idari yapılanma ve altyapı çalışmaları incelenmektedir.

## 5.1. Amerika Birleşik Devletleri (ABD)

First Responders Network Authority (FirstNet), ABD Ulusal Telekomünikasyon ve Bilgi Yönetimi Dairesi (NTIA) Ticaret Bölümü içinde bağımsız bir otoritedir. FirstNet, Ulusal Kamu Güvenliği Geniş Bant Ağının dağıtımını ve uygulanmasını yapmaktan sorumludur (DHS FirstNet, 2012).

Federal İletişim Komisyonu (Federal Communication Commission, FCC), Kolumbiya Bölgesi ve ABD topraklarındaki 50 eyalette, radyo, televizyon, uydu ve kablo ile devletlerarası ve uluslararası iletişimi düzenleyen bağımsız bir ABD devlet kurumudur. Kurum, Amerika Birleşik Devletleri Başkanı tarafından atanan ve ABD Senatosu tarafından onaylanan beş komisyon üyesi tarafından yönetilmektedir (FCC, 2014).

"Ulusal Genişbant Planı" Amerika'nın geleceği için bir yol haritası çizmektedir. Bu girişimler, iş alanları konusunda teşvik sağlama, ekonomik büyümeyi canlandırma ve eğitim, sağlık, iç güvenlik ve daha fazla alanda Amerika Birleşik Devletlerinin yeteneklerini artırma yönünde kazanımlar sağlamaktadır.

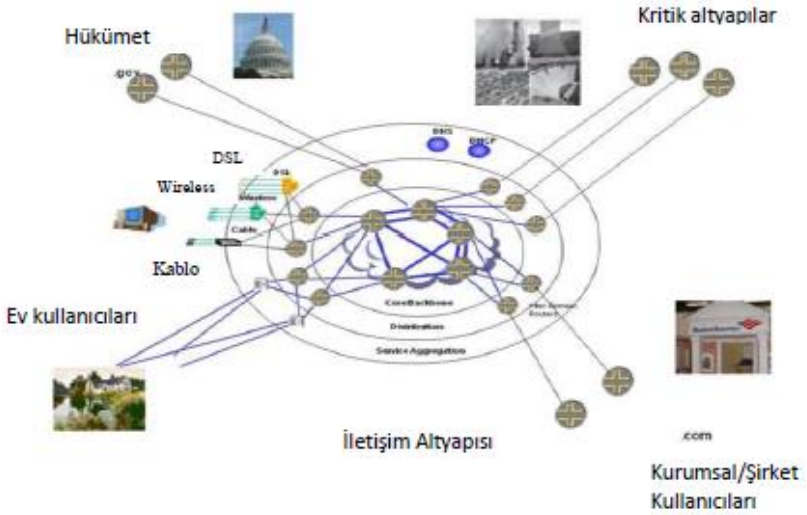
Siber güvenlik ve kritik genişbant altyapısının korunmasının teşviki için:

I. FCC'nin siber güvenlik için bir yol haritası çıkarması gerekmektedir.
II. FCC'nin genişbant servis sağlayıcılar için, kesintilerin raporlama gereksinimlerini genişletmesi gerekmektedir.
III. FCC, gönüllü siber güvenlik sertifikasyon aktivitesini oluşturmalıdır.
IV. FCC ve İç Güvenlik Bakanlığı, bir siber güvenlik bilgi raporlama sistemi oluşturmalıdır.
V. FCC, uluslararası katılım ve sosyal yardım alanlarındaki çalışmaları genişletmelidir.
VI. FCC, ağ esnekliği ve hazırlıklı olma (preparedness) konuları üzerinde araştırma yapmalıdır.
VII. FCC ve Ulusal İletişim Sistemi(NCS), öncelikli ağ erişimi ve genişbant iletişim için yönlendirme oluşturmalıdır.
VIII. FCC, genişbant iletişimin, güvenilirlik ve esnekliğini araştırılmalıdır.

"Ulusal Genişbant Planı" / Siber Güvenliğin İyileştirilmesi

Iletişim sağlayıcılar kritik altyapılarına yapılan saldırılarla oldukça sık karşılaşmaktadırlar. Devlet ve devlet dışı kuruluşlar; kritik altyapı kısımlarının işleyişini sağlamak için tasarlanmış sistemleri manipüle etmek ya da kontrol etmek için çeşitli verileri çalmak değiştirmek veya yok etmek konusundaki yeteneklerini göstermişlerdir. Ek önlemler, siber saldırılara karşı ticari iletişim altyapısını korumak için gerekli olabilmektedir. Bu önlemlerin, geniş bant iletişim güvenliği ve güvenilirliği artırmak için faydalı olacağı değerlendirilmektedir.

Şekil 5.1 Siber Dünya İletişim Altyapısı




Kaynak: Broadband, 2014

İç Güvenlik Bakanlığı, özel sektör sahipleri ve operatörlere destek ve uzmanlık sağlamaktan sorumludur. İç Güvenlik Bakanlığı kötü niyetli faaliyetler ile ilgili, .gov ağ trafiğini izlemek için saldırı tespit araçlarını kullanmakta ve siber güvenlik açıklarını gidermek için bu çıkan verileri kullanmaktadır. Ayrıca, İç Güvenlik Bakanlığı potansiyel siber tehditler hakkında bilgi sağlayan uyarılar ve bültenler yayımlamaktadır. 2012 yılında, İç Güvenlik Bakanlığı kamunun yanı sıra birçok hükümet, özel sektör ve kritik altyapı paydaşları ile paylaşılan 5.000'den fazla uyarıları ve öneri yayımlamıştır. İç Güvenlik Bakanlığı'nda bir siber bilgi koordinasyon merkezi, ulusal siber güvenlik ve İletişim Entegrasyon Merkezi (NCCIC) ve çeşitli operasyonel birimler faaliyet göstermektedir. Bu birimler olaylara yanıt ve bilgi sistemi operatörlerine teknik yardım sağlamaktan sorumludur. NCCIC, hükümet ve özel sektörün her kademesindeki siber topluluklarda ortak bir işletim profili oluşturmak için bu kanallar aracılığıyla toplanan bilgileri koordine etmektedir (DHS, 2013b).

Federal Ağların Dayanıklılığı, kritik siber güvenlik gereksinimlerini karşılayacak şekilde oluşturulan (Siber Güvenlik ve İletişim Ofisi içinde) ve altında dört şube bulunduran bir birimdir.

FNR altında görev yapan şubeler:

1. Gereksinim ve Edinimlerin Desteklenmesi (Requirements and Acquisition Support, RAS)
2. Ağ ve Altyapı Güvenliği (Network and Infrastructure Security, NIS)
3. Siber Güvenlik Güvencesi (Cybersecurity Assurance, CA)
4. Siber Güvenlik Performans Yönetimi (Cybersecurity Performance Management, CPM)

FNR ayrıca, ülkenin siber güvenlik duruşunu geliştirmek için federal hükümet ile işbirliği yapmaktadır. Bu işbirliği aşağıdaki konuları kapsamaktadır (DHS FNR, 2014):

- Federal hükümet içerisinde ortak gereksinimleri belirleme, çözümleri belirlemek için federal işletmenin bileşenleri ile işbirliği,
- Politika ve teknik çözümlerin uygulanması ve uygulanan çözümlerin etkinliğinin izlenmesidir.

## 5.2 Birleşik Krallık

Birleşik Krallık Hükümeti, 2011 yılı Kasım ayında "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world" isimli siber güvenlik belgesini yayımlamıştır. Bu kapsamda siber güvenlik için 2009-2013 yılları arasında 650 milyon sterlin bütçe ayrılmıştır.

Birleşik Krallık'da siber güvenliğin sağlanmasından sorumlu başlıca kuruluşlar şunlardır: Office of Cyber Security and Information Assurance, Cyber Security Operations Center (Wikipedia, 2014ç).

Ulusal Altyapının Korunması Merkezi (CPNI); Ulusal Altyapı Güvenlik Koordinasyon Merkezi (NISCC) ve Ulusal Güvenlik Danışma Merkezi (NSAC) 'nin öncül birimlerinin birleşmesiyle 1 Şubat 2007 tarihinde kurulmuştur.

CPNI, ulusal altyapılar genelinde işletmeler ve kuruluşlar için koruyucu güvenlik danışmanlığı sağlayan, tavsiyeler veren Birleşik Krallık hükümetinin yetkili bir makamıdır.

Tavsiyeleri, İngiltere'nin temel hizmetlerini (iletişim, acil hizmetler, enerji, finans, gıda, hükümet, sağlık, ulaşım ve su sektörlerinde tarafından sağlanan) terör ve diğer tehditlere karşı güvende tutmayı, ulusal altyapıdaki güvenlik açıklıklarını azaltmayı hedeflemektedir.

Bu hizmetlerin olmaması halinde, İngiltere'nin, ağır ekonomik zarar, ciddi toplumsal bozulmalar, hatta yaşamın büyük ölçekli kaybı da dâhil çok ciddi problemlerle karşılaşabileceği belirtilmektedir. CPNI'ın öncelikli tavsiyesi kritik ulusal altyapılara (CNI) yöneliktir (Wikipedia, 2014b).

CPNI koruyucu güvenlik tavsiyeleri sağlayarak ulusal güvenliği korumaktadır. Tavsiyeler fiziksel güvenlik, personel güvenliği ve siber güvenlik / bilgi güvencesini kapsamaktadır.

CPNI'ın koruyucu güvenlik tavsiyeleri, aşağıdaki maddelerin kombinasyonu üzerine kuruludur:

- Bilimin ne anlattığı (araştırma ve geliştirme programları)
- Ulusal güvenlik tehdit anlayışı
- Deneyim ve Uzmanlık
- Kamu ve özel sektör ortakları ile etkin ilişkiler
- Politika hususları/ değerlendirmeleri

Politika hususları, CPNI'nın koruyucu güvenlik tavsiyeleri üzerindeki temel yapı taşlarından biridir. CPNI'ın çalışmaları üzerinde etkisi olan çeşitli Hükümet politikaları aşağıda yer almaktadır:

I. Ulusal Güvenlik Stratejisi
Ulusal Güvenlik Stratejisi, İngiltere'nin güvenliğini ve dayanıklılığını sağlamak üzerine stratejik seçimler ortaya koymaktadır.

II. Stratejik Savunma ve Güvenlik Değerlendirmesi
Stratejik Savunma ve Güvenlik Değerlendirmesi, Ulusal Güvenlik Stratejisi hedeflerinin nasıl takip edileceğini, sürdürüleceğini ortaya koymaktadır.

III. Terörle Mücadele Stratejisi
Birleşik Krallık Hükümeti'nin terörle mücadele stratejisi uluslararası terörizm riskini azaltmayı hedeflemektedir.

IV. Siber Güvenlik Stratejisi
İngiltere'nin Siber Güvenlik Stratejisi 2011 yılı Kasım ayında yayımlanmıştır. İngiltere'nin ekonomik refahını destekleme, ulusal güvenliği koruma, daha güvenilir ve esnek dijital ortamda kamunun nasıl güvence altına alınacağını ortaya koymaktadır. Özellikle, kamu sektörü ve özel sektör arasındaki yakın işbirliğinin önemi vurgulanmaktadır.

V. Ulusal Risk Kayıt

İngiltere'nin ve vatandaşlarının, Ulusal Risk Değerlendirmesi (NRA) aracılığıyla, önümüzdeki beş yıl içinde karşı karşıya kalabileceği önemli görülen acil durumlar hükümet tarafından takip edilmektedir.

VI. Doğal afetlere karşı altyapının esnekliği/dayanıklılığı

Kabine Ofisi bünyesindeki Sivil Yükümlülükler Sekretaryası, doğal afetler sonucu oluşabilecek ciddi bozulmalar, kesintiler için gereken temel hizmetlerin ve kritik altyapıların dayanıklılığının iyileştirilmesi amacıyla, bir çapraz-sektör Kritik Altyapı Esneklik Programı (CIRP) geliştirmiştir.

Ulusal Telekomünikasyon ve Bilgi Yönetimi Dairesi (National Telecommunications and Information Administration, NTIA) ABD Ticaret Bakanlığı'nın Yürütme Organının yurt içi ve uluslararası telekomünikasyon ve bilgi teknolojisi konularındaki ana sözcüsü konumundaki bir dairesidir.

Kamu Hizmetleri Ağı (Public Service Network, PSN); İngiltere hükümeti birimleri arasındaki iletişim hizmetlerinin maliyetini azaltmakta ve vatandaşların yararına yeni, paylaşılan kamu hizmetleri sağlamaktadır (PSN, 2014).

PSN, daha etkin-maliyetli ve verimli standardize edilmiş BİT altyapısında bir ağ oluşturmaktadır. PSN farklı ve bağlantısı kesilmiş altyapıların yüzlercesinin değiştirilmesi ile, Merkez Hükümet ve Geniş Kamu Sektörü genelinde kuruluşlar için güvenli bir özel internet sağlamaktadır.

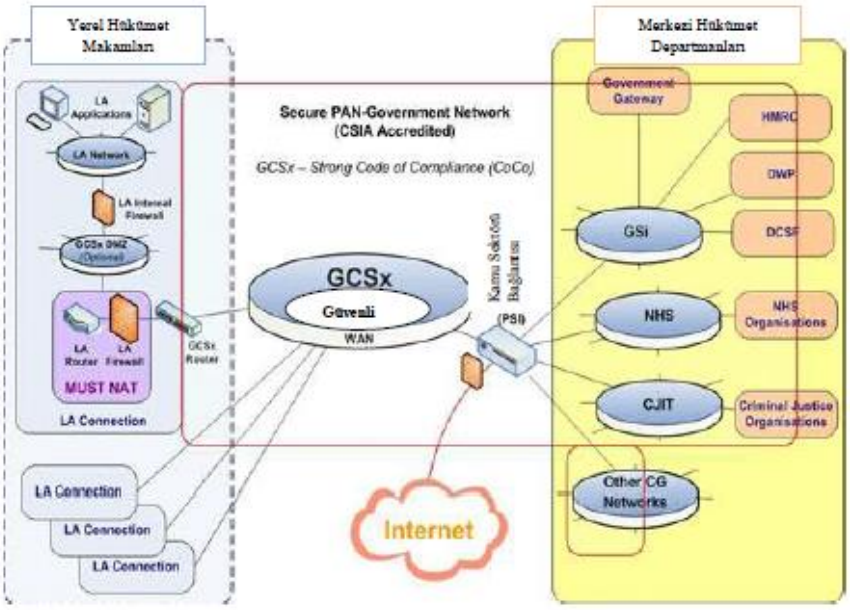
Hükümet Güvenli İç Ağı (GSI); bağlı kuruluşların elektronik ve güvenli iletişimini sağlayan Birleşik Krallık hükümeti geniş alan ağıdır. İngiltere'deki birçok kamu kuruluşu benzer akredite ağları arasında peer-to-peer (P2P) üzerinden dosyaları aktarmak için GSI kullanmaktadır. GSI, posta gönderme protokolü olarak SMTP kullanmaktadır.

GCSX ağı ise GSI'nin bir parçasını oluşturmaktadır ve neredeyse tüm merkezi departmanlara bağlantı sağlamaktadır. Hassas verilerin iletimi ise (hasta kimlik bilgileri vb.), GCSX bağlantısı üzerinden, bir GCSX e-posta hesabı kullanılarak yapılabilmektedir. GCSX ağı geniş Gsi'nin parçasıdır ve neredeyse tüm merkezi birimlerine bağlantı sağlamaktadır.

Güvenli bir geniş alan ağı olan, Birleşik Krallık Hükümeti İletişim Güvenli Dış ağı (The UK Government Connect Secure Extranet, GCSX) Ulusal Sağlık Servisi, Ceza Adalet Dış Ağı, Polis Ulusal Ağı gibi merkezi devlet daireleri ile özel, güvenli veri paylaşımı ve etkileşim yapmak için yerel kamu sektörü kuruluşları yetkililerine imkân sağlamaktadır. GCSX; merkezi hükümet departmanları ağlarının ayrı olarak bulunduğu birden fazla veri merkezinde bir araya getirilmiş yönetilen bir ağ servisidir (Techtarget, 2010).

Merkezi departmanlar, genel internet dışında güvenli iletişimi sağlamak için merkezi bölümün ağ etki alanını bağlayan güvenli bir geniş alan ağı köprüsü ile Kamu Sektörü Bağlantısı (Public Sector Interconnect, PSI) aracılığıyla GCSX'e bağlanmaktadır.

Şekil 5.2. Birleşik Krallık Hükümeti İletişim Güvenli Dış Ağı




Kaynak: GCSX, 2014

Bu ağ, yerel yönetimlerin birbirleriyle ve merkezi hükümet departmanları ile veri paylaşımı yapabilmesi için güvenli bir mekanizma sağlamaktadır.

## 5.3 Çin Halk Cumhuriyeti Hong Kong Özel İdari Bölgesi

Bu bölümde Çin Halk Cumhuriyeti Hong Kong Özel İdari Bölgesi hükümetinin bilişim teknolojileri güvenlik çerçevesi detaylı olarak incelenmektedir.

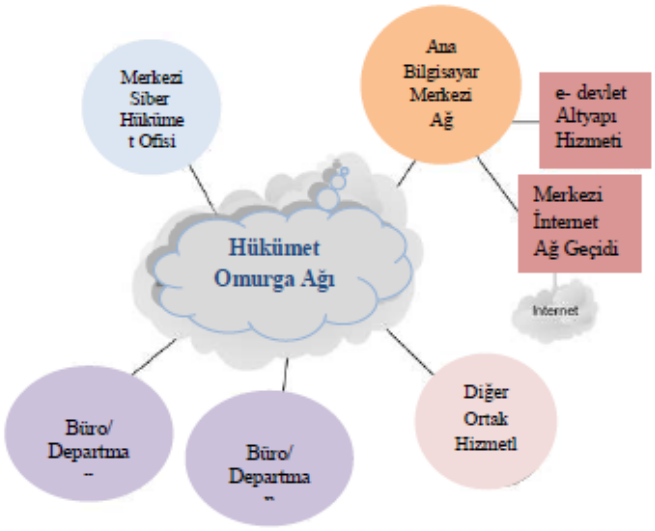
Hükümet Bilişim Kurulu Başkanı Ofisi (The Office of the Government Chief Information Officer, OGCIO) hükümet içinde ve dışında bilgi ve iletişim teknolojilerinin gelişimi konusunda liderlik sağlayan bir birimdir. Hükümet Bilişim Kurulu Başkanı (GCIO) başkanlığındaki, OGCIO, hükümete bilgi teknoloji hizmeti

ve desteği sağlamanın yanı sıra, Dijital 21 Stratejisinde bulunan ICT politikaları, stratejileri, programları ve önlemleri sorumluluğu ile ilgili tek bir odak noktası hizmeti sağlamaktadır. OGCIO ayrıca bilgisayar virüsü ve hükümete yönelik bilgi güvenliği olayları için 7x24 izleme ve raporlama sistemi sağlamakta ve idamesini sürdürmektedir (OGCIO, 2014)

Hükümet Omurga Ağı (GNET), ortak hizmetlerin yanı sıra hükümet büroları ve bölümlerine istikrarlı, güvenilir ve yüksek esneklik özelliği olan genişbant ağ bağlantısı sağlayan hükümet çapında bir ağ altyapısıdır.

Kendi GNET bağlantısı aracılığıyla diğer Gnet müşterilerle iletişime geçebilmesinin yanı sıra, bir Gnet müşterisi, "merkez internet ağ geçidi (CIG)" sistemi aracılığıyla dış dünyaya erişebilmektedir. Çok sayıda hükümet binası, büroları, bölümleri ve Ana Bilgisayar Merkezi (OGCIO Central Computer Centre (CCC)); Metro Ethernet WAN üzerinden veya yerel ethernet portları üzerinden GNET'e bağlanabilmektedir.

Şekil 5.3. Hükümet Omurga Ağı

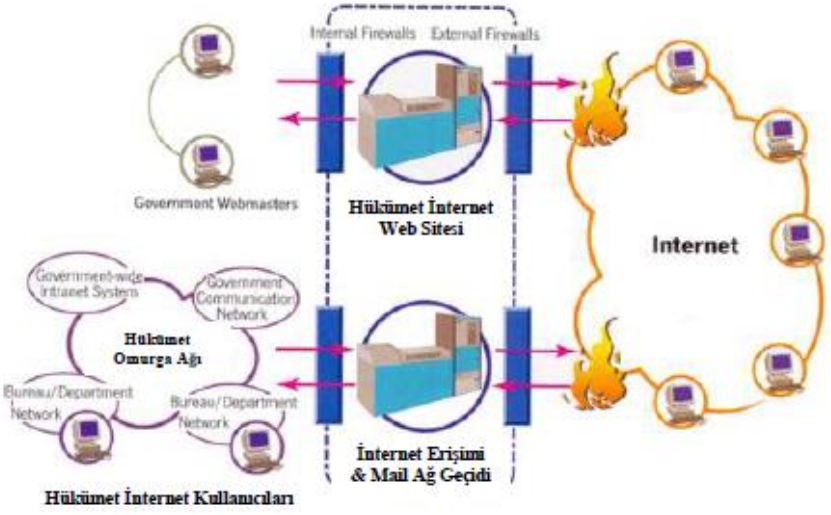



Kaynak: OGCIO Hükümet Omurga Ağı, 2014

**Merkezi internet ağ geçidi** (Central Internet Gateway, CIG) hükümet büroları ve bölümlerine bilgi dağıtımı, kamu ile yapılan işlemler ve iletişim konularında hizmet sağlamaktadır. CIG Sistemi ayrıca tüm hükümet büroları ve bölümlerine, hükümet internet siteleri, internet postaları ve internet erişim hizmetleri için merkezi barındırma hizmeti sunmaktadır. CIG sistemi, tüm internet kullanıcıları ile kesintisiz iletişimi sağlamak için, 2009 yılında, IPv6'ı destekleyecek şekilde geliştirilmiştir (OGCIO Hükümet Omurga Ağı, 2014).

İnternet üzerinden mail iletim gizliliğini sağlayan Basit Posta Aktarım Protokolünü (Simple Mail Transfer Protocol over Transport Layer Security (SMTP over TLS)) güçlendirmek için, sistem üzerinde iletim şifrelemesi için kullanılan Hongkong Post e-Cert mevcuttur.

Şekil 5.4. Merkezi İnternet Ağ Geçidi Sistemi




Kaynak: OGCIO CIG, 2014

OGCIO Ana Bilgisayar Merkezi (CCC), hükümetin kritik bilişim teknolojisi altyapısının önemli bir parçasıdır. Wan Chai, Sai Kung ve Tsuen Wan bölgelerinde olmak üzere üç adet veri merkezi bulundurmaktadır. CCC tarafından hizmeti sağlanan bu veri merkezleri ISO/IEC 2000 standardını almaya hak kazanmıştır.

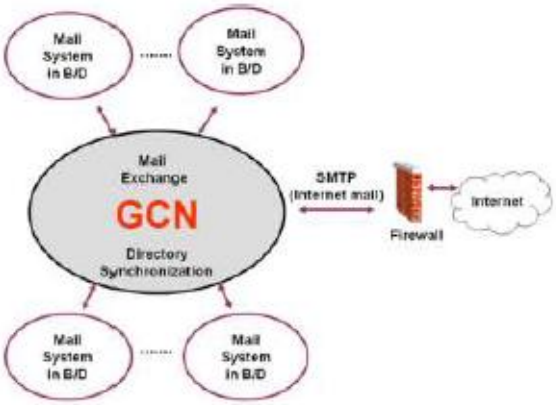
Özellikle hükümetin merkezi bilişim teknolojileri altyapısı ve sistemleri için hosting (işletme, yönetim ve bakım) hizmetleri vermektedir. Ayrıca kritik sistemler için felaket kurtarma (disaster recovery, DR) olanakları sağlamaktadır.

CCC Hükümetin aşağıdaki merkezi bilişim sistemlerini desteklemektedir (OGCIO CCC, 2014):

- Hükümet Omurga Ağı (Gnet),
- Merkezi internet ağ geçidi (CIG),
- Merkezi Siber Hükümet Ofisi (CCGO), (hükümetin merkezi iç bilgi portalıdır)
- Hükümet İletişim Ağı (GCN),
- GovHK çevrimiçi hizmetlerin arka uçlarına ulaşan çok sayıda sistem.

**Hükümet İletişim Ağı** (The Government Communication Network, GCN) hükümet büroları ve departmanları (B/Ds) arasında elektronik postaların gönderimi için ortak bir hizmet sağlamaktadır. Hükümet içinde yapılan elektronik mail iletişiminin yanı sıra, GCN ayrıca hükümet ve departmanlarına elektronik posta yoluyla internet üzerinden kamuoyu ile iletişim sağlayacak şekilde merkezi internet ağ geçidi sistemine bağlanmaktadır.

Şekil 5.5 Hükümet İletişim Ağı Topolojisi




Kaynak: Hükümet İletişim Ağı, 2014

# 6. TÜRKİYE'DE KAMU GÜVENLİ AĞI OLUŞTURULMASINA İLİŞKİN ÇALIŞMALAR VE ÖNERİLEN MODEL

Bu bölümde, Türkiye'de kamu güvenli ağı oluşturulmasına için yapılan çalışmalar, Türkiye için önerilen kamu güvenli ağı modeli ve dünya ülkelerinin kritik altyapı olarak belirlenen sektörleri ile ulusal çaptaki yapılanmaları incelenerek Türkiye için kritik altyapı olarak belirlenmesi önerilen alanlar incelenmektedir.

Hükümetin çeşitli kademelerinde, kamu güvenliği kurumları kamu güvenliği olayları ile karşılaştıklarında bilgi paylaşımında bulunmak ve iletişim kurmak için bir araya gelmektedir. Bu tür kurumlar arası işbirliği girişimleri kamu güvenliği ağının oluşturulması ile sonuçlanmıştır. Kamu güvenliği ağları hükümetin herhangi bir seviyesinde oluşturulabilir ve kendi kullanıcı tabanı ile bir veya birden çok coğrafyaya yayılabilmektedir (Wikipedia, 2013b).

Türkiye'de; kamu kurumlarının, herhangi bir güvenlikolayı ile karşılaşmadan, olağan bilgi akışının sağlandığı bir ağ kurulması öngörülmektedir.

## 6.1. Türkiye'de Kamu Güvenli Ağı Oluşturulması Çalışmaları

Türkiye'de kamu güvenli ağı oluşturulması çalışmalarının temelinin, 28 Temmuz 2006 tarihli ve 26242 sayılı resmi gazete yayımlanan Devlet Planlama Teşkilatı'nın "Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010)" 70 numaralı eylem maddesi ile başladığı kabul edilmektedir.

**Eylem:** "Kamu Güvenli Ağı"
**Açıklama:** "Kamu kurumlarının farklı geniş alan ağ altyapısı yatırımları yerine kamunun bu yöndeki ihtiyaçları ve internet çıkışları için ortak bir güvenli iletişim altyapısı kurulacak, e-devlet mimarisinin omurgası oluşturulacaktır."

**Sorumlu (S) ve İlgili (İ) Kuruluşlar:**

- TÜRKSAT (S)
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ)
- Devlet Planlama Teşkilatı (İ)
- TÜBİTAK, UEKAE (İ)

**Başlangıç tarihi:** 2006
**Süre:** 27 ay

**Durum/Yapılan Çalışmalar:** Eylem kapsamında; kamu kurumlarının farklı geniş alan ağ yatırımları yapma ihtiyacını ortadan kaldırmak üzere, kamu kurumlarının bu ihtiyaçları ve internet çıkışları için ortak bir güvenli iletişim altyapısının kurulması hedeflenmiştir. Eylemin sorumlu kurumu olan TÜRKSAT tarafından Kamu Güvenli Ağının tasarımına ilişkin ihtiyaç analizi yapmak ve çözüm mimarisi geliştirmek üzere çalışmalara başlanmış ve danışmanlık hizmeti alımına yönelik bir taslak şartname oluşturulmuştur. "Bilgi toplumu stratejisi ve eylem planı nihai değerlendirme raporu"nda bu yöndeki çalışmaların TÜRKSAT tarafından sonuçlandırılamadığı belirtilmektedir (Bilgi Toplumu, 2013).

Diğer taraftan, e-Devlet Kapısı üzerinden sunulan hizmetlere ilişkin, ilgili kamu kurumlarının e-Devlet Kapısına güvenli bağlantıları sağlanmıştır. Söz konusu çalışmalar Kamu Güvenli Ağının ilk aşamaları olarak değerlendirilmektedir. "Bilgi toplumu stratejisi ve eylem planı nihai değerlendirme raporu"nda tamamlanma oranı % 20-40 olarak ifade edilmiştir (Bilgi Toplumu, 2013).

2013 yılı sonrasında ise kamunun güvenli bir ağ üzerinden haberleşmesine ilişkin çalışmalar, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 9 numaralı "Kamu Güvenli İletişim Kurallarının Belirlenmesi / Kamu kurumları arasında güvenli veri paylaşımını sağlamak üzere kuralların ve prosedürlerin belirlenmesi" eylem maddesi ile de ilişkilendirilmektedir ve bu çalışmalar Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yürütülmektedir.

**Eylem:** Kamu güvenli iletişim kurallarının belirlenmesi

**Alt eylem:** Kamu kurumları arasında güvenli veri paylaşımını sağlamak üzere kuralların ve prosedürlerin belirlenmesi

**Sorumlu (S) ve İlgili (İ) Kuruluşlar:**

- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S)
- USOM (İ)
- Bilgi Teknolojileri ve İletişim Kurumu (İ)
- Kamu Düzeni ve Güvenliği Müsteşarlığı (İ)
- TÜBİTAK(İ)

Ayrıca, 20 Ekim 2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı, Bakanlığın Görev ve Yetkileri başlıklı 5. maddesi;

"(b) Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak" ve
"(c) Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak" fıkraları da kamunun güvenli olarak haberleşmesine yönelik yapılacak olan çalışmalar altında değerlendirilebilir.

## 6.2. Türkiye'de Kamu Güvenli Ağı Oluşturulmasına İlişkin Önerilen Model

Mevcut durumda kamu kurumlarının büyük bir çoğunluğu kendi birimleri ile iletişimde ve kendi iç uygulamalarında, VPN (Sanal Özel Ağ) teknolojisi kullanmakta, ancak, birbirleri ile olan veri iletişimini internet ortamından gerçekleştirmektedir. Bu durum siber güvenlik açısından oldukça büyük risk oluşturmaktadır. Kamu kurum ve kuruluşları arasında bilgi alışverişini güvenli bir

ortamda gerçekleştirmek amacıyla Kamu Güvenli Ağının oluşturulması ve hayata geçirilmesi gerekli görülmektedir.
Bu yapıda, tüm kamu kurum ve kuruluşları için ortak bir ağ kurulacağından maliyet tasarrufu da sağlamaktadır. Kamu Güvenli Ağı ile kamu kurumları kendi aralarında kapalı ve özel bir ağ üzerinden haberleşebilecektir.

VPN internet gibi halka açık telekominikasyon altyapılarını kullanarak kullanıcılar veya uzak ofisleri organizasyonun yerel bilgisayar ağına güvenli bir şekilde eriştirmeyi sağlamak için geliştirilmiş sanal bilgisayar ağ yapısıdır (Wikipedia, 2013a).

VPN ağları tünelleme protokolü kullanarak transferi gerçekleşen her veri paketini şifrelediği için güvenlidir. VPN ile veri transferi sırasında transferi gerçekleştirilecek paketleri güvenli olmayan ve herkes tarafından kullanılan çalışma ağları üzerinden transfer edilmeden önce şifrelenmektedir. Ayrıca söz konusu transferin gerçekleştiği network ağları da şifrelenmektedir. 3. şahısların özel ağlara bağlanmasını engellemek için PPTP (Noktadan Noktaya Tünel Protokolü) , L2TP (Katman İki Tünel Protokolü), SSTP, (Güvenli Yuva Tüneli Protokolü), IPSEC (Ağ Katmanı Güvenliği Protokolü) gibi güvenlik protokolleri kullanılmaktadır (VPNnedir, 2011).

Taşra birimleri ve merkezler de dâhil tüm kurumların erişim şebekesi, ağ cihazları ve transmisyon altyapısı ile tamamen kamuya özel farklı bir şebekenin kurulması, kamunun kapalı devre güvenilir bir ağ üzerinden haberleşmesi için gerekli görülmektedir. Yeni bir şebeke kurulması; maliyet ve zaman açısından değerlendirildiğinde dezavantajlı görünmektedir.

Ancak, sadece kamuya özel bir altyapı oluşturmak, geçici çözümlerle günü kurtarmaktan ziyade, kamunun iletişimini gerçek anlamda güvenli bir ağ üzerinden gerçekleştirmesi yönünden önem arz etmektedir. Yeni şebekenin idamesi ise, işletmeci gibi çalışacak olan ancak yüzde yüzü kamuya ait bir kamu şirketi tarafından sağlanmalıdır.

**Yeni Şebeke Kurulumu**

**Avantaj;**

Bütünüyle kamuya ait bir altyapı,

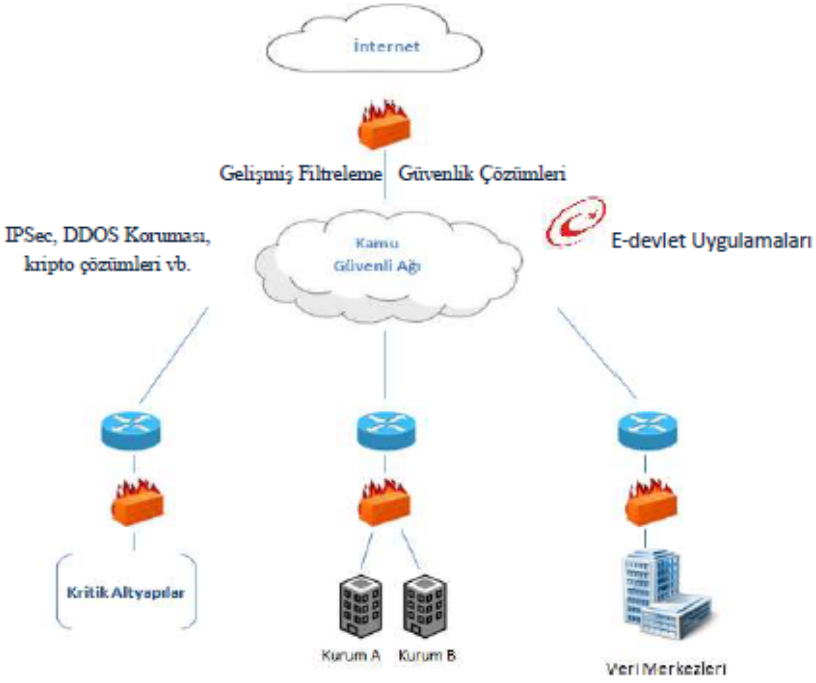
Gerçek anlamda güvenli bir ağ.

**Dezavantaj;**

Yüksek yatırım maliyeti,

Oluşturulması ve idamesinin sağlanması uzun süreç alacak bir model.

Şekil 6.1. Kamu Güvenli Ağı Modeli




Türkiye'de kamunun güvenli bir ağ üzerinden haberleşmesi için önerilen modelin ve idamesini sağlayacak olan birimin oluşturulmasının yanı sıra ulusal kamu güvenli ağı planı da hazırlanmalıdır. Planın, tüm kamu kurumları ve kritik altyapılara sahip kurumların elektronik ortamda güvenli iletişimini sağlayacak olan geniş alan ağının oluşturulması maksadıyla hazırlanması önerilmektedir. Plan; siber güvenlik ile ilgili ulusal ve uluslararası koordinasyon görevi bulunan UDHB tarafından oluşturulan ilgili kurum, kuruluş, dernek ve üniversitelerdeki yetkin ve yetkili temsilcilerin dâhil olduğu çalışma grubu tarafından hazırlanmalıdır.

Ulusal Kamu Güvenli Ağı Planında yer alması gereken temel hususlar şunlardır:

- Kamu Güvenli Ağı'nı kuracak ve idamesini sağlacak olan bir kurum oluşturulmalı veya ilgili mevcut bir kuruma bu görev verilmelidir. Kurum, yasal bir dayanak ile aldığı bu görevi kendi imkânları ile veya hizmet satın alma yöntemi ile yerine getirebilmelidir.

- Kamu Güvenli Ağı'na dâhil olması gereken kurum/kuruluşlar belirlenmelidir. Kamu kurum/kuruluşlarının yanı sıra kritik altyapı sektörü olarak belirlenen kurum/kuruluşlar da bu ağa dâhil edilmelidir.

- İdamesini sağlayacak olan kurum ".gov" alanlarındaki ağ akışını izlemeli ve burdan çıkan verileri kullanarak güvenlik açıklarını gidermelidir. Potansiyel siber tehditler ile ilgili Ulusal Siber Olaylara Müdahale Merkezine bilgi vermelidir. Siber saldırılar ile ilgili uyarılar ve bültenler yayımlama görevi bulunan Merkez ile işbirliği içerisinde olmalıdır.

- Ağ'a dâhil olan kurum/kuruluşların güvenliği için önlem ve öneriler hazırlanmalıdır.

Bilişim teknolojilerinin yoğun olarak kullanıldığı ve ağa dâhil edilmesi önerilen kritik altyapıya sahip kurum/kuruluşların da güvenliğine ilişkin alınacak önlem ve öneriler de söz konusu Ulusal Kamu Güvenli Ağı Planı'nda yer almalıdır.

Tez içerisinde ele alınan dünya ülkelerinin kritik altyapı olarak belirlenen sektörleri ve ulusal çaptaki yapılanmaları incelenerek, Türkiye için kritik altyapı olarak önerilen alanlar tespit edilmiştir.

Türkiye için *kritik altyapı* olarak belirlenmesi önerilen alanlar aşağıda yer almaktadır:

- Enerji
- Bilgi teknolojileri ve telekomünikasyon
- Gıda
- Su
- Ulaştırma
- Acil Durum Hizmetleri
- Kamu Hizmetleri
- Sağlık Hizmetleri
- Finans
- Bankacılık

Türkiye'deki kritik altyapı olarak belirlenen alanlar, sektör ve kurum bazında net bir şekilde belirlenmeli ve ilgili kurumlar ile paylaşılmalıdır. Kritik altyapıların korunması için "Kritik Altyapıların Korunması Merkezi" oluşturulmalı veya ilgili mevcut bir kurum içerisinde böyle bir yapılanma gerçekleştirilmelidir. Kritik altyapıların korunmasından sorumlu olan bu merkez, kritik altyapıların sahip olması gereken güvenlik gereksinimlerini belirlemeli, belirli zaman aralıkları ile uygulanıp uygulanmadığını tetkik etmelidir. Kritik altyapılarda olması gereken temel güvenlik gereksinimleri şunlardır:

- Sistemlere yalnızca yetkili personel tarafından fiziksel erişim sağlanması ve bu erişimin yönetilmesi,
- Yetkili personelin kullanıcı bilgilerinin yönetimi,
- Kayıt yönetimi ve sistem işletiminde görev yapan personelin rol ve sorumlulukların açık bir şekilde belirlenmesi ve görevler ayrılığı ilkesinin uygulanması,
- Kayıt yönetimi,
- Personelin eğitilmesi,
- İş sürekliliği ve personel sürekliliğinin sağlanması,

- Yedek sistem oluşturulması,
- Güvenlik yönetimi,
- Personel güvenliği,
- Politikanın belirlenmesi,
- Sistem ve bilgi bütünlüğünün korunması ve takibi,
- Planlama ve risk değerlendirme,
- Sistem tedarik, geliştirme ve bakım fonksiyonlarının yönetimi,
- Kullanılan yazılımlarının güvenliğinin ve teknik açıklıkların takibi, belirli aralıklarla testlerin uygulanması

Ayrıca, kritik altyapıların önemi konusundaki farkındalığın artırılması maksadı ile; belirlenecek bir ayın, "Kritik altyapıların dayanıklılığı" ayı olarak kabul edilmesi ve bu alanda önemli etkinliklerin (konferans, çalıştay vb.) düzenlenmesi önem arz etmektedir.

# SONUÇ VE ÖNERİLER

Türkiye'de, ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonunun sağlanması amacıyla mevzuat çalışmaları yapılmış olup, bakanlar kurulu kararı ve mevcut kanuna eklenen maddeler ile siber güvenliğe ilişkin yasal bir dayanak oluşturulmuştur. Ulusal siber güvenliğin sağlanması amacıyla strateji ve eylem planı hazırlanmış, sorumlu ve ilgili kuruluşlar belirlenmiş, takvime bağlanan eylemlere ilişkin çalışmalar başlatılmış ve sürdürülmektedir. Ülke örnekleri ve uluslararası kuruluşların bu alanda yaptığı çalışmalar ışığında, Türkiye'de siber güvenliğin sağlanması için gerekli olduğu düşünülen hukuki, idari ve uygulamaya dönük yapılması gereken bir takım çalışmalar bulunmaktadır. Bu kapsamda, ulusal siber güvenliğin sağlanmasına ilişkin öneriler bu başlık altında değerlendirilmiştir.

- Ulusal çapta siber güvenliği sağlamak, kamu ya da özel sektörün tek başına üstesinden gelemeyeceği kadar kapsamlı bir husustur. Bu nedenle, ulusal Siber Güvenliğin sağlanması konusunda kamu kurum/kuruluşları, özel sektör, üniversiteler ve sivil toplum kuruluşlarının işbirliği içerisinde çalışması oldukça önem arz etmektedir. Ülke çapında siber güvenliğin sağlanması, bu işbirliğinin oluşturulması ve etkin bir şekilde işlemesi ile mümkün olabilecektir. Stratejiler ve Eylem Planları, tüm bu paydaşların katkıları/görüşleri doğrultusunda hazırlanmalı ve uygulamaya geçirilmelidir. Temel olarak, bilgi akışı, siber tehdit istihbarat paylaşımı, eğitim, teknoloji desteği (yazılım/donanım) alanlarında işbirliği yapılmalıdır.

- Türkiye'de, siber güvenliğe ilişkin yasal bir dayanak olmasına rağmen, ihtiyaçları tümüyle karşılamadığı değerlendirilmektedir. Ulusal Siber Güvenlik Stratejisi ve 2013 2014 Eylem Planı, 2. Eylem maddesi gereği olarak da hayata geçirilmesi gereken "Siber Güvenlik Kanunu", hukuki boyutunun yanı sıra; teknik, idari, politik, ekonomik ve sosyal boyutları da ele alarak kapsamlı bir şekilde hazırlanmalı ve yayımlanmalıdır.

- Siber güvenlik alanında ulusal ve uluslararası koordinasyonun sağlandığı Ulusal Siber Olaylara Müdahale Merkezi kurulmuştur. Tüm kurum/kuruluşların irtibat noktası olan bu merkez, yetkilerini kanundan almalıdır. Belirli periyodlarda (örneğin; 6 ayda bir) istatistiki bilgiler yayınlayarak kamuoyunu bilgilendirmelidir. USOM bünyesinde, daimi olarak kolluk kuvveti temsilcisinin bulunmasının, işbirliği ve bilgi paylaşımının aktif olarak yapılabilmesi bakımından faydalı olacağı değerlendirilmektedir. USOM'un; FIRST, ITU-IMPACT, EGC gibi kuruluşlara üye olması ve bu kuruluşlarda yapılan çalışmaları aktif olarak takip etmesi, Türkiye'nin dünya çapında görünürlüğünün artması ve bu alandaki kazanımı açısından önem arz etmektedir. USOM'un etkin olarak çalışabilmesi için gereken ana unsur, kurumsal ve sektörel SOME'ler ile yapacak/yapıyor olduğu bilgi alışverişi/birlikte çalışılabilirliktir.

- Diğer ülke örnekleri incelendiğinde, siber güvenliğe ilişkin faaliyetlerin ayrı bir bakanlık altında ya da Türkiye'de olduğu gibi mevcut bir bakanlığın ilgili biriminde yürütüldüğü gözlemlenmektedir. Ancak, ulusal çapta siber güvenliğin sağlanması için çalışmaların yürütüldüğü bu birime ve bu alanda aktif çalışmaların yürütüldüğü kamu kurumlarına, üniversitelerin "Bilgisayar Mühendisliği, Elektronik Mühendisliği, Elektronik ve Haberleşme Mühendisliği, Telekomünikasyon Mühendisliği, Hukuk, Uluslararası İlişkiler, Bilişim Hukuku, Bilişim Sistemleri v.b" bölümlerinden mezun, yeterli sayıda personelin istihdam edilmesinin gerekli olduğu değerlendirilmektedir. Kamuda bu kurumlarda/birimlerde çalışan personelin bilgi güvenliği/siber güvenlik konularında eğitilmesi ve yetiştirilmesi hususu önemli bir ihtiyaç olarak değerlendirilmektedir. Kamu kurumlarında, bilgi güvenliği/siber güvenlik alanında yetkin personel bulunmalıdır.

- Bilgi güvenliği ve siber güvenlik alanında uzman personel yetiştirilmelidir. Bu alanda, YÖK ve üniversitelerimizin çalışmaları neticesinde, yüksek lisans ve doktora programları açılmaktadır. Ayrıca, üniversitelerin ilgili bölümlerinin lisans programlarında da "bilgi güvenliği/siber güvenlik" seçmeli derslerinin eklenmesi, öğrencilerin bu alanda bilgi sahibi olması ve uzmanlık alanı olarak

değerlendirebilme fırsatı yakalamaları yönünden faydalı olacağı değerlendirilmektedir.

- Siber güvenlik sağlanırken sanal ortamdan gelebilecek tehlikeler kadar fiziksel ortamdan gelen tehlikelerde önem arz etmektedir. Bu nedenle, kurum/kuruluşlarda sistem odasına sadece yetkili personel tarafından fiziksel erişim sağlanmalı ve yetkili olmayan bir kişinin sistem odasına girişi her ne sebeble olursa olsun sınırlandırılmalıdır.

- Kurumda çalışan personel "Bilgi güvenliği ve Siber Güvenlik" konularında eğitilmelidir. Kurum/kuruluşlardaki idari yönetim, tüm çalışanların güvenlik kontrollerine uymaları için gerekli önlemleri almalı, eğitim, seminer, konferans gibi etkinliklerle çalışanları bilinçlendirmelidir.

- Yazılımlarda olabilecek hata ve açıklıkları en aza indirmek amacıyla, belirli aralıklarla gerekli testler yapılmalı/yaptırılmalı güvenlik açıklıkları tespit edilmelidir. Özellikle kritik altyapılarda, sistemde uzun süre kalmayı amaçlayan ve belirli bir hedefe yönelik yapılan saldırılara karşı gelişmiş siber casusluk tespit analizleri yaptırılmalıdır. Sistemdeki cihazlara yapılacak teknik destek ve kontroller de belirli aralıklarla yapılmalıdır. Sistemin herhangi bir arıza ya da saldırı durumunda çalışamaz hale gelmesi durumunda devreye girebilecek bir yedek sistem mutlaka bulunmalıdır.

- Sistem kayıtları sadece yetkili kişi/kişiler tarafından erişilebilir olmalı ve kimse tarafından değiştirilemez durumda olmalıdır.

- Eğitimlerin yaygınlaştırılması ve farkındalığın artırılması amacıyla, halka açık bir bilinçlendirme kampanyası başlatılmalıdır. Medyanın desteği, siber güvenliğin sağlanması ve halkın bilinçlendirilmesi için oldukça gereklidir.

- Siber Güvenliğin sağlanmasında, kritik altyapıların korunmasına özellikle önem verilmesi gerekmektedir. Kritik altyapılarımıza yapılabilecek olası bir saldırı

sonucunda, büyük ölçekli ekonomik zarar hatta can kaybı yaşanması riski mevcuttur. Bu nedenle, Türkiye'de sektörel SOME'lerin kritik sektörlerde kurulması öngörüldüğünden, kritik altyapı listesinin tereddütlere yer vermeyecek şekilde hazırlanıp, resmi bir kanal yoluyla yayınlanması birçok kurumun gerekli güvenlik tedbirlerini alması açısından gerekli görülmektedir.

- Uluslararası işbirliğinin geliştirilmesinin de Türkiye'nin siber güvenliğinin iyileştirilmesine yönelik çalışmalarda önemli bir rol oynayacağı değerlendirilmektedir. Dünya çapında siber suç, siber savaş gibi kavramlar henüz netlik kazanmadığından, bu alanda uluslararası mevzuatda eksiklikler bulunmaktadır. Siber suçlar sözleşmesi genel bir çerçeve çizmekte ancak yeterli görülmemektedir. Bu nedenle, siber saldırmazlık anlaşması ve siber tehdit istihbaratlarının paylaşılması gibi konularda diğer ülkelerle uluslararası işbirliği yapmak ülkenin menfaatine olacaktır. Ayrıca, siber güvenlik ile ilgili olarak NATO, OECD, BM, ITU, Avrupa Konseyi, ENISA, Interpol, ETSI, OSCE, EUROPOL EC3 gibi uluslararası kuruluşlarla iletişim halinde olunması, çalışmalarına aktif olarak katılımda bulunulması ve siber güvenlik alanında uluslararası stratejimizin de net bir şekilde ortaya konulması gerekmektedir.

- Amerika Birleşik Devletleri, İtalya vb. ülkelerde olduğu gibi, Türkiye'de de üst yönetim kadrolarında "Siber güvenlik danışmanları" olmalıdır.

- Bilgi ve iletişim altyapılarında gelişmiş güvenlik teknolojileri kullanılmalıdır.

- Siber güvenliği sağlamaya yönelik ar-ge çalışmaları ile yerli ürün ve çözüm çalışmaları yapılmalıdır. Bilgi ve iletişim sistemlerinde kullanılan yazılım ve donanıma ilişkin tüm ürünlerin yerli üretim olması pek mümkün görülmemekte ancak, kullanılmakta olan ürünlerin testlerinin yerli ürünler ile yapılması siber güvenliğin sağlanması açısından oldukça faydalı çıktılar sağlayacaktır.

Bu nedenle; bu amaç doğrultusunda çalışacak ar-ge labaratuvarlarının oluşturulması, var olanların kamu desteği ile geliştirilmesi gerekmekte ve zararlı yazılımlara ilişkin ulusal bir veritabanına ihtiyaç duyulmaktadır.

- Olası bir siber savaş yaşanması durumunda, ülkenin sadece savunma yeteneğine sahip olmasının ve sadece savunmayı hedef alan politikaların geliştirilmesinin yeterli olmadığı düşünülmektedir. Bu nedenle Türkiye'de, devlet çatısı altında, aktif savunma yeteneğine sahip bir ekibin oluşturulmasının gerekli olduğu değerlendirilmektedir.

Türkiye'de kamu güvenli ağı oluşturulmasına ilişkin, taşra birimleri ve merkezler de dâhil tüm kurumların erişim şebekesi, ağ cihazları ve transmisyon altyapısı ile tamamen kamuya özel farklı bir şebeke kurulması önerilmektedir. Bu model, maliyet ve zaman açısından değerlendirildiğinde dezavantajlı görünmekte, ancak gerçek anlamda güvenli bir ağ oluşturmak için gerekli olduğu değerlendirilmektedir. Yeni şebekenin idamesi ise, işletmeci gibi çalışacak olan ancak yüzde yüzü kamuya ait bir kamu şirketi tarafından sağlanmalıdır. Söz konusu ağın oluşturulabilmesi maksadıyla öncelikle ulusal kamu güvenli ağı planı hazırlanmalıdır. Plan; siber güvenlik ile ilgili ulusal ve uluslararası koordinasyon görevi bulunan UDHB tarafından oluşturulan ilgili kurum, kuruluş, dernek ve üniversitelerdeki yetkin ve yetkili temsilcilerin dâhil olduğu çalışma grubu tarafından hazırlanmalıdır. Plan'ın hangi konuları içermesi gerektiğine bu tez çalışması içerisinde detaylı olarak yer verilmiştir.

Ayrıca, kritik altyapıların korunması için "Kritik Altyapıların Korunması Merkezi" oluşturulmalı veya ilgili mevcut bir kurum içerisinde böyle bir yapılanma gerçekleştirilmelidir. Kritik altyapıların korunmasından sorumlu olan bu merkez, kritik altyapıların sahip olması gereken güvenlik gereksinimlerini belirlemeli, belirli zaman aralıkları ile uygulanıp uygulanmadığını tetkik etmelidir. Kritik altyapılarda olması gereken temel güvenlik gereksinimlere bu tez çalışması içerisinde detaylı olarak yer verilmiştir.

# KAYNAKLAR

AKU, 2013, Spam Nedir, Afyon Kocatepe Üniversitesi Bilgi İşlem Daire Başkanlığı Bülteni, http://www.aku.edu.tr/AKU/DosyaYonetimi/BILGIISLEM/Duyurular/bultenler/nisan2013/, (Son Erişim: 09.04.2014)

ANIL Süleyman, 2004, NCIRC (NATO Computer Incident Response Capability), http://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf, (Son Erişim: 18.04.2014)

APCERT, 2013, http://www.apcert.org/documents/pdf/APCERTDrill2013PressRelease_AP.pdf , (Son Erişim: 18.06.2014)

ARNNET, 2014, http://www.arnnet.com.au/slideshow/341113/top_10_most_notorious_cyber_attacks_history/?image=2, (Son Erişim: 08.03.2014)

Avrupa Konseyi Siber Suçlar Sözleşmesi, 2008, http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/a/sibersuclar.pdf, (Son Erişim: 24.04.2014)

AYDIN, D. M. ,2005, e-Avrupa+ Ve Türkiye: Bilgi Teknolojileri Alanında Avrupa Birliği Kriterlerine Uyum. http://www.digitaldevlet.org/eAVRUPA.pdf., (Son Erişim: 18.06.2014)

Bakanlar Kurulu Kararı, 2013, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, T.C. Resmi Gazete, 28683

Bakanlar Kurulu Kararı, 2012a, Türkiye Cumhuriyeti Hükümeti ile Gürcistan Hükümeti Arasında Suçla Mücadelede İşbirliği Konulu Mutabakat Zaptı'nın Onaylanması Hakkında Karar, T.C. Resmi Gazete, 28378

Bakanlar Kurulu Kararı, 2012b, 20 Ekim 2012, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, T.C. Resmi Gazete, 28447

BGD, 2013, Hakkımızda, Bilgi Güvenliği Derneği, http://www.bilgiguvenligi.org.tr/hakkimizda.html, (Son Erişim: 09.04.2014)

BİAK, B., 2012, Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler Ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu, Türkiye Büyük Millet Meclisi

Bilgi Güvenliği, 2010, İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları, https://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html, (Son Erişim: 05.04.2014)

Bilgi Güvenliği Derneği, 2012, http://www.bilgiguvenligi.org.tr/index_files/sunumlar/siber_guvenlik_siber_savaslar_tbmm_internet_komisyonu_mayis_2012.pptx, (Son Erişim: 18.04.2014)

Bilgi Güvenliği Derneği, 2013, http://www.bilgiguvenligi.org.tr/hakkimizda.html, (Son Erişim: 18.04.2014)

Bilgi Toplumu Dairesi Başkanlığı, 2014, 2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Kalkınma Bakanlığı

Bilgi Toplumu, 2013, Bilgi Toplumu Stratejisi ve Eylem Planı Nihai Değerlendirme Raporu, Bilgi Toplumu Dairesi, Kalkınma Bakanlığı

Bilişim Dergisi, 2013, www.bilisimdergisi.org/pdfindir/s134/.../108-109.pdf, (Son Erişim: 05.04.2014)

Bilişim ve Teknoloji Hukuku Enstitüsü, 2012, Siber Güvenlik Raporu. İstanbul: İstanbul Bilgi Üniversitesi

Birleşik Krallık Ulusal Güvenlik Stratejisi Raporu, 2010, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

BMI, 2009, National Strategy for Critical Infrastructure Protection (CIP Strategy), s. 7

Borins, S., 2002, On the Frontiers of Electronic Governance: . A Report on the United States and Canada, International Review of Administrative Sciences

Broadband, 2012, National Broadnband Plan Connecting America – Public Safety, http://www.broadband.gov/plan/16-public-safety/, (Son Erişim: 18.04.2014)

Brown, M. M., & Brudney, J. L., 2001, Achieving advanced electronic government services: An examination of obstacles and implications from and international perspective, http://www.jstor.org/stable/3381211, (Son Erişim: 18.04.2014)

BSI, 2009, Act to Strengthen the Security of Federal Information Technology

BTK, 2012, Siber Kalkan Tatbikatı, Bilgi Teknolojileri ve İletişim Kurumu, http://btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/uskt2012.php, (Son Erişim: 05.03.2014)

BTK USGT, 2011, Ulusal Siber Güvenlik Tatbikatı, Bilgi Teknolojileri ve İletişim Kurumu, http://btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2011.php, (Son Erişim: 05.04.2014)

BTK 2. USGT, 2013, 2. Ulusal Siber Güvenlik Tatbikatı, Bilgi Teknolojileri ve İletişim Kurumu, http://btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2013.php, (Son Erişim: 05.04.2014)

BTK Tatbikat, 2014, Uluslararası Siber Kalkan Tatbikatı 2014, Bilgi Teknolojileri ve İletişim Kurumu, http://www.tk.gov.tr/sayfa.php?ID=328, (Son Erişim: 05.06.2014)

BTK, 2014a, Tatbikatlar, Bilgi Teknolojileri ve İletişim Kurumu, http://btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/tatbikatlar.php, (Son Erişim: 09.04.2014)

BTK, 2014b, USOM-SOME, Bilgi Teknolojileri ve İletişim Kurumu, http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usomsome.php, (Son Erişim: 05.06.2014)

CCDCOE, 2014, http://www.ccdcoe.org/523.html, (Son Erişim: 26.04.2014)

CISCO, 2013, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html, (Son Erişim: 26.02.2014)

CISCO 2014, 2014, Cisco 2014 Annual Security Report, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf, (Son Erişim: 25.05.2014)

ÇİFCİ Hasan, 2013, Her Yönüyle Siber Savaş, TÜBİTAK Popüler Bilim Kitapları, Ankara

DHS, 2013a, Public Safety Broadband: Fulfilling a 9/11 Commission Recommendation, Haziran 2012

DHS, 2013b, Güvenli Siber Ağlar, Amerika Birleşik Devletleri İç Güvenlik Bakanlığı Siber Güvenlik Sayfası, https://www.dhs.gov/secure-cyber-networks, 1 Kasım 2013, (Son Erişim: 17.04.2014)

DHS, 2014a, Office of Cybersecurity and Communications, http://www.dhs.gov/office-cybersecurity-and-communications, Nisan 2014, (Son Erişim: 24.05.2014)

DHS, 2014b, Critical Infrastructure Sectors, http://www.dhs.gov/critical-infrastructure-sectors, Haziran 2014, (Son Erişim: 24.05.2014)

DHS FirstNet, 2012, Nationwide Public Safety Broadband Network

DHS FNR, 2014, Federal Network Resilience, http://www.dhs.gov/federal-network-resilience, (Son Erişim: 24.04.2014)

EGM, 2013, Siber Suçlarla Mücadele Daire Başkanlığı, Emniyet Genel Müdürlüğü, http://www.egm.gov.tr/Sayfalar/SiberSuclarlaMucadeleDaireBaskanligi.aspx, (Son Erişim: 09.04.2014)

Elektronik Haberleşme Güvenliği Yönetmeliği, 20 Temmuz 2008, T.C. Resmi Gazete, 26942

Elektronik Haberleşme Kanunu, 10 Kasım 200, T.C. Resmi Gazete, 27050

ENISA ABD, 2011, USA - International National Strategy for Cyberspace

ENISA Japonya, 2013, Japon- Information Security Strategy for Protecting the Nation

ENISA Kanada, 2010, Canada's Cyber Security Strategy

ENISA Almanya, 2011, Cyber Security Strategy for Germany

ENISA Fransa, 2011, Information systems defence and security France's strategy

ENISA Birleşik Krallık, 2011, The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World

ENISA Çek Cumhuriyeti, 2011, Cyber Security Strategy of the Czech Republic For the 2011 – 2015 Period

ENISA İnternet Tehdit Raporu, 2013

ENISA İspanya, 2013, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf, (Son Erişim: 18.03.2014)

ENISA Japonya, 2014, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP_NCSS2.pdf, (Son Erişim: 18.05.2014)

ENİSA Kanada, 2010, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/canadas-cyber-security-strategy

ENISA Avusturya, 2013, Austrian Cyber Security Strategy

ENISA Yeni Zelanda, 2011, New Zealand's Cyber Security Strategy

ENISA Tatbikatlar, 2012, On National and International Cyber Security Exercises

ENISA Siber Avrupa Tatbikatı, 2014, Cyber Europe, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe

European Commission, 2014, Digital Agenda for Europe, http://ec.europa.eu/digital-agenda/digital-agenda-europe, (Son Erişim: 18.06.2014)

Fang, Z., 2002, E-Government in digital era: concept, practice, and development. International Journal of T he Computer, The Internet and Management

Fayfoundation, 2013, Cyber Crimes, s.3

FCC, 2014, What We Do, http://www.fcc.gov/what-we-do, (Son Erişim: 05.04.2014)

FISMA, 2002, Federal Information Security Management Act, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, (Son Erişim: 24.02.2014)

F-Secure H2,(2013), Threat Report H2

F-Secure, 2013, F-Secure Mobile Tehdit 2013 yılı 3. Çeyrek Raporu.

Fransa Veri Koruma Kanunu, 2014, http://uk.practicallaw.com/6-502-1481?service=crossborder (Son Erişim: 18.02.2014)

Fransa Sayısal Ekonomide Güveni Güçlendirme Kanunu, 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy-1/defence-security/cyber-security/, (Son Erişim: 18.02.2014)

GCSX, 2014, NRPF Connect, http://www.nrpfnetwork.org.uk/nrpfconnect/Pages/default.aspx, (Son Erişim: 18.04.2014)

GNS, 2012, National Cyber Security Strategies, http://www.gns.gov.pt/media/1238/ENISANationalCyberSecurityStrategies.pdf, (Son Erişim: 08.02.2014)

HGM, 2014, Görev Raporu (Siber Güvenlik Eğitimi - Washington, Amerika)

Hükümet İletişim Ağı, 2014, http://www.ogcio.gov.hk/en/infrastructure/e_government/gcn/gov_communication_network.htm, (Son Erişim: 18.06.2014)

IC3, 2014, About IC3, http://www.ic3.gov/about/default.aspx, (Son Erişim: 09.04.2014)

IC3, 2012, IC3 2012 Internet Crime Report

ICT SERT, 2012, http://www.isokalitebelgesi.com/iso_belgeleri_egitim_danismanlik/TS_ISO_IEC_27000_27001_27002_27003_27004_27005_22096/Bilgi_g%C3%BCvenligi_yonetim_sistemi_standart_standardi_standartlari_1.php, (Son Erişim: 15.04.2014)

İEM, 2014, Siber Suç Nedir, İstanbul Siber Suçlarla Mücadele Daire Başkanlığı, https://sibersuclar.iem.gov.tr/siber_suclari.html, (Son Erişim: 10.04.2014)

IGCC, 2012, China and Cybersecurity: Political, Economic, and Strategic Dimensions, Report from Workshops held at the University of California, San Diego

IMPACT, 2014, IMPACT Organization Chart, http://www.impact-alliance.org/download/pdf/about-us/IMPACT-organization-chart2014.pdf, (Son Erişim: 15.04.2014)

ISC, 2013, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2013

ITU, 2002, 56/121 Combating the criminal misuse of information technologies, Resolution adapted by the General Assembly

ITU, 2003, 57/239 Creation of a global culture of cybersecurity, Resolution adapted by the General Assembly

ITU, 2007, Cybersecurity Guide for Developing Countries (Gelişmekte Olan Ülkeler için Siber Güvenlik Rehberi)

ITU, 2013, Annual Security Roundup, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/rpt-cashing-in-on-digital-information-01.pdf, (Son Erişim: 15.04.2014)

ITU, 2014, About ITU, http://www.itu.int/en/about/Pages/default.aspx, (Son Erişim: 10.04.2014)

ITU Cybersecurity, 2014, ITU Cybersecurity Activities, http://www.itu.int/en/action/cybersecurity/Pages/default.aspx, (Son Erişim: 10.04.2014)

Japan White Paper, 2013, Defence of Japan, http://www.mod.go.jp/e/publ/w_paper/2013.html

Justice Laws, 2014, Canada Justice Laws Website, http://laws-lois.justice.gc.ca/eng/acts/c-46/page-166.html#docCont

Kanada Kamu Güvenliği, 2014a, Public Safety Canada, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx, Mart 2014, (Son Erişim: 24.05.2014)

Kanada Kamu Güvenliği, 2014b, Public Safety Canada, http://www.publicsafety.gc.ca/index-eng.aspxjl, Ağustos 2014, (Son Erişim: 24.05.2014)

Kanun, 2007, 23 Mayıs 2007, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651 sayılı), T.C. Resmi Gazete, 26530

Kanun, 2014a, 19 Şubat 2014, Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, T.C. Resmi Gazete, 28918

Kanun, 2014b, 2 Mayıs 2014, Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, T.C. Resmi Gazete, 28988

Kaspersky, 2013, Financial cyber threats in 2013

Kurul Kararı, 11 Temmuz 2006, Yüksek Seçim Kurulu Kurul Kararı, Bilgi Toplumu Stratejisi (2006-2010)" ve "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010), T.C. Resmi Gazete, 2006/38

Malwaretruth, 2014, The truth about Malware, http://www.malwaretruth.com/the-list-of-malware-types/, (Son Erişim: 18.08.2014)

MARTTİN Vedat, PEHLİVAN İhsan, 2010, ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme, Mühendislik Bilimleri ve Tasarım Dergisi, Cilt 1, Sayı 1, s.49-56

MERAL Mehmet, 2008, Siber Savunma: Ülkeler ve Stratejiler, 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı

MGK, 2013, http://www.mgk.gov.tr/calismalar/calismalar/016_siber_savasa_uygulanacak_hukuk_hakkinda_tallinn_el_kitabi.pdf, (Son Erişim: 26.03.2014)

NATO, 2011, Civil Emergency Planning Committee (CEPC), http://www.nato.int/cps/en/natohq/topics_50093.htm, (Son Erişim: 26.04.2014)

NATO, 2013, NATO Review, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, (Son Erişim: 26.04.2014)

NEC, 2013, Information Management, http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html (Son Erişim: 14.03.2014)

NISAC, 2013, National Infrastructure Simulation and Analysis Center, http://www.sandia.gov/nisac/, (Son Erişim: 24.05.2014)

Nova Infosec, 2014, Cyber Security versus Information Security, https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/, (Son Erişim: 06.05.2014)

NZSIS, 2013, New Zealand Security Intelligence Service, http://www.nzsis.govt.nz/about-us/, (Son Erişim: 06.03.2014)

OECD, 2012, Cybersecurity Policy Making at a Turning Point

OECD, 2013, WPISP, http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacy wpisp.htm, (Son Erişim: 05.04.2014)

OECD ICCP, 2010, Committee on Information, Communications and Computer Policy (ICCP), http://www.oecd.org/internet/ieconomy/37328586.pdf, (Son Erişim: 05.04.2014)

OGCIO CIG, 2014, Central Internet Gateway System, http://www.ogcio.gov.hk/en/infrastructure/e_government/cig/, (Son Erişim: 05.04.2014)

OGCIO, 2014, IT Security Framework in Government, http://www.ogcio.gov.hk/en/infrastructure/e_government/security/, (Son Erişim: 05.04.2014)

OGCIO Hükümet Omurga Ağı, 2014, Government Backbone Network, http://www.ogcio.gov.hk/en/infrastructure/e_government/gnet/government_backbone_network.htm, (Son Erişim: 05.04.2014)

OGCIO CCC, 2014, Central Computer Centre, http://www.ogcio.gov.hk/en/infrastructure/e_government/ccc/index.htm, (Son Erişim: 05.04.2014)

PSN, 2014, Public Services Network, https://www.gov.uk/public-services-network, (Son Erişim: 29.05.2014)

Rusya Federasyonu Bilgi Güvenliği Doktrini, 2000, Information Security Doctrine Of The Russian Federation, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument, (Son Erişim: 10.02.2014)

SANGER E. David, BARBOZA David, PERLROTH Nicole, 2013, Chinese Army Unit Is Seen as Tied to Hacking Against U.S., New York Times, 18 Şubat 2013

Siber Suçlar Sözleşmesi, 2001, Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, (Son Erişim: 14.03.2014)

Siber Güvenlik Yasa Tasarısı, 2012, Text of the Cybersecurity Act of 2012, https://www.govtrack.us/congress/bills/112/s2105/text, (Son Erişim: 24.05.2014)

SOMMER Peter, BROWN Ian, 2011, Reducing Systemic Cybersecurity Risk, http://www.oecd.org/governance/risk/46889922.pdf, (Son Erişim: 22.04.2014)

Symantec, 2013, İnternet Security Threat Report 2013

Symantec Appendix, 2013, İnternet Security Threat Report 2013 Appendix

Tallinn El Kitabı, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=%205903855/1802381, (Son Erişim: 04.04.2014)

TBD, 2013, TBD Sayısal Gündem 2020 Uzmanlık Grupları, http://www.tbd.org.tr/index.php?sayfa=inc_sayisal_gundem&c2=3791&mi=2, (Son Erişim: 08.08.2014)

Tebliğ, 2005, 24 Mart 2005, Tebliğ, e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı, T.C. Resmi Gazete, 2005/5

Tebliğ, 2013, 11 Kasım 2013, Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usül ve Esaslar Hakkında Tebliğ, T.C. Resmi Gazete, 28818

Tebliğ, 2010, 15 Ekim 2010, Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulamasına İlişkin Tebliğ, T.C. Resmi Gazete, 27730

Techtarget, 2010, UK Government Connect Secure Extranet (GCSX), http://searchsecurity.techtarget.co.uk/definition/UK-Government-Connect-Secure-Extranet-GCSX, (Son Erişim: 19.04.2014)

TSE, 2014, TSE Beyaz Şapkalı Hacker Eğitimleri, http://bilisim.tse.org.tr/docs/pentest/beyaz-sapkal%C4%B1-hacker-son.pdf?sfvrsn=2, (Son Erişim: 05.06.2014)

TÜBİTAK BİLGEM, 2013, Siber Güvenlik Enstitüsü, http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi, (Son Erişim: 09.04.2014)

TÜBİTAK, 2013, Siber güvenlik Yaz Kampı, http://www.tubitak.gov.tr/tr/haber/siber-guvenlik-yaz-kampi-2013-basvurulari-basladi, (Son Erişim: 05.06.2014)

Türk Ceza Kanunu, 12 Ekim 2004, T.C. Resmi Gazete, 25611

US-CERT, 2003, The National Strategy to Secure Cyberspace

USOM, 2013, USOM görevleri, çalışma usul ve esasları, http://usom.gov.tr/gonderilen_usom/files/USOM_USUL_ESAS.pdf, (Son Erişim: 03.03.2014)

VirtualPone, 2013, http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml, (Son Erişim: 03.03.2014)

VPNnedir, 2011, http://www.vpnnedir.org/vpn-nedir-virtual-private-network-teknolojisi-hakkinda.html, , (Son Erişim: 05.04.2014)

White House, 2008, The Comprehensive National Cybersecurity Initiative, Foreign Policy, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (Son Erişim: 24.02.2014)

Wikipedia, 2013a, http://tr.wikipedia.org/wiki/Virtual_Private_Network, Haziran 2013, (Son Erişim: 05.04.2014)

Wikipedia, 2013b, Public Safety Network, http://en.wikipedia.org/wiki/Public_safety_network, 15 Kasım 2013, (Son Erişim: 05.04.2014)

Wikipedia, 2014a, Cisco Systems, http://tr.wikipedia.org/wiki/Cisco_Systems, 27 Mart 2014, (Son Erişim: 02.01.2014)

Wikipedia, 2014b, Centre for the Protection of National Infrastructure, http://en.wikipedia.org/wiki/Centre_for_the_Protection_of_National_Infrastructure, 1 Nisan 2014, (Son Erişim: 05.04.2014)

Wikipedia, 2014c, Government Secure Intranet, http://en.wikipedia.org/wiki/Government_Secure_Intranet, 6 Ağustos 2014, (Son Erişim: 05.03.2014)

Wikipedia, 2014ç, Siber Savaş, http://tr.wikipedia.org/wiki/Siber_sava%C5%9F, 9 Ağustos 2014, (Son Erişim: 05.04.2014)

Wikipedia, 2014d, Birleşmiş Milletler, http://tr.wikipedia.org/wiki/Birle%C5%9Fmi%C5%9F_Milletler, 22 Ağustos 2014, (Son Erişim: 05.04.2014)

Wikipedia, 2014e, Cyber-attack, http://en.wikipedia.org/wiki/Cyber-attack, 25 Ağustos 2014, (Son Erişim: 26.04.2014),

Wikipedia, 2014f, Stuxnet, http://en.wikipedia.org/wiki/Stuxnet, 30 Ağustos 2014, (Son Erişim: 26.07.2014),

Wikipedia, 2014g, International Organization for Standardization, http://en.wikipedia.org/wiki/International_Organization_for_Standardization, 31 Ağustos 2014, (Son Erişim: 05.05.2014)

Yönetmelik, 2012, 24 Temmuz 2012, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, T.C. Resmi Gazete, 28363

# ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Ulaştırma ve Haberleşme Uzman ve Uzman Yardımcılarının Sınav, Atama, Çalışma Usul ve Esasları Hakkında Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığını tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

30.09.2014

Mehtap ŞEN

# ÖZGEÇMİŞ

1988 yılında Sakarya'nın Adapazarı ilçesinde doğdu. İlkokul, ortaokul öğrenimini Sakarya'da, lise öğrenimini ise Ankara'da tamamladı. 2009 yılında Uluslararası Kıbrıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünden mezun oldu. 2013 yılında ise Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği bölümünde yüksek lisansını tamamladı. 2010-2011 yılları arasında özel sektörde Bilgisayar Mühendisi olarak görev yaptı. 2011 yılı Mart ayından itibaren Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nda Ulaştırma ve Haberleşme Uzman Yardımcısı olarak görev yaptı. Halen Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Haberleşme Genel Müdürlüğü'nde çalışmaktadır.